4.1 ENUMERATION OVERVIEW

- Enumeration Concepts
- Enumeration Tools and Techniques

WHAT IS ENUMERATION?

- The systematic process of querying a target's servers and services for information
- The attacker utilizes information gathered during footprinting / reconnaissance to know which devices and services to query
- We exploit normal server functionality and protocols to gain more information about our target

We enumerate to find possible entry points into the target system!

INFORMATION ENUMERATED

- OS and service details
- Users and groups
- Email addresses and contact information
- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and DNS information
- Machine names
- Applications and banners

ENUMERATION APPROACH

- Enumeration should appear to the server as a normal client making legitimate information requests
- Your enumeration test should focus on the information you need
  - You want to avoid returning too much information that will clutter your results
- A combination of manual and automated testing will give the best results

BANNER GRABBING EXAMPLE

```
netcat www.someserver.com 80
```

```
HTTP/1.1 200 OK – Server: Microsoft-IIS/6 – Expires: Tue, 17 Jan 2011
01:41:33 GMT Date: Mon, 16 Jan 2011 01:41:33 GMT Content-Type:
text/html – Accept-Ranges: bytes – Last-Modified: Wed, 28 Dec 2010
15:32:21 GMT ETag: “b0aac0542e25c31:89d” Content-Length: 7369
```

NMAP ENUMERATION EXAMPLES

```
nmap -O 192.168.1.50
nmap -sV 192.168.1.20
nmap --script=smb-os-discovery <target>
```

RPCCLIENT ENUMERATION EXAMPLES

```
rpcclient <target IP> -U <username>
srvinfo
lookupnames administrator
lookupsids
```

```
rpcclient -U "" 192.168.1.20
```

METASPLOIT ENUMERATION EXAMPLE

```
use /auxiliary/scanner/smb/smb_lookupsid
set SMBUser moo
set SMBPass Pa22w0rd
set MinRID 1000
set MaxRID 1100
set RHOSTS 192.168.74.50

run
```

SERVICES ENUMERATION TOOLS

Port	Protocol and Service	Tool Examples and Comments
TCP 21	**Protocol:** FTP **Service:** FTP server	**Tools:** Telnet and FTP clients, nmap ftp-anon.nse, ftp-brute.nse, Metasploit modules: ftp/anonymous, ftp_login, and ftp_version **Comments:** Identify FTP servers, versions, and authentication requirements (including anonymous logins)
TCP 22	**Protocol**: SSH **Service**: SSH server	**Tools**: nmap, PuTTY/SSH clients, nmap ssh-brute.nse, ssh-run.nse, Metasploit modules: ssh_login, ssh_login_pubkey **Comments**: Linux servers, routers, switches, other network devices, jailbroken iPhones
TCP 23	**Protocol**: telnet **Service**: Telnet server	**Tools**: PuTTY/telnet clients, nmap telnet-brute.nse, telnet-ntlm-info.nse, Metasploit telnet_login, telnet_version modules **Comments**: Linux servers, routers, switches, other network devices
TCP 25	**Protocol**: SMTP **Service**: Email server	**Tools**: PuTTY/telnet clients, nmap smtp-enum-users.nse, smtp-commands.nse, smtp-open-relay.nse, smtp-brute.nse, Metasploit smtp_enum, smtp_version modules **Comments**: Extract email addresses; Enumerate SMTP server information. Search for open relays

SERVICES ENUMERATION TOOLS (CONT'D)

Port	Protocol and Service	Tool Examples and Comments
TCP 53	**Protocol**: DNS **Service**: DNS	**Tools**: dig, nslookup, nmap dns-brute.nse, Metasploit enum_dns module **Comments**: Elicit DNS zone transfers. Discover DNS subdomains
TCP 80	**Protocol**: HTTP **Service**: Web server	**Tools**: PuTTY/telnet clients, dirbuster, nmap http-enum.nse, http-title.nse, http-sitemap-generator.nse, Metasploit modules: http_cert, dir_listing, dir_scanner, dir_webdav_unicode_bypass, enum_wayback, files_dir, http_login, http/ssl, http_version, webdav_scanner, webdav_website_content **Comments**: Manually request web pages, enumerate directories, files, WebDAV features, versions, and more
TCP 135, 111	**Protocol**: RPC **Service**: Microsoft DCE/RPC Locator Service, *nix portmapper service	**Tools**: nmap rpcinfo.nse, rpc-grind.nse, msrpc-enum.nse, Metasploit dcerpc modules: endpoint_mapper, hidden, management, tcp_dcerpc_audito. **Comments**: Query and manipulate Remote Procedure Call (RPC)-based services such as Windows DCOM, and *nix NFS, nlockmgr, quotad, and mountd

SERVICES ENUMERATION TOOLS (CONT'D)

Port	Protocol and Service	Tool Examples and Comments
TCP 137	**Protocol**: NetBIOS **Service**: NetBIOS Name Service	**Tools**: nbtscan, nmap smb-enum-shares.nse, smb-enumdomains.nse, smb-os-discovery.nse **Comments**: List NetBIOS computer, user, group, workgroup, and domain names, domain controller roles, file and print sharing services, Microsoft Exchange services
TCP 139	**Protocol**: SMB **Service**: NetBIOS Session Service (SMB file and print service)	**Tools**: enum.exe (Windows), enum4linux.pl, smbclient, nmap smb-enum-shares.nse, smb-os-discovery.nse, Metasploit modules: smb_enumshares, smb/smb2, smb_version **Comments**: Retrieve directory information, list and transfer files. NSE scripts might not work on newer machines
UDP 161	**Protocol**: SNMP **Service**: SNMP	**Tools**: getif, SolarWinds NPM, PRTG, WhatsUp Gold, Nagios Core, Spiceworks, Observium, nmap snmp-info.nse, snmp-brute.nse, snmp-interfaces.nse, snmp-processes.nse, Metasploit snmp modules: snmp_enum, snmp_enumusers, snmp_enumshares, snmp_login **Comments**: Obtain information on dozens of data objects depending on device. Targets must have SNMP agent enabled; you must know the community string devices are using

SERVICES ENUMERATION TOOLS (CONT'D)

Port	Protocol and Service	Tool Examples and Comments
TCP/UDP 389	**Protocol**: LDAP **Service**: Microsoft Active Directory	**Tools**: Active Directory Users and Computers, ntdsutil.exe, OpenLDAP, LDAP Admin, LDP.exe, nmap ldap-search.nse, Metasploit module: enum_ad_computers **Comments**: Retrieve a wide range of information from Active Directory; Non-privileged users can query Active Directory for nearly all information. To capture password hashes, copy the database file ntds.dit using ntdsutil.exe, then use Windows Password Recovery Tool to extract the hashes
TCP 445	**Protocol**: RPC **Service**: Microsoft-DS Active Directory and SMB file sharing	**Tools**: rpcclient, Metasploit smb_login, smb_enumusers, & smb/psexec modules, nmap NSE smb-enum-* scripts, enum.exe, user2sid.exe, sid2user.exe, PowerShell, pstools **Comments**: Retrieve a very wide range of Microsoft computer and domain information
TCP 1433	**Protocol**: SQL **Service**: SQL Server	**Tools**: nmap mysql-info.nse, Metasploit modules: mssql_ping, mssql_enum, enum_domain_accounts, enum_sql_logins **Comments**: Locate and enumerate information including logins from Microsoft and MySQL SQL servers
TCP 3268	**Protocol:** LDAP **Service:** MS Active Directory Global Catalog Service	**Tools:** Same as for LDAP, but a different port **Comments:** The Active Directory Global Catalog maintains a listing for all objects in an entire Active Directory forest.

4.2 SMB AND NETBIOS ENUMERATION

- NetBIOS
- SMB
- Null User
- Tools

NETBIOS

- Network Basic Input/Output System
- An API and Layer 5 protocol
- Allows applications to communicate over a local area network (LAN) with device specific NetBIOS names
  - 1 - 15 alphanumeric characters (a hidden 16th character describes the name type)
  - Special characters can only include: - . _ $ (dash, period, underscore, dollar sign)
  - $ has special meaning (name or share exists but is hidden on the network)
  - Only the dash is compatible with DNS naming conventions
- Used by Microsoft for simple LAN communications, name resolution and file sharing
- Originally used by broadcast-based NetBEUI networking protocol
- Microsoft later made it a payload of TCP/IP (NetBIOS over TCP)
- TCP 137, 139; UDP 137, 138

NETBIOS NAMES

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

SERVER MESSAGE BLOCK (SMB)

- Microsoft file and print sharing protocol
- Microsoft Workstation Service (client) connects to a remote machine's Server Service (server)
- Also provides authenticated inter-process communication (IPC) among processes running on remote computers
- A hidden network share, known as IPC share (ipc$), is used on Windows computers
  - Facilitates communication between processes and remote computers

NETBIOS AND SMB

- Originally NetBIOS and SMB worked together:
  - An SMB client uses the NetBIOS API to send an SMB command to an SMB server
    - Listens for replies from the SMB server.
  - An SMB server uses the NetBIOS API to listen for SMB commands from SMB clients
    - Sends replies to the SMB client
- Since Windows 2000, SMB runs directly on TCP 445
- NetBIOS still exists for backward compatibility
- Linux/UNIX Samba server is a reverse-engineered SMBv1 File Server service
  - It has the same vulnerabilities as the Windows original

NetBIOS and SMB have a long history of vulnerabilities

NETBIOS / SMB ENUMERATION

- You can use SMB to make NetBIOS calls to a Microsoft Server Service
- You can enumerate:
  - Computer names
  - Share names
  - User names
  - Logon information
  - Password policy and hashes
  - NetBIOS computer and domain names
  - Active Directory domain and forest names
  - FQDNs
  - System time

NULL USER

- A null user is a pseudo account that has no username and password
- Was initially used by Windows systems to "log in" to each other to trade network browse lists
- For decades, the null session was an exploit that took advantage of the null user

```
net use \\<IP ADDRESS>\IPC$ "" /user:
```

- Mapping a drive to the IPC$ process then allows you to enumerate a lot of information via NetBIOS and SMB

NBTSTAT

- Windows utility
- Displays NetBIOS over TCP/IP protocol statistics, NetBIOS name tables for local and remote computers, and the NetBIOS name cache

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

NET COMMANDS

- Has 19 sub commands for enumerating information via NetBIOS

```
C:\Users\Chrys>net /?
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

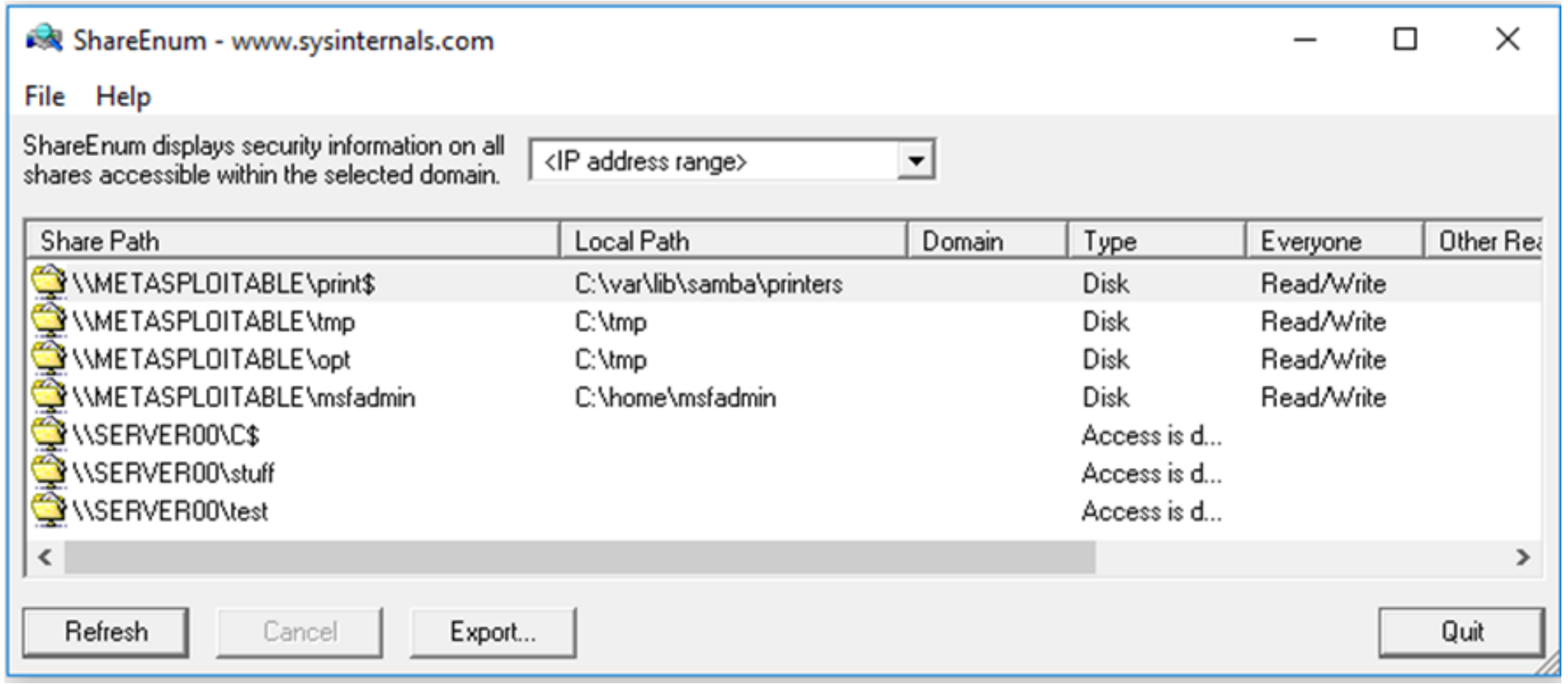
ENUM4LINUX

- Runs on Linux
- Enumerates NetBIOS information from Windows and Linux SAMBA
  - `-A all`
  - `-U get userlist`
  - `-M get machine list`
  - `-N get namelist dump (different from -U and-M)`
  - `-S get sharelist`
  - `-P get password policy information`
  - `-G get group and member list`

ENUM4LINUX EXAMPLE

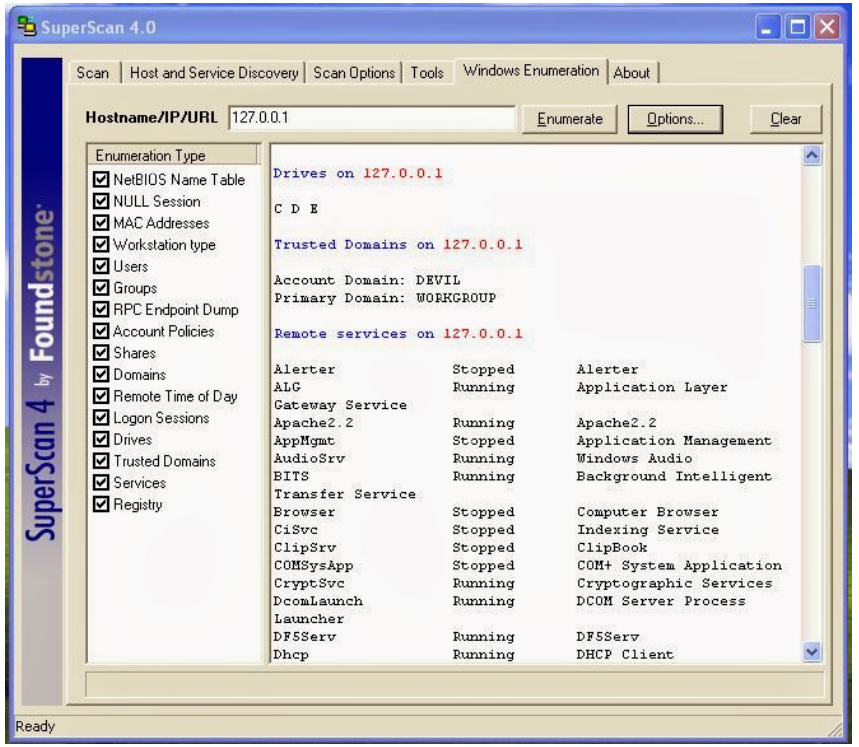
```
 ==========================================
|    Share Enumeration on 10.10.19.179     |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk      Network Logon Service
        profiles        Disk      Users profiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (polosmb server (Samba, Ubuntu
))
SMB1 disabled -- no workgroup available
```

SHAREENUM EXAMPLE



SUPERSCAN

- A connection-based TCP port scanner, pinger, and hostname resolver
  - Support for unlimited IP ranges
  - Host detection by multiple ICMP methods
  - TCP SYN and UDP scanning
  - Simple HTML report generation
  - Source port scanning
  - Hostname resolving
  - Banner grabbing
  - Windows host enumeration



ADDITIONAL NETBIOS ENUMERATION TOOLS

- NetBIOS Enumerator
- NSAuditor Network Security Auditor
  - Includes more than 45 network tools and utilities for network security auditing, network scanning, network monitoring, etc.
- Hyena
  - A GUI application for managing and security Microsoft operating systems
  - Shows shares
  - User logon name for Windows servers and domain controller
  - Displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.
- Winfingerprint
  - Shows operating system, enumerates users, groups, SIDs, transports, session, services, service pack and hotfix level, date and time, disks, and open TCP/UDP ports

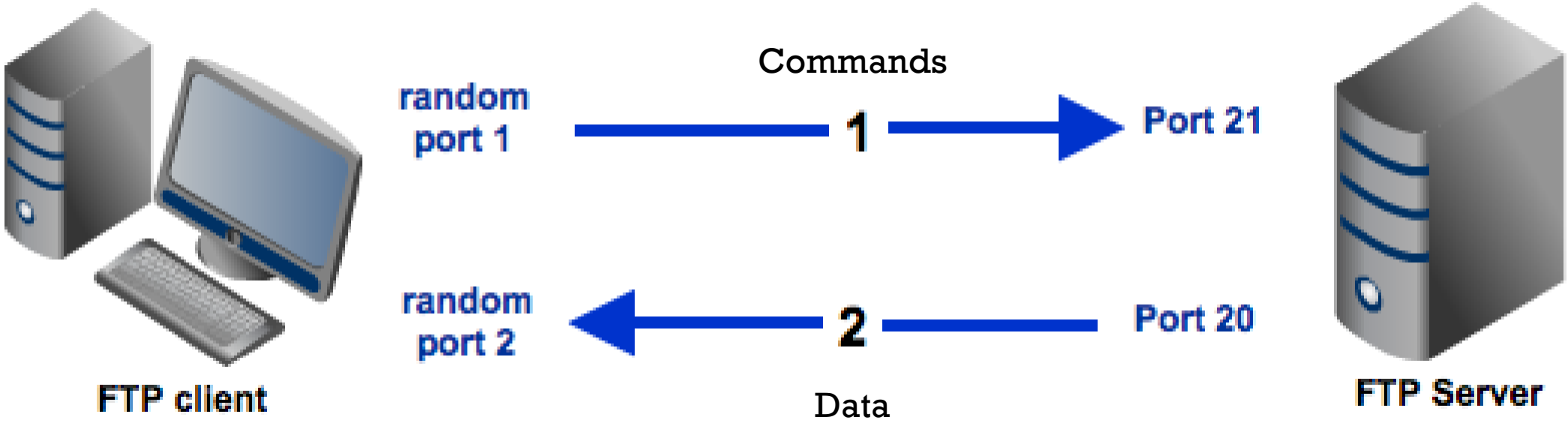
4.3 FILE TRANSFER ENUMERATION

- FTP
- TFTP
- NFS

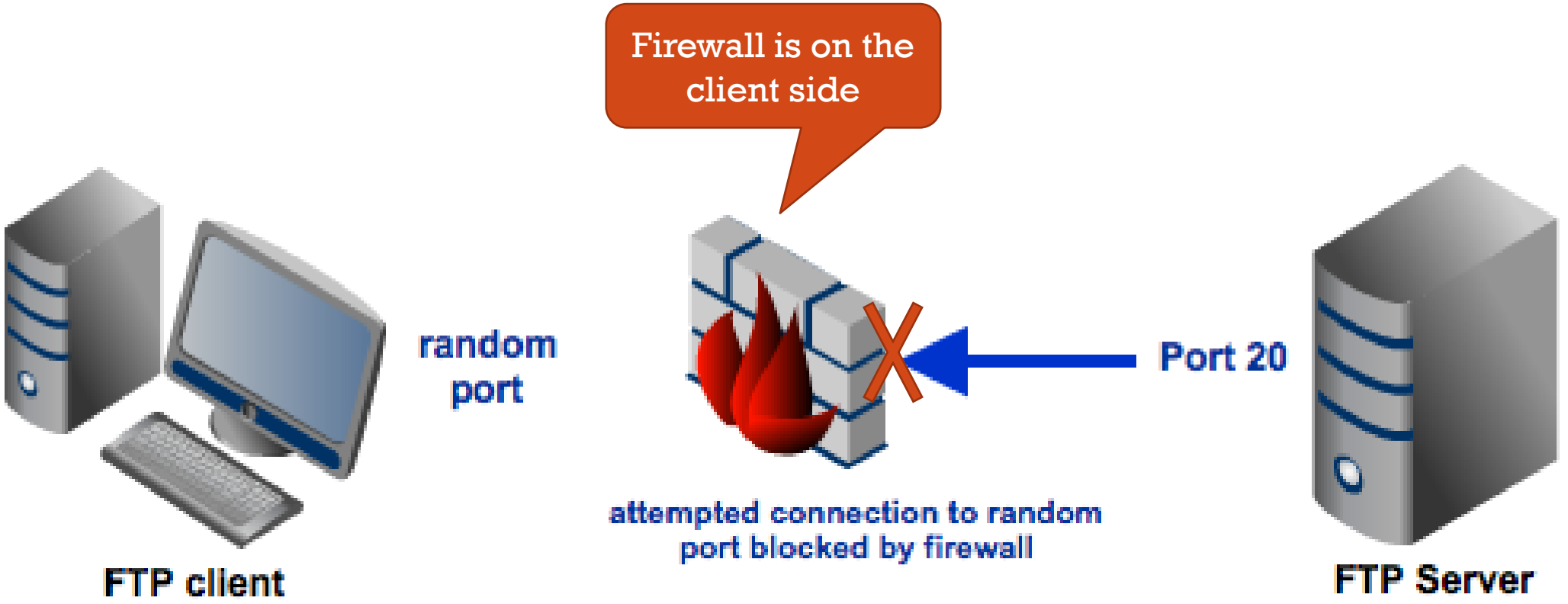
FILE TRANSFER PROTOCOL (FTP)

- A common, clear text file sharing protocol
  - Interactive
  - Has commands to list files and directories, upload and download files
  - TCP 21 (commands)
  - TCP 20 or random port (data transfer)
- An FTP server can be configured to:
  - Authenticate a user
  - Allow anonymous connections
- You can use the FTP protocol to enumerate

FTP ACTIVE MODE

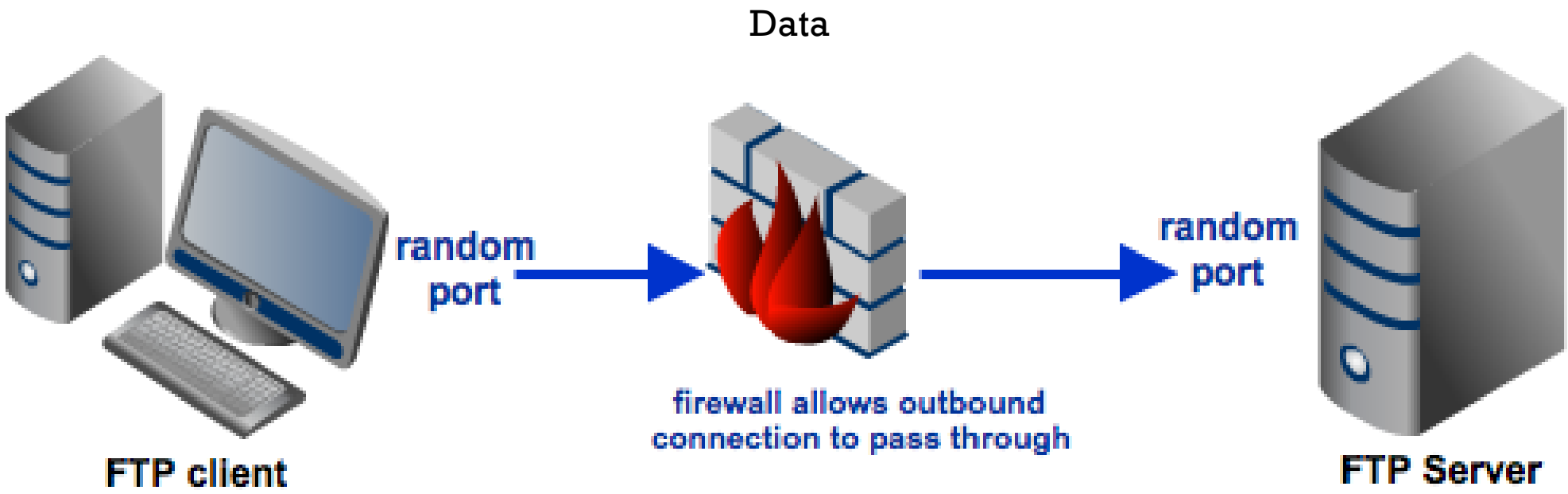


FTP ACTIVE MODE CHALLENGE



The server tries to initiate the data connection, which the client's firewall blocks

FTP PASSIVE MODE SOLUTION



The client initiates the data connection, which the client's firewall allows

FTP ENUMERATION

- You can use FTP commands to enumerate information from an FTP server:
  - Accounts
  - Passwords
  - Anonymous login capabilities
  - Port scanning other targets

FTP ENUMERATION TOOLS

- Netcat
  - Banner grab from an FTP server

```
kali@kali:~$ nc -nv 10.0.0.118 21
(UNKNOWN) [10.0.0.118] 21 (ftp) open
220 Welcome to vsFTPd 3.0.3
```

- Nmap scripts
  - ftp-anon – Checks if an FTP server allows anonymous logins.
  - ftp-brute – Performs brute-force password auditing against FTP servers.
  - ftp-bounce – Checks to see if an FTP server allows port scanning using the FTP bounce method.
- ftp-user-enum
  - Tool for enumerating OS-level user accounts via the ftp service
  - Works against the default Solaris in.ftpd and GNU inetutils ftpd

TRIVIAL FTP (TFTP)

- FTP's "Little Brother"
  - No authentication
  - Clear text
  - UDP 69
  - Non-interactive
  - No browsing the server directory
  - You must know the name of the file you want to download / upload
- Typically used to upload/download OS and config files for networking devices
  - You can try downloading a configuration file by its default name

```
TFTP.exe <host> GET startup-config
```

USING TFTP TO ENUMERATE INFORMATION

- You can try to download configuration files stored on a TFTP server
  - The service has no way to authenticate connections or enforce authorization

- Nmap has a script that will try to download files by supplying a list of file names

```
nmap -sU -p 69 --script tftp-enum.nse
--script-args tftp-enum.filelist=customlist.txt <host>
```

Making an unauthorized connection to a TFTP server is still unauthorized access!!

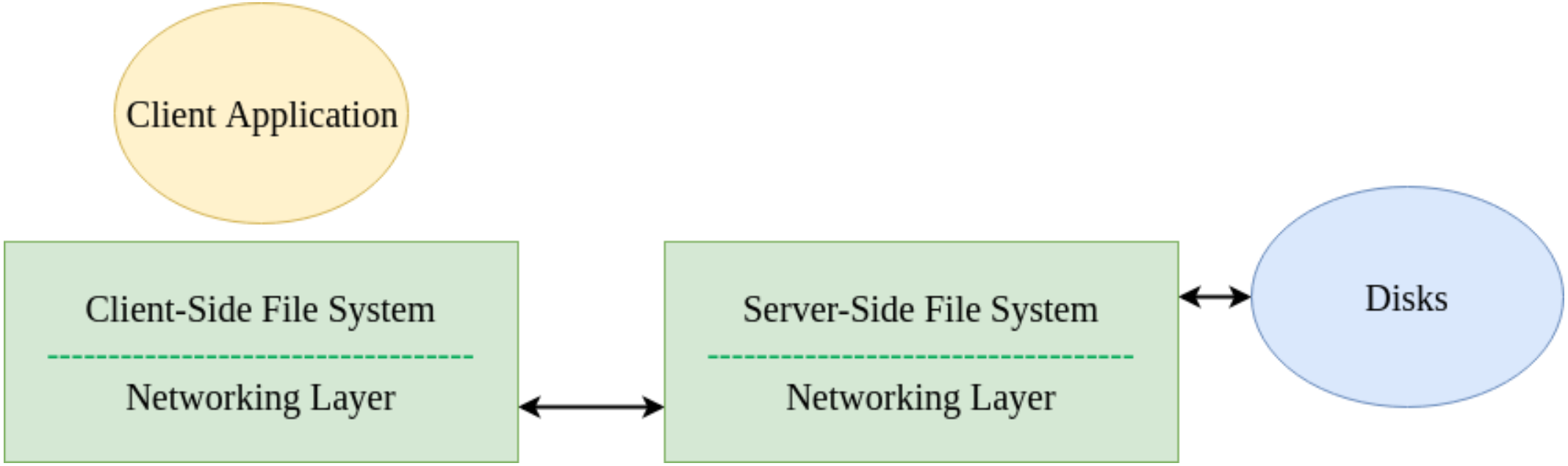
NETWORK FILE SYSTEM (NFS)

- The file sharing system for Linux/Unix
- Clients can "mount" (connect to) a share
- Tools to enumerate NFS include:
  - rpcinfo (part of Linux rpcbind)

    ```
    sudo apt install rpcbind
    ```

  - rpcscan (written in Python, available on GitHub)
  - SuperEnum (written in Python, available on GitHub)
- You can use the NFS client to enumerate shares on the network

NFS CONCEPTUAL DIAGRAM



NFS EXAMPLE

On the file server:

1. Add a line in the **/etc/exports** file to allow anyone on the subnet to read/write to the share:

```
/home/srvshare 192.168.1.0/24(rw,sync)
```

2. Run a command to export all shares listed in /etc/exports:

```
exportfs -a
```

3. Start the NFS server process:

```
/etc/init.d/nfs-kernel-server start
```

On the client:

```
mkdir /home/fromserver
sudo mount -t nfs <server IP>:/home/srvshare /home/fromserver
```

4.4 WMI ENUMERATION

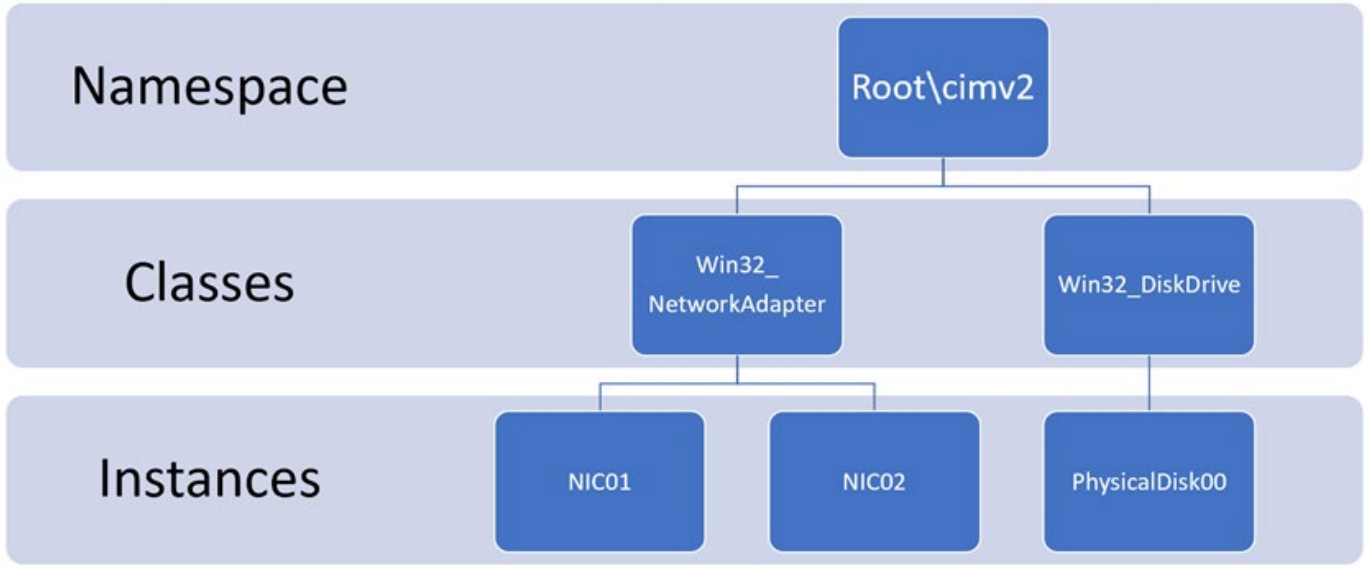
- Overview
- Namespace
- Querying
- Tools

WINDOWS MANAGEMENT INSTRUMENTATION (WMI)

- The Microsoft implementation of Web-Based Enterprise Management (WBEM)
- A standard technology for accessing management information in an enterprise environment
- Uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components
- Capable of obtaining management data from remote systems
  - Uses DCOM (TCP 135) to make these connections

WMI NAMESPACE

- WMI organizes its classes in a hierarchical namespace
  - Conceptually similar to a folder structure
- root/cimv2 is the default namespace
  - It contains 277 classes for computer hardware and configuration



COMMONLY QUERIED WMI CLASSES

- Win32_BIOS
- Win32_BootConfiguration
- Win32_ComputerSystem
- Win32_ComputerSystemEvent
- Win32_ComputerSystemProcessor
- Win32_CurrentTime
- Win32_DeviceSettings
- Win32_DiskPartition
- Win32_Group
- Win32_GroupUser
- Win32_IP4RouteTable
- Win32_LogicalDisk
- Win32_LogonSession
- Win32_NetworkAdapterConfiguration
- Win32_NetworkClient
- Win32_NetworkConnection
- Win32_NTDomain
- Win32_NTLogEvent
- Win32_OperatingSystem
- Win32_Process
- Win32_Processor
- Win32_Registry
- Win32_ScheduledJob
- Win32_SecurityDescriptor
- Win32_Service
- Win32_Share
- Win32_StartupCommand
- Win32_SystemAccount
- Win32_SystemBIOS
- Win32_SystemUsers
- Win32_UserAccount
- Win32_UserInDomain

COMMON POWERSHELL CMDLETS FOR WMI

- Get-CimClass
  - Returns all WMI classes
- Get-CimInstance -ClassName <name>
  - Returns information about a particular class
  - E.g. `Get-CimInstance –ClassName Win32_Processor`
- Get-CimInstance '*<string>*'
  - Returns all classes that have "processor" in the name
  - E.g. `Get-CimInstance '*processor*'`
- Get-CimInstance <class> | ft
  - Output results in table format
  - E.g. `Get-CimInstance Win32_process | ft`
- Get-CimInstance <class> | ft -autosize
  - Output results in table format, automatically resizing columns as needed
- Get-CimInstance <class> | fl
  - Output results in list format

Get-CimClass replaces the obsolete Get-WMIObject cmdlet

PowerShell is not case sensitive

QUERYING WMI WITH WQL

- WMI Query Language
- A subset of ANSI SQL
- Basic syntax:
  - `Select <property> from <WMI-class>`
- Examples:
  - `Select * from Win32_Bios`
  - `Select Name from Win32_Bios`
  - `Select name, version from Win32_Bios`
- Can be used in PowerShell, other scripts, and custom apps
- Sometimes has better performance than equivalent PowerShell cmdlets
  - Queries might also be more complex than the equivalent cmdlet

WMI ENUMERATION AND EXPLOIT TOOLS

Enumeration

- Solarwinds Free WMI Monitor
- WMI Explorer (CodePlex)
- WMI Explorer (Marc van Orsouw)
- Hyena
- PowerShell

Exploit

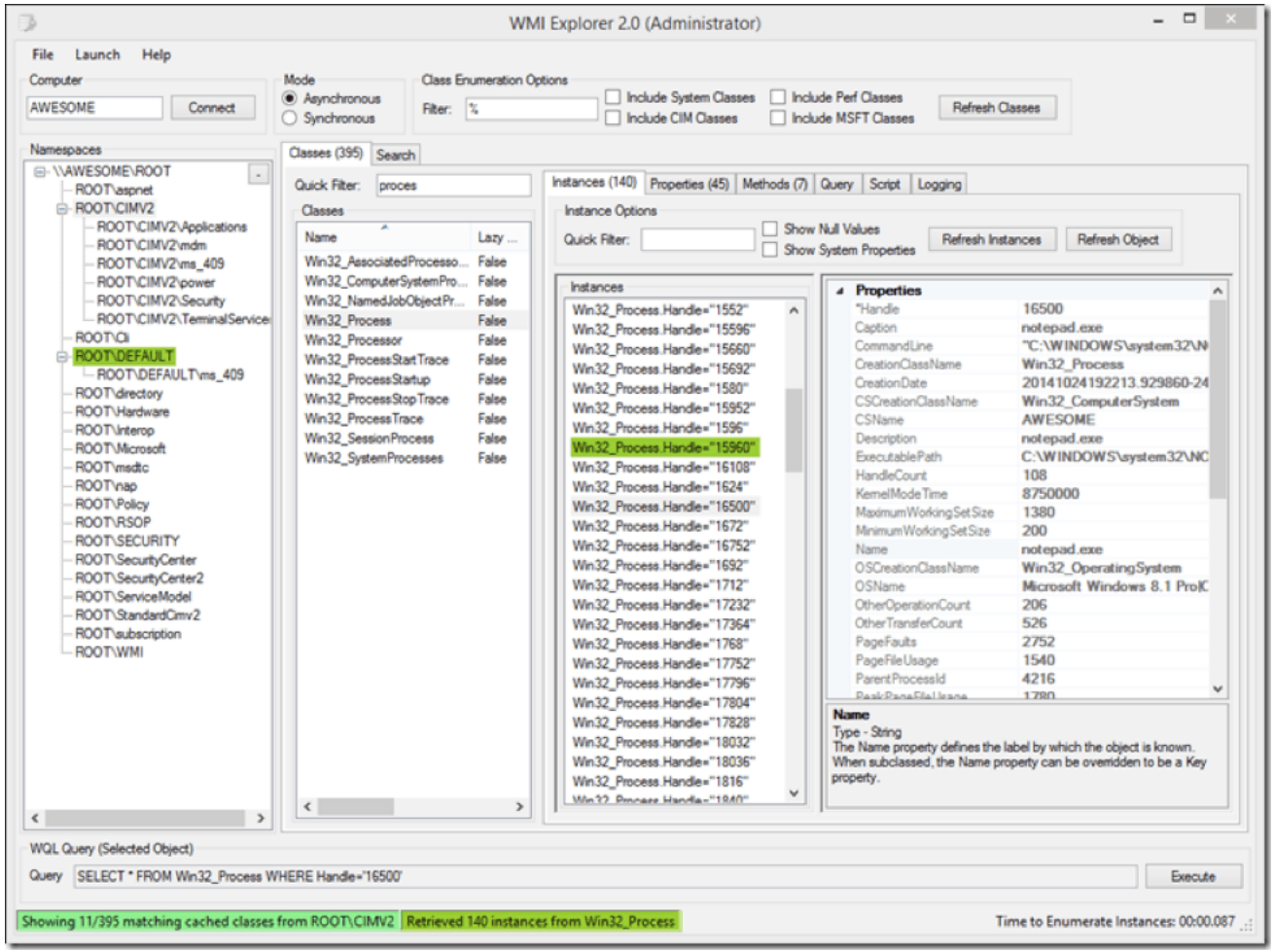
GitHub:

- WmiSploit
- SharpStrike
- WMEye
- Power

Metasploit:

- exploit/windows/local/wmi
- auxiliary/scanner/smb/impacket/wmiexec
- exploits/windows/local/wmi_persistence

WMI EXPLORER EXAMPLE



4.5 SNMP ENUMERATION

- SNMP
- OIDs
- MIB
- Tools

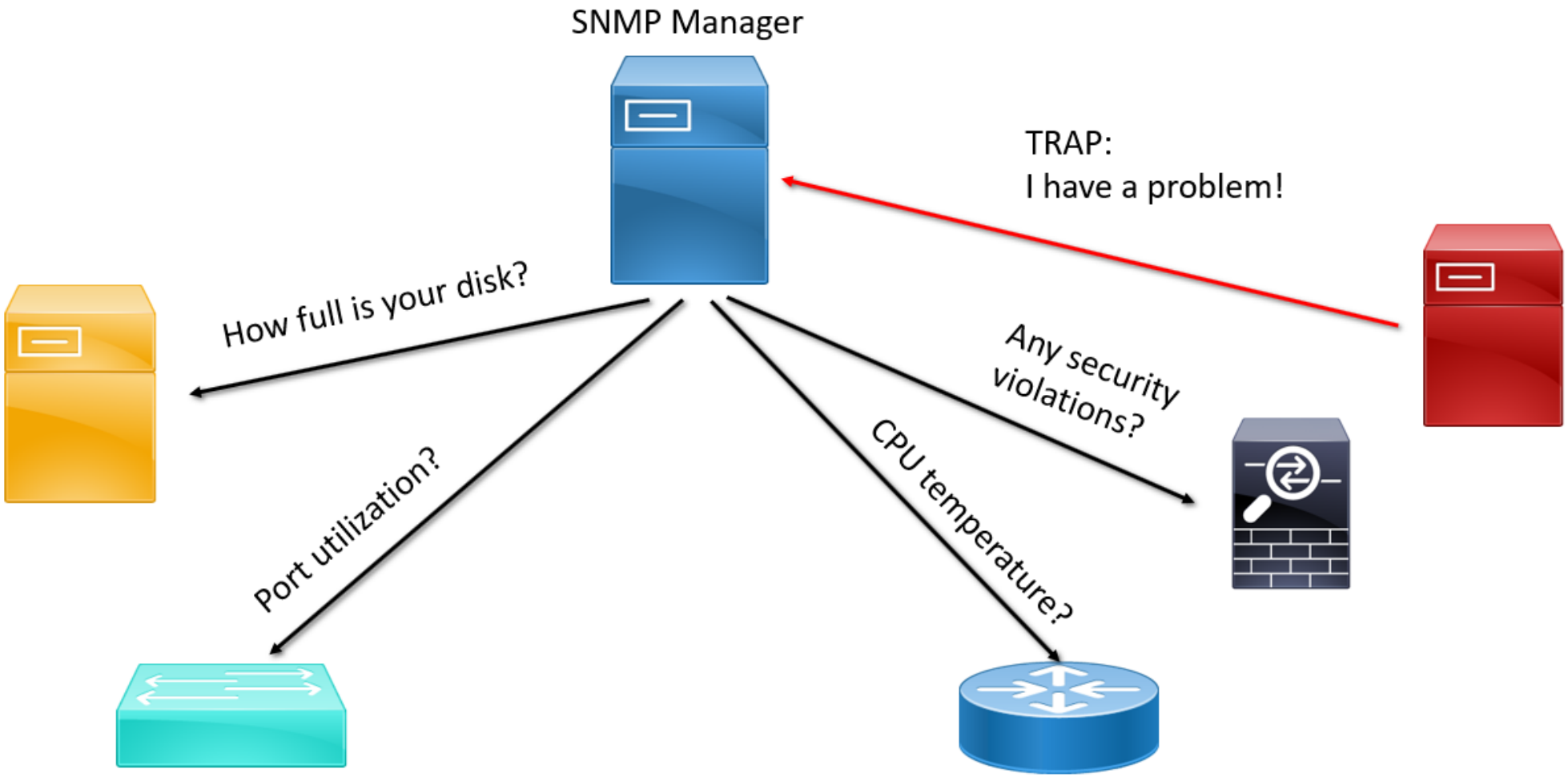
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Used to centrally monitor devices on a network
- An SNMP manager polls agents for information
  - Polling is done round-robin style, on a regular interval (every few minutes)
  - Manager is software on a server or workstation
  - Agent is small software installed or built into a device OS
- The manager uses a Management Information Base (MIB) to know what types of information an agent can provide
  - A MIB is a set of counters (Object IDs) relevant to the device

SNMP SECURITY

- SNMP has several versions that are still in use
  - v1, v2, v2c all communicate in clear text
  - v3 is encrypted
  - Not all devices support v3
- Both the manager and agent are configured with a simple authentication mechanism called the "community string"
  - Simple text string
  - An agent will only respond to a manager that has the same community string
  - There are two default community strings:
    - "Public" – for read-only queries
    - "Private" – for read/write communications
    - Many administrators do not change the default community strings
- SNMP Ports:
  - UDP 161 - Manager queries and agent replies
  - UDP 162 – Agents "raise traps" (send pre-configured alerts) to the manager

SNMP EXAMPLE



SNMP COMPONENTS

- Managed Device
  - Router, switch, hub, firewall, computer, server service (DHCP, DNS, etc.) printer, IoT device
- Agent
  - Software installed on managed device
  - Responds to the NMS
- Network Management System (NMS)
  - Typically software installed on a dedicated computer

OBJECT IDENTIFIER (OID)

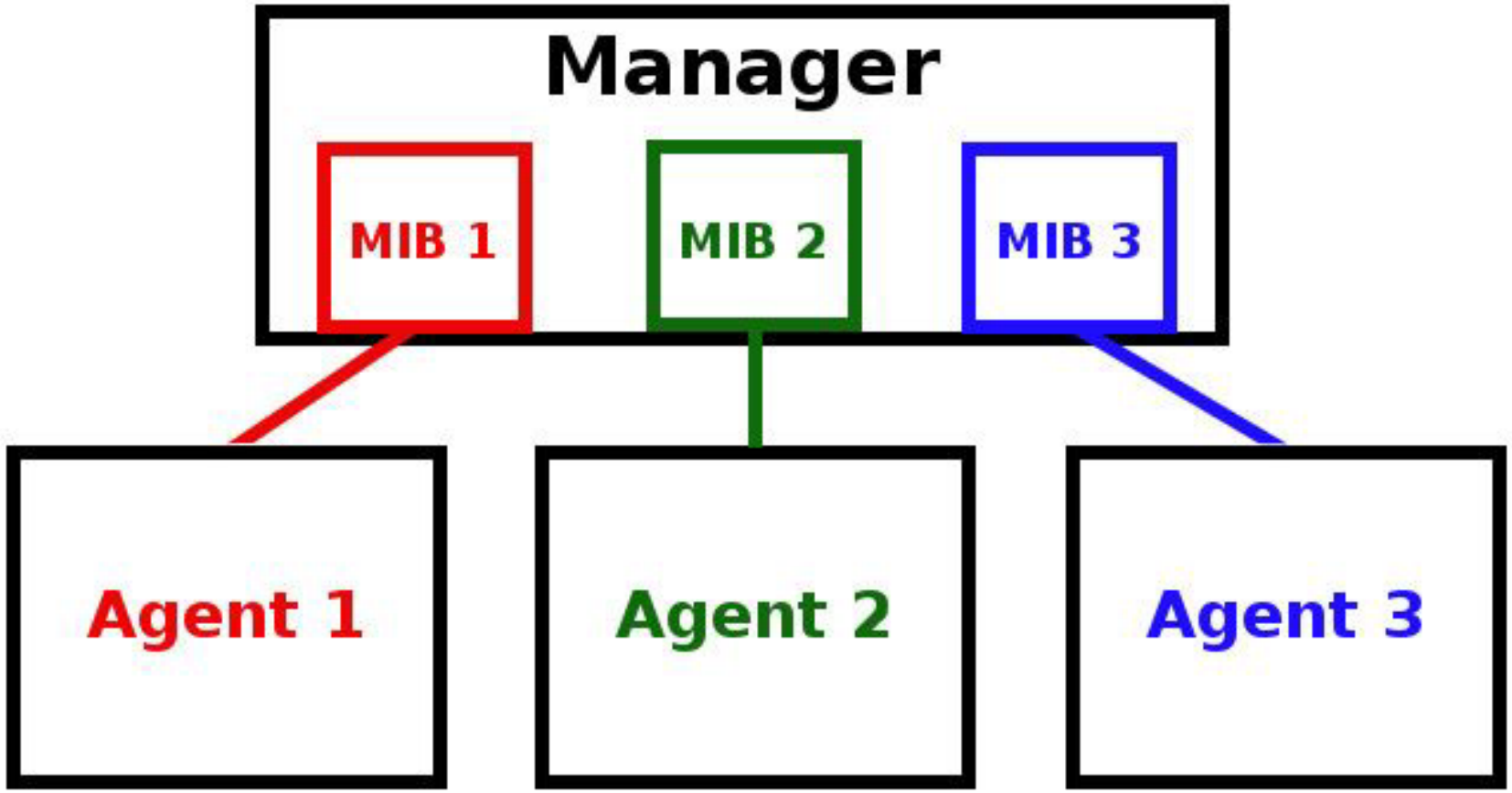
- Represents a single "question" an SMNP manager can ask an agent
- Identifies a very specific, unique counter on a device
- Has a corresponding name and data type
- When queried by manager, agent will return a value

Name/OID	Value	Type
.1.3.6.1.2.1.1.1.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0)	Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE ...	OctetString

MANAGEMENT INFORMATION BASE (MIB)

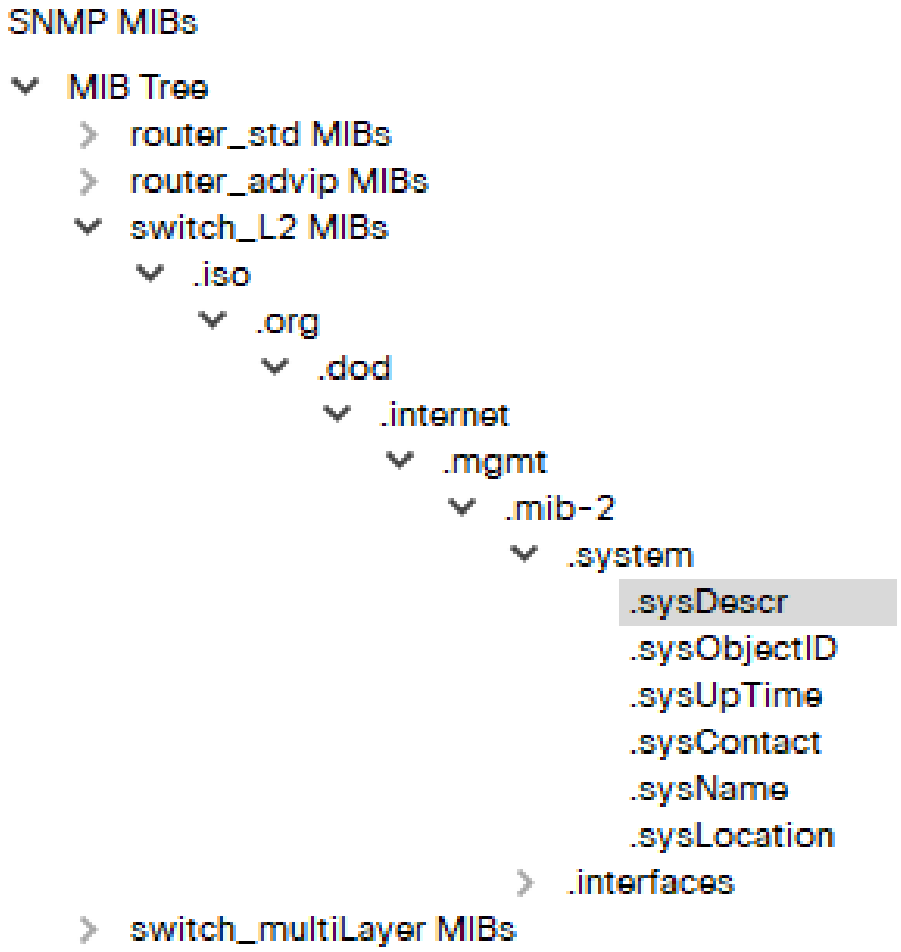
- A collection of OIDs stored in a text file
- A set of questions that an SNMP manager can ask a device regarding its status
- Standardized vendor-neutral MIBs define functionality common to all devices of the same type
- The manufacturer creates additional MIBs specific to their products
- An agent might use multiple MIBs to monitor one device
- Most SNMP managers have MIBs already installed
  - Vendor-neutral MIBs
  - Vendor-specific MIBs for popular products

SNMP MIBS AND AGENTS



MIB HIERARCHY

- All OIDs, regardless of manufacturer, are part of a global hierarchy
- Each OID is unique
- The SNMP manager must know what MIBs the agent is using
  - At least know a starting OID to query
  - The manager can then repeatedly issue a "get-next" command
  - The agent will provide information about successive OIDs
  - The manager does not need to OIDs for every single counter on the device



SNMP ENUMERATION

- SNMP is a good target for enumeration
- Often the defaults are not changed:
  - Community strings
  - Encryption levels
- Most versions use clear-text communications
  - Microsoft devices don't even support the encrypted version
  - You might be able to sniff community strings and manager-agent communications
- Many SNMP management tools include a feature to discover all the MIBs installed on the agents
- You can also "walk" the MIB
  - Start at a single common OID
  - Repeatedly ask the device to "get-next" until it runs out of OIDs to report on

INFORMATION SNMP CAN ENUMERATE

- Network devices
- Hosts
- Users and groups
- Services
- Installed software
- Network shares
- Device configurations
- IP and MAC addresses
- ARP tables
- Routing tables
- VLANs
- Port and interface status
- Network traffic
- and much, much more

SNMP ENUMERATION TOOLS

- Solar Winds Engineer's Toolset
- Nmap NSE scripts
  - There are 12 for snmp
- Metasploit snmp auxiliary modules
- Snmpwalk
- Snmpget
- SNMP Scanner
- Getif
- Observium
- OpUtils
- OIDVIEW SNMP MIB Browser
- iReasoning MIB Browser
- SNScan
- SoftPerfect Network Scanner
- SNMP Informant
- Net-SNMP
- NSauditor Network Security
- Spiceworks

COMMAND LINE SNMP ENUMERATION EXAMPLE

- `snmpget`
  - Query a single OID
- `snmpwalk`
  - Query an entire MIB starting from a particular OID

Snmpget and snmpwalk have the same syntax. Both Windows and Linux use these commands.

```
snmpget [options] [community string] [host name/address] [OID]
```

```
$ snmpget -v 2c 127.0.0.1 -c public .1.3.6.1.2.1.1.5.0
  SNMPv2-MIB::sysName.0 = STRING: centos7

$ snmpget -v 2c 127.0.0.1 -c public sysName.0
  SNMPv2-MIB::sysName.0 = STRING: centos7
```

METASPLOIT SNMP LOGIN ENUMERATION EXAMPLE

```
msf auxiliary(snmp_login) > run

[+] SNMP: 192.168.1.2 community string: 'public' info: 'GSM7224 L2 Managed Gigabit Switch'
[+] SNMP: 192.168.1.199 community string: 'public' info: 'HP ETHERNET MULTI-ENVIRONMENT'
[+] SNMP: 192.168.1.2 community string: 'private' info: 'GSM7224 L2 Managed Gigabit Switch'
[+] SNMP: 192.168.1.199 community string: 'private' info: 'HP ETHERNET MULTI-ENVIRONMENT'
[*] Validating scan results from 2 hosts...
[*] Host 192.168.1.199 provides READ-WRITE access with community 'internal'
[*] Host 192.168.1.199 provides READ-WRITE access with community 'private'
[*] Host 192.168.1.199 provides READ-WRITE access with community 'public'
[*] Host 192.168.1.2 provides READ-WRITE access with community 'private'
[*] Host 192.168.1.2 provides READ-ONLY access with community 'public'
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(snmp_login) >
```

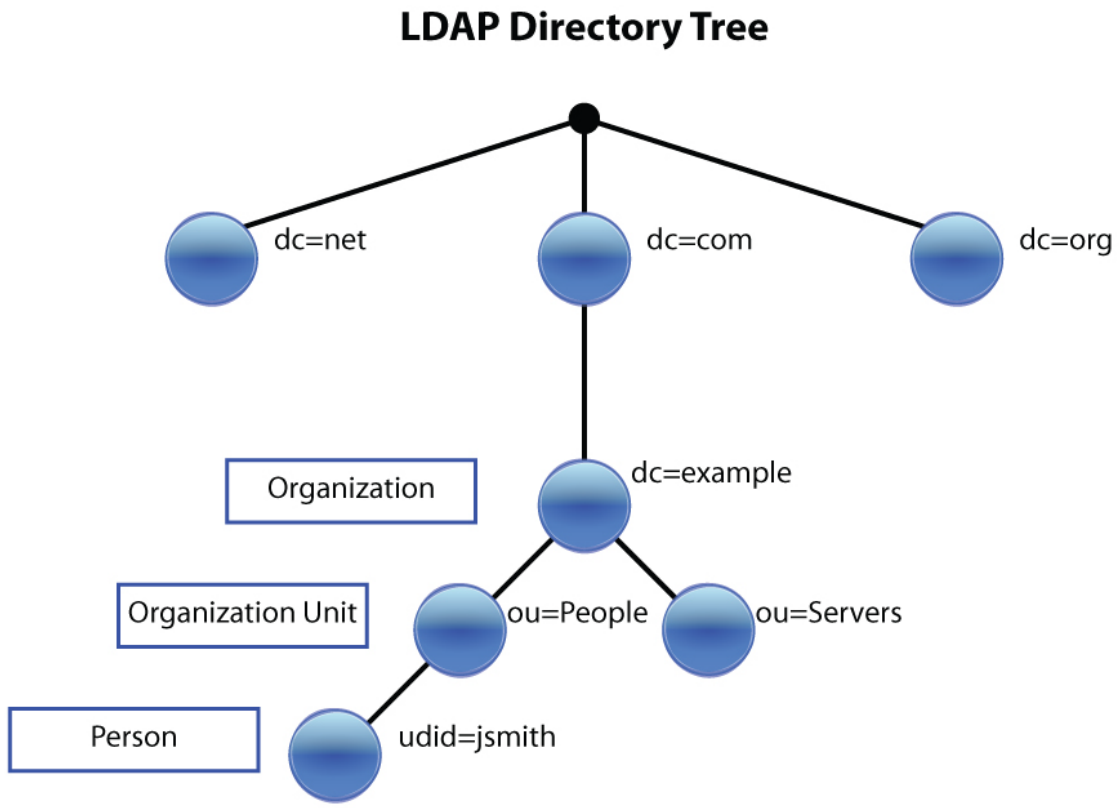
4.6 LDAP ENUMERATION

- LDAP
- X.500
- Tools

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

- The search and edit protocol for X.500-style directory service databases
- TCP 389
- Secure LDAP TCP 636
- Clear text by default
- Can be used to obtain a list of every object in the directory service database including:
  - User, Group, and Computer accounts
  - User department and contact information
  - Group membership
  - Network resource information
- Directory Service Examples:
  - Microsoft Active Directory Domain Services
  - Novell eDirectory
  - Open Software Foundation DCE Directory

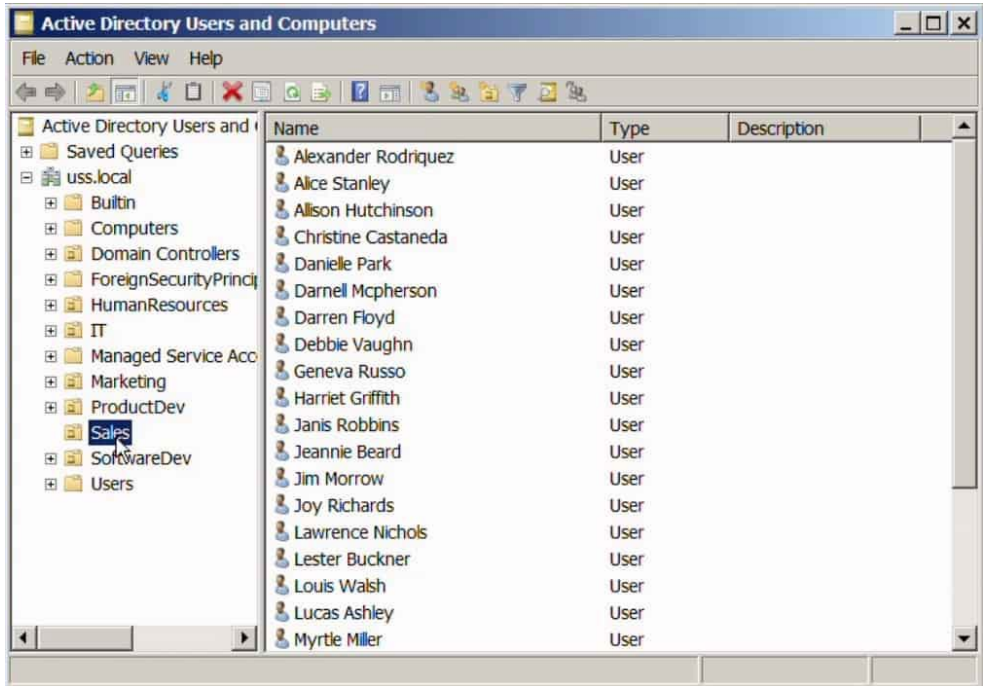
X.500 NAMING HIERARCHY



LDAP ENUMERATION TOOLS

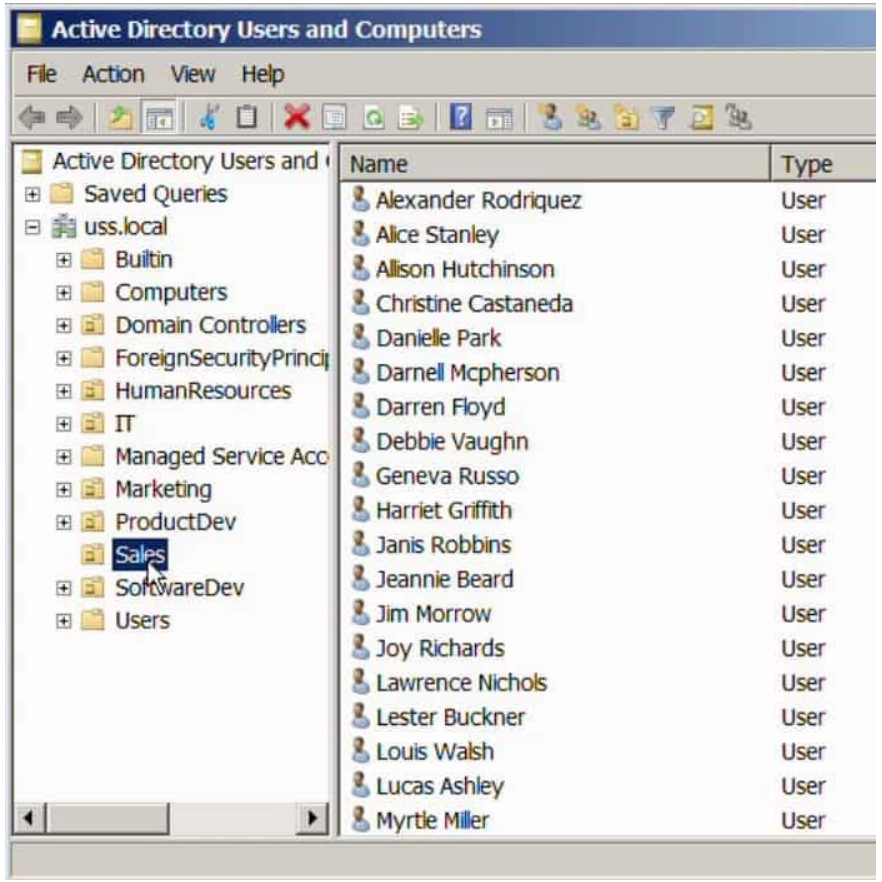
- Active Directory Users and Computers
- Softerra LDAP Administrator
- LDP.exe
- Metasploit auxiliary module ldap_hashdump
- Nmap NSE scripts for ldap
- JXplorer (available on www.jxplorer.org)
- Responder (available on GitHub)
  - This example queries an LDAP server out of eth0, forcing an LM hashing downgrade with verbose output

```
./Responder.py -I eth0 -rPv -I <server IP>
```



LDAP ENUMERATION EXAMPLE

```
PORT    STATE SERVICE REASON
389/tcp open  ldap    syn-ack
| ldap-search:
|   DC=cqure,DC=net
|     dn: CN=Administrator,CN=Users,DC=cqure,DC=net
|         sAMAccountName: Administrator
|     dn: CN=Guest,CN=Users,DC=cqure,DC=net
|         sAMAccountName: Guest
|     dn: CN=SUPPORT_388945a0,CN=Users,DC=cqure,DC=net
|         sAMAccountName: SUPPORT_388945a0
|     dn: CN=EDUSRV011,OU=Domain Controllers,DC=cqure,DC=net
|         sAMAccountName: EDUSRV011$
|     dn: CN=krbtgt,CN=Users,DC=cqure,DC=net
|         sAMAccountName: krbtgt
|     dn: CN=Patrik Karlsson,CN=Users,DC=cqure,DC=net
|         sAMAccountName: patrik
|     dn: CN=VMABUSEXP008,CN=Computers,DC=cqure,DC=net
|         sAMAccountName: VMABUSEXP008$
|     dn: CN=ldaptest,CN=Users,DC=cqure,DC=net
|_        sAMAccountName: ldaptest
```



4.7 DNS ENUMERATION

- DNS
- Tools
- NSLookup
- DIG

DNS ENUMERATION

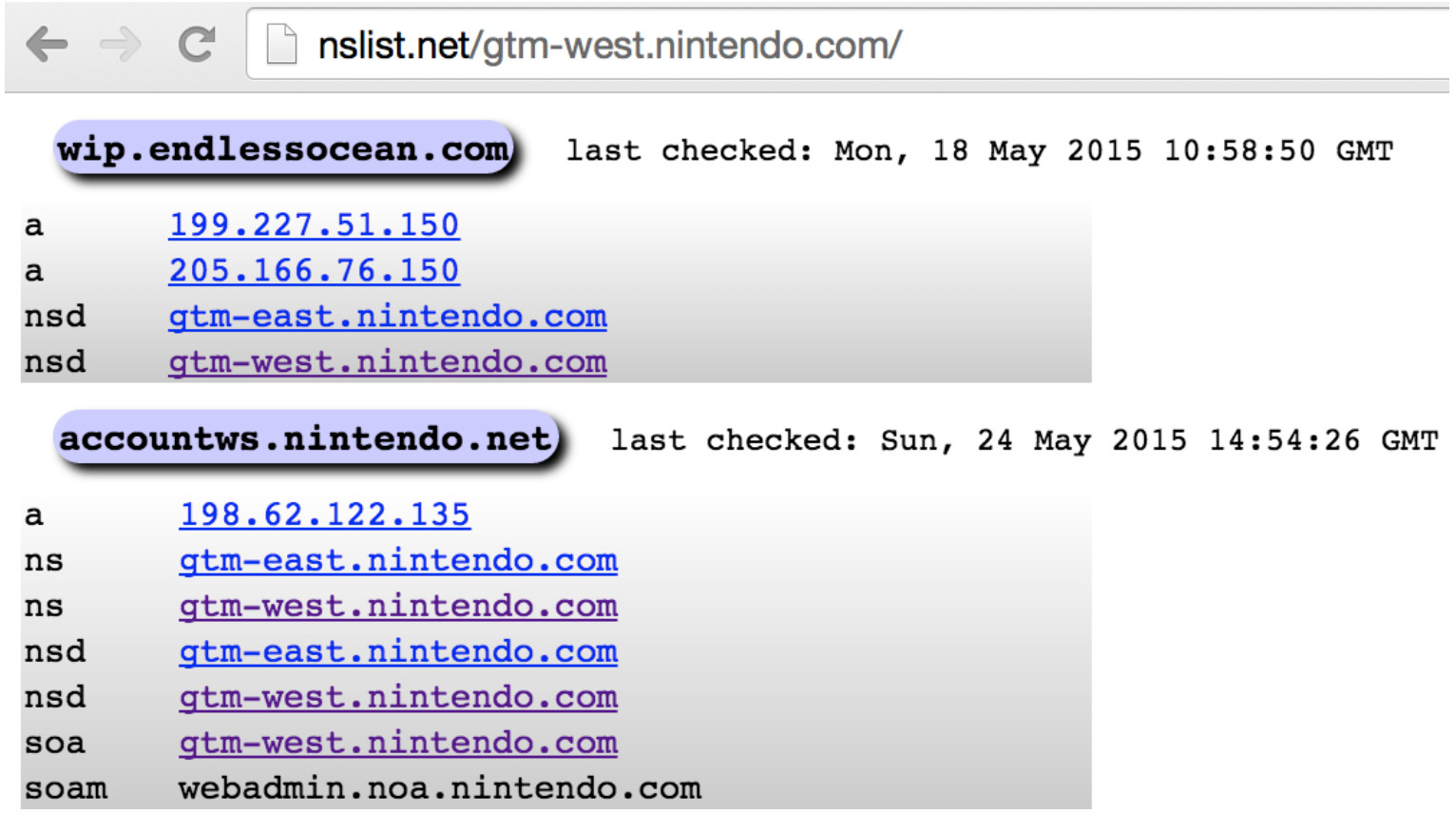
- Query a DNS server for its records:
  - A, AAAA
  - NS
  - MX
  - CNAME
  - PTR
  - SOA
- Obtain individual records or "zone transfer" the entire database file
  - Exploit DNS AXFR (all transfer) vulnerability
  - Some DNS servers will transfer their entire zone to any requestor without requiring authentication
  - This saves the attacker time
  - You can also just manually request all the various record types and end up with the same content

DNS ENUMERATION TOOLS

- Dig
- Fierce
- Nslookup
- Host
- dnsrecon.py
- dnsenum.pl
- Metasploit auxiliary module dns_enum
- Nmap NSE script dns-brute
- SecurityTrails advanced DNS enumeration

SITES TO CROSS-REFERENCE DOMAINS, HOSTNAMES, AND IP ADDRESSES

- nslist.net
- iplist.net



DNSRECON ENUMERATION EXAMPLE

```
root@encode:/pentest/enumeration/dns/dnsrecon# ./dnsrecon.py -d cisco.com
[*] Performing General Enumeration of Domain: cisco.com
[-] DNSSEC is not configured for cisco.com
[*]      SOA dns-rtp2-2-l.cisco.com 64.102.255.43
[*]      NS ns2.cisco.com 64.102.255.44
[*]      NS ns1.cisco.com 72.163.5.201
[*]      MX alln-mx-01.cisco.com 173.37.145.198
[*]      MX rcdn-mx-01.cisco.com 72.163.7.166
[*]      MX ams-mx-01.cisco.com 64.103.36.169
[*]      MX rtp-mx-01.cisco.com 64.102.255.47
[*]      A cisco.com 198.133.219.25
[*]      AAAA cisco.com 2001:420:1101:1::a
[*]      TXT cisco.com v=spf1 ip4:171.68.0.0/14 ip4:64.100.0.0/14 ip4:64.104.0.0/16 ip4:72.1
63.7.160/27 ip4:72.163.197.0/24 ip4:128.107.0.0/16 ip4:144.254.0.0/16 ip4:66.187.208.0/20 ip
4:173.37.86.0/24 ip4:173.36.130.0/24 ip4:204.15.81.0/26 ip4:216.206.186.129/25 ip4:208.90.57
.0/26 mx:res.cisco.com ~all
[*] Enumerating SRV Records
[*]      SRV _sips._tcp.cisco.com vcsgw.cisco.com 64.102.249.41 5061 0
[*]      SRV _sip._tcp.cisco.com vcsgw.cisco.com 64.102.249.41 5060 0
[*]      SRV _h323ls._udp.cisco.com vcsgw.cisco.com 64.102.249.41 1719 0
[*]      SRV _h323cs._tcp.cisco.com vcsgw.cisco.com 64.102.249.41 1720 0
[*]      SRV _sipfederationtls._tcp.cisco.com sip.oscar.aol.com 205.188.153.55 5061 1
[*]      SRV _xmpp-server._tcp.cisco.com isj3jxf.webexconnect.com 66.163.36.133 5269 1
[*]      SRV _xmpp-client._tcp.cisco.com isj3cmx.webexconnect.com 66.163.36.130 5222 1
[*] 7 Records Found
```

NSLOOKUP

- Microsoft tool for querying DNS
  - `nslookup [-option] [name | -] [server]`
- You can also install on Linux
  - `sudo apt install dns-utils`
  - `sudo dnf install bind-utils`
- Depends on the existence of a reverse lookup zone to work properly

NSLOOKUP EXAMPLES

```
nslookup example.com

nslookup -type=ns example.com

nslookup -type=soa example.com

nslookup -query=mx example.com

nslookup -type=any example.com

nslookup example.com ns1.nsexample.com

nslookup 10.20.30.40

nslookup -type=ptr 96.96.136.185.in-addr.arpa
```

NSLOOKUP EXAMPLES

```
C:\Windows\system32>nslookup -type=mx eccouncil.org
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
eccouncil.org   MX preference = 0, mail exchanger = eccouncil-org.mail.protection.outlook.com
```

```
C:\Windows\system32>nslookup -type=A eccouncil-org.mail.protection.outlook.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    eccouncil-org.mail.protection.outlook.com
Addresses:  104.47.74.10
          104.47.73.10
```

DIG

- *Nix tool for querying DNS
- You can also install (slightly older version) on Windows
- Syntax:

```
dig Hostname

dig DomaiNameHere

dig @DNS-server-name Hostname

dig @DNS-server-name IPAddress

dig @DNS-server-name Hostname|IPAddress type
```

DIG EXAMPLES

```
dig www.example.com A
dig 74.125.236.167
dig +short example.com MX
dig +short example.com TXT
dig +short example.com NS
dig example.com ANY
```

DIG AND FIERCE ZONE TRANSFER EXAMPLES

- Try a zone transfer by guessing the domain that the server is authoritative for:

```
dig axfr @<DNS_IP> <DOMAIN>
```

- Try to perform a zone transfer against every authoritative name server
  - If it doesn't work, launch a dictionary attack:

```
fierce --domain <DOMAIN> --dns-servers <DNS_IP>
```

DIG EXAMPLE

```
C:\Users\Administrator>dig @8.8.8.8 ccsf.edu any

; <<>> DiG 9.8.5-P2 <<>> @8.8.8.8 ccsf.edu any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17281
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ccsf.edu.                      IN      ANY

;; ANSWER SECTION:
ccsf.edu.               3599    IN      TXT     "v=spf1 include:spf.protection.o
utlook.com -all"
ccsf.edu.               3599    IN      MX      0 ccsf-edu.mail.eo.outlook.com.
ccsf.edu.               21599   IN      A       147.144.1.212
ccsf.edu.               21599   IN      SOA     ns3.ccsf.edu. root.ccsf.edu. 201
4101500 43200 3600 1814400 10800
ccsf.edu.               21599   IN      NS      ns4.cenic.org.
ccsf.edu.               21599   IN      NS      ns6.cenic.org.
ccsf.edu.               21599   IN      NS      ns5.cenic.org.
ccsf.edu.               21599   IN      NS      ns3.ccsf.edu.

;; Query time: 62 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Jan 22 13:09:39 Pacific Standard Time 2015
;; MSG SIZE  rcvd: 267
```

DNS ENUMERATION EXAMPLE

- What do you see in this exhibit?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.d
omain.com. 131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 INSOA srv1.domain.com. hostsrv1.do
main.com. 131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

DNS ENUMERATION EXAMPLE

- The hacker used DIG to successfully transfer the zone and enumerate the hosts
- AXFR domain.com

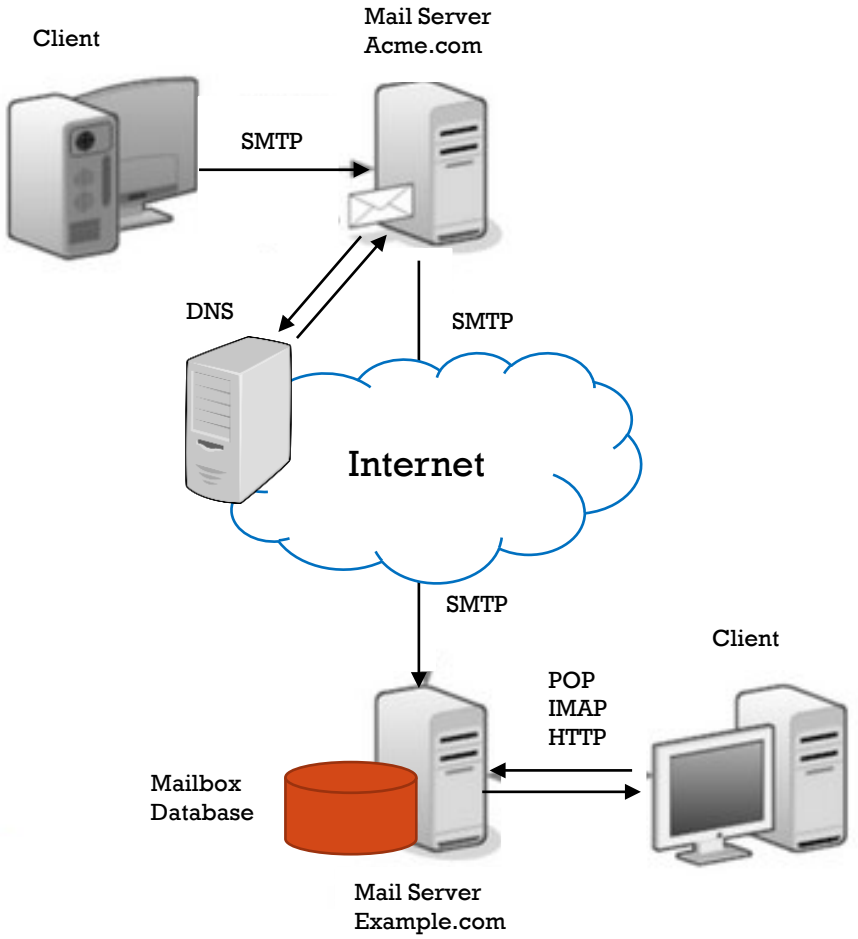
```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.d
omain.com. 131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 INSOA srv1.domain.com. hostsrv1.do
main.com. 131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

4.8 SMTP ENUMERATION

- Email
- SMTP
- Tools

HOW EMAIL WORKS

- ACME client uses SMTP to send email message to email server for acme.com
- Local email server performs DNS lookup to find MX record and IP address (A/AAAA record) of email server for example.com
- Acme.com email server uses SMTP to deliver message to example.com email server
- Example.com email server puts message into example.com client mailbox
- Example.com client later retrieves message using POP3, IMAP4, HTTP, or even RPC



SMTP ENUMERATION

- Simple Mail Transfer Protocol (SMTP) has three built-in commands
  - VRFY – validates that an email address actually exists for a user
  - EXPN – request or expand a mailing list into individual recipients
  - RCPT TO – Specifies the actual recipient(s)
- As an attacker, you can use the SMTP commands manually to enumerate valid email addresses

SMTP ENUMERATION TOOLS

- telnet
- netcat
- NetScanTool Pro
- smtp-user-enum
- smtp_user_enum.py
- Kali iSMTP
- Metasploit auxiliary module smtp_enum
- nmap NSE script smtp-enum-users

TELNET SMTP ENUMERATION EXAMPLE

```
telnet <email server> 25
vrfy test@example.com
```

If you receive a message **code 250,251,252:**

The server has accepted the request and the user account is valid

If you receive a message **code 550:**

The user account is invalid

SEND AN EMAIL USING TELNET

```
telnet mail.example.com 25
ehlo example.com
mail from: username@example.com
rcpt to: friend@hotmail.com, friend2@yahoo.com
data

Subject: My Telnet Test Email
Hello,
This is an email sent by using the telnet command.
Your friend,
Me

.

q
```

Send interactively, one line at a time

Send all at once, pressing <Enter>.<Enter> to finish

Press q to quit session

METASPLOIT SMTP ENUMERATION EXAMPLE

1. In Kali Linux, create a list of possible email addresses and save to your Desktop as user.txt
2. Open Metasploit Framework
3. In the Metasploit console enter these commands:

```
use auxiliary/scanner/smtp/smtp_enum
set rhosts <email server IP>
set rport 25
set USER_FILE /root/Desktop/user.txt
exploit
```

SMTP-USER-ENUM EXAMPLE

Verify that moo@example.com is a valid email address:

```
smtp-user-enum -M VRFY -D example.com -u moo -t <email server IP>
```

SMTP-USER-ENUM EXAMPLE

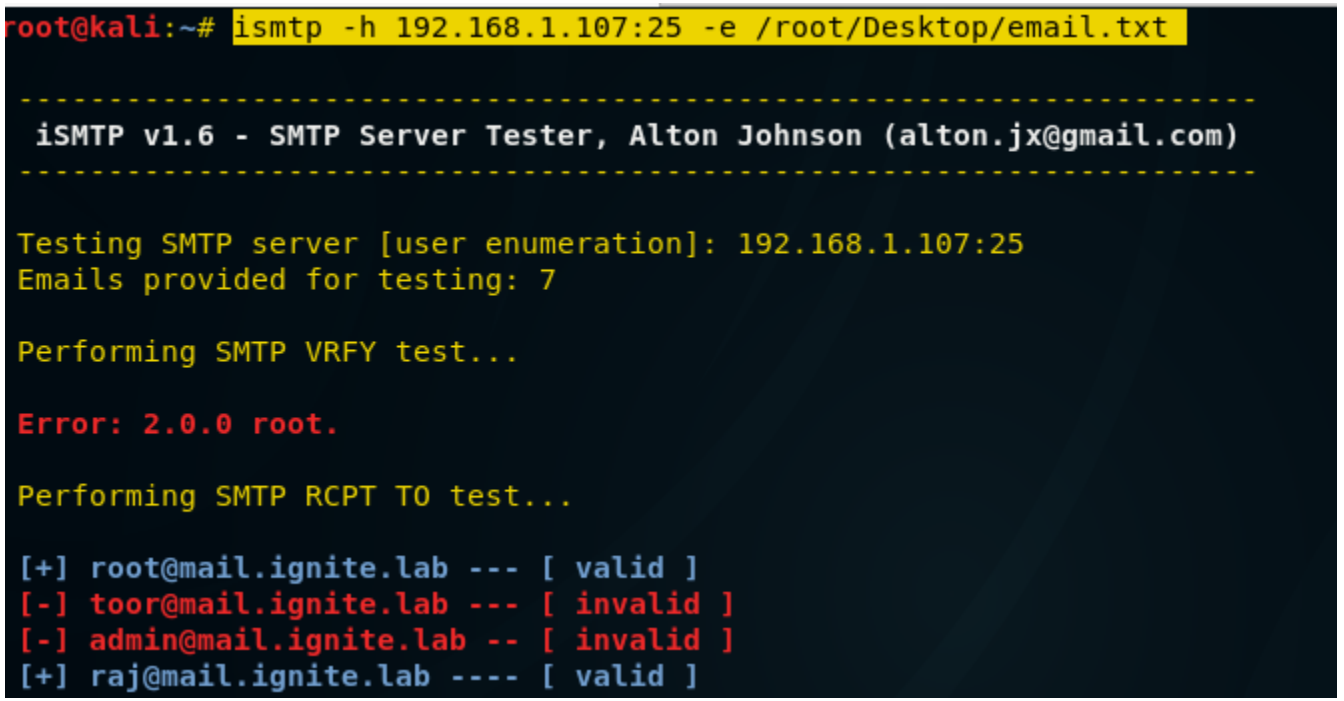
- Supply a list of usernames and verify if they exist:

```
root@kali:~# smtp-user-enum -M VRFY -U /root/Desktop/pass.txt -t 192.168.91.130
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /root/Desktop/pass.txt
Target count ............. 1
Username count ........... 25
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Apr  6 00:56:45 2017 #########
192.168.91.130: games exists
192.168.91.130: nobody exists
192.168.91.130: bind exists
```

ISMTP EXAMPLE

- Verify that email addresses supplied in the email.txt list actually exist

```
ismtp -h <email-server-IP>:25 -e /root/Desktop/email.txt
```



4.9 REMOTE CONNECTION ENUMERATION

- Telnet
- SSH
- RPC

TELNET ENUMERATION

- TCP 23
- Used to obtain a command prompt of the remote host
- Can also be used to banner grab

```
telnet <target> <port>
```

- nmap has several telnet enumeration scripts
  - Run all nmap telnet scripts against a target:

```
nmap -n -sV -Pn --script "*telnet* and safe" -p 23 <target>
```

  - Brute force password via telnet

```
Nmap –script telnet-brute <target>
```

SSH ENUMERATION

- TCP 22
- Secure replacement for telnet
- Client and server exchange public keys to create a session key
- Includes Secure FTP (SFTP) and Secure Copy (SCP)
- Login syntax = `ssh <username>@<hostname>`
- Some SSH implementations have default usernames and passwords
  - Example: jailbroken iPhone SSH service uses `root / alpine`
- Nmap, Metasploit and Searchsploit have various tools for SSH enumeration and exploitation

SSH ENUMERATION EXAMPLE

1. Use nmap to determine if a host is running an SSH service
2. Use nmap to query the version of SSH
3. Use a Metasploit module to enumerate SSH users
4. Check the Kali searchsploit module to see if an enumeration (or other) exploit exists for the SSH service
5. Search for nmap scripts related to SSH enumeration

SSH ENUMERATION EXAMPLE STEP #1

Use nmap to determine if a host is running an SSH service

```
nmap <target>
```

```
Nmap scan report for 10.10.10.226
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp
```

SSH ENUMERATION EXAMPLE STEP #2

Run default nmap scripts to query the version of SSH

```
nmap -sC -sV <IP>
```

```
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
Run default script against target: nmap -sC -sV <IP>
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-03 08:05 EDT
Nmap scan report for 10.10.10.211
Host is up (0.17s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 fd:80:8b:0c:73:93:d6:30:dc:ec:83:55:7c:9f:5d:12 (RSA)
|   256 61:99:05:76:54:07:92:ef:ee:34:cf:b7:3e:8a:05:c6 (ECDSA)
|_  256 7c:6d:39:ca:e7:e8:9c:53:65:f7:e2:7e:c7:17:2d:c3 (ED25519)
```

SSH ENUMERATION EXAMPLE STEP #3

Use nmap scripts to enumerate users, brute force logins, obtain keys,etc.

```
ls /usr/share/nmap/scripts/ | grep ssh
```

```
root@kali:~# ls /usr/share/nmap/scripts/ | grep ssh
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
```

SSH ENUMERATION EXAMPLE STEP #4

Use Metasploit modules to enumerate SSH users or login information

```
search ssh_enumusers
search ssh_login
```

```
msf5 > search ssh_enumusers

Matching Modules
================

   Name                                    Disclosure Date  Rank    Check  Description
   ----                                    ---------------  ----    -----  -----------
   auxiliary/scanner/ssh/ssh_enumusers                      normal  Yes    SSH Username Enumeration
```

```
msf5 > search ssh_login

Matching Modules
================

   Name                                     Disclosure Date  Rank    Check  Description
   ----                                     ---------------  ----    -----  -----------
   auxiliary/scanner/ssh/ssh_login                           normal  Yes    SSH Login Check Scanner
   auxiliary/scanner/ssh/ssh_login_pubkey                    normal  Yes    SSH Public Key Login Scanner
```

SSH ENUMERATION EXAMPLE STEP #5

Use the Kali searchsploit module to search for version-specific exploits

```
searchsploit openssh
```

```
root@kali:~# searchsploit openssh
----------------------------------------------------- ----------------------------------------
 Exploit Title                                       |  Path
                                                     | (/usr/share/exploitdb/)
----------------------------------------------------- ----------------------------------------
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Esc | exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Se | exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution      | exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote Stack Overflow    | exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite            | exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration              | exploits/linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)        | exploits/linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One     | exploits/unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow | exploits/linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)  | exploits/unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)  | exploits/unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service | exploits/multiple/dos/2444.sh
```

REMOTE PROCEDURE CALL (RPC)

- TCP 135
- Used by Windows processes to make requests of each other over the network

RPC ENUMERATION TOOLS

- rpcinfo
  - Make a connection to an RPC server and receive information about that server
- rpcclient
  - Enumerate and manage domain and SAM users and SIDs, groups, shares, domain info, privileges and more
  - Will attempt to connect via null session
    - If this is unsuccessful a username and password must be supplied
- Nmap script msrpc-enum
  - Queries an MSRPC endpoint mapper for a list of mapped services
  - Displays the gathered information

RPCCLIENT COMMANDS

Command	Interface	Description
queryuser	SAMR	Retrieve user information.
querygroup	SAMR	Retrieve group information.
querydominfo	SAMR	Retrieve domain information.
enumdomusers	SAMR	Enumerate domain users.
enumdomgroups	SAMR	Enumerate domain groups.
createdomuser	SAMR	Create a domain user.
deletedomuser	SAMR	Delete a domain user.
lookupnames	LSARPC	Look up usernames to SID values.

SAMR = Security Account Manager (SAM) Remote Protocol
LSARPC = Local Security Authority (Domain Policy) Remote Protocol

RPCCLIENT COMMANDS (CONT'D)

Command	Interface	Description
lookupsids	LSARPC	Look up SIDs to usernames (RID cycling).
lsaaddacctrights	LSARPC	Add rights to a user account.
lsaremoveacctrights	LSARPC	Remove rights from a user account.
dsroledominfo	LSARPC-DS	Get primary domain information.
dsenumdomtrusts	LSARPC-DS	Enumerate trusted domains within an AD forest

RPCCLIENT EXAMPLES

```
┌──(root kali)-[~]
└─# rpcclient -U Administrator%Ignite@123 192.168.1.172
rpcclient $> srvinfo
        192.168.1.172  Wk Sv Sql PDC Tim Din NT
        platform_id     :       500
        os version      :       10.0
        server type     :       0x80142f
```

```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[yashika] rid:[0x44f]
user:[geet] rid:[0x450]
user:[aarti] rid:[0x451]
user:[raj] rid:[0x642]
user:[pavan] rid:[0x643]
user:[SVC_SQLService] rid:[0x838]
user:[jeenali] rid:[0x83a]
user:[japneet] rid:[0x83b]
user:[ignite] rid:[0x83c]
```

```
rpcclient -U "" 192.168.1.20

srvinfo
lookupnames administrator
lookupsids
enumdomusers
```

4.10 WEBSITE ENUMERATION

- Overview
- Methods
- Tools

WHAT CAN A WEBSITE REVEAL?

- Usernames and passwords
- Email addresses and contact information
- Domain names, host names and IP addresses
- Links and URLs
- Technologies used by the organizations
- Employee, customer and other confidential information
- Internal resources
- Potential vectors for attack

USING A BROWSER TO ENUMERATE

- The simplest way to start website enumeration
- View the HTML source of a web page
- Attempt to open a browser to popular directory names
- Note the HTTP response code:
  - 404 = "Not Found“
  - 403 = "Forbidden“
  - 402 = "Payment Required“
  - 401 = "Unauthorized" (Must authenticate first)
  - 200 = "OK“
- Directories that don't return a 404 exist
  - `http://www.example.tld/admin (401)`
  - `http://www.example.tld/content (402)`
  - `http://www.example.tld/cgi-bin (403)`
  - `http://www.example.tld/test (404)`
  - `http://www.example.tld/logs (200)`

BANNER GRABBING WITH TELNET AND NETCAT

Using Telnet

```
telnet 192.168.10.100 8000
```

After making the connection, press **Ctrl+]** to break, then enter quit

Using Netcat

```
echo -en "GET / HTTP/1.0\n\n\n"| nc www.comptia.org 80 | grep Server
```

NON-STANDARD PORTS

- Some websites are deliberately configured to use non-standard ports
- nmap -sV can detect this

```
nmap -PN -sT -sV -p0-65535 <target>
```

NMAP WEBSITE ENUMERATION SCRIPTS

- nmap --script=http-enum <target>
- nmap --script=http-drupal-enum <target>
- nmap –-script=http-php-version <target>
- nmap --script=http-webdav-scan <target>
- nmap --script=http-wordpress-enum <target>

METASPLOIT WEBSITE SCANNING MODULES

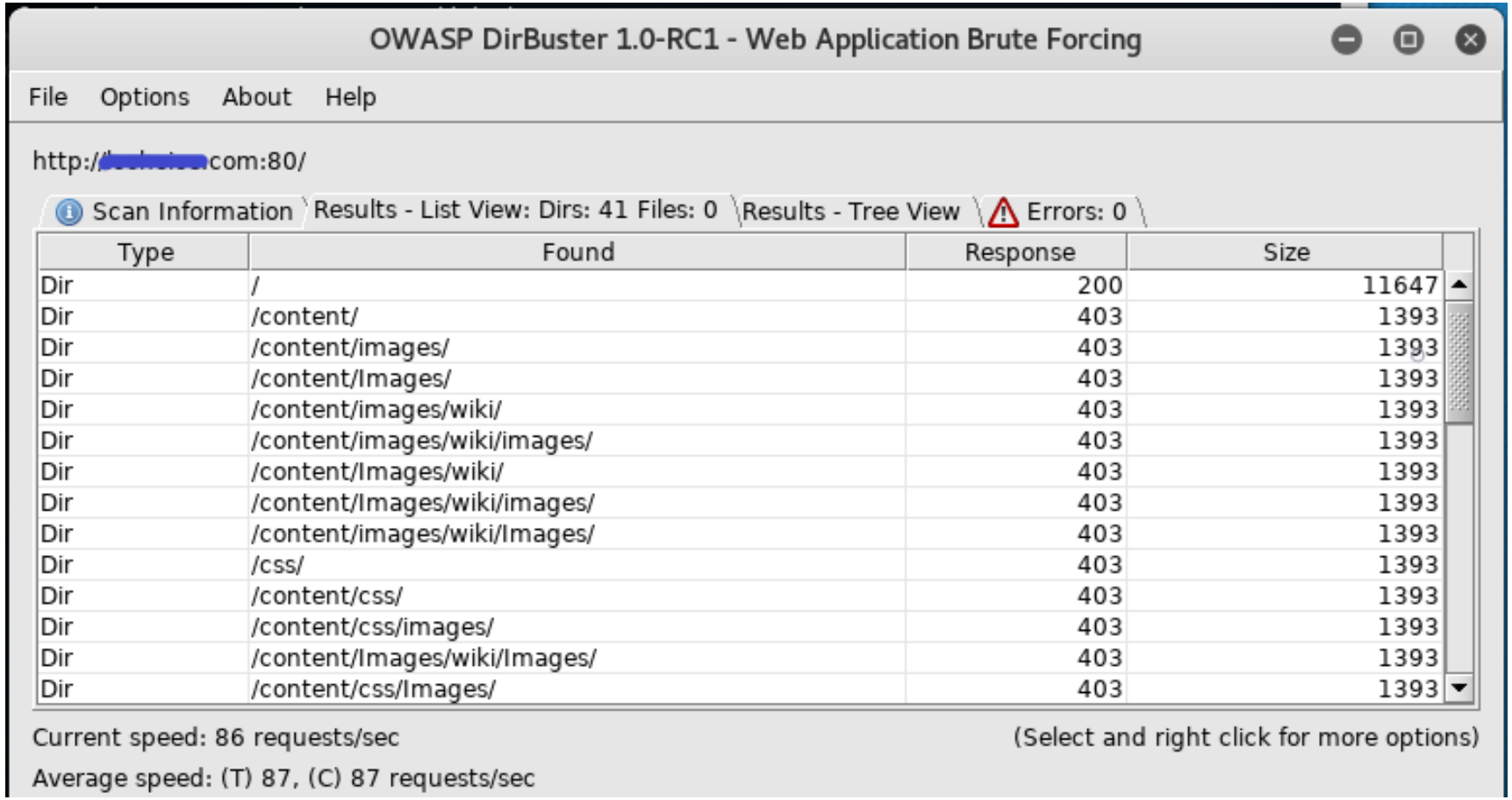
Metasploit has 281 web scanning modules including:

- auxiliary/scanner/http/apache_userdir_enum
- auxiliary/scanner/http/tomcat_enum
- auxiliary/scanner/http/chromecast_webserver
- auxiliary/scanner/http/brute_dirs.
- auxiliary/scanner/http/dir_listing
- auxiliary/scanner/http/dir_scanner
- auxiliary/scanner/http/http_version
- auxiliary/scanner/http/wordpress_login_enum

WEBSITE ENUMERATION TOOLS

- Enumeration Techniques:
  - Google Dorks
  - Word lists
  - Brute Forcing
  - Third party services
  - SSL Certificates
  - DNS Zone Transfer
- Web Technologies Used:
  - Whatweb
  - Wappalyzer
  - Netcraft
  - IDServe
- Subdomain Enumeration:
  - Wfuzz
  - WPScan
  - Amass
  - Assetfinder
  - SubBrute
  - SubExtractor
  - Subfinder
  - Sublist3r
  - PureDns
- Hidden Objects Enumeration:
  - DirBuster
  - Dirb
  - dirsearch.py
  - GoBuster
  - Ffuf
  - feroxbuster

DIRBUSTER EXAMPLE



4.11 OTHER ENUMERATION TYPES

- NTP
- VoIP
- IPSEC
- IPv6
- BGP

NTP ENUMERATION

- Network Time Protocol (NTP) is used to synchronize clocks of network devices
- UDP 123
- Can maintain time to within 10 milliseconds over the public Internet
- Attackers query NTP for
  - List of hosts connected to NTP server
  - Clients IP addresses, system names, and operating systems
  - Internal IP addresses can be acquired if the NTP server is on the DMZ

Active Directory clients use Windows Time (not NTP) to synchronize their clocks to the domain
The Active Directory PDC Emulator domain controller is the time source for the domain.
It can synchronize to other sources via NTP.

NTP COMMANDS

- Ntpdate
  - Query a time server

```
ntpdate -q pool.ntp.org
```

- Ntptrace
  - Traces a chain of NTP servers back to the primary source

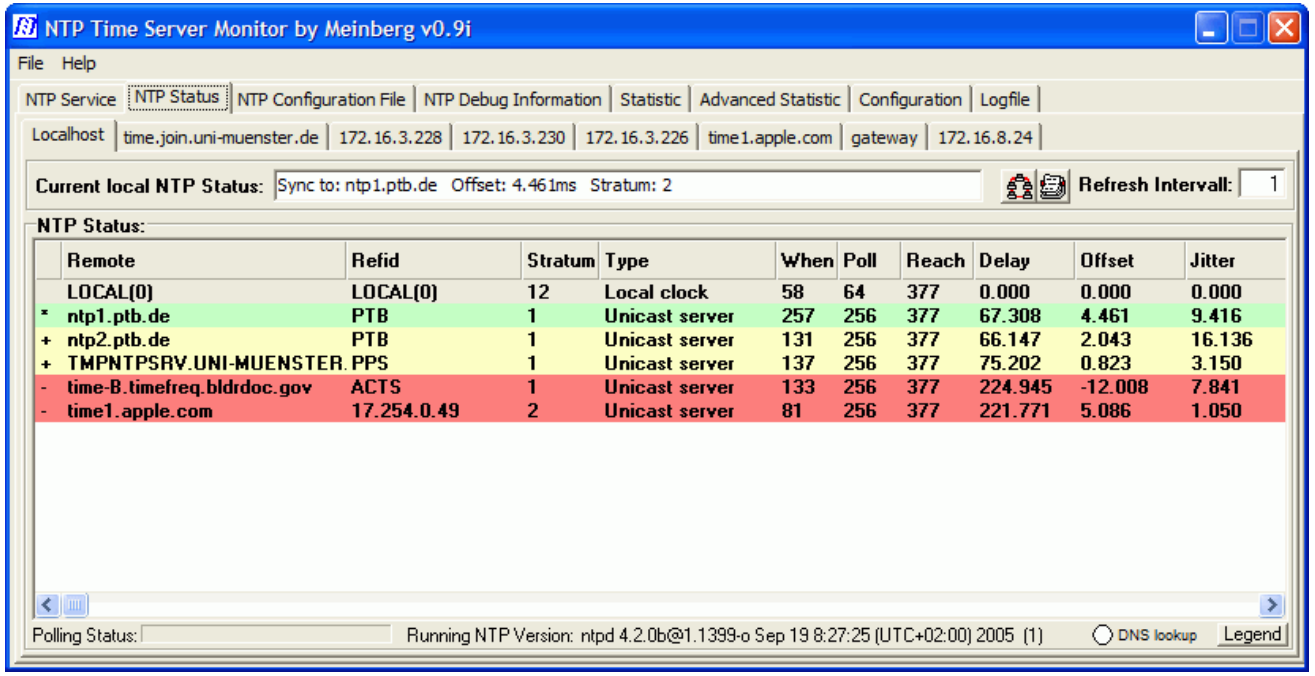
```
ntptrace
```

- Ntpdc
  - Monitors operation of the NTP server
  - This example requests the last 600 clients that connected to the NTP time server:

```
ntpdc -n -c monlist <IP or hostname of time server>
```

NTP ENUMERATION TOOLS

- NTP Time Server Monitor
- NTP Server Scanner
- Nmap
- Wireshark
- AtomSync
- NTPQuery
- PresenTense NTP Auditor
- PresenTense Time Server
- PersenTense Time Client
- NTP Time Server Monitor
- LAN Time Analyser



VOIP ENUMERATION

- VoIP uses SIP (Session Initiation Protocol) to manage voice and video calls over IP
  - TCP 5060 - Clear Text
  - TCP 5061 - SIP-TLS (encrypted)
- Data is carried by:
  - Real-time Transport Protocol (RTP) UDP 5004
  - and Real-time Transport Control Protocol (RTCP UDP 5005)
- VoIP enumeration provides sensitive information such as:
  - VoIP gateway (connects SIP system to PSTN)
  - IP-PBX systems (routes calls inside the VoIP network)
  - client software
  - user phone extensions
- This information can be used to launch various VoIP attacks such as:
  - DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, etc.

VOIP ENUMERATION (CONT'D)

Discover target VoIP information through:

- Google search and Shodan for public information
- Nmap and Sipvicious to map the internal VoIP network
- Wireshark to identify SIP users
- Job sites that list knowledge of a specific VoIP system as a skills requirement

Search for the following information:

- The public IP of the server
- The VoIP network / infrastructure
- Devices connected to the VoIP network, their open ports, and running services
- Users information (extension, the device information, and logs)
- Information about the VoIP server (model, vendor, OS, ports, etc.)

GOOGLE DORKS TO FIND VOIP TARGETS

Google Dork	Description
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
inurl:"NetworkConfiguration" cisco	Find the Cisco phone details
inurl:"ccmuser/logon.asp"	Find Cisco call manager
intitle:asterisk.management.portal web-access	Finds the Asterisk web mgmt portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:" SPA Configuration"	Search Linksys phones

Note: Asterisk is a popular open source IP PBX

SIPVICIOUS

- A SIP auditing tool used to scan for and enumerate SIP devices and accounts
- Sends SIP INVITE or OPTION packets looking for responses from live hosts
  - Logs the results to a file
- Attacks include:
  - SIP flood, RTP flood, SIP enumeration, Digest leak, RTP Bleed and RTP inject, fuzzing


```
recv 410 bytes from udp/[163.172.88.109]:5103 at 03:11:13.624446:
   ----------------------------------------------------------------------
   OPTIONS sip:50901@158.69.       SIP/2.0
   Via: SIP/2.0/UDP 127.0.1.1:5103;branch=z9hG4bK-1476081341;rport
   Content-Length: 0
   From: "sipvicious"<sip:100@1.1.1.1>;tag=396534353461623731336334013130313231353436373 2
   Accept: application/sdp
   User-Agent: friendly-scanner
   To: "sipvicious"<sip:100@1.1.1.1>
   Contact: sip:50901@127.0.1.1:5103
   CSeq: 1 OPTIONS
   Call-ID: 5449423760275061575872 19
   Max-Forwards: 70
```

SIPVICIOUS EXAMPLE

```
root@kali:~# svmap 192.168.1.0/24 -v

INFO:ImaFly:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:ImaFly:Looks like we received a SIP request from 192.168.1.20:5060
INFO:ImaFly ip:Looks like we received a SIP request from 192.168.1.21:5060
INFO:ImaFly:Looks like we received a SIP request from 192.168.1.22:5060
```

IPSEC ENUMERATION

- IPSEC VPNs are digitally signed and optionally encrypted using DES, 3DES or AES
- You can use nmap or other scanners to identify IPSEC VPN servers
- Internet Key Exchange (IKE) is the handshake protocol used at the start of an IPSEC session
- You can also use `ike-scan` and `psk-crack` to try to capture and crack an IKE pre-shared key hash

IKE-SCAN

- A command-line tool that uses the IKE protocol to discover, fingerprint and test IPsec VPN servers
- Can do two things:
  - Determine which hosts are running IKE
    - This is done by displaying those hosts which respond to the IKE requests sent by ike-scan.
  - Determine which IKE implementation the hosts are using
    - Done by recording the times of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns.
  - Can identify VPNs from manufacturers including Checkpoint, Cisco, Microsoft, Nortel, and Watchguard

PSK-CRACK

- Attempts to crack IKE Aggressive Mode pre-shared keys
  - Keys must have been previously gathered using **ike-scan** with the **--pskcrack** option
- Can work in dictionary or brute-force mode

```
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "123456" matches SHA1 hash d46e5c224092fedda5a1733aa71e515d0dfbb97e
Ending psk-crack: 1 iterations in 0.014 seconds (72.87 iterations/sec)
```

DNS IPV6 GRINDING

- You can identify IPv6 servers through DNS grinding
- DNS grinding is a dictionary attack using a list of possible host names
  - Uses AAAA requests
- Grinding tools include:
  - dnsdict6
  - dnsrevenum6
  - These are part of the thc-ipv6 tool suite

```
sudo apt install thc-ipv6
```

IPV6 ENUMERATION EXAMPLE

```
# dnsdict6 -4 -t 16 example.com
Starting enumerating example.com. - creating 16 threads for 798 words...
Estimated time to completion: 1 to 1 minute

Detected openDNS, this might increase performance
Warning: wildcard domain configured
*.example.com. ->2606:2800:220:1:248:1893:25c8:1946
Warning: wildcard domain configured (2nd test)
www.example.com. ->2606:2800:220:1:248:1893:25c8:2033
www.example.com. -> 93.184.216.34

Found 1 domain name, 1 unique ipv4 and 2 unique ipv6 addresses for example.com.
```

BGP

- Border Gateway Protocol (BGP) is the routing protocol used on the Internet
- ISPs use BGP to choose Internet routes
  - BGP has slow convergence
  - An entire Autonomous Systems is treated as a “hop”
- Traffic between Internet-based networks is controlled by using BGP and autonomous system (AS) numbers

BGP (CONT'D)

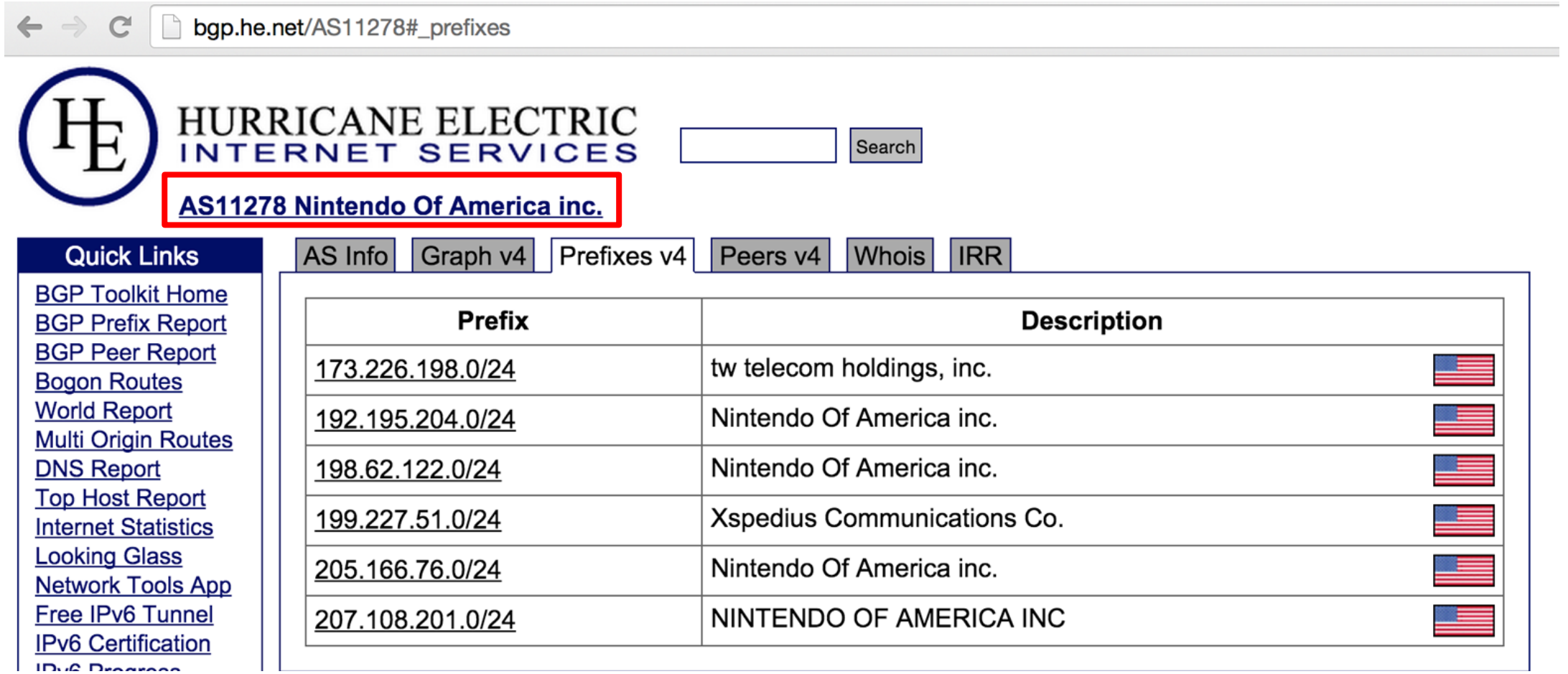
- Organizations use BGP
- IANA assigns AS numbers to RIRs
- RIRs allocate numbers to ISPs and large organizations so that they can manage their IP router networks and upstream connections.
- You can use whois and HE BGP Toolkit to enumerate:
  - An organization's AS numbers and IP addresses (referred to as "prefixes")
- Knowing IP addresses gives you targets to scan

BGP ENUMERATION EXAMPLE

- Whois query reveals netblocks and AS numbers for the company Nintendo

```
whois -a "nintendo*"

Nintendo Of America inc. NINTENDO-COM (NET-205-166-76-0-1)
205.166.76.0 - 205.166.76.255
NINTENDO HEADQUARTERS 1 NINTENDOHEADQUARTERS1 (NET-70-89-123-72-1)
70.89.123.72 - 70.89.123.79

Nintendo Of America inc. (AS11278) NINTENDO 11278
```

BGP ENUMERATION EXAMPLE (CONT'D)



4.12 ENUMERATION COUNTER-MEASURES AND REVIEW

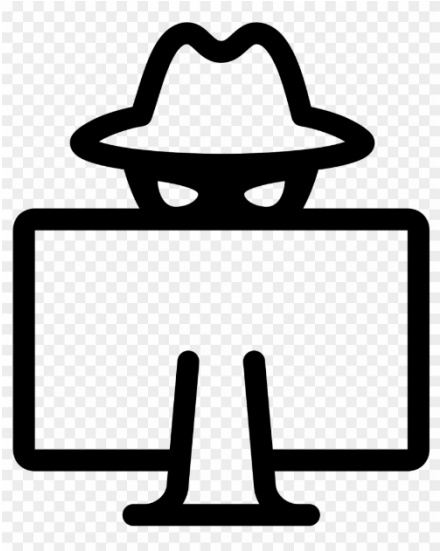
- Countermeasures
- Review

ENUMERATION COUNTERMEASURES

- When possible, use protocols that are encrypted, rather than clear text
- Disable NetBIOS and SMBv1
- Change the SNMP community string
- Disallow DNS zone transfers to unknown servers
- Maintain separate DNS servers for internal and public records (split DNS)
- Consider disabling VRFY and EXPN commands on your email server
- Use file system and share permissions to restrict access to sensitive content
- Perform your own enumeration to see what types of information an attacker can obtain
  - Remediate when possible

ENUMERATION REVIEW

- Enumeration is the systematic process of querying a target's servers and services for information
- Enumeration should appear to the server as a normal client making legitimate information requests
- You can enumerate information about the OS, its services, users and groups, network information, machine names, configuration settings, installed apps and service banners



- Many network protocols can be used for enumeration including:
  - NetBIOS/SMB, FTP/TFTP, NFS
  - SNMP
  - Telnet, SSH, RPC
  - SMTP
  - HTTP, DNS,
  - LDAP, SQL, NTP
  - IPSEC, IPv6, SIP, BGP and others