

C PENT

Certified Penetration Testing Professional

Module 03

Open Source Intelligence (OSINT)

MODULE OBJECTIVE

Learn various skills and techniques to gather intelligence about the target from various publicly available sources.

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

Module Objective

This module discusses various skills and techniques to gather intelligence about the target from publicly available sources such as the World Wide Web (WWW), through website analysis, by using tools/frameworks/scripts, and so on. In particular, it explores the Open Source Intelligence (OSINT) methodology.



"Open Source Intelligence (OSINT) gathering is required for all types of penetration tests."

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

"Open Source Intelligence (OSINT) gathering is required for all types of penetration tests."



OSINT through the WWW

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

OSINT through the WWW

This step involves gathering information about a target organization from all the available sources on the WWW. Searching the WWW helps the penetration tester in obtaining information such as URLs, locations, establishment details, number of employees, the specific range of domain names, and contact information of the target organization.

Finding the Domain and Sub-domains of the Target



- Check for the company's URL in the **engagement letter** or use a search engine such as **Google** or **Bing**.
- Subdomains represent different applications and help in viewing the attack surface of a target organization.

```

[~]bob@parrot: ~/Downloads/subbrute-master
[~]subbrute.py certifiedhacker.com
certifiedhacker.com
www.certifiedhacker.com
tcp.certifiedhacker.com
ftp.certifiedhacker.com
git.certifiedhacker.com
udp.certifiedhacker.com
domainkey.certifiedhacker.com
pkixrtp.certifiedhacker.com
siprtp.certifiedhacker.com
siprtp.certifiedhacker.com
afpovertcp.certifiedhacker.com
autodiscover.certifiedhacker.com
caldav.certifiedhacker.com
certificates.certifiedhacker.com
cisco-phone-http.certifiedhacker.com
cisco-phone-tftp.certifiedhacker.com
cisco-sds.certifiedhacker.com
ciscocsp.certifiedhacker.com
collab-edge.git.certifiedhacker.com

```

Source: <https://github.com>

```

[~]bob@parrot: ~/
[~]nmap --script dns-brute www.certifiedhacker.com
Starting Nmap 7.18 : https://nmap.org at 2020-04-08 03:59 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)

3306/tcp open  mysql
5432/tcp open  postgresql

Host script results:
(dns-brute)
DNS Brute force hostnames:
www.certifiedhacker.com - 162.241.216.11
blog.certifiedhacker.com - 162.241.216.11
mail.certifiedhacker.com - 162.241.216.11
smtp.certifiedhacker.com - 162.241.216.11
ftp.certifiedhacker.com - 162.241.216.11
www.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 25.72 seconds

```

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

Finding the Domain and Sub-domains of the Target (Cont'd)



```

[~]bob@parrot: ~/
[~]dnmap certifiedhacker.com
dnmap 0.38 - DNS Networks Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for certifiedhacker.com using built-in wordlist
[+] using maximum random delay of 10 wallsecond(s) between requests

blog.certifiedhacker.com
IP address #1: 162.241.216.11

panel.certifiedhacker.com
IP address #1: 162.241.216.11

events.certifiedhacker.com
IP address #1: 162.241.216.11

ftp.certifiedhacker.com
IP address #1: 162.241.216.11

```

```

[~]root@parrot: ~/home/bob
[~]#for _ in $(cat /dev/urandom | fold -n 10000 | tr -dc 'a-z' | fold -w 100 | xargs -n 100 shuf | xargs -n 100 cat); do
  DNS Servers for certifiedhacker.com:
  msl.bluelhost.com
  m2.bluelhost.com

Trying zone transfer first...
Testing msl.bluelhost.com
Request timed out or transfer not allowed.
Testing m2.bluelhost.com
Request timed out or transfer not allowed.

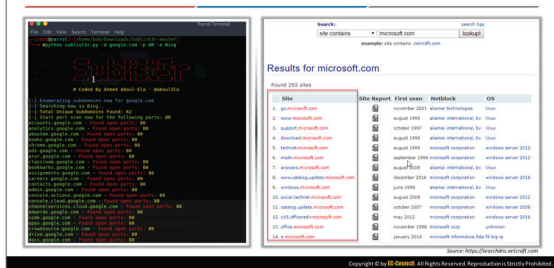
Unsuccessful in zone transfer (it was worth a shot)
Phay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
None found.
Now performing 2280 tests...
162.241.216.11 blog.certifiedhacker.com
162.241.216.11 events.certifiedhacker.com
162.241.216.11 ftp.certifiedhacker.com
162.241.216.11 www.certifiedhacker.com

```

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

C PENT

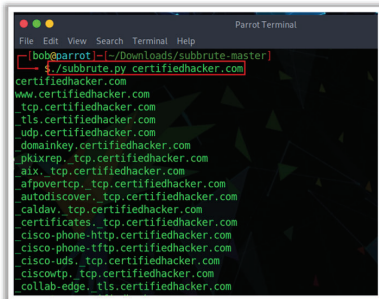


Finding the domain and subdomains of the target is an important step in the penetration testing process as they indicate various network ranges in use. The penetration tester can check for the company's URL in the engagement letter or use a search engine such as Google or Bing to identify the domain of the target. Subdomains generally represent different applications and help view the attack surface of a target organization. Many subdomains also host nonpublic applications that are generally more insecure than public applications.

Many tools are available for discovering the domain and subdomain of the target. Many of these tools are used for enumeration, which is the process of extracting usernames, machine names, network resources, shares, and services from a system. Some of these tools are discussed below.

Source: <https://github.com>

SubBrute is a DNS meta-query spider that enumerates DNS records and subdomains. It includes a fast DNS resolution pipeline for any DNS record type. Further, it has a feature to detect subdomains when their resolution is intentionally blocked, which sometimes occurs in cases where a subdomain is intended for use on an internal network. It is a DNS spider that recursively crawls enumerated DNS records.



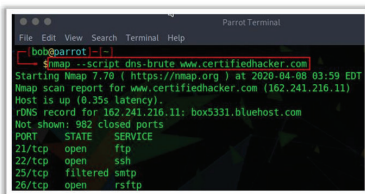
```
Parrot Terminal
File Edit View Search Terminal Help
[ bob@parrot ~ ] [ - / Downloads / subbrute-master ]
$ ./subbrute.py certifiedhacker.com
certifiedhacker.com
www.certifiedhacker.com
tcp.certifiedhacker.com
tls.certifiedhacker.com
udp.certifiedhacker.com
domainkey.certifiedhacker.com
pkixrep._tcp.certifiedhacker.com
aix._tcp.certifiedhacker.com
afpovertcp._tcp.certifiedhacker.com
autodiscover._tcp.certifiedhacker.com
caldav._tcp.certifiedhacker.com
certificates._tcp.certifiedhacker.com
cisco-phone-http.certifiedhacker.com
cisco-phone-tftp.certifiedhacker.com
cisco-uds._tcp.certifiedhacker.com
ciscowtp._tcp.certifiedhacker.com
collab-edge._tls.certifiedhacker.com
```

Figure 3.1: Screenshot of SubBrute

- **Nmap**

Source: <https://nmap.org>

Nmap is a utility for network discovery and security auditing. By using Nmap with dns-brute, scripts written using the Nmap scripting engine (NSE) can be utilized to enumerate DNS hostnames by the brute-force guessing of common subdomains. With the dns-brute.srv argument, dns-brute can also attempt to enumerate common DNS Service (SRV) records. Wildcard records are listed as “*A” and “*AAAA” for IPv4 and IPv6, respectively.



```
Parrot Terminal
File Edit View Search Terminal Help
[ bob@parrot ~ ] [ - ]
$ nmap --script dns-brute www.certifiedhacker.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-08 03:59 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.35s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
26/tcp    open  rsftp
```

Figure 3.2: Screenshot of Nmap using dns-brute

```

3306/tcp open    mysql
5432/tcp open    postgresql

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   news.certifiedhacker.com - 162.241.216.11
|   blog.certifiedhacker.com - 162.241.216.11
|   mail.certifiedhacker.com - 162.241.216.11
|   smtp.certifiedhacker.com - 162.241.216.11
|   ftp.certifiedhacker.com - 162.241.216.11
|   www.certifiedhacker.com - 162.241.216.11
|_

Nmap done: 1 IP address (1 host up) scanned in 25.72 seconds

```

Figure 3.3: Screenshot of Nmap using dns-brute

■ dnsmap

Source: <https://github.com>

dnsmap is mainly meant to be used by penetration testers during the information-gathering/enumeration phase of infrastructure security assessments. During the enumeration stage, the security consultant typically discovers the target company's IP net blocks, domain names, phone numbers, and so on. dnsmap helps penetration testers in finding new domain names that will allow them to map obscure or difficult-to-find net blocks of the target organization.

```

File Edit View Search Terminal Help

bob@parrot:~$ dnsmap certifiedhacker.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gncitizen.org)

[+] searching (sub)domains for certifiedhacker.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

blog.certifiedhacker.com
IP address #1: 162.241.216.11

cpanel.certifiedhacker.com
IP address #1: 162.241.216.11

events.certifiedhacker.com
IP address #1: 162.241.216.11

ftp.certifiedhacker.com
IP address #1: 162.241.216.11

```

Figure 3.4: Screenshot of dnsmap

- **fierce**

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/bob]
#fierce -dns certifiedhacker.com
DNS Servers for certifiedhacker.com:
    ns1.bluehost.com
    ns2.bluehost.com
Trying zone transfer first...
Testing ns1.bluehost.com
    Request timed out or transfer not allowed.
Testing ns2.bluehost.com
    Request timed out or transfer not allowed.
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
162.241.216.11 blog.certifiedhacker.com
162.241.216.11 events.certifiedhacker.com
162.241.216.11 ftp.certifiedhacker.com
162.241.216.11 imap.certifiedhacker.com

```

Figure 3.5: Screenshot of fierce

- **Sublist3r**

Source: <https://github.com>

Sublist3r is a Python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the target domain. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates subdomains using Netcraft, VirusTotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/bob/Downloads/Sublist3r-master
#python sublist3r.py -d google.com -p 80 -e Bing

          SUBLIST3R
          [REDACTED]
          # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Bing..
[-] Total Unique Subdomains Found: 62
[-] Start port scan now for the following ports: 80
accounts.google.com - Found open ports: 80
analytics.google.com - Found open ports: 80
aboutme.google.com - Found open ports: 80
books.google.com - Found open ports: 80
chrome.google.com - Found open ports: 80
ads.google.com - Found open ports: 80
arvr.google.com - Found open ports: 80
classroom.google.com - Found open ports: 80
bookmarks.google.com - Found open ports: 80
assignments.google.com - Found open ports: 80
careers.google.com - Found open ports: 80
contacts.google.com - Found open ports: 80
admin.google.com - Found open ports: 80
console.actions.google.com - Found open ports: 80
console.cloud.google.com - Found open ports: 80
channelservices.cloud.google.com - Found open ports: 80
adwords.google.com - Found open ports: 80
code.google.com - Found open ports: 80
apps.google.com - Found open ports: 80
crowdsourcing.google.com - Found open ports: 80
drive.google.com - Found open ports: 80
docs.google.com - Found open ports: 80

```

Figure 3.6: Screenshot of Sublist3r

▪ Netcraft

Source: <https://searchdns.netcraft.com>

Netcraft provides Internet security services including antifraud and antiphishing services, application testing, and Payment Card Industry (PCI) scanning. They also analyze many aspects of the Internet, including the market share of web servers, operating systems (OSes), hosting providers, and Secure Sockets Layer (SSL) certificate authorities. The Netcraft toolbar helps a penetration tester search for the domain and subdomains of a target organization.

Search: [search tips](#)

example: site contains .netcraft.com

Results for microsoft.com

Found 292 sites

Site	Site Report	First seen	Netblock	OS
1. go.microsoft.com		november 2001	akamai technologies	linux
2. www.microsoft.com		august 1995	akamai international, bv	linux
3. support.microsoft.com		october 1997	akamai international, bv	linux
4. download.microsoft.com		august 1999	akamai international, bv	linux
5. technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
6. msdn.microsoft.com		september 1998	microsoft corporation	windows server 2012
7. answers.microsoft.com		august 2009	akamai international, bv	linux
8. www.catalog.update.microsoft.com		december 2016	microsoft corporation	windows server 2016
9. windows.microsoft.com		june 1998	akamai international, bv	linux
10. social.technet.microsoft.com		august 2008	microsoft corporation	windows server 2012
11. catalog.update.microsoft.com		october 2007	microsoft corporation	windows server 2008
12. o15.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2016
13. office.microsoft.com		november 1998	microsoft corp	unknown
14. e.microsoft.com		january 2014	microsoft informatica ltda f5 big-ip	

Figure 3.7: Screenshot of Netcraft

Finding Similar or Parallel Domain Names



- Search for **similar domain names** and record the findings.
- For example, if the target company is called **xsecurity.com**, then look for **xsecurity.org**, **xsecurity.net**, **xsecurity.biz**, **xsecurity.tv**, **www.xsecurity.com**, **www.xsecuritycom.com**, **www-xsecurity.com**, **www_xsecurity.com**, **www.xsecurity_.com**, **ysecurity.com**, **zsecurity.com**, etc.
- Use **urlcrazy** to find similar domains.

[illegible]

Copyright © by TE-Source. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Similar or Parallel Domain Names

It is important for a penetration tester to identify similar or parallel registered domain names of the target organization. These domain names help them identify how to exploit typosquatting errors by redirecting the victim to a malicious website. For example, if the target organization is called xsecurity.com, then the penetration tester should look for the following:

- xsecurity.org
- xsecurity.net
- xsecurity.biz
- xsecurity.tv
- wwwxsecurity.com
- wwwxsecuritycom.com
- www-xsecurity.com
- www_xsecurity.com
- www_xsecurity_.com
- ysecurity.cm
- zsecurity.com

Tools such as URLCrazy can also be used to search for similar domain names and record the findings.

▪ URLCrazy

Source: <https://github.com>

URLCrazy is a tool used to study domain-name typos and URL hijacking. It is used to generate and test domain typos and variations to detect and perform typosquatting, URL hijacking, phishing, and corporate espionage. It helps a penetration tester perform the following:

- Detect typosquatters profiting from typos on the domain name.
- Protect the brand by registering popular typos.
- Identify typo domain names that will receive traffic intended for another domain.
- Conduct phishing attacks during a penetration test.

```

Parrot Terminal
File Edit View Search Terminal Help
--(bob@parrot:~)~
--$ urlcrazy -p microsoft.com
/usr/share/urlcrazy/tld.rb:81: warning: key "2nd_level_registration" is duplicated and overwritten on line 81
/usr/share/urlcrazy/tld.rb:89: warning: key "2nd_level_registration" is duplicated and overwritten on line 89
/usr/share/urlcrazy/tld.rb:91: warning: key "2nd_level_registration" is duplicated and overwritten on line 91
URLCrazy Domain Report
Domain      : microsoft.com
Keyboard    : qwerty
Host       : 2020-04-08 07:26:32 -0400

# Please wait. 130 hostnames to process

Type Type      Type      Pop  DNS-A      CC-A      DNS-MX
Extn
-----
Character Omission microsoft.com 199.59.242.153 CN,CHINA mx76.m2bp.com
.com
Character Omission microsoft.com 208.91.197.26 VG,VIRGIN ISLANDS (BRITISH)
.com
Character Omission microsoft.com 40.76.4.15 US,UNITED STATES
.com
Character Omission microsoft.com 104.215.148.63
.com
Character Omission microsoft.com 104.215.95.187
.com
Character Omission microsoft.cn 40.76.4.15 US,UNITED STATES
.cn
Character Omission microsoft.com 40.76.4.15 US,UNITED STATES
.com

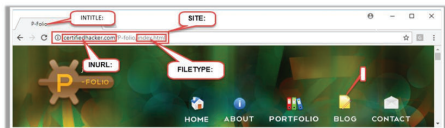
```

Figure 3.8: Screenshot of URLCrazy

Refining Web Searches using Advanced Operators



- Use Google's advanced operators to refine web searches with the Google search engine and **create complex queries** to find, filter, and sort specific information regarding the target.



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

Refining Web Searches using Advanced Operators (Cont'd)



Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location, source:
Product Search	allintext:, allintitle:

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

Refining Web Searches using Advanced Operators (Cont'd)



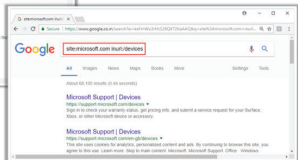
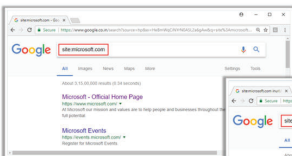
Uses of some advanced operators supported by Google

Operator	Purpose
Or	Searches for a given term or its equivalent
" "	Searches for a specific term
-	Removes pages related with the specified term from the results
[site:]	Restricts the results to those websites in the given domain
[intitle:]	Restricts the results to those pages containing the search keyword in the title
[allintitle:]	Restricts the results to those websites with all the search keywords in the title
[allintext:]	Searches pages with content specified in the search criteria
[inurl:]	Restricts the results to those pages containing the search keyword in the URL
[allinurl:]	Restricts the results to those pages containing all the search keywords in the URL
[link:]	Searches web pages that contain links to the specified web page
[info:]	Presents some information that Google has about a particular web page
[related:]	Searches web pages that are similar to a specified web page
[cache:]	Displays web pages stored in the Google cache
[location:]	Finds information for a specific location

Note: You can also combine these operators to obtain more specific result

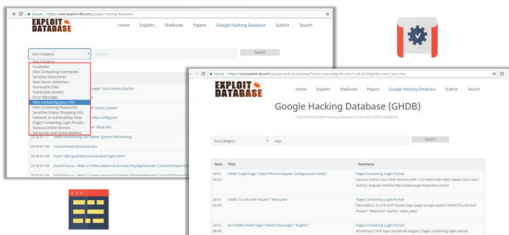
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Refining Web Searches using Advanced Operators (Cont'd)



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

Refining Web Searches using Advanced Operators (Cont'd)



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

Refining Web Searches using Advanced Operators (Cont'd)



Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Looks for the Asterisk Management Portal
inurl:"NetworkConfiguration" cisco	Finds Cisco phone details
inurl:"cmmuser/login.asp"	Finds the Cisco call manager
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:" SPA Configuration"	Searches Linksys phones

Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with group passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's Secure Sockets Layer (SSL)-VPN login portal
!Host=*. * intext:enc_UserPassword= * ext:pcf	Looks for profile configuration files (.pcf) containing user VPN profiles
filetype:pcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login details
filetype:pcf vpn OR Group	Finds publicly accessible .pcf files used by VPN clients

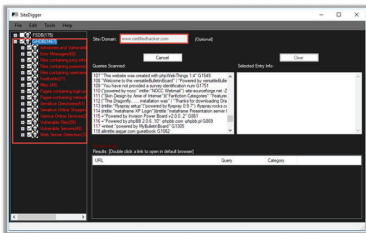
Source: <https://www.exploit-db.com>

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

Refining Web Searches using Advanced Operators (Cont'd)



- Use **Sitedigger** to automate the Google hacking process.



Source: <https://www.micr0f0n.com>

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

Refining Web Searches using Advanced Operators (Cont'd)



- Use the **Google Hacking Diggity Project** to employ search engines such as Google, Bing, and Shodan to quickly identify vulnerable systems and sensitive data in networks.



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

Refining Web Searches using Advanced Operators

Google's advanced operators can be used to refine a search and create complex queries to find, filter, and sort specific information regarding the target. Google hacking is a hacking technique to locate specific strings within search results by using an advanced operator in the Google search engine. Well-composed queries can return valuable data about a target company. Through Google hacking, a penetration tester can find websites vulnerable to numerous exploits and vulnerabilities. The Google Hacking Database (GHDB), a database of queries, can be used to

identify sensitive data. By using advanced Google search operators, the penetration tester can locate specific strings such as specific versions of vulnerable web applications.

The syntax to use an advanced search operator is “operator search_term.” The following screenshot demonstrates some advanced search operators.

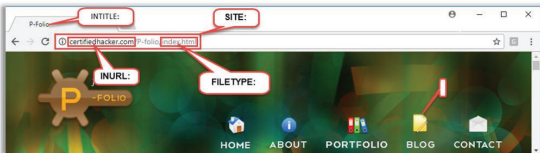


Figure 3.9: Advanced search operators and their relation to a web address

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

The following table lists the search operators that work with each Google search service.

Search Service	Search Operators
Web Search	allinanchor; allintext; allintitle; allinurl; cache; define; filetype; id; inanchor; info; intext; intitle; inurl; link; related; site;
Image Search	allintitle; allinurl; filetype; inurl; intitle; site;
Groups	allintext; allintitle; author; group; insubject; intext; intitle;
Directory	allintext; allintitle; allinurl; ext; filetype; intext; intitle; inurl;
News	allintext; allintitle; allinurl; intext; intitle; inurl; location; source;
Product Search	allintext; allintitle;

Table 3.1: Google search services and advanced operators

The following are some popular Google advanced search operators:

- **or:** searches for a given term or its equivalent
- **“ ”:** searches for a specific term
- **-:** removes pages related with the specified term from the results
- **site:** restricts the search results to the specified site or domain
- **intitle:** restricts the results to those pages containing the specified term in the title

- **allintitle:** restricts the results to those pages containing all the query terms specified in the title
- **allintext:** searches pages with content specified in search criteria
- **inurl:** restricts the results to those pages containing the word specified in the URL
- **allinurl:** restricts the results to those pages containing all the query terms specified in the URL
- **link:** searches websites or pages that contain links to the specified website or page
- **info:** finds information for the specified web page
- **related:** displays websites that are similar or related to the specified URL
- **cache:** displays Google's cached version of a web page, instead of the current version of the web page
- **location:** finds information for a specific location
- **define:** finds definitions of words, phrases, and acronyms
- **filetype:** allows searching based on a file extension
- **id:** an undocumented alias for info
- **inanchor:** restricts results to those pages containing the query terms specified in the anchor text on links to the page
- **allinanchor:** restricts results to those pages containing all query terms specified in the anchor text on links to the page
- **author:** restricts Google Groups results to include newsgroup articles by the specified author; the author can be a full or partial name or email address
- **group:** restricts Google Groups results to newsgroup articles from certain groups or subareas
- **insubject:** restricts articles in Google Groups to those that contain the specified terms
- **intext:** restricts results to documents containing the term in the text
- **source:** restricts results to articles from the news source with the specified ID

Note: These operators can be combined to obtain specific results.

Example: Use the Google advanced operator syntax `[site:microsoft.com inurl:/devices]` to find sensitive information about a target organization and its devices. Use `[site:microsoft.com -site:www.microsoft.com]` to find all the pages related to the subdomains of the target organization. Use `[site:microsoft.com intitle:support]` to retrieve all the web pages containing "support" in the title of the pages in the domain specified by the site operator.

The following figures show screenshots of the Google search engine results page displaying the results for the queries mentioned above.

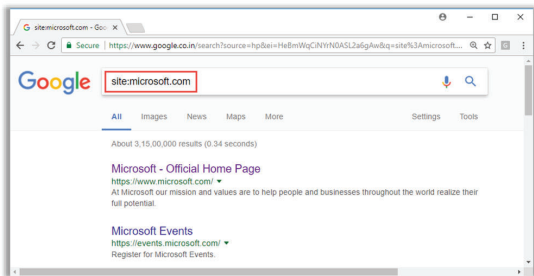


Figure 3.10: Screenshot of the Google search engine results page for **site:microsoft.com**

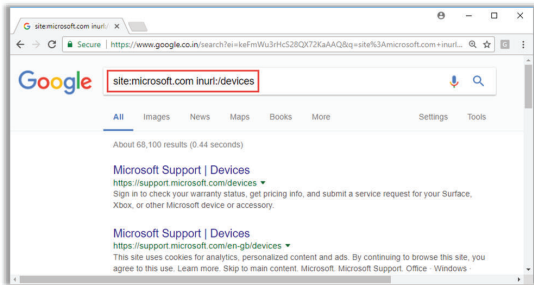


Figure 3.11: Screenshot of the Google search engine results page for **site:microsoft.com inurl:/devices**

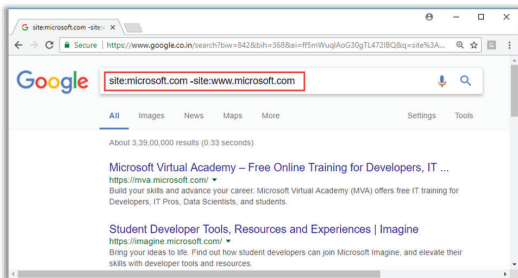


Figure 3.12: Screenshot of the Google search engine results page for `site:microsoft.com -site:www.microsoft.com`

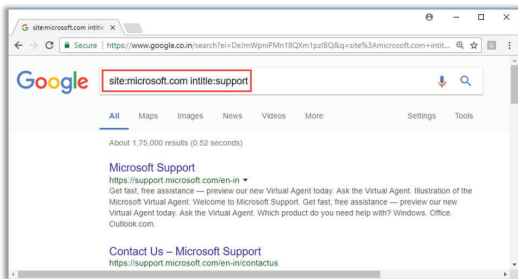


Figure 3.13: Screenshot of the Google search engine results page for `site:microsoft.com intitle:support`

Google Hacking Database

Source: <https://www.exploit-db.com>

The GHDB is an authoritative source for querying the ever-widening reach of the Google search engine. Google Hacking/Dorking can be used to perform an advanced search. The GHDB includes search terms for files containing usernames, vulnerable servers, and even passwords. The Exploit Database (Exploit DB) is a Common Vulnerabilities and Exposures (CVE)-compliant archive of

public exploits and the corresponding vulnerable software, and it was developed for use by penetration testers and vulnerability researchers.

The following are the categories in the GHDB:

- Footholds
- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages
- Files Containing Juicy Info
- Files Containing Passwords
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Advisories and Vulnerabilities

The screenshot shows the GHDB website interface. At the top is the 'EXPLOIT DATABASE' logo and a navigation menu with links: Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. The main heading is 'Google Hacking Database (GHDB)' with a subtitle 'Search the Google Hacking Database or browse GHDB categories'. Below this is a search bar with a dropdown menu set to 'Any Category' and a 'Search' button. A table of results is displayed below the search bar.

Date	Title	Category
2017-07-17	index of .htdocs	Sensitive Directories
2017-07-17	"You're successfully running JSON Server"	Files Containing juicy info
2017-07-14	inurl:"ADVANCED/COMMON/TOPI"	Various Online Devices
2017-07-14	intitle:"Namenode Information"	Various Online Devices
2017-07-14	inurl:"sap/recuperadocumentossq.aspx"	Various Online Devices
2017-07-14	inurl:login.cgi intitle:NETGEAR	Various Online Devices
2017-07-07	filetype:txt "wordfence"	Advisories and Vulnerabilities
2017-06-27	"Sorting Logs:" "Please enter your password:" "Powered By" -urlscan -alamy	Footholds

Figure 3.14: Screenshot of the Google Hacking Database

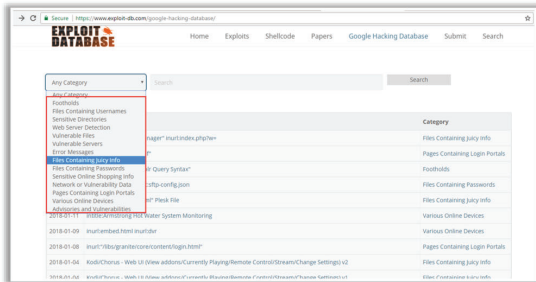


Figure 3.15: Screenshot of the Google Hacking Database showing various categories

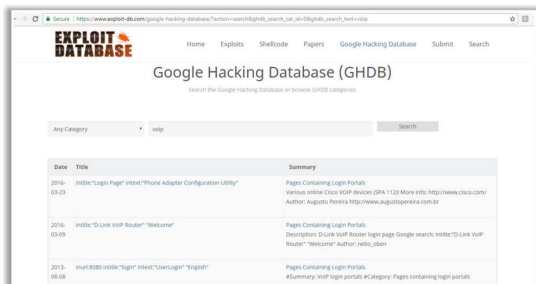


Figure 3.16: Screenshot of the Google Hacking Database showing results of voice over IP (VoIP) vulnerabilities

Google search queries for VoIP footprinting and VPN footprinting

A penetration tester can write Google search queries using advanced operators that help refine searches to expose sensitive information, vulnerabilities, and passwords. These Google hacking operators can be used for VoIP and virtual private network (VPN) footprinting. Furthermore, these operators can be used to remove information such as pages containing login portals, VoIP login portals, and directory with keys of VPN servers.

The following tables list some Google hacking operators to obtain specific information related to VoIP and VPN footprinting, respectively.

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Looks for the Asterisk Management Portal
inurl:"NetworkConfiguration" cisco	Finds Cisco phone details
inurl:"ccmuser/logon.asp"	Finds the Cisco call manager
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:"SPA Configuration"	Searches Linksys phones

Table 3.2: Google search queries for VoIP footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with group passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*. * intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf) files containing user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login details
filetype:pcf vpn OR Group	Finds publicly accessible.pcf used by VPN clients

Table 3.3: Google search queries for VPN footprinting

Tools such as SiteDigger can be used to automate the Google hacking process.

- **SiteDigger**

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

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on websites. It supports proxy

and Tor. Further, it provides results in real time and includes a configurable result set and updated signatures. It can also save the signature selection and result set.

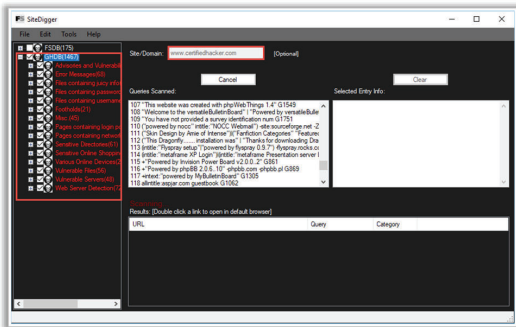


Figure 3.17: Screenshot of SiteDigger

Google Hacking Diggity Project

Source: bishopfox.com

With the Google Hacking Diggity Project, search engines such as Google, Bing, and Shodan can be utilized to quickly identify vulnerable systems and sensitive data in networks.

Google Hacking Diggity Project attack tools enable finding information disclosures and exposed vulnerabilities before others do. It consists of various attack and defense tools. The following are the Google Hacking Diggity Project attack tools:

- Search Diggity
- GoogleDiggity
- BingDiggity
- FlashDiggity
- DLPDiggity
- LinkFromDomaindiggity
- CodeSearchDiggity
- MalwareDiggity

- PortScanDiggity
- NotinMyBackYard
- Bing BinaryMalware
- SHODANDiggity



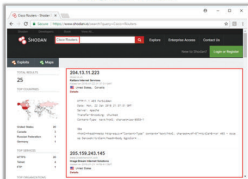
Figure 3.18: Screenshot of Google Hacking Diggity Project

Footprinting the Target using Shodan

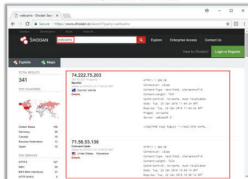


- Shodan is a search engine for **finding specific devices** and **device types** that exist online and are open on the Internet. It finds devices such as webcams, routers, switches, and Internet of things (IoT) devices.

Searching Cisco routers worldwide with their public IP addresses



Searching webcams worldwide with their public IP addresses



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

Footprinting the Target using Shodan

- Shodan

Source: <https://www.shodan.io>

Shodan is a search engine for finding specific devices and device types that exist online and are open on the Internet. It finds devices such as webcams, routers, switches, and other Internet of things (IoT) devices connected to the Internet. Shodan can be used to discover which devices are connected to the Internet, where they are located, and who is using them. It allows one to keep track of all the devices on the network that are directly accessible through the Internet. It also allows the user to find devices based on city, country, latitude/longitude, hostname, operating system, and IP address. Further, it helps the penetration tester search for known vulnerabilities and exploits across Exploit DB, Metasploit, CVE, Open Source Vulnerability Database (OSVDB), and Packetstorm with a single interface. This information helps the penetration tester identify potential vulnerabilities and find effective exploits.

The following screenshot shows the use of Shodan to search for Cisco routers worldwide with their public IP addresses.

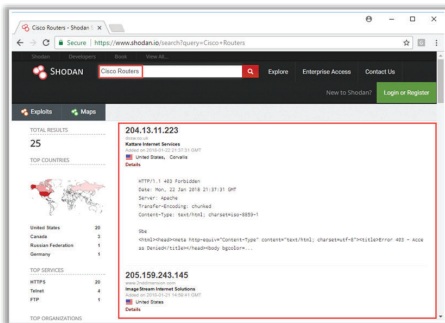


Figure 3.19: Screenshot of Shodan searching for Cisco routers

The following screenshot shows the use of Shodan to search for webcams worldwide with their public IP addresses.

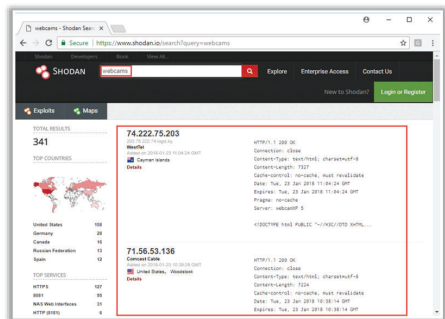
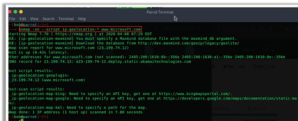


Figure 3.20: Screenshot of Shodan searching for webcams

Finding the Geographical Location of a Company



- Use **Google Maps** or **Google Earth** to find the geographical location of the target company.
- Find a neighboring company and famous **landmarks** such as theaters and restaurants.
- Find the **traffic condition** around the company
- The company's location can also be found using other services:
 - <http://www.wikimapia.org>
 - <https://www.mapquest.com>
 - <https://www.waze.com/en-GB/livemap>
 - <https://www.bing.com/maps>



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

Finding the Geographical Location of a Company

A penetration tester can use tools such as Google Maps and Google Earth for finding the geographical location of the target organization. These tools allow them to find and explore most locations on the Earth. They provide information such as images of buildings, as well as surroundings including Wi-Fi networks. Tools such as Google Maps can be used to even locate entrances of buildings, security cameras, and gates. By using these tools, the penetration tester can find a neighboring company and famous landmarks such as theaters and restaurants. These tools provide interactive maps, outline maps, satellite imagery, and information on how to interact with and create one's own maps. Google Maps, Yahoo Maps, and other tools provide driving directions and traffic conditions, locate landmarks, and provide detailed address and contact information.

■ Google Maps

Source: <https://www.google.com/maps>

Google Maps provides a Street View feature that presents a series of displays, images of buildings, as well as surroundings, including Wi-Fi networks. Google Maps can be used to find or locate, for example, entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources such as electricity connections; additionally, it can measure the distance between different objects.

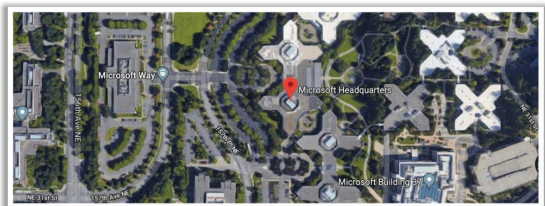


Figure 3.21: Screenshot of Google Maps

- **Nmap**

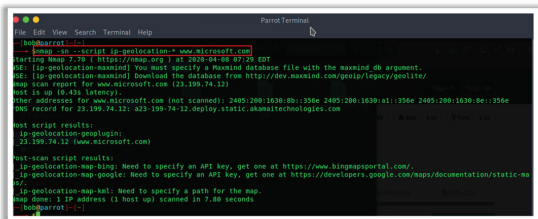
Source: <https://nmap.org>

Nmap is a utility for network discovery and security auditing. The Nmap ip-geolocation script can be used to identify the physical location of an IP address and Global Positioning System (GPS) coordinates of the target. The NSE scripts available for this purpose are listed below:

- **ip-geolocation-geoplugin**
Attempts to identify the physical location of an IP address using the Geoplugin geolocation web service
- **ip-geolocation-ipinfodb**
Attempts to identify the physical location of an IP address using the IPInfoDB geolocation web service
- **ip-geolocation-map-bing**
Queries the Nmap registry for the GPS coordinates of targets stored by previous geolocation scripts and renders a Bing Map of markers representing the targets
- **ip-geolocation-map-google**
Queries the Nmap registry for the GPS coordinates of targets stored by previous geolocation scripts and renders a Google Map of markers representing the targets
- **ip-geolocation-map-kml**
Queries the Nmap registry for the GPS coordinates of targets stored by previous geolocation scripts and produces a Keyhole Markup Language (KML) file of points representing the targets

- **ip-geolocation-maxmind**

Attempts to identify the physical location of an IP address using a Geolocation Maxmind database file



```
Parrot Terminal
File Edit View Search Terminal Help
--[bob@barrot:~]$ nmap -sn --script ip-geolocation-maxmind www.microsoft.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-08 07:29 EDT
NSE: [ip-geolocation-maxmind] You must specify a Maxmind database file with the maxmind.db argument.
NSE: [ip-geolocation-maxmind] Download the database from http://dev.maxmind.com/geoip/legacy/geolite/
Nmap scan report for www.microsoft.com (23.199.74.12)
Host is up (0.43s latency).
Other addresses for www.microsoft.com (not scanned): 2405:200:1630:8b::356e 2405:200:1630:a1::356e 2405:200:1630:8e::356e
DNS record for 23.199.74.12: 923-199-74-12.deploy.static.akamaitechnologies.com

Host script results:
  ip-geolocation-geoplugin:
    23.199.74.12 (www.microsoft.com)

Nmap scan script results:
  ip-geolocation-map-bing: Need to specify an API key, get one at https://www.bingmapsportal.com/.
  ip-geolocation-map-google: Need to specify an API key, get one at https://developers.google.com/maps/documentation/static-ma
  ps/.
  ip-geolocation-map-hel: Need to specify a path for the map.
Nmap done: 1 IP address (1 host up) scanned in 7.80 seconds
--[bob@barrot:~]$
```

Figure 3.22: Screenshot of Nmap

The following are some other services that can be used to find the target's location:

- <http://www.wikimapia.org>
- <https://www.mapquest.com>
- <https://www.waze.com/en-GB/livemap>
- <https://www.bing.com/maps>

Listing Employees and their Email Addresses



- 1 Sign up as a customer and **request a** presentation.
- 2 Gather all possible information about the company and connect with various people.
- 3 Look for contact information and telephone extensions.
- 4 Look for the **employees' business** and personal email accounts.

Example:

- If John Stevens' business email is johns@xsecurity.com, then identify his personal email accounts such as **jstevens@yahoo.com** or **jjstevens@hotmail.com**.
- Send an email to John stating that a file cannot be sent to his business **email account** and asking him if he has any other email account.



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

Listing Employees and their Email Addresses

To attempt social engineering on the target organization, the penetration tester must gather the email addresses of the employees. For gathering such information, they must browse the company's website, analyze their services, sign up as a customer, and request for a service from the company.

This allows them to gather all possible information about the target organization such as the structure of email addresses, internal mailing lists and typical sender of internal mailings, and contact information and telephone extensions of employees. If the penetration tester has succeeded in gathering the business mail addresses of employees, then they attempt to find their personal email IDs as well because communicating through a personal email ID helps them befriend an employee more easily without leaving any clue for the target organization. After gathering the required list of email IDs, the penetration tester can contact a specific person and attempt to influence that person using various social engineering techniques such as disguising and prompting the employee to provide their credentials.

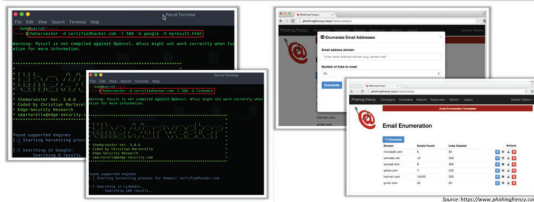
For example, consider the following scenario:

- If John Stevens' business email is johns@xsecurity.com, then identify his personal email accounts such as jstevens@yahoo.com, jjstevens@hotmail.com, and so on.
- Send an email to John stating that a file cannot be sent to his business email account and asking him if he has any other email account.

Identifying Key Email Addresses through Email Harvesting



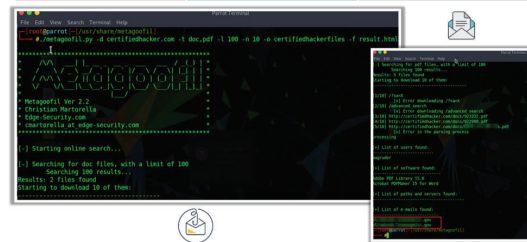
- Use email harvesting tools such as **theHarvester**, **Phishing Frenzy**, and **Metagoofil** to enumerate publicly available email addresses of the target organization.



Source: <https://www.fishingnews.co.uk>

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

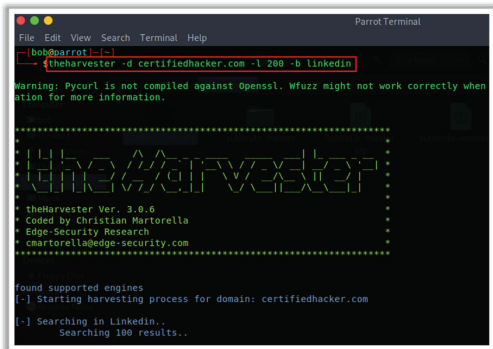
Identifying Key Email Addresses through Email Harvesting (Cont'd)



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

Identifying Key Email Addresses through Email Harvesting

Email harvesting is a process in which a large number of email addresses are obtained through different methods. It is mainly used for bulk emailing or for spamming. A penetration tester can use email harvesting tools such as theHarvester and Phishing Frenzy to enumerate publicly available email addresses of the target organization. These tools gather email addresses from popular sites such as social networking sites, forums, and blogs.



```
File Edit View Search Terminal Help
[bo@parrot:~]$ theharvester -d certifiedhacker.com -l 200 -b linkedin
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when
ation for more information.

*****
* theHarvester Ver. 3.0.6 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****

found supported engines
[-] Starting harvesting process for domain: certifiedhacker.com
[-] Searching in LinkedIn..
    Searching 100 results..
```

Figure 3.24: Screenshot of theHarvester searching in LinkedIn

▪ Phishing Frenzy

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

Phishing Frenzy is an open-source Ruby on Rails application that is leveraged by penetration testers to manage email phishing campaigns. It streamlines the phishing process and provides users a realistic phishing campaign through features such as campaign management, template reuse, and statistical generation.

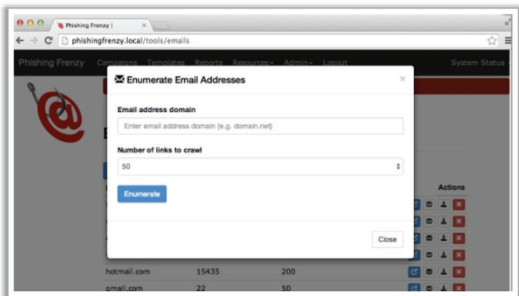


Figure 3.25: Screenshot of Phishing Frenzy showing the process of enumerating email addresses

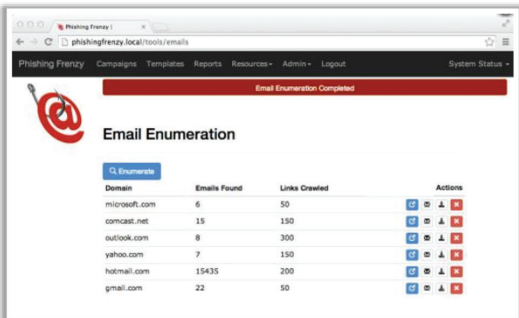


Figure 3.26: Screenshot of Phishing Frenzy showing results of enumerated email addresses

- **Metagoofil**

Source: <http://www.edge-security.com>

Metagoofil is an information-gathering tool designed for extracting the metadata of public documents (PDF, doc, xls, ppt, docx, pptx, and xlsx) belonging to a target company.

Metagoofil performs a search in Google to identify and download documents to a local disk and then extracts the metadata with different libraries such as Hachoir and PDFMiner. With the results, it generates a report with usernames, software versions, and servers or machine names, which helps penetration testers in the information-gathering phase.

As shown in figures below, on executing a scan for documents from a domain (**-d *certifiedhacker.com***) that are doc and PDF files (**-t *doc, pdf***), the result displays email addresses found in the domain.

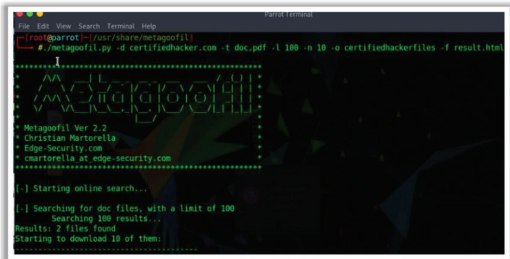
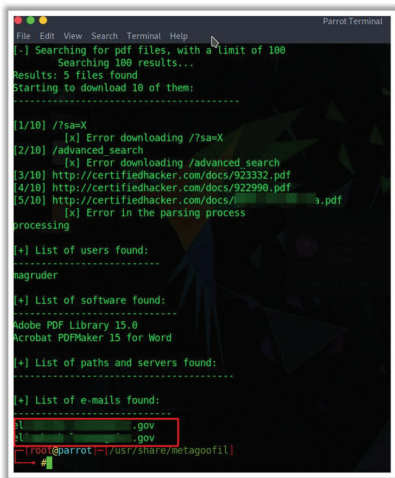


Figure 3.27: Screenshot of Metagoofil



```
Parrot Terminal
File Edit View Search Terminal Help
[-] Searching for pdf files, with a limit of 100
    Searching 100 results...
Results: 5 files found
Starting to download 10 of them:
-----
[1/10] /?sa=X
    [x] Error downloading /?sa=X
[2/10] /advanced_search
    [x] Error downloading /advanced_search
[3/10] http://certifiedhacker.com/docs/923332.pdf
[4/10] http://certifiedhacker.com/docs/922990.pdf
[5/10] http://certifiedhacker.com/docs/.....a.pdf
    [x] Error in the parsing process
processing
[+] List of users found:
-----
magruder

[+] List of software found:
-----
Adobe PDF Library 15.0
Acrobat PDFMaker 15 for Word

[+] List of paths and servers found:
-----

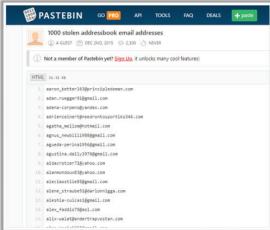
[+] List of e-mails found:
-----
el .....gov
el .....gov
[+] root@parrot: /usr/share/metagoofil
#
```

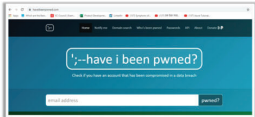
Figure 3.28: Screenshot of Metagoofil enumerating email address

Enumerating Key Email Addresses from Pastebin and HaveIBeenPwned



- Look for email addresses disclosed by third-party password dumps such as **Pastebin** and **HaveIBeenPwned**.
- Use utilities such as **SimplyEmail** and **Pepe** to collect email addresses from Pastebin.





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

Enumerating Key Email Addresses from Pastebin and HaveIBeenPwned

One can obtain a large number of email addresses from websites such as Pastebin HaveIBeenPwned. These websites are designed for storing and sharing text (code snippets) online for review. They are used for posting data containing personal information such as names, addresses, dates of birth, telephone numbers, and email addresses extracted from insecure databases. Hence, they are major sources of third-party-disclosed email addresses.

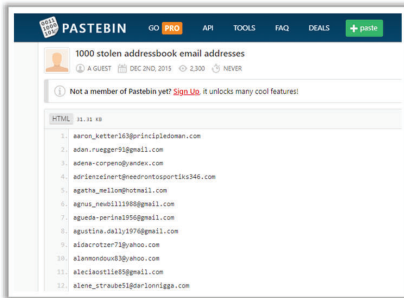


Figure 3.29: Screenshot of Pastebin

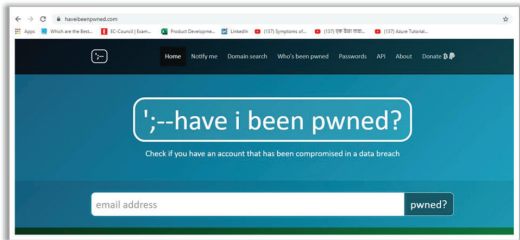


Figure 3.30: Screenshot of HavelBeenPwned

Tools such as Pepe and SimplyEmail can be used to collect email addresses.

- **Pepe:** It can be used to collect email address from Pastebin, Google, Trumail, Pipl, FullContact and HavelBeenPwned. The user can notify the person about their leaked password by sending an email. It supports only one format—email:password.
- **SimplyEmail:** It is an email enumeration tool. Further, it is an expansion of theHarvester and allows users to easily build modules for a framework.

Listing Key Personnel of the Company



- Use a search engine such as **Google** to find the key personnel of the company and crosslink information.
- Use **dice.com**, **Monster**, and other job sites to look for key personnel information.
- Headhunters might have employee **profiles**.



Look for the following in background checks on key employees:

- Resumes
- Work experience
- Completed projects
- Promotions
- Accomplishments



Example

- Consider John Stevens, the CFO of XSECURITY corporation; search for "John Stevens joining XSECURITY" in **Google** and look for deep links.



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

Listing Key Personnel of the Company

Gathering background details of key personnel can provide vital information about the target organization as they have the most crucial responsibilities. For example, in a typical company, the CEO, president, vice president, and managers can be called key personnel.

Search engines such as Google can be used to find the key personnel of the company and crosslink information. Furthermore, dice.com, Monster, and other job sites can be used to find information on key personnel. Headhunters can also help as they might have employee profiles.

For example, consider John Stevens, who is the CFO of XSECURITY corporation; a penetration tester can search for "John Stevens joining XSECURITY" in Google and look for deep links.

Once the penetration tester finds the profiles of the key personnel, they attempt to obtain background information. The tester focuses more on their resumes, work experience, completed projects, promotions, and accomplishments. The resume would provide information such as the name, age, sex, contact information, home address, email IDs, and phone numbers. Apart from personal details, their qualifications, university name, school name, aggregate marks, and graduation year can also be obtained. Other information includes the person's total work experience, the organizations for which they have worked, the projects on which they have worked, and their comments. The background check should also include any promotions the person has received within a specific duration and their major achievements in the organization. The information obtained here can help in performing social engineering.

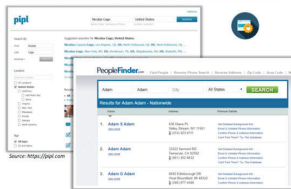
Using People Search Online Services to Collect Information



- Information about an individual can be found in various people search websites such as **pipl**, **Spokeo**, and **PeopleFinder**.

A people search returns the following information about a person:

- Photos and residential addresses
- Contact numbers
- Date of birth
- Email addresses
- Satellite pictures of private residences



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

Using People Search Online Services to Collect Information

If the penetration tester has failed in finding a person's details through search engines, then they attempt to find the information using people search websites such as pipl, Spokeo, and PeopleFinder. These websites have direct access to invisible web information, unlike normal search engines. They provide information such as photos and residential addresses, contact numbers, dates of birth, email addresses, and satellite pictures of private residences.

Some people search online services are discussed below.

pipl

Source: <https://pipl.com>

People search is one of the most widely used people search engines. It generally provides accurate outputs, which include personal web pages, press mentions, and social networking pages, against the given person's name, email address, social username, or phone number.

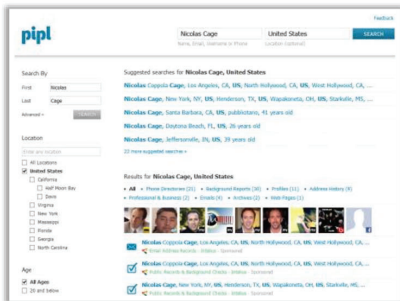


Figure 3.31: Screenshot of pipl

■ PeopleFinder

Source: <https://peoplefinder.com>

PeopleFinder is a one-stop resource for people searching online. It has indexed millions of publicly available records and provides a simple search format for up to 80% of the people currently residing in the United States. In addition to free people searches, PeopleFinder has search portals for reverse phone lookups. It also provides comprehensive white pages that give instant access to millions of records.

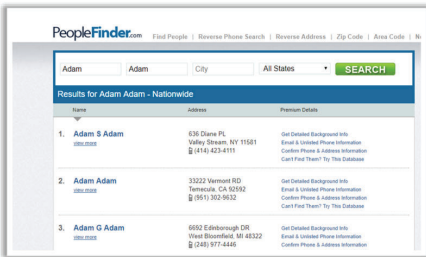


Figure 3.32: Screenshot of PeopleFinder

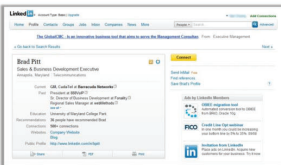
Browsing Social Network Websites to Find Information on the Company and Employees



- Register with fake profiles in **social network websites** such as LinkedIn and Facebook and attempt to join the target organization's community or employee groups where personal and company information are shared.
- Gather personal **email IDs, phone numbers**, and addresses of **key personnel** or employees.

Social networking websites to find information on the company:

- <https://www.linkedin.com>
- <https://www.facebook.com>
- <https://twitter.com>
- <https://www.pinterest.com>
- <https://plus.google.com>
- <https://instagram.com>



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

Browsing Social Network Websites to Find Information on the Company and Employees

Today, several social network websites are used globally for contacting and connecting with friends, friends of friends, and relatives through posts, instant messages, and so on. In such websites, anybody can view an individual's profile and obtain general information about them.

A penetration tester can register with fake profiles in social network websites such as LinkedIn and Facebook, and they can attempt to join the target organization's community or employee groups where personal and company information are shared. Moreover, these websites may have several communities based on the name of the company, hobbies, and extracurricular activities. The penetration tester can search for communities related to a company and gather personal email addresses, phone numbers, and addresses of key personnel or employees, and they can craft phishing emails or vishing calls to compromise the target organization.

The following screenshot illustrates information obtained through LinkedIn.

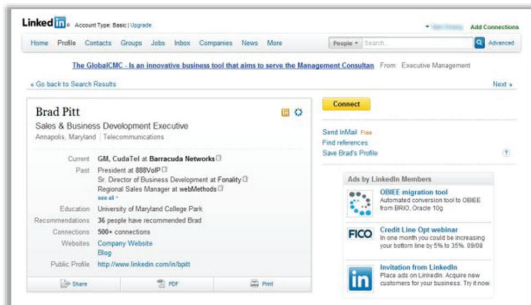


Figure 3.33: Screenshot of LinkedIn

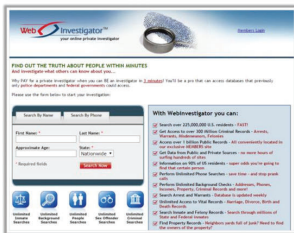
The following are some social networking websites in which information about the target company can be found:

- <https://www.linkedin.com>
- <https://www.facebook.com>
- <https://twitter.com>
- <https://www.pinterest.com>
- <https://plus.google.com>
- <https://instagram.com>

Using Web Investigation Tools to Extract Sensitive Data about the Company



- Use the Web Investigator tool to search **online records** in many categories such as background searches and people searches.



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

Using Web Investigation Tools to Extract Sensitive Data about the Company

Web investigation tools help penetration testers obtain crucial information about the target organization. They can use tools such as Web Investigator to search online records in many categories such as background searches and people searches.

■ Web Investigator

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

Web Investigator is a company that provides search services for online records in many categories. It systematically gathers databases, sources, and data-center links to provide investigation services.

With Web Investigator, the penetration tester can do the following:

- Perform online investigation on civil records, background records, criminal records, legal records, social security number (SSN) records, credit records, and so on.
- Perform people search.
- Perform reverse lookups on phone numbers, email addresses, and IP addresses.
- Gather data from both public and private sources.
- Perform unlimited business searches.
- Access public and private records.
- Perform unlimited background checks.
- Investigate and find property records.



[Members Login](#)

FIND OUT THE TRUTH ABOUT PEOPLE WITHIN MINUTES

And investigate what others can know about you...

Why PAY for a private investigator when you can BE an investigator in 3 minutes? You'll be a pro that can access databases that previously only police departments and federal governments could access.

Please use the form below to start your investigation:

Search By Name

Search By Phone

First Name: *

Last Name: *

Approximate Age:

State: *

Nationwide

* Required fields

Search Now

With WebInvestigator you can:

- ☒ Search over 225,000,000 U.S. residents - FAST!
- ☒ Get Access to over 300 Million Criminal Records - Arrests, Warrants, Misdemeanors, Felonies
- ☒ Access over 1 billion Public Records - All conveniently located in our exclusive MEMBERS site
- ☒ Get Data from Public and Private Sources - no more hours of surfing hundreds of sites
- ☒ Information on 90% of US residents - super odds you're going to find that certain person
- ☒ Perform Unlimited Phone Searches - save time - and stop prank calls
- ☒ Perform Unlimited Background Checks - Addresses, Phones, Incomes, Property, Criminal Records and more!
- ☒ Search Arrest and Warrants - Database is updated weekly
- ☒ Unlimited Access to Vital Records - Marriage, Divorce, Birth and Death Records
- ☒ Search Inmate and Felony Records - Search through millions of State and Federal inmates
- ☒ Find Property Records - Neighbors yards full of junk? Need to find the owners of the property?



Unlimited Inmate Searches



Unlimited Background Searches



Unlimited People Searches



Unlimited Sex Offender Searches



Unlimited Criminal Searches

Figure 3.34: Screenshot of Web Investigator

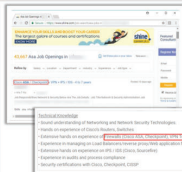
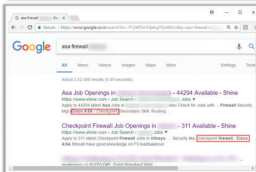
Identifying the Type of Network Devices used in the Organization



- Google certain keywords with the organization's name.
- For example, **ASA firewall** with [company Name]



- This may yield relevant information in **job sites**, **professional** or **social networking sites**, etc., from which the devices used in the target organization can be determined.

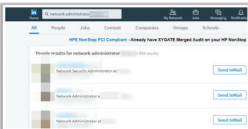
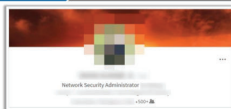


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying the Type of Network Devices used in the Organization (Cont'd)



- LinkedIn profiles** of network administrators of the target company



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

Identifying the Type of Network Devices used in the Organization (Cont'd)



- Search for the company's job postings in major **newspapers, classifieds, and job search engines** to gather its infrastructure details:

- <https://www.linkedin.com>
- <http://www.monster.com>
- <https://www.careerbuilder.com>
- <https://www.dice.com>
- <https://www.indeed.com>
- <https://www.usajobs.gov>

- Look for **system administrators, database operators, and security administrators**.
- Companies list the experience required, which indicates the **technology infrastructure** they have.

- Look for information such as job **requirements, employee profiles, hardware information, and software information**.

Example: The company advertises Required: System administrator with work experience in Oracle, Cisco routers, and Checkpoint firewall.

- This indicates that the company has the following infrastructure in their organization:

- Oracle database server
- Cisco routing devices
- Checkpoint firewalls



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

Identifying the Type of Network Devices used in the Organization (Cont'd)



Example:

Job Summary Location Atlanta, GA 30316 Industries Computer Software Job Type • Full Time • Employee Education Level Bachelor's Degree Career Level Manager (Manager/ Supervisor of Staff) Salary \$5,000.00 - 100,000.00 \$ / year Job Reference Code 2534	Sr. Network Administrator About the Job Responsibilities: The Senior Network Administrator is responsible for maintaining Exchange/ Communicator, the LAN and WAN operating infrastructure while working in a team of Administrators & Software Developers. Such responsibilities will include: System upgrades, system documentation, daily administration and problem-resolution, as well as assisting staff and users in problem resolution relating to hardware, software, and communication issues. S/he will participate in the design and planning of the infrastructure to support new applications, technologies and security, and thereafter play a key role in the maintenance of such tools. Essential Administration Functions: - Active Directory experience in trouble shooting - AD replication (LAN/ WAN) DNS (Replication & Resolution), DHCP & IPsec scopes - Administration and complete support and upgrade of the MS-Exchange/ Lync - Virtualization administrator (VMware & Hyper-V), EMC & Dell SAN Administration, Cisco Firewalls & Switches Administration, Barracuda Hardware Appliances, Silver Peak Data compression devices, VCDP Phone System Administration and Video Conferencing - Excellent understanding and ability to troubleshoot Smart Phone and active sync, Power shell commands, and patching with WSUS - TCP/IP Routing services including but not limited to Firewalls, switches, DNS, DHCP, Microsoft Active Directory, Internet Information Services, e-mail, hardware load balancers, and Anti-Spam devices - LAN/WAN connectivity at corporate offices, colocation, and all customer installations - Site Implementations - Purchase, configuration, and installation of equipment, software & services of all customer sites using project management methodologies - Installation of all server & desktop software including but not limited to Windows 2008/2012/2016 Server, Windows 7/8.1, Exchange 2010/2013, Symantec Anti-Virus, IPS and all associated add-on tools, SQL Server, Accounting systems, and Microsoft Office and Adobe Desktop products - First support of all off-site Operations and Sales equipment
--	--

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

Identifying the Type of Network Devices used in the Organization

A penetration tester needs to obtain information about various networking devices used in the target organization. This task is essential while performing penetration testing to understand the network infrastructure and installation design of the target organization. The task can be performed in various ways.

Obtaining information from Google

Google is a powerful tool for searching information that the tester needs to gather from the target organization without leaving any tracks of their activity. Googling a certain network-device-related keyword with the organization name can reveal whether it is using that network device.

The following figure shows the result of searching in Google with “ASA firewall” and the name of the target company.

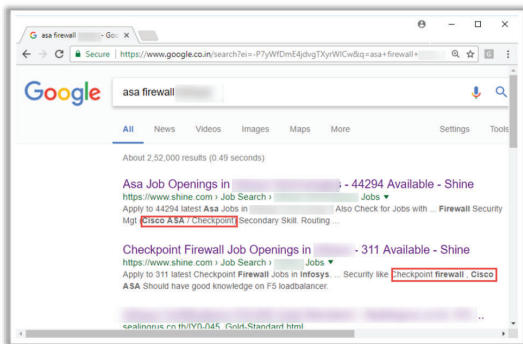


Figure 3.35: Screenshot of a Google search for “ASA firewall” and the name of the target company

As shown in the figure, the results contain information about the usage of the Cisco ASA firewall in the target organization. Clicking on the links may yield relevant information in job sites, professional or social networking sites, and so on, from which the penetration tester can obtain information about the devices used in the target organization.

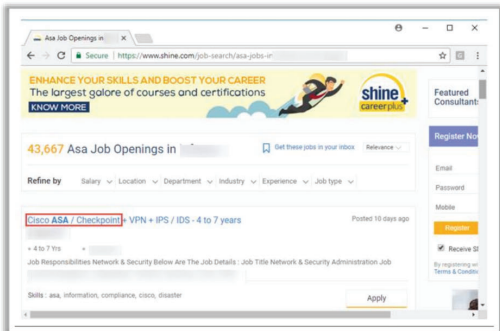


Figure 3.36: Screenshot of a job site obtained from Google search results



Figure 3.37: Screenshot of a job description obtained from Google search results

Obtaining information from LinkedIn

LinkedIn can be a major source for gathering technical information about the target organization, as most employees maintain accounts in it.

The penetration tester can login to LinkedIn and search for the devices used by the company by providing the company name, work roles, or email addresses of employees working in the target company. They focus on the network administrators while searching for individuals as their profiles generally hold key information about the target organization.

The screenshots in the below figures reveal information about the network infrastructure used by the target organization.

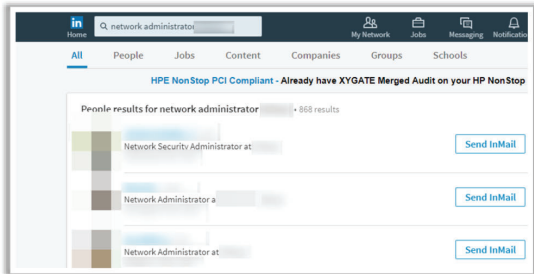


Figure 3.38: Screenshot of job listings on LinkedIn

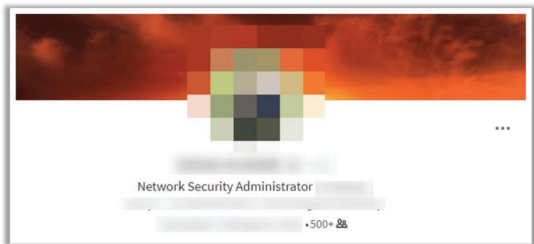


Figure 3.39: Screenshot of job profile on LinkedIn

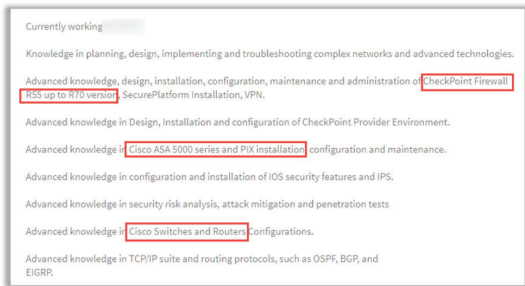


Figure 3.40: Screenshot of job description on LinkedIn

Obtaining information from job portals

Most organizations seek the assistance of online job portals to look for the desired candidates who could meet the organization's business requirements. To filter candidate profiles, recruiters provide a detailed list of required knowledge on software, platforms, and technologies in the job descriptions. Companies also list the experience required, which indicates the technology infrastructure they have.

Penetration testers can search for these job postings in major newspapers, classifieds, and job search engines to gather a company's infrastructure details. The following are some popular job portals:

- <https://www.linkedin.com>
- <https://www.monster.com>
- <https://www.careerbuilder.com>
- <https://www.dice.com>
- <https://www.indeed.com>
- <https://www.usajobs.gov>

The penetration tester looks for system administrators, database operators, and security administrators and attempt to gather information such as job requirements, employee profiles, hardware information, and software information.

For example, suppose a company posts the following job listing: "Required: system administrator with work experience in Oracle, Cisco routers, and Checkpoint firewall." This listing indicates that the company has the following infrastructure in their organization:

- Oracle database server
- Cisco routing devices
- Checkpoint firewalls

The screenshot below shows a company's job posting and job description.

Job Summary

Location
Atlanta, GA 30316

Industries
Computer Software

Job Type
• Full Time
• Employee

Education Level
Bachelor's Degree

Career Level
Manager (Manager/
Supervisor of Staff)

Salary
80,000.00 - 100,000.00 \$ /
year

Job Reference Code
2534

Sr. Network Administrator

About the Job

Responsibilities:
The Senior Network Administrator is responsible for maintaining Exchange/ Communicator, the LAN and WAN operation infrastructure while working in a team of IT Administrators & Software Developers. Such responsibilities will include: System upgrades, system documentation, daily administration and problem resolution, as well as assisting staff and users in problem resolution relating to hardware, software, and communication issues. She will participate in the design and planning of the infrastructure to support new applications, technologies and security, and thereafter play a key role in the maintenance of such tools.

Essential Administration Functions:

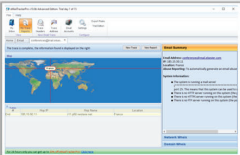
- Active Directory experience in trouble shooting – AD replication (LAN/ WAN) DNS (Replication & Resolution), DHCP & Split scopes
- Administration and complete support and upgrade of the MS-Exchange/ Lync.
- Virtualization administration (VMWare & Hyper-V), EMC & Dell SAN Administration, Cisco Firewalls & Switches Administration, Barracuda Hardware Appliances, Silver Peak Data compression devices, VOIP Phone system Administration and Video Conferencing
- Excellent understanding and ability to troubleshoot Smart Phone and active sync, Power shell commands, and patching with WSUS
- TCP/IP Routing services including but not limited to Firewalls, switches, DNS, DHCP, Microsoft Active Directory, Internet Information Services, e-mail, hardware load balancers, and Anti-Spam devices.
- LAN/Wan connectivity at corporate offices, collocation, and all customer installations.
- Site implementations – Purchase, configuration, and installation of equipment, software & services at all customer sites using project management methodologies.
- Installation of all server & desktop software including but not limited to Windows 2008/2012R2 Server, Windows 7/8.1, Exchange 2010/2013, Symantec Anti-Virus, IIS and all associated add-on tools, SQL Server, Accounting systems, and Microsoft Office and Adobe Desktop products.
- Field support of all off-site Operations and Sales equipment.

Figure 3.41: Screenshot of a job posting

Looking for Sensitive Information in Email Headers

Track email communication using email tracking tools such as **eMailTrackerPro** and perform **email header analysis** to gather sensitive information about a target recipient.

Look for information such as the recipient's system IP address, recipient's browser and operating system (OS) information, and Multipurpose Internet Mail Extensions (MIME) version.



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

Looking for Sensitive Information in Email Headers

Penetration testers can perform email tracking to monitor the emails of a particular user by using tools such as eMailTrackerPro and performing email header analysis to gather sensitive information about a target recipient. Email tracking allows testers to collect information such as IP addresses, mail servers, and service providers involved in sending the mail. An email header contains the details of the sender, routing information, date, subject, and recipient. Penetration testers look for the information such as the IP address of the recipient's system, recipient's browser and OS information, and Multipurpose Internet Mail Extensions (MIME) version.

The following information can be gathered using email tracking tools:

- **IP address of the recipient's system:** Allows tracking the recipient's IP address
- **OS and browser information:** Reveals information about the OS and browser used by the recipient
- **MIME version:** Allows finding the MIME version as well as the content type and subtype used for the body of the email message
- **Geolocation:** Estimates and displays the location of the recipient on the map and may even calculate the distance from the user's location
- **Email received and read:** Notifies when the email is received and read by the recipient
- **Read duration:** Reveals the time spent by the recipient on reading the mail
- **Proxy detection:** Provides information about the type of server used by the recipient
- **Links:** Checks whether the links sent to the recipient through the email have been clicked

- **Forward email:** Determines whether the email sent to the user is forwarded to another person
- **Device type:** Provides information about the type of device used to open and read the email such as a desktop computer, mobile device, or laptop

Tools such as eMailTrackerPro can be used to gather sensitive information in the email headers.

▪ eMailTrackerPro

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

eMailTrackerPro analyzes email headers and reveals information such as the sender's geographical location and IP address. It helps the penetration tester trace more than one IP address or domain name at a time. By using this tool, the tester can trace as many IP addresses and domain names as required and either output the results to a new tab or an Excel/HTML file.

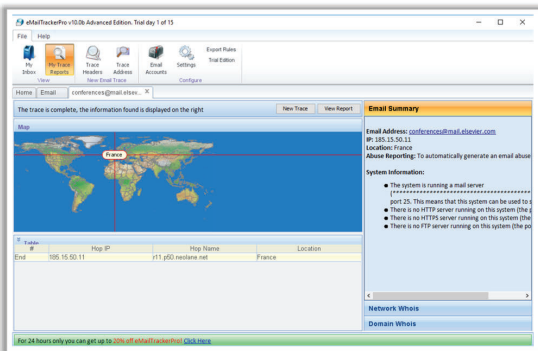


Figure 3.42: Screenshot of eMailTrackerPro



Figure 3.43: Screenshot of tracking email header

Looking for Valuable Information in NNTP Usenet Newsgroups



- The Network News Transfer Protocol (NNTP) relays **Usenet news articles** from discussions over a newsgroup.
- **Usenet newsgroups** can be good source to gather valuable information about the target.
- People seek help by posting questions and asking for solutions on Usenet newsgroups.
- Search **newsgroups** or **mailing lists** for useful information posted by anyone from the target organization.

Sample Newsgroup Posting

From: adams@certifiedhacker.com
Subject: Apache Problem
Newsgroups: comp.infosystems.www.servers.unix, comp.os.linux, alt.apache.configuration,
comp.lang.java.programmer
Date: 2016-02-27 09:19:28 PST

I am having a problem with Apache reverse proxy not communicating with web applications using
HTTP 1.1 keepalive. I am using Apache 1.3.23 on **Red Hat Linux 6.2**. It is compiled with
mod_proxy and mod_ssl.

Any ideas would be greatly appreciated.
Thank you.

adams@certifiedhacker.com
Sr. Systems Administrator
certifiedhacker.com



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

Looking for Valuable Information in NNTP Usenet Newsgroups

A penetration tester can find valuable information about the target organization by browsing Usenet newsgroups. The Network News Transfer Protocol (NNTP) relays Usenet news articles from discussions over a newsgroup. People seek help by posting questions and asking for solutions on Usenet newsgroups. Many professionals use these newsgroups to resolve their technical issues. To obtain solutions for these issues, they occasionally post more detailed information about the target than needed. Thus, the penetration tester can search the newsgroups or mailing lists for useful information posted by anyone from the target organization.

The following screenshot shows a sample newsgroup post. In this example, a system administrator named Adams has posted about a problem he is facing with Apache reverse proxy running on a Red Hat Linux 6.2 machine. By observing this post, a penetration tester can understand that the target organization is using a Red Hat Linux 6.2 machine that is running Apache web server 1.3.23. This information helps in performing web server and web application penetration testing.

A screenshot of a Usenet newsgroup posting. The text is enclosed in a rectangular box with a thin grey border. The text is as follows:

From: adams@certifiedhacker.com
Subject: Apache Problem
Newsgroups: comp.infosystems.www.servers.unix, comp.os.linux, alt.apache.configuration,
comp.lang.java.programmer
Date: 2018-02-27 09:19:28 PST

I am having a problem with Apache reverse proxy not communicating with web applications using
HTTP 1.1 keepalive. I am using Apache 1.3.23 on Red Hat Linux 6.2. It is compiled with
mod_proxy and mod_ssl.

Any ideas would be greatly appreciated.
Thank you.

adams@certifiedhacker.com
Sr. Systems Administrator
certifiedhacker.com

The phrase "not communicating" is underlined in red. The phrase "Red Hat Linux 6.2" is also underlined in red.

Figure 3.44: Screenshot of sample Usenet newsgroup posting

Other Useful Footprinting Activities to Find Information about the Target



-  Search for the company's information in online **trade association directories**.
-  Collect the company's information through **groups, forums, and blogs**.
-  Search for press releases issued by the company using Google/Yahoo Finance.
-  Search for the **link popularity** of the company's website.
-  Monitor the target using **alerts** such as Google Alerts, Yahoo Alerts, and Twitter Alerts.
-  Gather **competitive intelligence** by visiting websites such as EDGAR Database, Business Wire, LexisNexis, and Hoovers.
-  Search and list the **products/services** sold by the company.
-  Compare the **prices of products** or services with those of the competitor.

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

Other Useful Footprinting Activities to Find Information about the Target

The following are some additional footprinting activities a penetration tester can perform to obtain additional information about the target organization:

- **Search for the company's information in online trade association directories.**

The penetration tester can use online trade association directories to gather information about a company such as its name and address, a contact and their designation, phone and fax numbers, URLs and email addresses, descriptions of services and membership statistics, information on publications and newsletters, meeting and convention information, nonprofit/for-profit status, Standard Industrial Classification (SIC) code, industry category, year established, and staff size.

- **Collect the company's information through groups, forums, and blogs.**

Many Internet users take advantage of blogs, groups, and forums for knowledge-sharing purposes. Therefore, the penetration tester can focus on groups, forums, and blogs to find sensitive information about the target such as public network information, system information, and personal information on employees.

- **Search for press releases issued by the company using Google/Yahoo Finance.**

To know how a company is faring in business, the penetration tester can use finance tools from Google and Yahoo. They can also obtain more information on partners associated with the company and its global presence.

- **Search for the link popularity of the company's website.**

Many services provide information about the popularity of a certain website. These services can be utilized to obtain a complete report on how many people access the target company's website daily.

- **Monitor the target using alerts such as Google Alerts, Yahoo Alerts, and Twitter Alerts.**

Alerts are content monitoring services that provide automated up-to-date information based on user preference, usually via email or SMS. The penetration tester can obtain updated information about the target periodically from alert services.

- **Gather competitive intelligence by visiting websites such as EDGAR Database, Business Wire, LexisNexis, and Hoovers.**

Gathering competitor documents and records helps in assessing the growth of the target company. The penetration tester can obtain information such as the company's establishment date, strategies used for the development of the company, and location of the company and its branches.

- **Search and list the products/services sold by the company.**

The penetration tester can use various techniques such as visiting the company's website, requesting a product catalog, and sending an email asking for the price of a product to obtain the list of products/services sold by the company.

- **Compare the prices of products or services with those of the competitor.**

To compare the prices of products or services with those of competitors, the penetration tester must visit the website of the target organization and check the following points:

- Merchant ratings of the company
- Customer reviews
- List of products and services provided by the company

By referring to these details, the tester can track the status of the company among its customers and merchants.



OSINT through Website Analysis

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

OSINT through Website Analysis

An organization's website is the first place to obtain sensitive information such as names and contact details of the leaders of the organization, upcoming project details, and partner information. Penetration testers can perform website analysis on the target organization to obtain details such as web-page posting patterns and revision numbers, old information about the company, and web updates.

Searching for Contact Information, Email Addresses, and Telephone Numbers from the Company Website



Search for useful information on the website:



- Company contact names, phone numbers, and email addresses
- Company locations and branches
- Partner information
- News
- Links to other sites



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

Searching for Contact Information, Email Addresses, and Telephone Numbers from the Company Website

The target company's website is a good source for a penetration tester to gather crucial information on it. Generally, organizations use websites to inform the public about what they do, the type of services or products they provide, contact details, and so on. This information is helpful in performing further penetration testing.

For example, the penetration tester can search for the following information on the company's website:

- Company contact names, phone numbers, and email addresses
- Company locations and branches
- Partner information
- News
- Links to other sites
- Product, project, or service data

Searching for Web-page Posting Patterns and Revision Numbers



- Search for **copyright notices** on the web.



- Search and note down the **revision number** of a product.



- Search the **document numbers** assigned to documents after revision.



- Examples: **Document Version1a** and **Version45.3c**.



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

Searching for Web-page Posting Patterns and Revision Numbers

Copyright is a protecting entity provided by the law of a country that grants the creator of an original work exclusive rights for its use and distribution. To restrict third parties from accessing their data freely, most organizations ensure that there is a copyright notice on every piece of their published work.

A typical copyright notice contains the following information:

- Copyright symbol
- Year of the creation
- Author name
- Rights statement

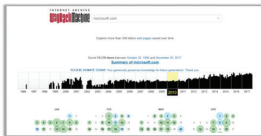
A penetration tester can search for copyright notices on the web and use these details to perform deep analysis on the target organization.

The penetration tester should search for and note down the revision number of a product. The revision number is a unique string that acts as an identifier for the revision of a given document. The revision number can be within the documents of the company. Document numbers that are assigned to the documents after revision can be found from the Internet and recorded for future assessment. Examples of document numbers are Document Version1a and Version45.3c.

Searching Archive.org for Old Information about the Company



- Search backdated webpages in the <https://www.archive.org> Wayback Machine.
- Record the changes from different time periods.
- New products, press releases, mistakes, and contact information can be found in the Internet archive.



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

Searching Archive.org for Old Information about the Company

Internet archives may also provide sensitive information that has been removed from the WWW. The website <https://www.archive.org> is an Internet Archive Wayback Machine that helps penetration testers retrieve archived versions of the target website. As the working environment and business requirements change, the organizations update their websites to provide clear information about them. When the organizations update their websites, the old information is no longer available on the Internet and becomes inaccessible to the penetration tester. Therefore, to retrieve such old information about the target organization, the tester can use online tools such as Archive.org that provide older versions of target websites. By using these tools, the tester can also search for backdated web pages and record the changes from different time periods. These Internet archives help in gathering information such as new products, press releases, mistakes, and contact information.

The following screenshots show the summary and details of archived versions of a target organization.

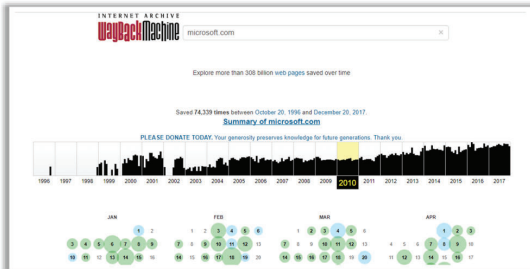


Figure 3.45: Screenshot of Archive.org showing a summary of the target website



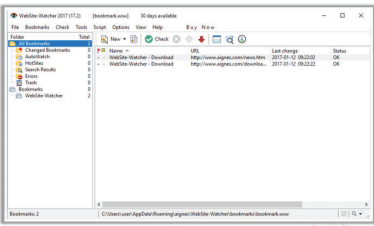
Figure 3.46: Screenshot of Archive.org showing an archived web page of the target website

Monitoring Web Updates using WebSite-Watcher

WebSite-Watcher automatically checks web pages for updates and changes.

It allows monitoring new pages, postings, RSS feeds, and newsgroups.





Folder	Name	URL	Last change	Status
Changed Bookmarks	0			
Autobatch	0			
AutoGlas	0			
Search Results	0			
Tools	0			
Errors	0			
Bookmarks	0			
WebSite-Watcher	2			

Source: <http://lognes.com>

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

Monitoring Web Updates using WebSite-Watcher

Penetration testers can use web update-monitoring tools to detect any changes or updates in a website. These tools not only monitor web updates but also notify or send alerts to the penetration testers through email or SMS. There are various web update-monitoring tools such as WebSite-Watcher to track and monitor web updates.

■ WebSite-Watcher

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

WebSite-Watcher helps track websites for updates and automatic changes. When an update or change occurs, WebSite-Watcher automatically detects and saves the last two versions onto the user's local drive. It also highlights changes in text. It is a useful tool for monitoring sites to gain a competitive advantage.

Features

- WebSite-Watcher can automatically detect and notify users about updates, making frequent manual checking of updates unnecessary.
- It monitors web pages, password-protected pages, forums for new postings and replies, RSS feeds, newsgroups, and local files.
- It allows the user to know what their competitors are doing by scanning their websites.
- The site can keep track of new software versions or driver updates.
- It stores images of the modified websites to a local drive.

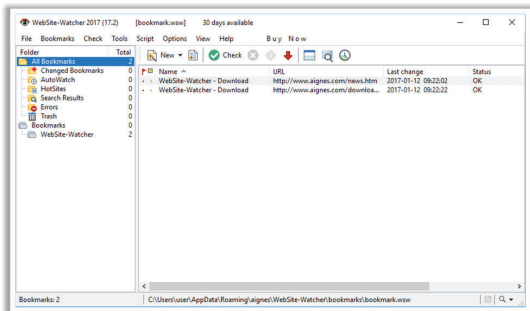
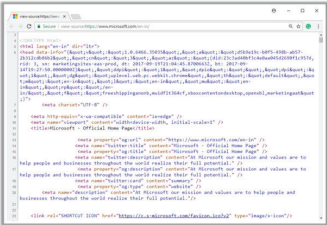


Figure 3.47: Screenshot of WebSite-Watcher

Examining the HTML Source of Web Pages



- Look for **sensitive information** in comments.
- This may yield information about back-end technologies, external links, file system structure, script type, etc.



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

Examining the HTML Source of Web Pages

HTML source code includes sensitive information in the form of comments and metadata such as usernames, passwords, structured query language (SQL) code, internal IP addresses, debugging information, back-end technologies, external links, file system structure, script type, improper server configurations, and page responses for valid versus invalid data. The HTML source code of a web page can be examined to find the inherent threats in it. This will help in escalating the chain of attacks to the target website.

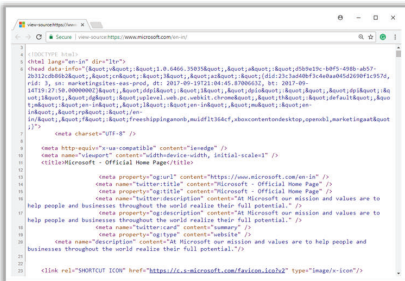


Figure 3.48: Example of the HTML source code of a web page



OSINT through DNS Interrogation

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

OSINT through DNS Interrogation

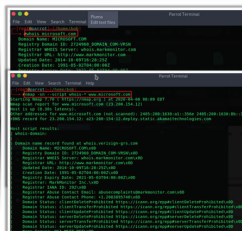
DNS interrogation is the process of collecting information about the DNS servers and the corresponding DNS records of a target organization. An organization may contain multiple internal and external DNS servers that can provide information such as domain names, contact information, domain owner details, usernames, computer names, and IP addresses. Penetration testers can use various automated tools such as Whois, nslookup, dnsrecon, and dnsenum to perform DNS interrogation.

Performing Whois Lookups



- Whois databases are maintained by **regional Internet registries (RIRs)** and contain personal information about **domain owners**.
- The Whois tool sends a query to the **Whois databases** and obtains personal details.
- The **Whois query returns** the following:
 - Domain name details
 - Contact details of the domain owner
 - Domain name servers
 - IP address and NetRange
 - Domain creation date and expiry records
 - Physical location
 - Telephone number and email address
 - Technical and administrative contacts

RIRs:



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

Performing Whois Lookups (Cont'd)



Whois Lookup using Perl Script

```
#!/usr/bin/perl -w
use strict;
use Net::Whois::Raw;
die "Usage: perl netRange.pl <IP Address>" unless
$ARGV[0];
foreach(split(/\n/,whois(shift))) {
    print $_,"\n" if(m/^(netrange|orgname)/i);
}
```

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

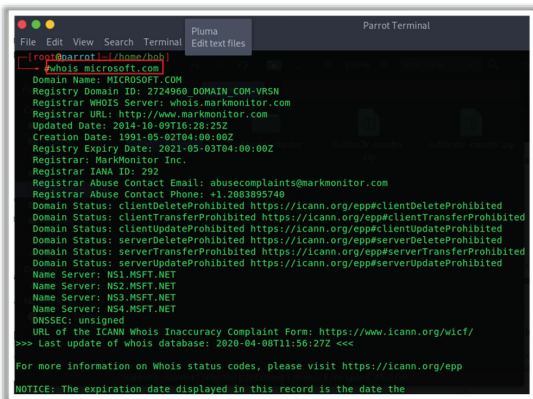
Performing Whois Lookups

Penetration testers can perform Whois lookups using Whois query and the response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. Whois databases are maintained by regional Internet registries (RIRs) and contain personal information about domain owners.

Whois tools can be used to send a query to the Whois database servers to obtain personal details such as the following:

- Domain name details
- Contact details of the domain owner
- Domain name servers
- IP address and NetRange
- Domain creation date and expiry records
- Physical location
- Telephone number and email address
- Technical and administrative contacts

After obtaining the above details, the penetration tester can create a map of the target organization's network, mislead domain owners with social engineering, and then obtain internal details of the network. The screenshot below shows how to perform a Whois lookup on a target.

A screenshot of a terminal window titled "Parrot Terminal". The terminal shows a command prompt where the user has entered "whois microsoft.com". The output displays detailed domain information for MICROSOFT.COM, including registry details, registrar information, creation and expiry dates, and domain status codes. The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", "Pluma", and "Edit text files". The user's prompt is "[root@parrot:~]#".

```
[root@parrot:~]# whois microsoft.com
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2014-10-09T16:28:25Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.MSFT.NET
Name Server: NS2.MSFT.NET
Name Server: NS3.MSFT.NET
Name Server: NS4.MSFT.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-04-08T11:56:27Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

Figure 3.49: Screenshot of a Whois lookup

The penetration tester can use tools such as Whois and Nmap to perform Whois lookups on the target network.

▪ Nmap

Source: <https://nmap.org>

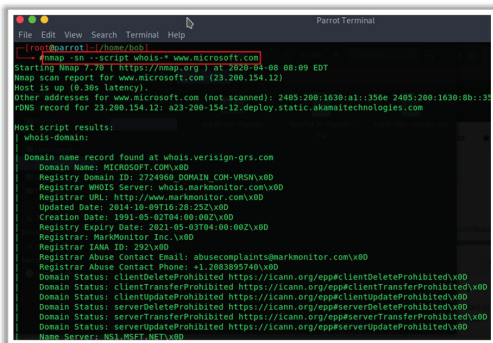
By using Nmap Whois NSE scripts, the tester can perform Whois lookups to obtain information such as the domain name of the target, Whois services, and target IP address. The following are some Whois NSE scripts:

○ whois-domain

Attempts to retrieve information about the domain name of the target

○ whois-ip

Queries the Whois services of RIRs and attempts to retrieve information about the IP address assignment that contains the target IP address



```

[root@parrot:~/home/bob]
→ nmap -sn --script whois-* www.microsoft.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-08 08:09 EDT
Nmap scan report for www.microsoft.com (23.200.154.12)
Host is up (0.36s latency).
Other addresses for www.microsoft.com (not scanned): 2405:200:1630:a1::356e 2405:200:1630:8b::35
rDNS record for 23.200.154.12: a23-200-154-12.deploy.static.akamaitechnologies.com

Host script results:
| whois-domain:
|
| Domain name record found at whois.verisign-grs.com
| Domain Name: MICROSOFT.COM\x00
| Registry Domain ID: 2724960_DOMAIN_COM-VRSN\x00
| Registrar WHOIS Server: whois.markmonitor.com\x00
| Registrar URL: http://www.markmonitor.com\x00
| Updated Date: 2014-10-09T16:28:25Z\x00
| Creation Date: 1991-05-02T04:00:00Z\x00
| Registry Expiry Date: 2021-05-03T04:00:00Z\x00
| Registrar: MarkMonitor Inc.\x00
| Registrar IANA ID: 292\x00
| Registrar Abuse Contact Email: abusecomplaints@markmonitor.com\x00
| Registrar Abuse Contact Phone: +1.2083895740\x00
| Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited\x00
| Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited\x00
| Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited\x00
| Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited\x00
| Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited\x00
| Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited\x00
| Name Server: NS1.MSFT.NET\x00

```

Figure 3.50: Screenshot of a Whois lookup using Nmap

Regional Internet Registries

The following are some important RIRs.

▪ American Registry for Internet Numbers (ARIN)

Source: <https://www.arin.net>

ARIN provides services related to the technical coordination and management of Internet number resources. ARIN offers its services in three areas:

- Registration—pertains to the technical coordination and management of Internet number resources

- Organization—pertains to the interaction of ARIN members and stakeholders with ARIN
- Policy development—facilitates the development of policy for the technical coordination and management of Internet number resources in the ARIN region

ARIN also develops technical services to support the evolving needs of the Internet community.

- **African Network Information Center (AFRINIC)**

Source: <https://www.afrinic.net>

AFRINIC is the RIR for Africa and is responsible for the distribution and management of Internet number resources such as IP addresses and autonomous system numbers (ASNs) for the African region.

- **Réseaux IP Européens Network Coordination Centre (RIPE NCC)**

Source: <https://www.ripe.net>

RIPE NCC provides Internet resource allocations, registration services, and coordination activities that support the operation of the Internet globally.

- **Asia Pacific Network Information Center (APNIC)**

Source: <https://www.apnic.net>

APNIC is one of five RIRs charged with ensuring the fair distribution and responsible management of IP addresses and related resources required for the stable and reliable operation of the global Internet.

- **Latin American and Caribbean Network Information Center (LACNIC)**

Source: <https://www.lacnic.net>

LACNIC is an international nongovernmental organization responsible for assigning and administering Internet numbering resources (IPv4 and IPv6), ASN, reverse resolution, and other resources for the Latin American and Caribbean regions.

Whois Lookup using Perl Script

Whois searches can be automated using Perl or Common Gateway Interface (CGI) scripts. One can perform standard searches, multi searches, and name searches using such scripts.

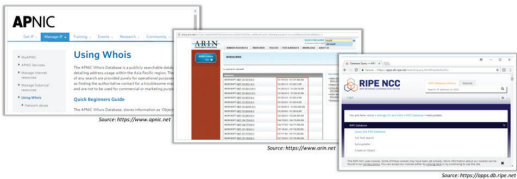
The following is a sample Perl script to perform a Whois search:

```
#!/usr/bin/perl -w
use strict;
use Net::Whois::Raw;
die "Usage: perl netRange.pl <IP Address>" unless $ARGV[0];
foreach(split(/\n/,whois(shift))) {
    print $_,"\n" if(m/^(netrange|orgname)/i);
}
```

Finding the IP Address Block Allocated to the Organization



- When an organization does not provide their IP range, it must be determined using **IP registries**.
- IP registries help in **finding the IP range** belonging to the target organization.

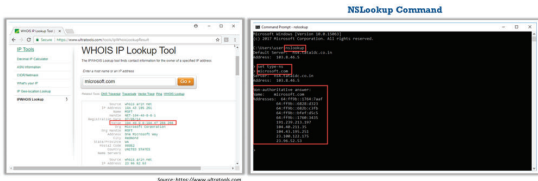


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding the IP Address Block Allocated to the Organization (Cont'd)



- Alternatively, any **Whois database** available online or offline can be used to retrieve the IP range.
- The following Whois tool can help in **retrieving the IP range** of the target organization.



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

Finding the IP Address Block Allocated to the Organization

When an organization does not provide a penetration tester their IP range, the tester needs to find it using IP registries (RIRs), which generally control the assignment and distribution of IP addresses. IP registries help in finding the IP range belonging to the target organization. By obtaining the IP range, the tester can retrieve more information about the target such as the structure of the network, live hosts in the network, network topology, access-control devices, and OSes used. To find the network range of the target, the penetration tester needs to enter

the server IP address gathered in the previous step by using a Whois database search tool. The following are some Whois database tools provided by IP registries.

- **APNIC Whois Search**

Source: <https://www.apnic.net>

The APNIC Whois Database is a publicly searchable database detailing address usage within the Asia Pacific region. The APNIC Whois Database stores information as “Objects.” Objects can contain the following information:

- IP address ranges
- Routing policies
- Reverse DNS delegations
- Network contact information



Figure 3.51: Screenshot of APNIC Whois search

- **ARIN Whois-RWS**

Source: <http://whois.arin.net>

ARIN’s Whois RESTful Web Service (Whois-RWS) is a new directory service for accessing registration data contained within ARIN’s registration database. Whois-RWS can be integrated into command line scripts similar to Whois or RWhois, or it can be accessed with a web browser.

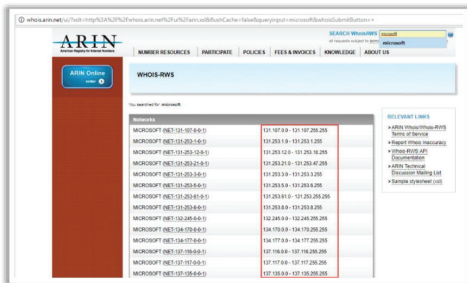


Figure 3.52: Screenshot of ARIN Whois-RWS

■ RIPE Database (Whois)

Source: <https://apps.db.ripe.net>

RIPE's Database Whois service shows full object details that include contact and registration information for IP addresses, ASNs, organizations or customers associated with these resources, and related points of contact. It also performs inverse lookup.

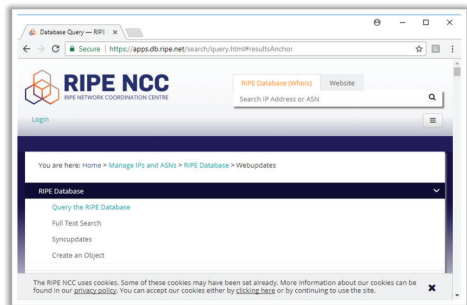


Figure 3.53: Screenshot of RIPE database (Whois)

One can also use any Whois database available online or offline to retrieve the IP range. The following lookup tools can help in retrieving the IP range of the target organization.

- **Whois IP Lookup Tool**

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

The IP Whois Lookup tool displays as much information as possible for a given IP address, and the information is sourced from the RIR to which the address belongs. It finds contact information for the owner of a specified IP address.

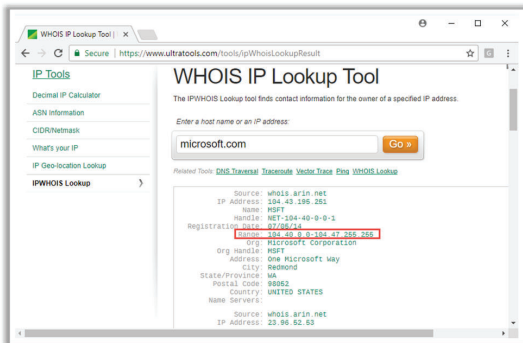


Figure 3.54: Screenshot of Whois ip lookup tool

- **Nslookup**

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

Nslookup is a useful tool for troubleshooting DNS problems such as hostname resolution. On startup, Nslookup shows the hostname and IP address of the DNS server that is configured for the local system, as shown in the below figure.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>nslookup
Default Server: ns4.cataidc.co.in
Address: 103.8.46.5

> set type=ns
> microsoft.com
Server: ns4.cataidc.co.in
Address: 103.8.46.5

Non-authoritative answer:
Name: microsoft.com
Addresses: 64:ff9b::1764:7aaf
          64:ff9b::6828:d323
          64:ff9b::682b:c3fb
          64:ff9b::bfef:d5c5
          64:ff9b::1760:3435
          191.239.213.197
          104.40.211.35
          104.43.195.251
          23.100.122.175
          23.96.52.53
```

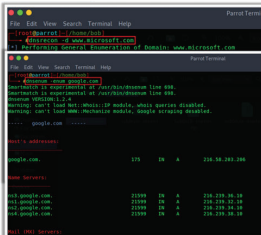
Figure 3.55: Screenshot of Nslookup

Finding the DNS Records for the Domain



DNS records provide important information about the location and type of servers

- **A** - Points to a host's IP address
- **MX** - Points to a domain's mail server
- **NS** - Points to a host's name server
- **CNAME** - Canonical naming that allows aliases for a host
- **SOA** - Indicates authority for a domain
- **SRV** - Service records
- **PTR** - Maps an IP address to a hostname
- **RP** - Responsible person
- **HINFO** - Host information record including the CPU type and OS
- **TXT** - Unstructured text records

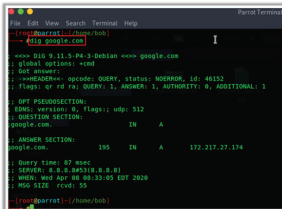


Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

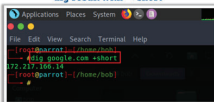
Finding the DNS Records for the Domain (Cont'd)



DNS interrogation with the dig command



Obtaining only IP addresses from the dig result with "+short"



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

Finding the DNS Records for the Domain (Cont'd)



Obtaining a dig result with specific records

```

Fig. 5-61 View Search Terminal Help
[robert@root:~]$ dig google.com -t SOA

; <<<< Dig 9.11.5-P4-3-Debian <<<< google.com -t SOA
; global options: <none>
; got answer?
; >>>>HEADER<<<< opcode: QUERY, status: NOERROR, id: 50628
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
; OPT PSEUDOSECTION:
; DNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; google.com.                IN      SOA
; ANSWER SECTION:
; google.com.                28      IN      SOA      ns1.google.com.
;                               <<<<
; Query time: 115 msec
; SERVER: 9.9.9.955(9.9.9.9)
; WHEN: Wed Apr 08 06:39:06 EDT 2020
; MSG SIZE: 774rd 00

Fig. 5-62 View Search Terminal Help
[robert@root:~]$ dig google.com -t AAAA

; <<<< Dig 9.11.5-P4-3-Debian <<<< google.com -t AAAA
; global options: <none>
; got answer?
; >>>>HEADER<<<< opcode: QUERY, status: NOERROR, id: 26108
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; DNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; google.com.                IN      AAAA
; ANSWER SECTION:
; google.com.                239     IN      AAAA      2001:690:4002:800::2000
;                               <<<<
; Query time: 79 msec
; SERVER: 9.9.9.955(9.9.9.9)
; WHEN: Wed Apr 08 06:43:02 EDT 2020
; MSG SIZE: 774rd 00

Fig. 5-63 View Search Terminal Help
[robert@root:~]$ dig google.com -t MX

; <<<< Dig 9.11.5-P4-3-Debian <<<< google.com -t MX
; global options: <none>
; got answer?
; >>>>HEADER<<<< opcode: QUERY, status: NOERROR, id: 26108
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; DNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; google.com.                IN      MX
; ANSWER SECTION:
; google.com.                239     IN      MX      10 smtp.google.com.
;                               <<<<
; Query time: 79 msec
; SERVER: 9.9.9.955(9.9.9.9)
; WHEN: Wed Apr 08 06:43:02 EDT 2020
; MSG SIZE: 774rd 00
  
```

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

Finding the DNS Records for the Domain (Cont'd)



Dig using a Perl script

```

#!/usr/bin/perl -w
use Net::DNS::Dig;
use strict;

my $dig = new Net::DNS::Dig();
my $dom = shift or die "Usage: perl dig.pl <domain>";
my $obj = $dig->for($dom, 'A');
#print $obj->sprintf;
# print entire dig query response
print "CODE: ", $obj->rcode(1), "\n";
# Dig Response Code
my $mx = Net::DNS::Dig->new()->for($dom, 'MX')->data();
while(my($val,$server) = each(%$mx)){
    print "MX: ", $server, " - ", $val, "\n";
}
  
```

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

Finding the DNS Records for the Domain (Cont'd)



Obtaining a name server from a Whois lookup result

```
File Edit View Search Terminal Help
[ro@barrot:~]$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2133014 DOMAIN COM-VEN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: https://www.markmonitor.com
Updated Date: 2020-09-09T15:30:04Z
Creation Date: 1997-09-25T04:00:00Z
Registry Expiry Date: 2028-09-10T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar SARA ID: 202
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1 2083805449
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp/clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp/serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp/serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp/serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/whois-form
Last update of whois database: 2020-04-08T12:45:07Z
For more information on Whois status codes, please visit https://icann.org/epp
```

```
File Edit View Search Terminal Help
[ro@barrot:~]$ cat rr |grep Name
Domain Name: GOOGLE.COM
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

```
File Edit View Search Terminal Help
[ro@barrot:~]$ cat rr |grep Name |grep -v Domain
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

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

Finding the DNS Records for the Domain (Cont'd)



DNS Lookup Tool

The UltraTool DNS Lookup provides a report on DNS records for a specified domain or hostname.

This UltraTool DNS tool performs an authoritative DNS lookup and provides details about common resource record types for root server, TLD server and nameserver information.

Enter a host name or domain name

microsoft.com

GO

Answer: Trace

microsoft.com results:

ns4.msft.net.

Type	Address	TTL
A	193.239.252.107	3600
NS	194.43.204.36	3600
NS	194.43.204.263	3600
NS	23.100.122.175	3600
NS	23.100.122.53	3600

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

Domain DNS Lookup for: microsoft.com

Live DNS lookup results

A records

TYPE	ADDRESS	TTL	MORE INFO
A	104.43.195.251	641	IP1 Traceroute (100s)
A	23.100.122.175	641	IP1 Traceroute (100s)
A	23.96.52.53	641	IP1 Traceroute (100s)
A	191.239.213.197	641	IP1 Traceroute (100s)
A	104.40.211.35	641	IP1 Traceroute (100s)

Source: <https://dig.whois.com.au>

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

Finding the DNS Records for the Domain

A penetration tester must retrieve DNS records for the target domain. DNS records reveal information such as domain names, computer names, and IP addresses about a particular network. DNS information can be used to determine key hosts in the network, their locations, and the types of servers present in the target network.

The following table lists the DNS records that can be determined by gathering DNS information.

Record Type	Description
A	Points to a host's IP address
MX	Points to a domain's mail server
NS	Points to a host's name server
CNAME	Canonical naming that allows aliases for a host
SOA	Indicates authority for a domain
SRV	Service records
PTR	Maps an IP address to a hostname
RP	Responsible person
HINFO	Host information record including the CPU type and OS
TXT	Unstructured text records

Table 3.4: List of DNS records

The following are tools that can be used to retrieve information about DNS records.

- **dnsrecon**

Source: <https://github.com>

dnsrecon is a powerful DNS enumeration script that provides the ability to do the following:

- Check all NS records for zone transfers.
- Enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT).
- Perform common SRV record enumeration and top-level domain (TLD) expansion.
- Check for wildcard resolution.
- Brute-force the subdomain and host A and AAAA records.
- Perform a PTR record lookup for a given IP range or CIDR.
- Check DNS server cached records for A, AAAA, and CNAME records, provided a list of host records in a text file to check.
- Enumerate common DNS records in the local network.

```

[ root@parrot ] ~/home/bob
# dnsrecon -d www.microsoft.com
[*] Performing General Enumeration of Domain: www.microsoft.com
[-] DNSSEC is not configured for www.microsoft.com
[*] SOA n0dsdpb.akamaiedge.net 88.221.81.192
[-] Could not Resolve NS Records for www.microsoft.com
[-] Could not Resolve MX Records for www.microsoft.com
[*] CNAME www.microsoft.com www.microsoft.com-c-3.edgekey.net
[*] CNAME www.microsoft.com-c-3.edgekey.net www.microsoft.com-c-3.
[*] CNAME www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
[*] A e13678.dspb.akamaiedge.net 23.199.74.12
[*] CNAME www.microsoft.com www.microsoft.com-c-3.edgekey.net
[*] CNAME www.microsoft.com-c-3.edgekey.net www.microsoft.com-c-3.
[*] CNAME www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
[*] AAAA e13678.dspb.akamaiedge.net 2405:200:1630:a1::356e
[*] AAAA e13678.dspb.akamaiedge.net 2405:200:1630:8e::356e
[*] Enumerating SRV Records
[-] No SRV Records Found for www.microsoft.com
[+] 0 Records Found
[ root@parrot ] ~/home/bob

```

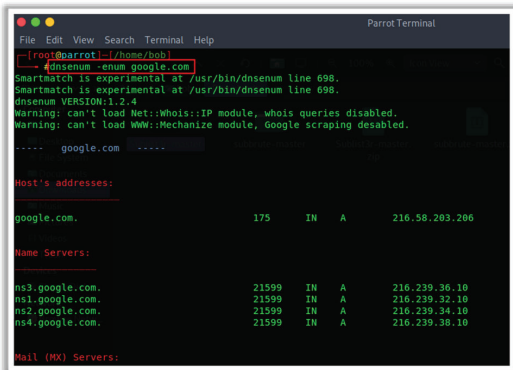
Figure 3.56: Screenshot of dnsrecon

▪ dnsenum

Source: <https://github.com>

dnsenum is a Perl script that enumerates the DNS information of a domain to discover noncontiguous IP blocks. This tool performs the following operations:

- Obtain the host's address (A record).
- Obtain the name servers (threaded).
- Obtain the MX record (threaded).
- Perform axfr queries on name servers and obtain BIND VERSION (threaded).
- Obtain extra names and subdomains via Google scraping (Google query = "allinurl: -www site:domain").
- Brute-force subdomains from a file can also perform recursion on a subdomain that has NS records (all threaded).
- Calculate C class domain network ranges and perform Whois queries on them (threaded).
- Perform reverse lookups on net ranges (C class or/and Whois net ranges) (threaded).
- Write to domain_ips.txt file ip-blocks.



```
File Edit View Search Terminal Help
[root@parrot:~/home/bob]
#dnsenum -enum google.com
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4
Warning: can't load Net::Whois::IP module, whois queries disabled.
Warning: can't load WWW::Mechanize module, Google scraping disabled.

----- google.com -----
Host's addresses:

google.com.                175      IN      A       216.58.203.206

Name Servers:

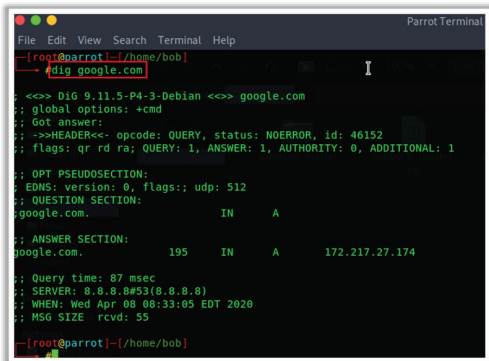
ns3.google.com.            21599    IN      A       216.239.36.10
ns1.google.com.            21599    IN      A       216.239.32.10
ns2.google.com.            21599    IN      A       216.239.34.10
ns4.google.com.            21599    IN      A       216.239.38.10

Mail (MX) Servers:
```

Figure 3.57: Screenshot of dnsenum

- **dig command**

The dig command can be used to query DNS name servers to retrieve information about the target host addresses, name servers, mail exchanges, and so on. The following figures illustrate how to perform DNS interrogation with the dig command and obtain information such as IP addresses, specific DNS records, and name servers.



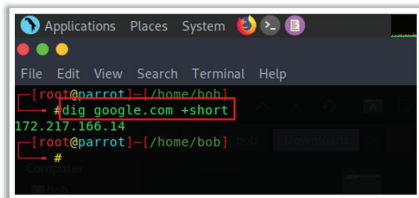
```
[root@parrot]~/home/bob
#dig google.com

<<>> DiG 9.11.5-P4-3-Debian <<>> google.com
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46152
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; QUESTION SECTION:
; google.com.                IN      A
;
; ANSWER SECTION:
; google.com.                195     IN      A      172.217.27.174
;
; Query time: 87 msec
; SERVER: 8.8.8.8#53(8.8.8.8)
; WHEN: Wed Apr 08 08:33:05 EDT 2020
; MSG SIZE rcvd: 55

[root@parrot]~/home/bob
```

Figure 3.58: Screenshot of DNS interrogation with dig



```
[root@parrot]~/home/bob
#dig google.com +short
172.217.166.14
[root@parrot]~/home/bob
```

Figure 3.59: Screenshot of obtaining only IP addresses from the dig result with "+short"

```

root@parrot: ~/home/bob
#dig google.com -t SOA

<<>> DiG 9.11.5-P4-3-Debian <<>> google.com -t SOA
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 50920
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;google.com.                IN      SOA
;; ANSWER SECTION:
google.com.                28      IN      SOA      ns1.google.com. dns-admin.google.com. 305219598 900 900 1000 60

;; Query time: 1150 msec
;; SERVER: 8.8.8.0#53(8.8.8.8)
;; WHEN: Wed Apr 08 08:39:06 EDT 2020
;; MSG SIZE rcvd: 89
  
```

Figure 3.60: Screenshot of obtaining a dig result with SOA records

```

root@parrot: ~/home/bob
#dig google.com -t mx

<<>> DiG 9.11.5-P4-3-Debian <<>> google.com -t mx
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 28319
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;google.com.                IN      MX
;; ANSWER SECTION:
google.com.                270     IN      MX      50 alt4.aspmx.l.google.com.
google.com.                270     IN      MX      40 alt3.aspmx.l.google.com.
google.com.                270     IN      MX      30 alt2.aspmx.l.google.com.
google.com.                270     IN      MX      20 alt1.aspmx.l.google.com.
google.com.                270     IN      MX      10 aspmx.l.google.com.

;; Query time: 111 msec
;; SERVER: 8.8.8.0#53(8.8.8.8)
;; WHEN: Wed Apr 08 08:40:36 EDT 2020
;; MSG SIZE rcvd: 147

root@parrot: ~/home/bob
  
```

Figure 3.61: Screenshot of obtaining a dig result with MX records

```

[ root@parrot ] - [ /home/bob ]
# dig google.com -t AAAA

; <<>> DiG 9.11.5-P4-3-Debian <<>> google.com -t AAAA
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 36108
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                IN      AAAA

;; ANSWER SECTION:
google.com.                259     IN      AAAA    2404:6800:4002:806::200e

;; Query time: 76 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Apr 08 08:43:02 EDT 2020
;; MSG SIZE rcvd: 67

[ root@parrot ] - [ /home/bob ]

```

Figure 3.62: Screenshot of obtaining a dig result with AAAA records

- **dig using a Perl script:** The following Perl script executes the dig command to query DNS name servers to retrieve information about the target host addresses, name servers, and mail exchanges:

```

#!/usr/bin/perl -w
use Net::DNS::Dig;
use strict;

my $dig = new Net::DNS::Dig();
my $dom = shift or die "Usage: perl dig.pl <domain>";
my $dobj = $dig->for($dom, 'A');
#print $dobj->sprintf;

# print entire dig query response
print "CODE: ", $dobj->rcode(1), "\n";

# Dig Response Code
my $mx = Net::DNS::Dig->new()->for($dom, 'MX')->rdata();
while(my($val,$server) = each(%mx)){
    print "MX: ", $server, " - ", $val, "\n";
}

```

Whois in Parrot OS

The Whois lookup tool can be used in Parrot OS to retrieve information about the target's name servers. The following figure illustrates the retrieval of all the information related to the target domain.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~/home/bob
#whois google.com > rr
[root@parrot] ~/home/bob
#cat rr
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514 DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-04-08T12:45:07Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
  
```

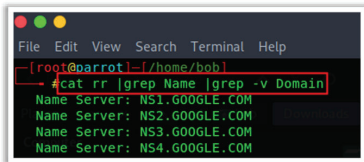
Figure 3.63: Screenshot of Whois in Parrot

The following figures show the retrieval of only the name server information from the output of a Whois lookup using the cat command.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~/home/bob
#cat rr | grep Name
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
  
```

Figure 3.64: Screenshot of obtaining the name server from the Whois result



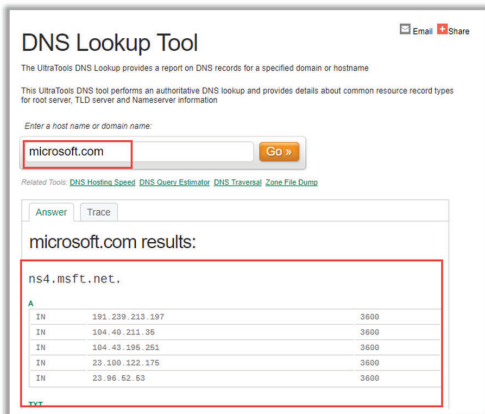
```
File Edit View Search Terminal Help
[root@parrot:~/home/bob]
#cat rr |grep Name |grep -v Domain
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

Figure 3.65: Screenshot of an alternate command to obtain the name server from the Whois result

- **UltraTools DNS Lookup Tool**

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

UltraTools DNS Lookup provides a report on DNS records for a specified domain or hostname. This tool performs a comprehensive DNS lookup and provides details about common resource record types for root server, TLD server, and name server information.



DNS Lookup Tool

The UltraTools DNS Lookup provides a report on DNS records for a specified domain or hostname

This UltraTools DNS tool performs an authoritative DNS lookup and provides details about common resource record types for root server, TLD server and Nameserver information

Enter a host name or domain name:

Related Tools: [DNS Hosting Speed](#) [DNS Query Estimator](#) [DNS Traversal](#) [Zone File Dump](#)

microsoft.com results:

ns4.msft.net.

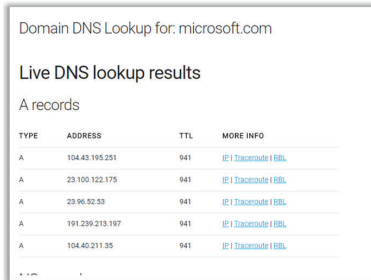
A	IN	191.239.213.197	3600
	IN	104.40.211.35	3600
	IN	104.43.196.251	3600
	IN	23.100.122.175	3600
	IN	23.96.52.53	3600

Figure 3.66: Screenshot of the UltraTools DNS Lookup Tool

- **DNS Lookup**

Source: <https://www.whois.com.au>

DNS Lookup is a browser-based network tool that displays publicly available DNS records for the domain name being queried. DNS records queried include A, AAAA, CNAME, MX, NS, SOA, and TXT.



The screenshot shows a web interface for a DNS lookup tool. At the top, it says 'Domain DNS Lookup for: microsoft.com'. Below that is the heading 'Live DNS lookup results' and a sub-heading 'A records'. A table displays five A records for the domain. Each row includes the record type (A), the IP address, the TTL (941), and a 'MORE INFO' link with sub-links for IP, Traceroute, and BBL.

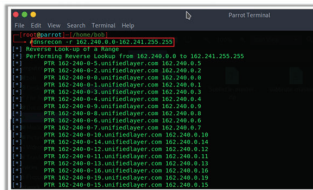
TYPE	ADDRESS	TTL	MORE INFO
A	104.43.195.251	941	IP Traceroute BBL
A	23.100.122.175	941	IP Traceroute BBL
A	23.96.52.53	941	IP Traceroute BBL
A	191.239.213.197	941	IP Traceroute BBL
A	104.40.211.35	941	IP Traceroute BBL

Figure 3.67: Screenshot of DNS lookup

Performing Reverse Lookups



- Perform reverse DNS lookups on the target's IP range to locate a **DNS PTR record** for those IP addresses.

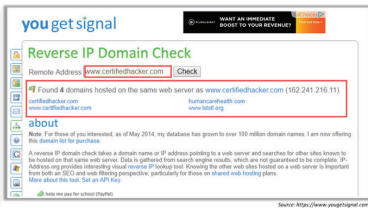


Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Performing Reverse Lookups (Cont'd)



- Find the other domains that share the same **web server**.
- Use a reverse IP domain check utility such as **YouGetSignal** to list the possible domains that are hosted on the same server.

Source: Atlas Obscura, www.atlasobscura.com

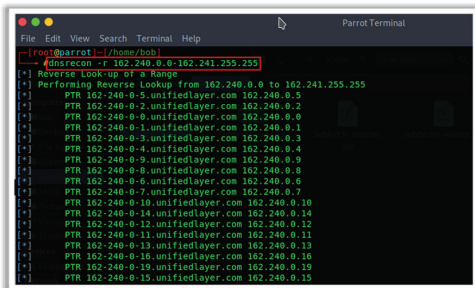
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Performing Reverse Lookups

While a DNS lookup is used for finding the IP addresses for a given domain name, and a reverse DNS lookup is performed to obtain the domain name of a given IP address. When a user types a domain name in browser to look for a domain, the DNS converts that domain name into an IP address and forwards the request for further processing. This conversion of a domain name to an IP address is performed by an A record. Reverse DNS lookup can be performed on an IP range to locate a DNS PTR record for those IP addresses.

When an IP address or a range of IP addresses is available, penetration testers can perform reverse DNS lookups to obtain the corresponding domain name. Tools such as `dnsrecon` and Reverse IP Domain Check can be used for performing reverse DNS lookups on the target host.

- **dnsrecon**



```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot ~]# dnsrecon -r 162.240.0.0-162.241.255.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.240.0.0 to 162.241.255.255
[*] PTR 162-240-0-5.unifiedlayer.com 162.240.0.5
[*] PTR 162-240-0-2.unifiedlayer.com 162.240.0.2
[*] PTR 162-240-0-0.unifiedlayer.com 162.240.0.0
[*] PTR 162-240-0-1.unifiedlayer.com 162.240.0.1
[*] PTR 162-240-0-3.unifiedlayer.com 162.240.0.3
[*] PTR 162-240-0-4.unifiedlayer.com 162.240.0.4
[*] PTR 162-240-0-9.unifiedlayer.com 162.240.0.9
[*] PTR 162-240-0-8.unifiedlayer.com 162.240.0.8
[*] PTR 162-240-0-6.unifiedlayer.com 162.240.0.6
[*] PTR 162-240-0-7.unifiedlayer.com 162.240.0.7
[*] PTR 162-240-0-10.unifiedlayer.com 162.240.0.10
[*] PTR 162-240-0-14.unifiedlayer.com 162.240.0.14
[*] PTR 162-240-0-12.unifiedlayer.com 162.240.0.12
[*] PTR 162-240-0-11.unifiedlayer.com 162.240.0.11
[*] PTR 162-240-0-13.unifiedlayer.com 162.240.0.13
[*] PTR 162-240-0-16.unifiedlayer.com 162.240.0.16
[*] PTR 162-240-0-19.unifiedlayer.com 162.240.0.19
[*] PTR 162-240-0-15.unifiedlayer.com 162.240.0.15
  
```

Figure 3.68: Screenshot of DNS lookup using `dnsrecon`

One can find other domains that share the same web server using tools such as Reverse IP Domain Check. These tools list out the possible domains that are hosted on the same web server.

- **Reverse IP Domain Check**

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

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server.

The screenshot shows the 'you get signal' Reverse IP Domain Check tool. At the top, there is a navigation bar with the logo 'you get signal' and a banner for 'PLAYREVIEW' that says 'WANT AN IMMEDIATE BOOST TO YOUR REVENUE?'. Below the banner, the main heading is 'Reverse IP Domain Check'. A form field labeled 'Remote Address' contains the text 'www.certifiedhacker.com' and a 'Check' button. Below the form, a message states: 'Found 4 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11)'. A red box highlights the following domains: certifiedhacker.com, www.certifiedhacker.com, humancarehealth.com, and www.lstsl.org. Below this, there is an 'about' section with a note about the database's growth and a description of the tool's functionality. At the bottom, there is a 'help me pay for school (PayPal)' button.

Figure 3.69: Screenshot of a reverse IP domain check

Performing DNS Zone Transfer



- If the DNS server allows **zone transfers**, then use this technique to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.
- Perform DNS zone transfer using tools such as **nslookup**, **dig**, and **dnsrecon**. If the DNS zone transfer setting is enabled on the target name server, it will give the **DNS information**; else, it will return an error saying it has failed or will deny the zone transfer.

Linux DNS zone transfer using the dig command

```

msf5 > use exploit/multi/http/sslstrip
[*] Using configured LHOST: 10.10.10.10
msf5 > run
[*] SSLStrip is running on 10.10.10.10:8080

```

Windows DNS zone transfer using the nslookup command

[illegible]

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

Performing DNS Zone Transfer (Cont'd)



```
File Edit View Search Terminal Help
[+] root@parrot: ~/home/bob
[+] nslookup -t axtf -d certifiedhacker.com
[+] Testing NS servers for zone transfer.
[+] Checking for zone transfer for certifiedhacker.com name servers
[+] Resolving SOA Record
[+]      SOA ns1.bluehost.com 162.159.24.80
[+] Resolving NS Records
[+] NS Servers found:
[+]      NS ns1.bluehost.com 162.159.24.80
[+]      NS ns2.bluehost.com 162.159.25.175
[+] Removing any duplicate NS server IP Addresses...
[+]
[+] Trying NS server 162.159.25.175
[+] 162.159.25.175 Has port 53 TCP Open
[+]   Zone Transfer Failed!
[+]   Zone transfer error: NOTIMP
[+]
[+] Trying NS server 162.159.24.80
[+] 162.159.24.80 Has port 53 TCP Open
[+]   Zone Transfer Failed!
[+]   Zone transfer error: NOTIMP
[+]
[+] root@parrot: ~/home/bob
```



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

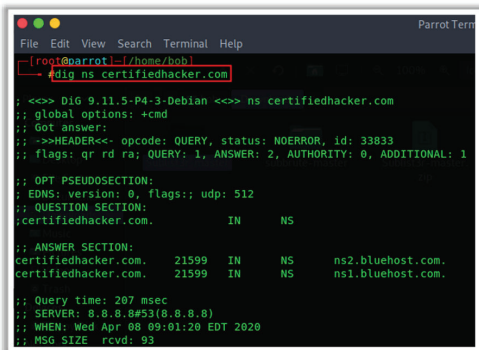
Performing DNS Zone Transfer

In most cases, a DNS server maintains a spare or secondary server for redundancy that holds all the information stored in the main server. The DNS server uses zone transfer to distribute changes made to the main server to the secondary server(s). If the DNS server of the target organization allows zone transfers, then DNS zone transfer can be performed to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, and so on assigned within a target domain.

Penetration testers can perform DNS zone transfer using tools such as nslookup, dig command, and dnsrecon. If the DNS zone transfer setting is enabled on the target name server, it will give the DNS information; else, it will return an error saying it has failed or will deny the zone transfer.

- **dig command**

Using the dig command, the penetration tester can query DNS name servers to retrieve information about the target host addresses, name servers, mail exchanges, and so on. The following figures illustrate how to perform DNS zone transfer using the dig command.



```

[root@parrot]~[/home/bob]
#dig ns certifiedhacker.com

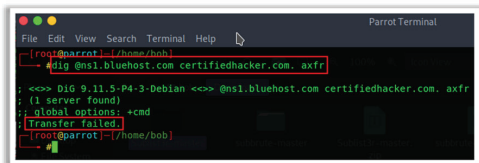
<<>> DiG 9.11.5-P4-3-Debian <<>> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 33833
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;certifiedhacker.com.          IN      NS

;; ANSWER SECTION:
certifiedhacker.com.  21599  IN      NS      ns2.bluehost.com.
certifiedhacker.com.  21599  IN      NS      ns1.bluehost.com.

;; Query time: 207 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Apr 08 09:01:20 EDT 2020
;; MSG SIZE rcvd: 93
  
```

Figure 3.70: Screenshot of Linux DNS zone transfer using the dig command



```

[root@parrot]~[/home/bob]
#dig @ns1.bluehost.com certifiedhacker.com. axfr

<<>> DiG 9.11.5-P4-3-Debian <<>> @ns1.bluehost.com certifiedhacker.com. axfr
(1 server found)
;; global options: +cmd
Transfer failed.

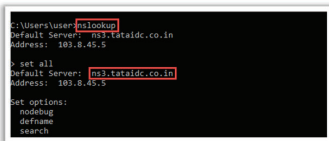
[root@parrot]~[/home/bob]
#
  
```

Figure 3.71: Screenshot of Linux DNS zone transfer using the dig command

▪ Nslookup

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

Nslookup is a useful tool for troubleshooting DNS problems such as hostname resolution. On startup, Nslookup shows the hostname and IP address of the DNS server that is configured for the local system. The figure below shows a screenshot of Windows DNS zone transfer using the nslookup command.

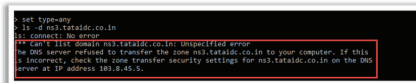


```
C:\Users\user> nslookup
Default Server: ns3.tataidc.co.in
Address: 103.8.45.5

> set all
Default Server: ns3.tataidc.co.in
Address: 103.8.45.5

Set options:
nodebug
defname
search
```

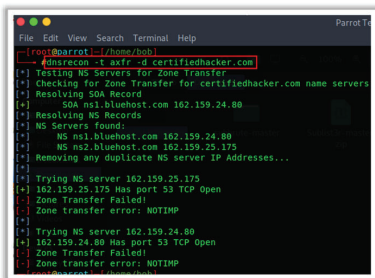
Figure 3.72: Screenshot of Windows DNS zone transfer using the nslookup command



```
> set type=any
> ls -d ns3.tataidc.co.in
ls: connect: No error
Can't list domain ns3.tataidc.co.in: Unspecified error
The DNS server refused to transfer the zone ns3.tataidc.co.in to your computer. If this
is incorrect, check the zone transfer security settings for ns3.tataidc.co.in on the DNS
server at IP address 103.8.45.5.
```

Figure 3.73: Screenshot of Windows DNS zone transfer using the nslookup command showing an error

▪ dnsrecon



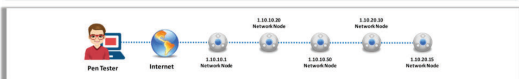
```
File Edit View Search Terminal Help
[root@parrot:~/home/bob]
# dnsrecon -t axfr -d certifiedhacker.com
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for certifiedhacker.com name servers
[*] Resolving SOA Record
[*] SOA ns1.bluehost.com 162.159.24.80
[*] Resolving NS Records
[*] NS Servers found:
[*] NS ns1.bluehost.com 162.159.24.80
[*] NS ns2.bluehost.com 162.159.25.175
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 162.159.25.175
[*] 162.159.25.175 Has port 53 TCP Open
[*] Zone Transfer Failed!
[*] Zone transfer error: NOTIMP
[*]
[*] Trying NS server 162.159.24.80
[*] 162.159.24.80 Has port 53 TCP Open
[*] Zone Transfer Failed!
[*] Zone transfer error: NOTIMP
[root@parrot:~/home/bob]
```

Figure 3.74: Screenshot of DNS zone transfer using dnsrecon

Drawing a Network Diagram using Traceroute Analysis



- Conduct a traceroute analysis to extract information about the **network topology**, **trusted routers**, and **firewall locations**.
- For example, after running **several traceroutes**, the following information may be obtained:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 1.10.20.10, third to last hop is 1.10.10.1
 - traceroute 1.10.10.10, second to last hop is 1.10.10.50
 - traceroute 1.10.20.15, third to last hop is 1.10.10.1
 - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, draw the **network diagram**.



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

Drawing a Network Diagram using Traceroute Analysis (Cont'd)

[illegible]

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

Drawing a Network Diagram using Traceroute Analysis

A penetration tester must identify the structure of the target organization's network. By identifying the structure of the network, they can draw the network diagram of the target network to obtain information such as its topology, path to the target hosts in the network and position of firewalls, intrusion detection systems (IDSs), trusted routers, and other access-control devices in the network. By identifying the devices connected in the network, the vulnerabilities in those devices can be discovered.

Traceroute tools such as traceroute and tracert can be used to remove information about the complete path that a packet travels, addresses, identity of devices in that path, and network latency. For example, after running several traceroutes, the following information may be obtained:

```
traceroute 1.10.10.20, second to last hop is 1.10.10.1
traceroute 1.10.20.10, third to last hop is 1.10.10.1
traceroute 1.10.20.10, second to last hop is 1.10.10.50
traceroute 1.10.20.15, third to last hop is 1.10.10.1
traceroute 1.10.20.15, second to last hop is 1.10.10.50
```

After obtaining the result to the above queries, this information can be put together to draw the network diagram shown in the below figure.



Figure 3.75: Sample network diagram of a target

The following are some traceroute tools.

- **traceroute**

traceroute is a Linux network diagnosis tool for identifying and measuring the path taken by an IP packet in a distributed network environment. The screenshot below shows the use of the traceroute command on a target domain.

```

File Edit View Search Terminal Help
root@parrot:~# traceroute microsoft.com
traceroute to microsoft.com (40.112.72.205), 30 hops max, 60 byte packets
 1 10.10.10.1 (10.10.10.1) 1.332 ms 1.432 ms 1.529 ms
 2 192.168.225.1 (192.168.225.1) 2.823 ms 2.811 ms 2.794 ms
 3 * * *
 4 10.71.235.35 (10.71.235.35) 82.928 ms 82.929 ms 10.71.235.50 (10.71.235.50) 86.78
 5 172.16.93.211 (172.16.93.211) 93.582 ms 99.178 ms 99.178 ms
 6 172.26.31.14 (172.26.31.14) 102.776 ms 172.26.31.10 (172.26.31.10) 70.119 ms 172.2
 6.31.14 (172.26.31.14) 70.662 ms
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 ae71-0.1er01.bom02.ntwk.msn.net (207.46.41.245) 92.052 ms 72.549 ms be-20-0.lbr01.
 bom02.ntwk.msn.net (104.44.23.213) 216.502 ms
13 ae21-0.eur01.bom02.ntwk.msn.net (104.44.232.249) 82.399 ms * 107.125 ms
14 be-20-0.lbr01.bom02.ntwk.msn.net (104.44.23.213) 242.309 ms be-16-0.lbr02.par30.ntw
 k.msn.net (104.44.28.108) 234.950 ms be-3-0.lbr02.par21.ntwk.msn.net (104.44.7.48) 232
 423 ms
15 104.44.17.81 (104.44.17.81) 242.388 ms be-0-0.lbr02.mrs29.ntwk.msn.net (104.44.19.1
 2) 259.314 ms 104.44.17.81 (104.44.17.81) 257.203 ms
16 be-16-0.lbr02.par30.ntwk.msn.net (104.44.28.108) 208.088 ms be-5-0.lbr01.dub08.ntwk
 msn.net (104.44.17.88) 208.035 ms be-3-0.lbr02.par21.ntwk.msn.net (104.44.7.48) 268.0
 72 ms
17 ae100-0.icr01.dub08.ntwk.msn.net (104.44.11.70) 233.774 ms 219.904 ms 104.44.17.81
 104.44.17.81 230.108 ms

```

Figure 3.76: Screenshot of the traceroute command

■ tracert

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

tracert is a Windows diagnostic utility that determines the route to a destination by sending Internet Control Message Protocol echo packets to the destination. The screenshot below shows the use of the tracert command on a target domain.

```
C:\windows\system32>tracert moreprocess.com

Tracing route to moreprocess.com [198.154.213.123]
over a maximum of 30 hops:

  0  1 ms  <1 ms  1 ms  D-Link.Home [192.168.1.1]
  1  29 ms  27 ms  30 ms  ABTS-KK-Static-001.228.178.122.
  2  26 ms  26 ms  27 ms  ABTS-KK-Static-221.32.166.122.a
  3  26 ms  28 ms  26 ms  AES-Static-025.102.22.125.airte
  4  278 ms  278 ms  278 ms  182.79.255.33
  5  279 ms  278 ms  280 ms  tgl-2.bp01.nycn.acedc.net [198.
  6  316 ms  389 ms  298 ms  ves9.a06.ppop.acedc.net [199.5
  7  301 ms  308 ms  312 ms  vrmsh.unifiedlayer.com [199.58.
  8  *  *  *  Request timed out.
  9  301 ms  288 ms  286 ms  198.154.213.123
Trace complete.
```

Figure 3.77: Screenshot of the tracert command

■ Nmap

Source: <https://nmap.org>

The Nmap traceroute-geolocation NSE script can be used to list the geographic locations of each hop in a traceroute and optionally save the results to a KML file plottable on Google Earth and Maps.

```
Parrot Terminal

File Edit View Search Terminal Help

[~]-[conf@parrot:~/hacking]
-> nmap --traceroute --script traceroute-geolocation www.certifiedhacker.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-08 09:45 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.35s latency):
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered snmp
26/tcp    open  rsftp
33/tcp    open  domain
39/tcp    open  http
118/tcp   open  pop3
143/tcp   open  imap
143/tcp   open  https
145/tcp   open  snmp3
554/tcp   open  rtsp
587/tcp   open  submission
893/tcp   open  imaps
898/tcp   open  pop3s
1723/tcp  open  pptp
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql
3432/tcp  open  postgresql
```

Figure 3.78: Screenshot of Nmap

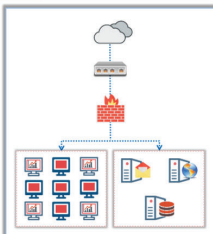
Creating a Topological Map of the Network



- Create **physical** and **logical topology** maps of the target organization's network based on the information gathered in the previous step.
- The physical topology map shows the placement of various components of the network such as servers, clients, routers, and hubs, including their location and cable installation, while the logical topology map shows how data flow within a network.
- Use tools such as **SmartDraw**, **Gifly**, etc.



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



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

Creating a Topological Map of the Network

Penetration testers can create physical and logical topology maps of the target organization's network based on the information gathered in the previous step. By creating the physical and logical topology of the target network, the tester can identify the network address space and devices connected in the network. The physical topology map shows the placement of various components of the network such as servers, clients, routers, and hubs, including their location and cable installation, while the logical topology map shows how data flow within a network.

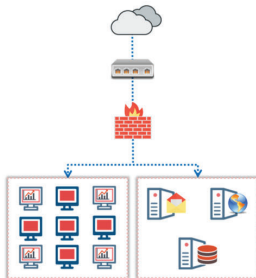


Figure 3.79: Topological map of a network

The following are some tools that can be used to draw the topological map of the target network.

- **Gliffy**

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

Gliffy is an online HTML5 cloud-based drawing tool that allows the user to create Unified Modeling Language (UML) diagrams, Venn diagrams, network diagrams, and various other diagram solutions. It offers many features to create appealing flowcharts and is supported by all major web browsers such as Chrome and Firefox.

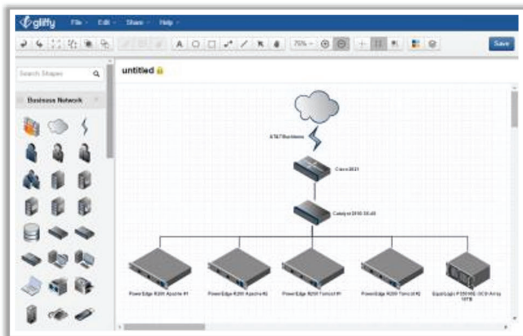


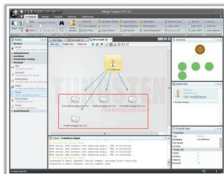
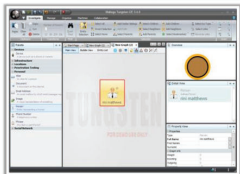
Figure 3.80: Screenshot of Gliffy

Automating the OSINT Process using Tools/Frameworks/Scripts

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

Maltego

- Use the Maltego tool to determine the **relationships and real-world links** among people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files.



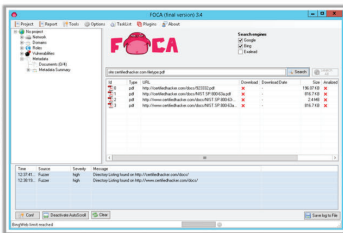
Source: <https://www.patrnas.com>

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

FOCA



- **Use Fingerprinting Organizations with Collected Archives (FOCA)** to find metadata and hidden information in the documents it scans.
- FOCA can be used to perform various data analyses such as **metadata extraction**, **network analysis**, DNS snooping, proxy search, **fingerprinting**, and open directory search.

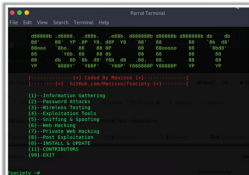


Source: <https://www.civildigital.com>

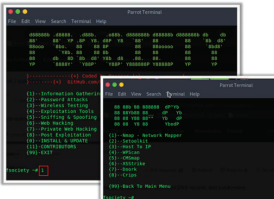
Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

F_{society}

- Fscociety is a **penetration testing framework**, which includes scripts that a penetration tester needs



Source: <https://github.com>

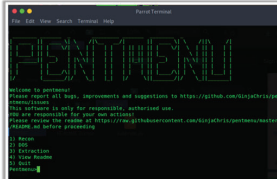
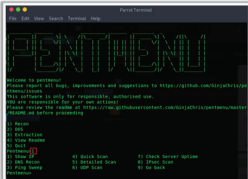


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

PENTMENU



 PENTMENU is a **bash script** inspired by pentbox that is designed to be a simple solution to implement various network pen testing functions including **information reconnaissance**.

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

Automating the OSINT Process using Tools/Frameworks/Scripts

Penetration testers can automate open-source information-gathering process using various tools, frameworks, and scripts. These tools help in collecting basic information about the target organization such as the target's IP location, routing information, business information, address, phone number and SSN, details about the source of an email or a file, and DNS information.

The following are some OSINT-gathering tools.

- **Maltego**

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

Maltego is an OSINT and forensics application. As a platform developed to deliver a clear threat picture to the environment that an organization owns and operates, Maltego is useful during the information-gathering phase of all security-related work. It also demonstrates the complexity and severity of single points of failure, as well as trust relationships that exist within the scope of the infrastructure. The unique perspective that Maltego offers to both network- and resource-based entities is the aggregation of information posted across the Internet.

It can be used to determine the relationships and real-world links between people, social networks, companies, organizations, websites, Internet infrastructure (domains, DNS names, Netblocks, and IP addresses), phrases, affiliations, documents, and files.

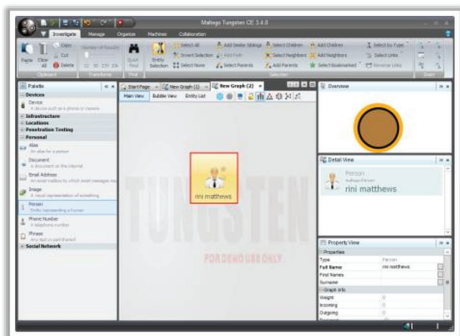


Figure 3.81: Screenshot of Maltego

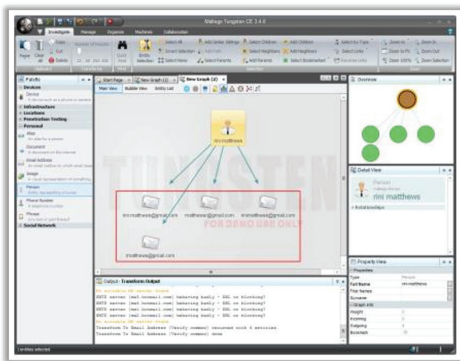


Figure 3.82: Screenshot of Maltego showing links

- **FOCA**

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

Fingerprinting Organizations with Collected Archives (FOCA) is capable of scanning and analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, and PDF files. Using FOCA, it is possible to launch multiple attacks and analysis techniques such as the extraction of metadata and hidden information, network analysis, DNS snooping, proxy search, fingerprinting, and open directory search.

Features:

- **Web search**

FOCA searches for hosts and domain names through URLs associated to the main domain. Each link is analyzed to remove new host and domain names.

- **DNS search**

FOCA checks each domain to ascertain which are the hostnames configured in NS, MX, and SPF servers to discover new host and domain names.

- **IP resolution**

Each hostname is resolved by comparison to the DNS to obtain the IP address associated with the server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.

- **PTR scanning**

To find more servers in the same segment of a determined address, IP FOCA executes a scan of PTR logs.

- **Bing IP**

For each IP address discovered, FOCA launches a search process for new domain names associated with that IP address.

- **Common names**

The common names module performs dictionary attacks against the DNS.

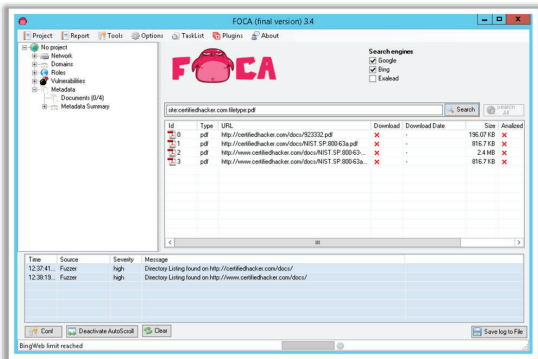


Figure 3.83: Screenshot of FOCA

▪ F Society

Source: <https://github.com>

F Society is a penetration testing framework that includes scripts required for penetration testing. It consists of a huge collection of tools with functions ranging from information gathering to post-exploitation. It includes various information-gathering tools such as Nmap, Setoolkit, Host to IP, WPScan, CMS Scanner, XSSStrike, Dork—Google Dorks Passive Vulnerability Auditor, and Crips.

```

Parrot Terminal
File Edit View Search Terminal Help

d88888b .d8888. .d88b. .o88b. d888888b d88888b d888888b db db
88' 88' YP .8P Y8. d8P Y8 88' 88 88 8b d8'
88ooo 8bo 88 88 8P 88 88ooooo 88 8b d8'
88 88 Y8b. 88 88 8b 88 88 88 88
88 db 8D 8b d8' Y8b d8 88. 88. 88 88
YP '8888Y' 'Y88P' 'Y88P' Y888888P Y88888P YP YP

}-----{+} Coded By Manisso {+}-----{
}-----{+} GitHub.com/Manisso/fsociety {+}-----{

(1)--Information Gathering
(2)--Password Attacks
(3)--Wireless Testing
(4)--Exploitation Tools
(5)--Sniffing & Spoofing
(6)--Web Hacking
(7)--Private Web Hacking
(8)--Post Exploitation
(9)--INSTALL & UPDATE
(11)--CONTRIBUTORS
(99)--EXIT

fsociety ~#
  
```

Figure 3.84: Screenshot of Fsoociety

```

Parrot Terminal
File Edit View Search Terminal Help

d88888b .d8888. .d88b. .o88b. d888888b d88888b d888888b db db
88' 88' YP .8P Y8. d8P Y8 88' 88 88 8b d8'
88ooo 8bo 88 88 8P 88 88ooooo 88 8b d8'
88 88 Y8b. 88 88 8b 88 88 88 88
88 db 8D 8b d8' Y8b d8 88. 88. 88 88
YP '8888Y' 'Y88P' 'Y88P' Y888888P Y88888P YP YP

}-----{+} Coded By Manisso {+}-----{
}-----{+} GitHub.com/Manisso/fsociety {+}-----{

(1)--Information Gathering
(2)--Password Attacks
(3)--Wireless Testing
(4)--Exploitation Tools
(5)--Sniffing & Spoofing
(6)--Web Hacking
(7)--Private Web Hacking
(8)--Post Exploitation
(9)--INSTALL & UPDATE
(11)--CONTRIBUTORS
(99)--EXIT

fsociety ~# 1
  
```

Figure 3.85: Screenshot of Fsoociety showing how to select information-gathering tools

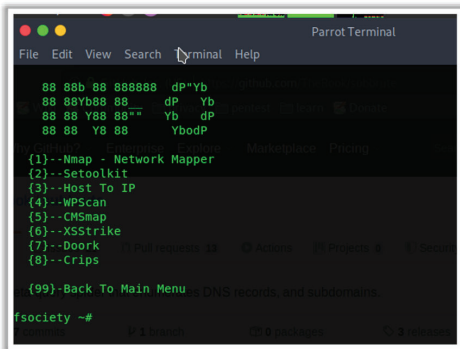


Figure 3.86: Screenshot of F Society showing information-gathering tools

■ PENTMENU

Source: <https://github.com>

PENTMENU is a bash script inspired by pentbox that is designed to be a simple solution to implement various network penetration testing functions including network attacks and information reconnaissance. Wherever possible, it uses readily available software commonly installed on most Linux distributions without having to resort to multiple specialist tools. PENTMENU consists of various modules such as Recon, denial of service (DoS), and extraction. The Recon module consists of functions such as Show IP, DNS Recon, Ping Sweep, Quick Scan, and User Datagram Protocol (UDP) Scan.

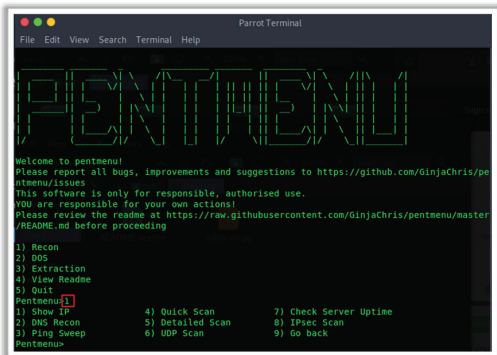


Figure 3.87: Screenshot of PENTMENU showing Recon functions

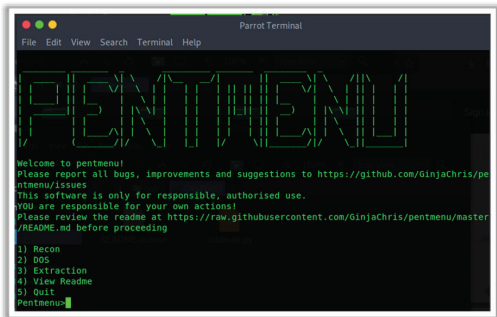


Figure 3.88: Screenshot of PENTMENU

Document the Result



- Document the result obtained through **OSINT**.
- The document should include the following **valuable information**:



- Domain and subdomains
- Physical location
- Employees
- Telephone numbers and email addresses
- Products/services
- Network devices
- Website directory, technology, and external links
- Public IP address block
- DNS records



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

Document the Result

Documenting the result is an important step for any penetration test. While conducting a penetration test, the tester must document all the successful results obtained through OSINT. Once all the steps are completed, they must reconstruct the results in detail. After completion of all the phases of penetration testing, this document serves as the basis for generating the final report. It must include valuable and detailed information about identified vulnerabilities such as the following:

- Domain and subdomains
- Physical location
- Employees
- Telephone numbers and email addresses
- Products/services
- Network devices
- Website directory, technology, and external links
- Public IP address block
- DNS records

EC-Council

Certified Security Analyst

OSINT Through World Wide Web(WWW)

Test 1: Find the Domain and Sub-domains of the Target

Target Organization	Certifiedhacker	
Search Engine Used	Google	
Found Domain	http://certifiedhacker.com/	
Found the Sub-domains of the Target Successfully	☐ Yes	☐ No
Command/tool Used	dnsmmap, dns-brute, sublist3r, netcraft,	
Domain and Sub-domains Identified:	1. www.certifiedhacker.com 2. news.certifiedhacker.com 3. mail.certifiedhacker.com 4. ftp.certifiedhacker.com 5. 6.	

Results Analysis: |

Possible Attack Surfaces of Target Organization are listed below:

1. www.certifiedhacker.com

2. news.certifiedhacker.com

3. mail.certifiedhacker.com

4. ftp.certifiedhacker.com

Figure 3.89: Sample OSINT document