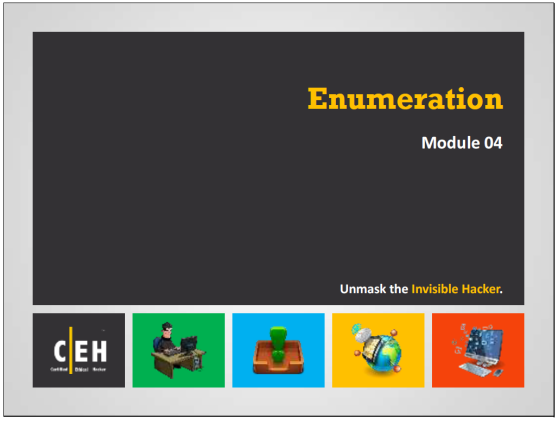
Enumeration

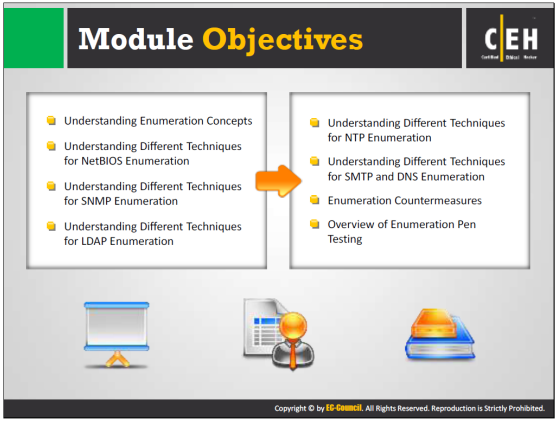
Module 04



Ethical Hacking and Countermeasures v9

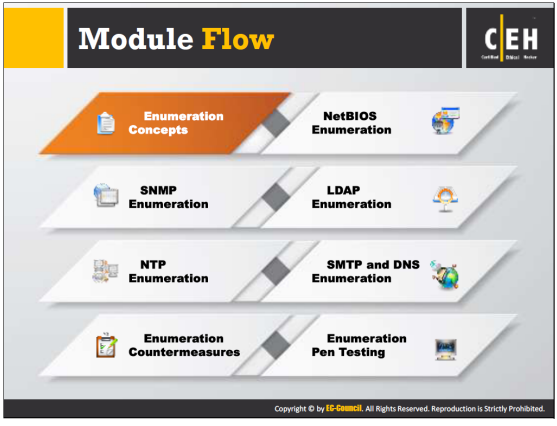
Module 04: Enumeration

Exam 312-50

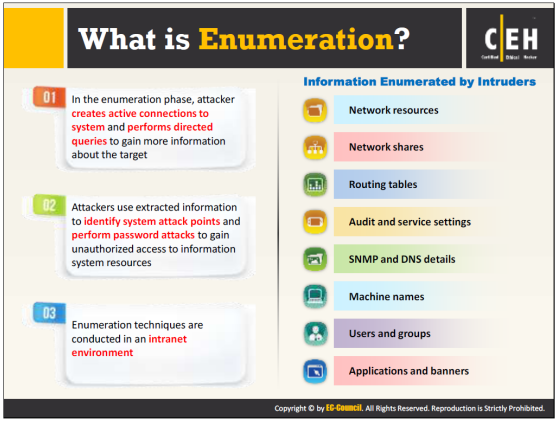


In the previous modules, you learned about footprinting and scanning networks. The next phase is enumeration.

This module starts with an introduction to enumeration concepts. The module provides an insight into different techniques for NETBIOS, SNMP, LDAP, NTP, SMTP, and DNS enumeration. Later the module discusses enumeration countermeasures. The module ends with an overview of pen testing steps that an ethical hacker should follow to perform a security assessment of a target.



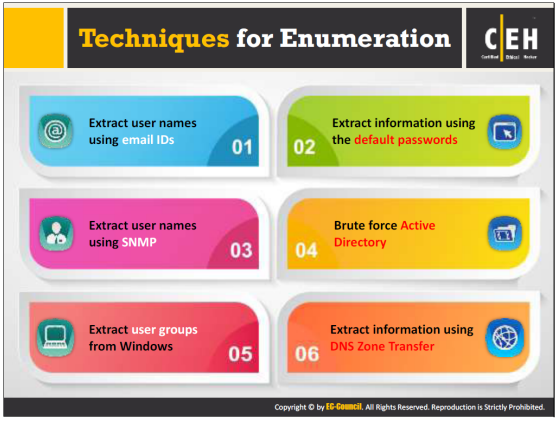
Each section of this module deals with different services and ports to enumerate. Before beginning with the actual enumeration process, we will discuss enumeration concepts.



Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system or network. In the enumeration phase, attackers create active connections to the target system and perform directed queries to gain more information about the target. The attackers use the information collected by means of enumeration to identify the vulnerabilities or weak points in the system security, which helps them exploit the target system. Enumeration techniques work in an intranet environment.

During enumeration attackers may stumble upon a remote IPC share, such as IPC$ in Windows, which they can probe further for null sessions to collect information about other shares and system accounts.

The previous modules highlighted how attackers gather necessary information about a target without really getting on the wrong side of the legal barrier. However, enumeration activities may be illegal depending on the organization policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing enumeration.



To extract information about a target:

- **Extract user names using email IDs**

  Every email address contains two parts: the user name and the domain name. The structure of an email address is username@domainname. Consider abc@gmail.com; in this email address, the "abc" (the string of characters preceding the '@' symbol) is the user name and "gmail.com" (the string of characters following the '@' symbol) is the domain name.

- **Extract information using the default passwords**

  Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often neglect to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases the task of an attacker in enumerating and exploiting the target system.

- **Brute force Active Directory**

  Microsoft Active Directory is susceptible to a username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid user names. An attacker who succeeds in extracting valid user names can conduct a brute-force attack to crack the respective passwords.

- **Extract information using DNS Zone Transfer**

  A network administrator can use DNS Zone Transfer to replicate Domain Name System (DNS) data across a number of DNS servers, or to back up DNS files. The administrator needs to execute a specific zone transfer request to the name server. If the name server permits zone transfer, it will convert all the DNS names and IP addresses hosted by that server to ASCII text.

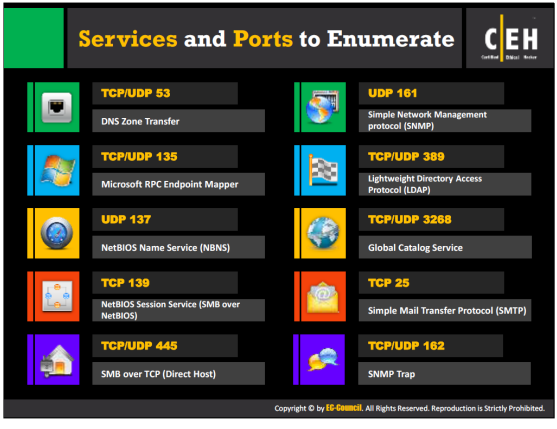
  If the network administrators did not configure the DNS server properly, the DNS Zone transfer is an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup.

- **Extract user groups from Windows**

  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command line method.

- **Extract user names using SNMP**

  Attackers can easily guess the read-only or read-write community strings using the SNMP API to extract user names.



Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols manage data communications between terminals in a network.

TCP is a connection-oriented protocol. It is capable of carrying messages or email over the Internet. It provides a reliable multi-process communication service in a multi-network environment. The features and functions of TCP include:

- Supports acknowledgement for receiving data through sliding window acknowledgement system
- Provides automatic retransmission of lost or acknowledged data
- Provides addressing and multiplexing data
- Capability to establish, manage, and terminate the connection
- Offers quality of service transmission
- Provides congestion management and flow control.

UDP is a connectionless protocol, which provides unreliable service. It carries short messages over a computer network.

Applications include:

- Streaming audio
- Video

- Teleconferencing.

Services and TCP/UDP ports to enumerate might include:

TCP/UDP 53: DNS Zone Transfer

The DNS resolution process establishes communication between DNS clients and DNS servers. DNS clients send DNS messages to DNS servers listening on UDP port 53. In case the DNS message size exceeds the default size of UDP (512 octets), the response contains only data that UDP can accommodate, and the DNS server sets a flag to indicate the truncated response. The DNS client can now resend the request via TCP over port 53 to the DNS server. In this approach, the DNS server uses UDP as a default protocol and, in case of lengthy queries where UDP fails, uses TCP as a backup failover solution. Some malwares such as ADM worm, Bonk Trojan, etc., uses port 53 to exploit vulnerabilities within DNS servers. This can help intruders to launch attacks.

TCP/UDP 135: Microsoft RPC Endpoint Mapper

Source: *https://technet.microsoft.com*

RPC is a protocol used by a client system to request a service from the server. An endpoint is the protocol port on which the server listens for the client's remote procedure calls. RPC endpoint mapper enables RPC clients to determine the port number currently assigned to a specific RPC service. There is a flaw in the part of RPC that exchanges messages over TCP/IP. Failure results due to the incorrect handling of malformed messages. This affects the RPC endpoint mapper that listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC Endpoint Mapper process on a server, in order to launch a Denial of Service (DoS) attack.

UDP 137: NetBIOS Name Service (NBNS)

NBNS, also known as Windows Internet Name Service (WINS), provides name resolution service for computers running NetBIOS. NetBIOS Name Servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. The job of NBNS is to match IP addresses with NetBIOS names and queries. Attackers usually attack the name service first.

Typically, NBNS uses UDP 137 as its transport protocol. It can also use TCP 137 as its transport protocol for few operations, though this might never happen in practice.

TCP 139: NetBIOS Session Service (SMB over NetBIOS)

This is perhaps the most well-known Windows port. It is used to transfer files over a network. Systems use this port for both NULL Session establishment and file and printer sharing. A system administrator considering restricting access to ports on a Windows system should make TCP 139 a top priority. An improperly configured TCP 139 port can allow an intruder to gain unauthorized access to critical system files or the complete file system, resulting in data theft or other malicious activities.

TCP/UDP 445: SMB over TCP (Direct Host)

Windows supports file and printer sharing traffic using the Server Message Block (SMB) protocol directly hosted on TCP. In earlier OSs, SMB traffic required the NetBIOS over TCP (NBT) protocol to work on a TCP/IP transport. Direct hosted SMB traffic uses port 445 (TCP and UDP) instead of NETBIOS.

UDP 161: Simple Network Management protocol (SNMP)

Simple Network Management Protocol (SNMP) is widely used in network management systems to monitor network attached devices such as routers, switches, firewalls, printers, servers, etc. It consists of a manager and agents. The agent receives requests on Port 161 from the managers, and responds to the managers on Port 162.

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

LDAP is a protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. By default, LDAP uses TCP or UDP as its transport protocol over port is 389.

TCP/UDP 3268: Global Catalog Service

Microsoft's Global Catalog Server, a domain controller that stores extra information, uses port 3268; its database contains rows for every object in the entire organization instead of rows for only the objects in one domain. Global Catalog allows one to locate objects from any domain without having to know the domain name. LDAP in Global Catalog Server uses port 3268. This service listens to port 3268 through a TCP connection. Administrators use Port 3268 for troubleshooting issues in the Global Catalog by connecting to it using LDP.

TCP 25: Simple Mail Transfer Protocol (SMTP)

SMTP is a TCP/IP mail delivery protocol. It transfers email across the Internet and across the local network. It runs on the connection-oriented service provided by Transmission Control Protocol (TCP), and it uses well-known port number 25.

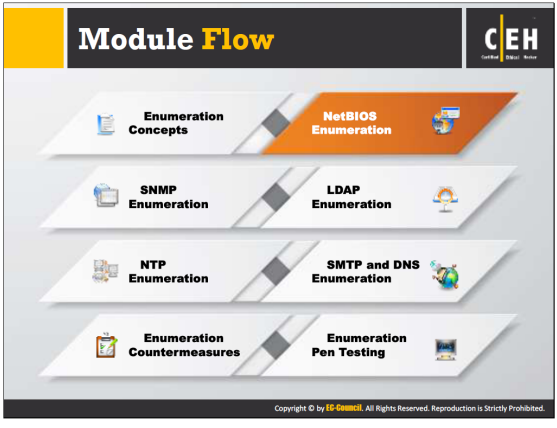
Some of the commands used by SMTP and their respective syntax:

Hello	HELO <sending-host>
From	MAIL FROM:<from-address>
Recipient	RCPT TO:<to-address>
Data	DATA
Reset	RESET
Verify	VRFY<string>
Expand	EXPN<string>
Help	HELP[string]
Quit	QUIT

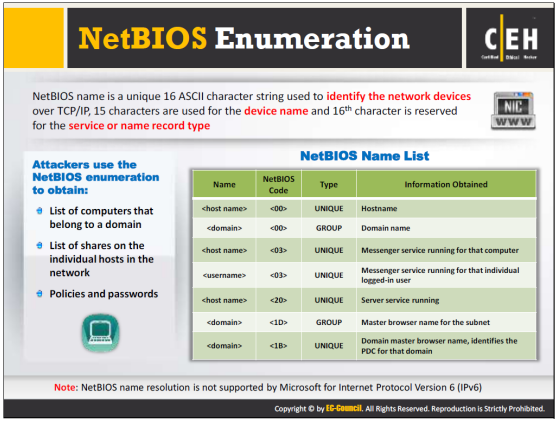
TABLE 4.1: SMTP commands and their respective syntax

TCP/UDP 162: SNMP Trap

Simple Network Management Protocol Trap (SNMP Trap) uses TCP/UDP port 162 to receive notifications such as optional variable bindings, sysUpTime value, etc., from agent to manager.



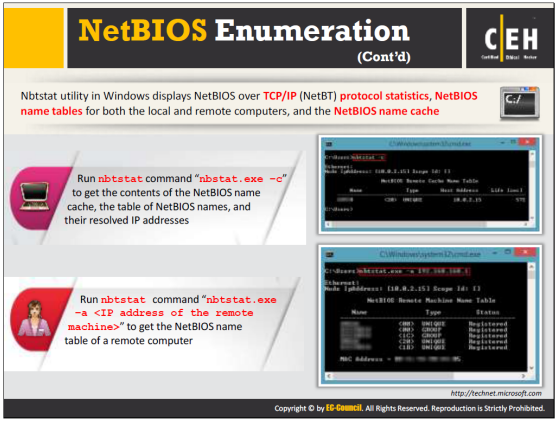
So far, we have discussed enumeration concepts and resources that provide valuable information. To enumerate the target network, consider NetBIOS first, as it extracts a lot of sensitive information about the target such as users, network shares, etc. This section describes NETBIOS enumeration, the information obtained, and various NETBIOS enumeration tools.



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

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

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



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

Nbtstat Syntax:

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

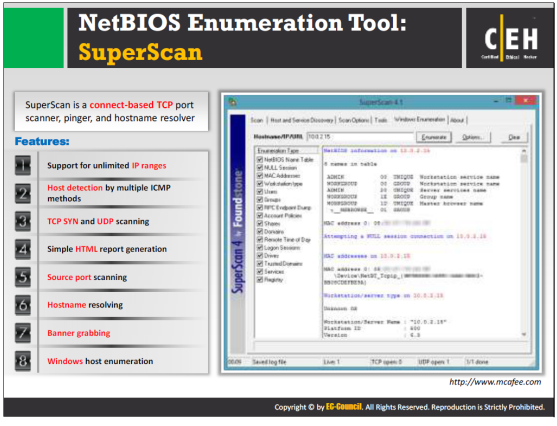
The table shown below displays various Nbtstat parameters and their respective functions:

Nbtstat Parameters	Function
`-a RemoteName`	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
`-A IPAddress`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses

`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by broadcast or WINS server.
`-R`	Purges the name cache and reloads all #PRE entries from LMHOSTS.
`-RR`	Releases and reregisters all names with the name server.
`-s`	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names.
`-S`	Lists the current NetBIOS sessions and their status with the IP addresses.
`Interval`	Redisplays selected statistics, pausing the number of seconds specified in Interval between each display.

TABLE 4.2: Nbtstat parameters and their respective functions

Source: *http://technet.microsoft.com*

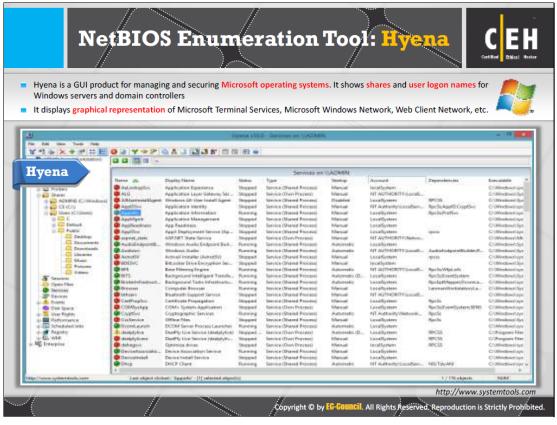


SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver. It performs ping sweeps and scans any IP range with multithreading and asynchronous technique.

Features:

- IP and port scan order randomization
- IP address import supporting ranges and CIDR formats
- Built-in port list description database

Source: http://www.mcafee.com



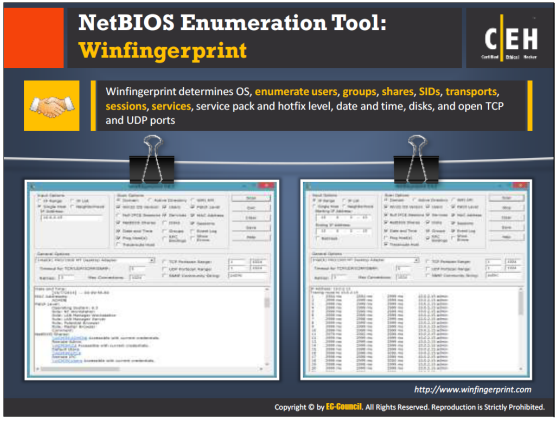
Hyena manages and secures Windows operating systems. It uses a Windows Explorer-style interface for all operations. It supports management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers, print jobs, sessions, open files, disk space, user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

It displays a graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.

Features:

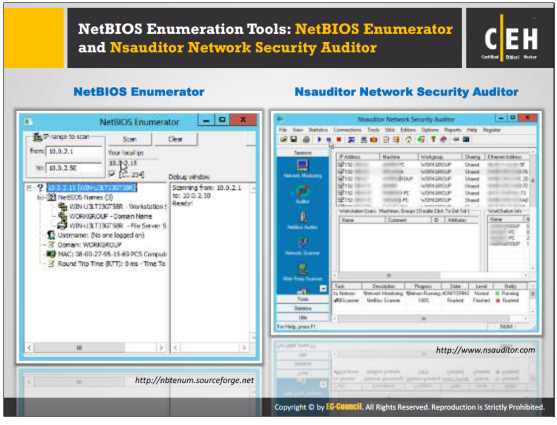
- **Group Member Matrix** - Presents all members of multiple groups in a simple grid, including direct, indirect (nested), and primary membership
- **Active Editor Improvements** – The new release of Hyena includes new feature enhancements to the Editor, including support for multi-valued attributes, account expiration date, as well as multi-selection and update capabilities.

Source: http://www.systemtools.com



Winfingerprint is a host/network enumeration scanner. It is capable of performing SMB, TCP, UDP, ICMP, RPC, and SNMP scans. Winfingerprint input options include: IP range (Netmask and Inverted Netmask supported), IP list, single host, and neighborhood. Using SMB, Winfingerprint can enumerate OS, users, groups, SIDs, password policies, services, service packs and hotfixes, NETBIOS shares, transports, sessions, disks, security event log, and time of day utilizing NT domain (NET*), Active Directory, or WMI APIs. Winfingerprintcli is the command line version of Winfingerprint that supports single host, list of hosts, or IP range scans and contains the same features as Winfingerprint.

Source: *http://www.winfingerprint.com*



NetBIOS Enumerator

Source: *http://nbtenum.sourceforge.net*

NETBIOS Enumerator is an effective tool when you want to determine how to use remote network support and how to deal with some other interesting web techniques, such as **SMB**.

Nsauditor Network Security Auditor

Source: *http://www.nsauditor.com*

Nsauditor Network Security Auditor is a network security auditing tools suite that performs network auditing, network scanning, vulnerability scanning, network monitoring, etc.

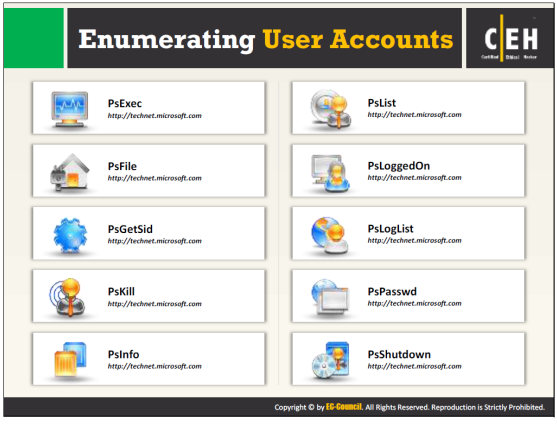
The NetBIOS Auditor in the Nsauditor Network Security Auditor tool set discovers NetBIOS names. NetBIOS names are the names of the Services and Machines. NetBIOS Scanner explores networks, scans a network within a given range of IP addresses and lists computers, which offer NetBIOS resource sharing service as well as name tables and NetBIOS connections.

Features:

- Scans networks and hosts for vulnerabilities, and provides security alerts
- Checks the enterprise network for all potential methods that a hacker might use to attack it, and creates a report of potential problems
- Reduces the total cost of network management in enterprise environments by enabling IT personnel and systems administrators gather a wide range of information from all the

computers in the network without installing server-side applications, and creates a report of potential problems.

- Provides insight into services running locally, with options to dig down into each connection and analyze the remote system, terminate connections, and view data.
- Identifies security holes and flaws in networked systems.
- Includes firewall system, real-time network monitoring, packet filtering and analyzing software.



Commands for Enumerating user accounts include:

PsExec

Source: *http://technet.microsoft.com*

PsExec is a lightweight telnet-replacement that can execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful usage include launching interactive command prompts on remote systems and remote-enabling tools like Ipconfig that otherwise do not have the ability to show information about remote systems.

Syntax: `psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-ns][-r servicename][-h][-l][-s|-e][-x][-I [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]`

PsFile

Source: *http://technet.microsoft.com*

PsFile is a command-line utility that shows a list of files on a system that opened remotely, and it can close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system opened by remote systems. Typing a command followed by "- " displays information on the syntax for the command.

Syntax: `psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]`

PsGetSid

Source: http://technet.microsoft.com

PsGetSid translates SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates a SID into the name that represents it. It works across the network to query SIDs remotely.

Syntax: `psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]`

PsKill

Source: http://technet.microsoft.com

PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. Running PsKill with a process ID directs it to kill the process of that ID on the local computer. If a process name is specified, PsKill will kill all processes that have that name. One need not install a client on the target computer to use PsKill to terminate a remote process.

Syntax: `pskill [- ] [-t] [\\computer [-u username] [-p password]] <process name | process id>`

PsInfo

Source: http://technet.microsoft.com

PsInfo is a command-line tool that gathers key information about local or remote legacy Windows NT/2000 systems, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, the install date of the system, and if it is a trial version, the expiration date. By default, PsInfo shows information for the local system. Specify a remote computer name to obtain information from the remote system.

Syntax: `psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]`

PsList

Source: http://technet.microsoft.com

PsList is a command-line tool that displays information about process CPU and memory information or thread statistics. Tools in the Resource kits, pstat and pmon, show different types of data, but display only the information regarding the processes on the system on which the tools are run.

PsLoggedOn

Source: http://technet.microsoft.com

PsLoggedOn is an applet that displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one. If a user name is specified instead of a computer, PsLoggedOn searches the computers in the network neighborhood and reveals if the user currently logged on. PsLoggedOn's definition of a locally logged on user is one that has a

profile loaded into the Registry, so PsLoggedOn determines who is logged on by scanning the keys under the HKEY_USERS key. For each key that has a name or user SID (security Identifier), PsLoggedOn looks up the corresponding user name and displays it. To determine who logged onto a computer via resource shares, PsLoggedOn uses the NetSessionEnum API.

Syntax: `psloggedon [- ] [-l] [-x] [\\computername | username]`

PsLogList

Source: http://technet.microsoft.com

The elogdump utility dumps the contents of an Event Log on a local or remote computer. PsLogList is a clone of elogdump except that PsLogList can log in to remote systems in situations where the user's security credentials would not permit access to the Event Log, and PsLogList retrieves message strings from the computer on which the event log resides. The default behavior of PsLogList is to display the contents of the System Event Log on the local computer, with visually friendly formatting of Event Log records.

Syntax: `psloglist [-] [\\computer[,computer[,...] | @file [-u username [-p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e ID[,ID[,..]]] [-o event source[,event source][,..]]] [-q event source[,event source][,..]]] [-l event log file] <eventlog>`

PsPasswd

Source: http://technet.microsoft.com

PsPasswd can change an account password on local or remote systems, enabling administrators to create batch files that run PsPasswd against the computers they manage in order to perform a mass change of the administrator password. PsPasswd uses Windows password reset APIs, so it does not send passwords over the network in the clear.

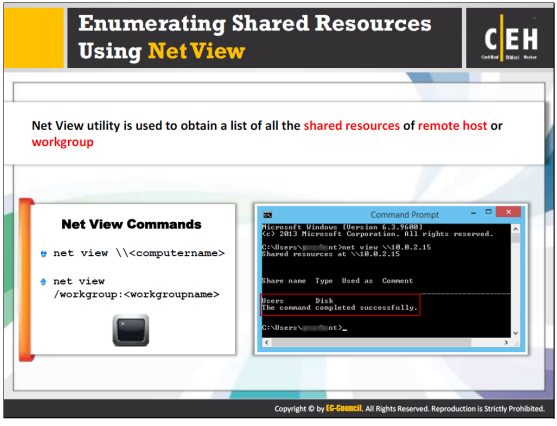
Syntax: `pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] Username [NewPassword]`

PsShutdown

Source: http://technet.microsoft.com

PsShutdown can shut down or reboot local or remote computer. It requires no manual installation of client software.

Syntax: `psshutdown [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]`



Net View is a command line utility that displays a list of computer or network resources. It displays a list of computers in the specified workgroup, or shared resources available on the specified computer.

Usage:

net view \\<computername>

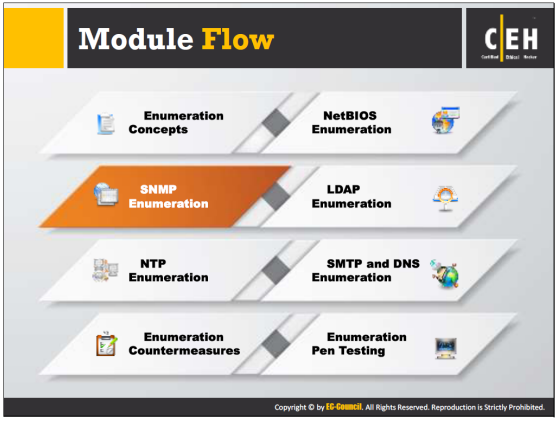
Where <computername> is the name of a specific computer, whose resources you want to view

Or

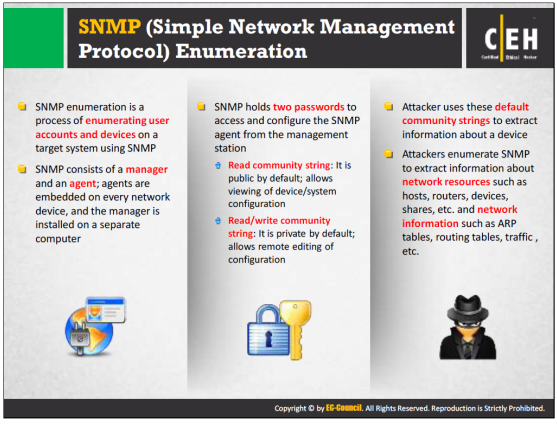
net view /workgroup:<workgroupname>

<workgroupname> is the name of the workgroup whose shared resources you want to view

The snapshot in the slide shows shared resources available on the specified computer (10.0.2.15).



This section describes SNMP enumeration, information extracted via SNMP enumeration, and various SNMP enumeration tools used to enumerate user accounts and devices on a target system.



SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on Windows and UNIX networks on networking devices.

SNMP enumeration is the process of creating a list of the user's accounts and devices on a target computer using SNMP. SNMP employs two types of software components for communication. They are the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Almost all the network infrastructure devices such as routers, switches, etc. contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are the configuration variables accessible by the agent software. SNMP management stations send requests to set values to some variables. Traps let the management station know if anything has happened at the agent's side, such as a reboot, interface failure, or any other abnormal event.

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

The two SNMP passwords are:

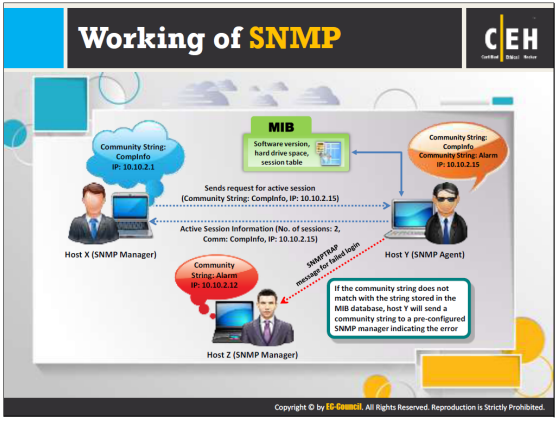
- **Read community** string:

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

- **Read/write community** string:
  - Configuration on the device can be changed or edited using this password.
  - These strings are private.

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

Commonly used SNMP enumeration tools include SNMPUtil and IP Network Browser.



SNMP uses a disturbed architecture comprising SNMP managers, SNMP agents, and several related components. Commands associated with SNMP include:

- **GetRequest**

  Used by the SNMP manager to request information from the SNMP agent

- **GetNextRequest**

  Used by the SNMP manager continuously to retrieve all the data stored in the array or table

- **GetResponse**

  Used by the SNMP agent to satisfy a request made by the SNMP manager

- **SetRequest**

  Used by the SNMP manager to modify the value of a parameter within the SNMP agent's Management Information Base (MIB)

- **Trap**

  Used by the SNMP agent to inform the pre-configured SNMP manager of a certain event

Given below is the communication process between the SNMP manager and the SNMP agent:

- The SNMP manager (Host X, 10.10.2.1) uses the GetRequest command to send a request for the number of active sessions to the SNMP agent (Host Y, 10.10.2.15). To perform this step, the SNMP manager uses the SNMP service libraries such as Microsoft SNMP Management API library (Mgmtapi.dll) or Microsoft WinSNMP API library (Wsnmp32.dll).
- The SNMP agent (Host Y) receives the message and verifies if the community string (CompInfo) is present on its MIB, checks the request against its list of access permissions for that community, and verifies the source IP address.
- If the SNMP agent does not find the community string or access permission in the Host Y's MIB database and the SNMP service is set to send an authentication trap, it sends an authentication failure trap to the specified trap destination, Host Z.
- The master agent component of the SNMP agent calls the appropriate extension agent to retrieve the requested session information from the MIB.
- Using the session information that it retrieved from the extension agent, the SNMP service forms a return SNMP message that contains the number of active sessions and the destination IP address (10.10.2.1) of the SNMP manager, Host X.
- Host Y sends the response to Host X.

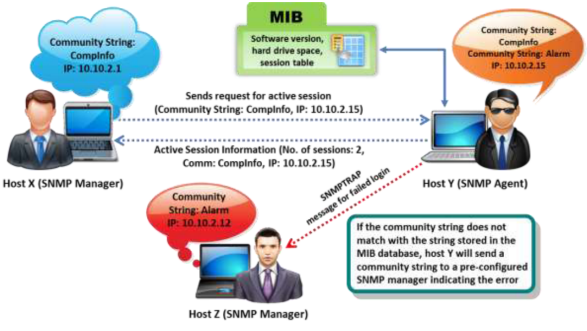
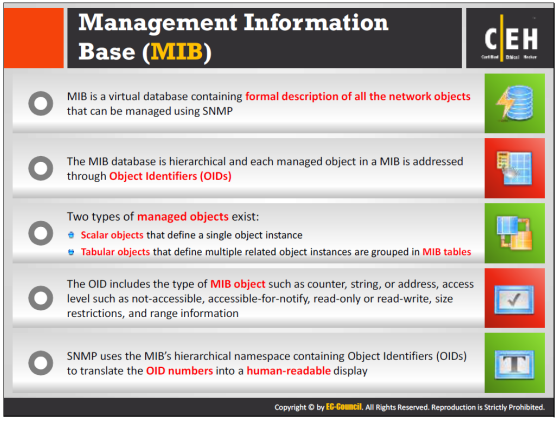


FIGURE 4.1: Diagrammatic illustration about Working of SNMP

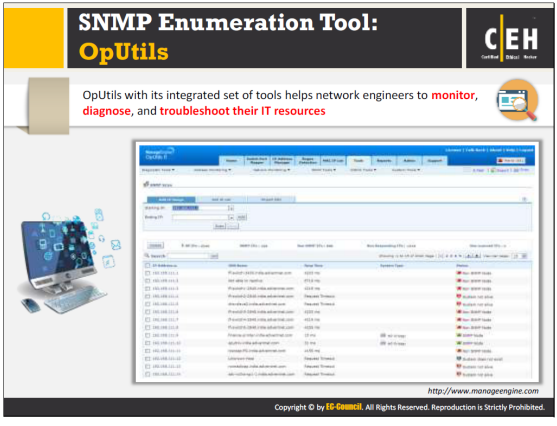


MIB is a virtual database containing a formal description of all the network objects that SNMP manages. It is a collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers. Object ID (OID) is the numeric name given to the object, and begins with the root of the MIB tree. The object identifier can uniquely identify the object present in the MIB hierarchy.

MIB-managed objects include scalar objects that define a single object instance and tabular objects that define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information. The SNMP manager converts the OID numbers into a human-readable display using MIB as a codebook.

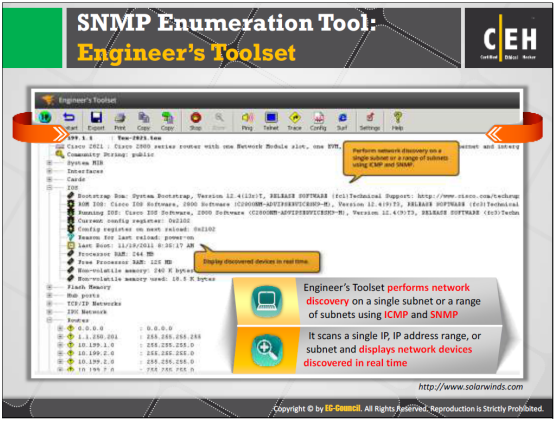
A user can access the contents of the MIB using a web browser either by entering the IP address and Lseries.mib or by entering DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib. Microsoft provides the list of MIBs that are installed with the SNMP Service in the Windows resource kit. The major ones are:

- **DHCP.MIB**: Monitors network traffic between DHCP servers and remote hosts
- **HOSTMIB.MIB**: Monitors and manages host resources
- **LNMIB2.MIB**: Contains object types for workstation and server services
- **WINS.MIB**: For Windows Internet Name Service



OpUtils is switch port and IP address management software. It contains a collection of tools that network engineers can use to monitor, diagnose, and troubleshoot networking issues. Using OpUtils one can manage IP address, map switch ports, detect rogue devices, monitor bandwidth usage, monitor DHCP server, backup Cisco config files, view SNMP traps sent from network devices, get MAC IP list, monitor and troubleshoot the network, etc.

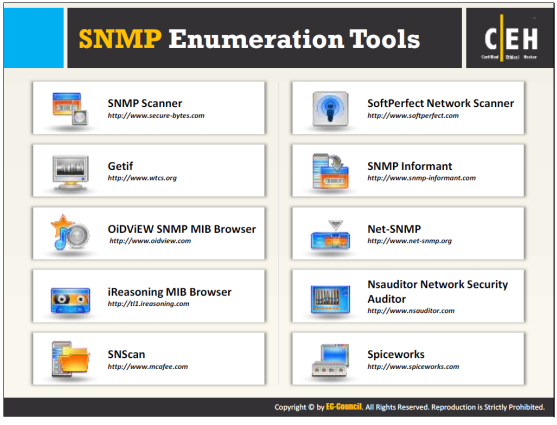
Source: http://www.manageengine.com



IP Network Browser application in the Engineer's Toolset performs network discovery on a single subnet or a range of subnets using ICMP and SNMP. It scans a single IP, IP address range, or subnet and displays network devices in real time, providing immediate access to detailed information about the devices on network.

On a Cisco router, the application will determine the current IOS version and release, as well as identify cards installed into the slots, the status of each port, and ARP tables. When it discovers a Windows server, it returns information including interface status, bandwidth utilization, services running, and even details on installed software.

Source: http://www.solarwinds.com



Other SNMP enumeration tools include:

SNMP Scanner

Source: *http://www.secure-bytes.com*

Simple Network Management Protocol (SNMP) is a UDP-based, application layer network protocol that manages devices on an IP network. The SNMP community string or community name defines the relationship between an SNMP server system and the client systems. This string acts like a password to control devices like Windows Server, or Cisco routers' access to the server.

SNMP Scanner uses SNMP MIB and SNMP traps to monitor routers in a network. SNMP Scanner is a network tool that checks default SNMP community names running on the IP network against a file containing default community string names, in order to ensure that the community string is not common or easily guessable. Most SNMP software uses default communities like:

Write = private

Read = public

Getif

Source: http://www.wtcs.org

Getif is a Windows GUI-based SNMP MIB Browser and network utility that collects and graphs information from SNMP devices. It can graph OID values over time, display the device's interface information, routing, and ARP tables, as well as do basic port scans, Traceroutes, NSLookups, and IP Scans.

OiDViEW SNMP MIB Browser

Source: http://www.oidview.com

OiDViEW SNMP MIB Browser is a network management analysis tool that uses SNMP communication to talk to various agents and devices on a computer network. It uses standard SNMPv1, SNMPv2c, and SNMPv3 protocols to manage any SNMP capable device on the network (e.g. routers, switches, printers, servers, probes, etc.). OiDViEW's SNMP MIB Browser can load standard and proprietary MIB files, view and manipulate data available in an SNMP agent by browsing MIBs, and perform other SNMP management operations. MIB Browser can also analyze SNMP mibwalk files.

iReasoning MIB Browser

Source: http://tl1.ireasoning.com

iReasoning MIB browser manages SNMP-enabled network devices and applications. It loads standard, proprietary, and some mal-formed MIBs. It issues SNMP requests to retrieve an agent's data, or make changes to the agent. A built-in trap receiver can receive and process SNMP traps according to its rule engine.

Features:

- Support for SNMPv1, v2c and v3 (USM and VACM)
- Support for SNMPv3 USM, including HMAC-MD5, HMAC-SHA, CBC-DES, CFB128-AES-128, CFB128-AES-192, CFB128-AES-256 (128-bit, 192-bit and 256-bit AES) algorithms
- Trap Receiver with rule engine to process traps and trigger actions if certain conditions are satisfied
- Log window to display application log and SNMP packets exchanged between browser and agents
- Port view (bandwidth utilization, error percentages) for network interface cards
- Switch port mapper for mapping switch ports
- Table view for MIB tables
- SNMPv3 USM user management (usmUserTable in SNMP-USER-BASED-SM-MIB)
- Performance graph tool for monitoring of numerical OID values

SNScan

Source: http://www.mcafee.com

SNScan is a Windows-based SNMP detection utility that identifies SNMP-enabled devices on a network. It identifies devices that are potentially vulnerable to SNMP-related security threats. It scans SNMP specific ports and uses standard as well as user-defined SNMP community names. SNScan can use user-defined community names to more effectively evaluate the presence of SNMP-enabled devices in more complex networks.

SNScan provides information gathering. While not indicating whether SNMP-enabled devices are vulnerable to specific threats, SNScan can identify potential areas of exposure to SNMP-related vulnerabilities.

SoftPerfect Network Scanner

Source: http://www.softperfect.com

SoftPerfect Network Scanner is a multi-threaded IP, NetBIOS, and SNMP scanner. The program pings computers, scans for listening TCP/UDP ports, and displays which types of resources computers share on the network, including system and hidden ones. It can also mount shared folders as network drives, browse them using windows explorer, filter the results list, etc. SoftPerfect Network Scanner can check for a user-defined port, and report if one is open.

Features:

- Detects hardware MAC-addresses
- Detects hidden shared folders and writable ones
- Detects internal and external IP addresses
- Retrieves currently logged-on users, configured user accounts, uptime, etc.
- Launches external third party applications
- Exports results to HTML, XML, CSV and TXT
- Supports Wake-On-LAN, remote shutdown, and sending network messages
- Retrieves system information via WMI
- Retrieves information from remote registry, file system and service manager.

SNMP Informant

Source: http://www.snmp-informant.com

SNMP Informant products are Simple Network Management Protocol (SNMP) extension agents that can access Windows OS and Application Server Performance Counters, WMI classes and other server information through the SNMP protocol. It accesses SNMP Informant agent information using either SNMPv1 or SNMPv2 protocols from an SNMP Network Management System (NMS).

Net-SNMP

Source: http://www.net-snmp.org

Net-SNMP is a suite of applications used to implement SNMP v1, SNMP v2c and SNMP v3 using both IPv4 and IPv6. The suite includes:

The suite includes:

- Command-line applications to:
  - retrieve information from an SNMP-capable device, either using single requests (snmpget, snmpgetnext), or multiple requests (snmpwalk, snmptable, snmpdelta)
  - manipulate configuration information on an SNMP-capable device (snmpset)
  - retrieve a fixed collection of information from an SNMP-capable device (snmpdf, snmpnetstat, snmpstatus)
  - convert between numerical and textual forms of MIB OIDs, and display MIB content and structure (snmptranslate)
- A graphical MIB browser (tkmib), using Tk/perl
- A daemon application for receiving SNMP notifications (snmptrapd)
- An extensible agent for responding to SNMP queries for management information (snmpd).
- A library for developing new SNMP applications, with both C and Perl APIs

Nsauditor Network Security Auditor

Source: http://www.nsauditor.com

Nsauditor Network Security Auditor is a network security auditing tools suite, which includes tools and utilities for network auditing, network scanning, vulnerability scanning, network monitoring, etc.

The suite's SNMP auditor tool walks through all SNMP MIBs of nodes and audits SNMP community names using values stored in xml database.

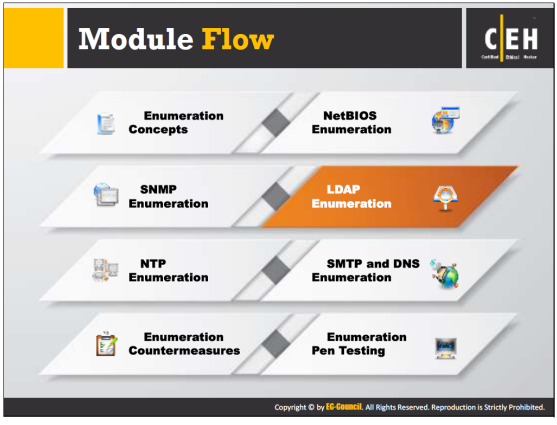
Features:

- Scans networks and hosts for vulnerabilities, and provides security alerts
- Checks the enterprise network for all potential methods that a hacker might use to attack it and create a report of potential problems that were found
- Reduces the total cost of network management in enterprise environments
- Provides insight into services running locally, with options to dig down into each connection and analyze the remote system, terminate connections and view data
- Helps network administrators to identify security holes and flaws in their networked systems
- Includes firewall system, real-time network monitoring, packet filtering and analyzing software

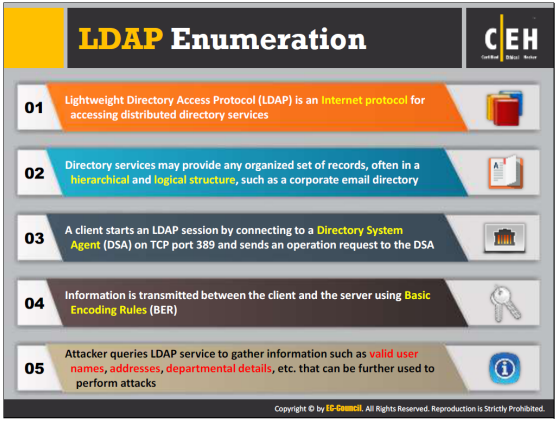
Spiceworks

Source: *http://www.spiceworks.com*

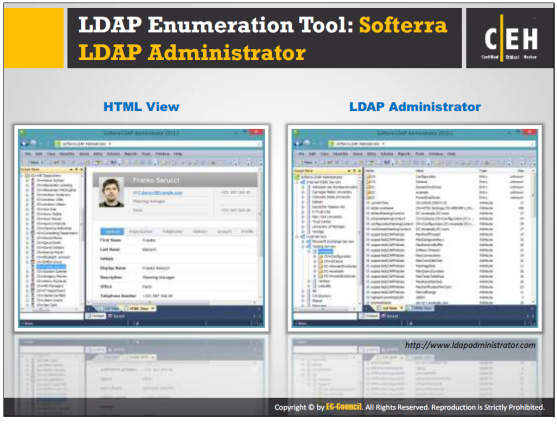
Spiceworks SNMP monitoring software finds connected devices on the network, the amount of bandwidth they use, information on each of the network devices, etc. It also supports SNMP v3 to securely connect to those network devices.



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



LDAP accesses directory listings within an Active Directory or from other directory services. LDAP is a hierarchical or logical form of a directory, similar to a company's org chart. It uses DNS for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a Directory System Agent (DSA) typically on TCP port 389 and sends an operation request to the DSA. Basic Encoding Rules (BER) transmits information between the client and the server. One can anonymously query the LDAP service for sensitive information such as user names, addresses, departmental details, server names, etc., which an attacker can use to launch attacks.

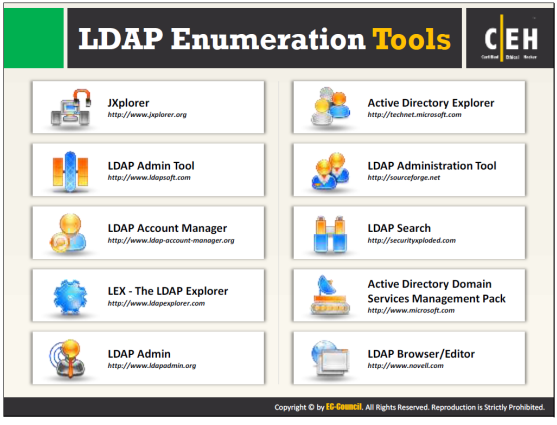


Softerra LDAP Administrator is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, Netscape/iPlanet, etc. It browses and manages LDAP directories. It provides a wide variety of features essential for LDAP development, deployment, and administration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

Features:

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

Source: http://www.ldapadministrator.com



There are many LDAP enumeration tools that access the directory listings within Active Directory or other directory services. Using these tools attackers can enumerate information such as valid user names, addresses, departmental details, etc. from different LDAP servers.

Examples of LDAP enumeration tools include:

JXplorer

Source: http://www.jxplorer.org

JXplorer is a cross-platform LDAP browser and editor. It is a standards-compliant, general-purpose LDAP client used to search, read, and edit a standard LDAP directory, or a directory service with an LDAP or DSML interface.

Features:

- SSL/TLS support
- SASL Authentication
- Unicode support
- LDIF import/export
- Offline LDIF file editing
- DSML support
- Configurable HTML templates/forms

- Pluggable Editors and Security Providers

LDAP Admin Tool

Source: http://www.ldapsoft.com

LDAP Admin Tool is a GUI administration tool for LDAP management, control, and development. It performs mass edit entries using SQL-like syntax, accomplishes LDAP administration operations in a few mouse clicks, views and edits data including binary and images, exports and imports data to/from popular file formats, edits attributes using different editors, manages LDAP users and their privileges and offers many other admin and user functions.

LDAP Account Manager

Source: http://www.ldap-account-manager.org

LDAP Account Manager (LAM) is a web frontend for managing entries (e.g., users, groups, DHCP settings) stored in an LDAP directory. It abstracts from the technical details of LDAP and allows persons without a technical background to manage LDAP entries. If needed, power users may still directly edit LDAP entries via the integrated LDAP browser.

LEX - The LDAP Explorer

Source: http://www.ldapexplorer.com

LEX - The LDAP Explorer can browse and search any LDAP directory. LEX finds attributes of an object including the system and operational attributes by evaluating the directory schema. LEX - The LDAP Explorer is helpful when you develop LDAP applications or when you maintain and automate your directory environment with scripts.

LDAP Admin

Source: http://www.ldapadmin.org

LDAP Admin is a Windows LDAP client and administration tool for LDAP directory management. This application lets the user browse, search, modify, create, and delete objects on LDAP server. It also supports complex operations such as directory copy and move between remote servers and extends the common edit functions to support specific object types (such as groups and accounts).

Features:

- Browsing and editing of LDAP directories
- Recursive operations on directory trees (copy, move and delete)
- Modify operations on datasets
- Binary attribute support
- Schema browsing
- LDIF export and import
- Password management (supports crypt, md5, sha, sha-crypt, samba)
- LDAP SSL support (using Windows API)

Active Directory Explorer

Source: *http://technet.microsoft.com*

Active Directory Explorer (AD Explorer) is an advanced Active Directory viewer and editor. It navigates an AD database, defines favorite locations, views object properties and attributes without having to open dialog boxes, edits permissions, views an object's schema, and executes sophisticated searches that one can save and re-execute. AD Explorer also saves snapshots of an AD database for off-line viewing and comparisons.

LDAP Administration Tool

Source: *http://sourceforge.net*

LDAP Administration Tool browses LDAP-based directories and add/edit/delete entries contained within. It stores profiles for quick access to different servers. There are also different views available such as users, groups, and hosts that allow one to easily manage objects without having to deal with the intricacies of LDAP.

Features:

- User, Group Computer, and Contact views
- Directory browser
- Schema browser
- LDIF imports and exports
- Samba and Active Directory support
- Mass-edit support
- Plugin support for adding 3rd party views and attribute viewers
- Integration with GNOME

LDAP Search

Source: *http://securityxploded.com*

LDAP Search remotely searches Directory servers such as eDirectory, Active Directory etc. It provides options to tweak search queries, thus making the search operation more efficient. It also helps in troubleshooting any problems associated with LDAP Directory servers.

Features:

- Supports both normal LDAP (port 389) as well as LDAPSSL (port 636) protocol
- Allows user to specify server certificate during SSL connection
- Provides search options that can be used to customize the query

  Base DN - Indicates the sub object for search operation

  Filter - Specifies the type of object to search

  Attributes - Custom attributes filter down the search result

Scope - This specifies the depth of the level to search for under base DN

Timeout - This controls the time taken for LDAP search operation

Active Directory Domain Services Management Pack

Source: http://www.microsoft.com

The Active Directory Domain Services Management Pack for System Center provides both proactive and reactive monitoring of the Active Directory deployment. It monitors events that various Active Directory components and subsystems place in the application, system, and service event logs. It also monitors the overall health of the Active Directory system and provides alerts for critical performance issues. The monitoring that this management pack provides includes monitoring of domain controllers and monitoring of health from the perspective of clients that use Active Directory resources.

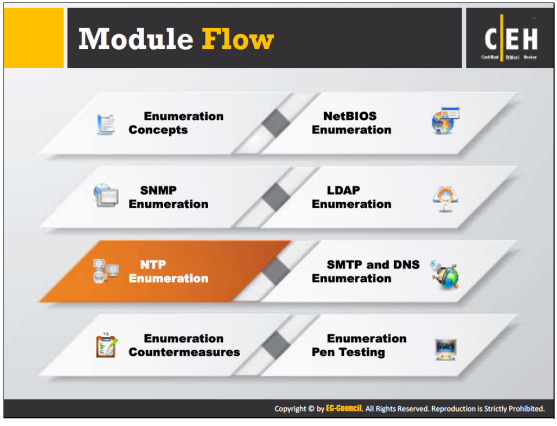
LDAP Browser/Editor

Source: http://www.novell.com

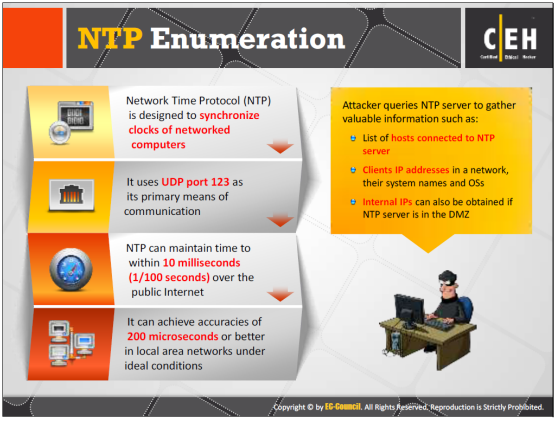
The LDAP Browser/Editor provides a user-friendly Windows Explorer-like interface to LDAP directories with tightly integrated browsing and editing capabilities.

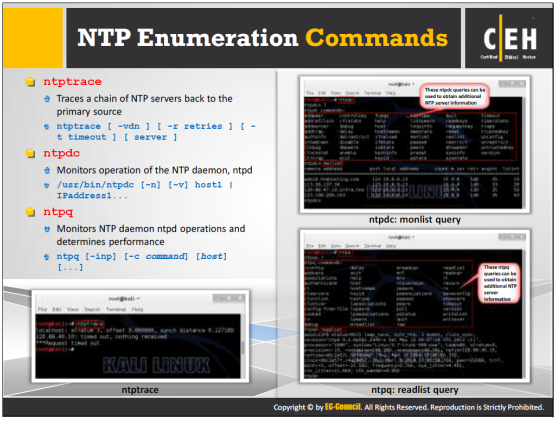
Features:

- Browsing, searching, and editing of the Directory Information Tree
- LDIF support - Entire trees and single entries can be easily exported to and imported from LDIF
- Object templates - Object templates helps in creating and adding new entries. The admins can create templates manually or automatically (from existing entries).
- Binary value support - Binary value support can save or load attributes contents from file.
- Named sessions - Allows for working with LDAP severs with different configurations
- Attribute viewers/editors - Each attribute can be associated with a particular viewer/editor that helps to display/edit the contents of the attribute in a specific manner



Administrators often overlook the NTP server in terms of security. However, if queried properly, it can provide valuable network information to the attackers. Therefore, it is necessary to know what information an attacker can obtain about a network through NTP enumeration. This section describes NTP enumeration, information extracted via NTP enumeration, various NTP enumeration commands, and NTP enumeration tools.





NTP enumeration commands include **ntpdate**, **ntptrace**, **ntpdc**, and **ntpq** to query the NTP server for valuable information.

ntpdate

This command collects the number of time samples from a number of time sources.

Syntax: `ntpdate [-bBdoqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [server/IP_address]`

-a key	Enable the authentication function/specify the key identifier to be used for authentication
-B	Force the time to always be slewed
-b	Force the time to be stepped
-d	Enable debugging mode
-e authdelay	Specify the processing delay
-k keyfile	Specify the path for the authentication key file as the string keyfile. The default is /etc/ntp.keys
-o version	Specify NTP version for outgoing packets as the integer version, can be 1 or 2. Default is 3
-p samples	Specify # of samples to be acquired from each server, with values from 1-8. Default is 4

`-q`	Query only - don't set the clock
`-s`	Divert logging output from the standard output (default) to the system syslog facility
`-t timeout`	Specify the maximum time waiting for a server response. Default is 1 second
`-u`	Use an unprivileged port or outgoing packets
`-v`	Be verbose

TABLE 4.3: ntpdate parameters and their respective functions

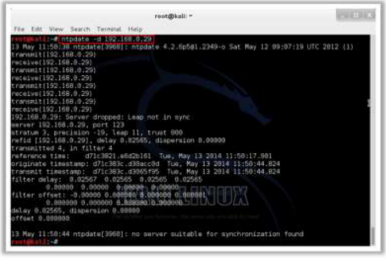


FIGURE 4.2: Screenshot of ntpdate command showing debugging information for a given IP

ntptrace

This command determines from where the NTP server gets time and follows the chain of NTP servers back to its prime time source.

Syntax: `ntptrace [-vdn] [-r retries] [-t timeout] [servername/IP_address]`

`-d`	Display debugging output
`-n`	Does not print host names only IP addresses. May be useful if a name server is down.
`-r retries`	Sets the number of retransmission attempts for each host (default = 5)
`-t timeout`	Sets the retransmission timeout (in seconds) (default = 2)
`-v`	Prints verbose information about the NTP servers

TABLE 4.4: ntptrace parameters and their respective functions

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
192.168.0.1: stratum 2, offset 0.0114273, synch distance 0.115554
192.168.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```

ntpdc

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

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

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

TABLE 4.5: ntpdc parameters and their respective functions

ntpq

This command monitors NTP daemon `ntpd` operations and determine performance.

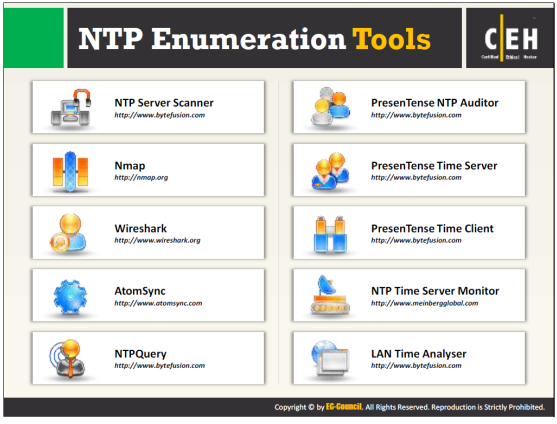
Syntax: `ntpq [-inp] [-c command] [host/IP_address]`

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

TABLE 4.6: ntpq parameters and their respective functions

Example:

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



Given below are some of the NTP Enumeration Tools:

NTP Server Scanner

Source: *http://www.bytefusion.com*

NTP Server Scanner locates NTP and SNTP servers on a network or the Internet. It helps administrators to set up and configure time management on their networks. The utility automatically scans and displays available servers.

Nmap

Source: *http://nmap.org*

Nmap obtains and prints an NTP server's monitor data. Monitor data is a list of the most recently used (MRU) having NTP associations with the target. Each record contains information about the most recent NTP packet sent by a host to the target including the source and destination addresses and the NTP version and mode of the packet. With this information, it is possible to classify associated hosts as servers, peers, and clients.

Wireshark

Source: *http://www.wireshark.org*

Wireshark is a network protocol analyzer that allows capturing and interactively browsing the traffic running on a computer network. The display filter reference contains a complete list of NTP display filter fields. Entering `ntp` allows you to filter only the NTP based traffic. Entering

`udp port 123`, one can filter NTP protocols while capturing, on the well-known NTP UDP port 123.

AtomSync

Source: http://www.atomsync.com

AtomSync is a time synchronization utility that connects a PC to an Internet timeserver to retrieve the official time. AtomSync then compares the differences between the times and makes the proper adjustments. If the PC is part of the LAN, AtomSync act as a timeserver itself and broadcasts the time to all the PCs on the network.

NTPQuery

Source: http://www.bytefusion.com

This utility is a diagnostic tool for NTP and SNTP servers. It verifies connectivity from time clients to NTP servers. It helps administrators to set up and configure time management on networks. NTPQuery simulates a time client, displaying detailed information about the client request and the server reply without actually modifying the local system time.

PresenTense NTP Auditor

Source: http://www.bytefusion.com

PresenTense NTP Auditor monitors a computer's built-in clock and compares its time to the real time. It allows monitors and records a computer's time and graphs the difference between it and up to three national reference clocks on the Internet.

PresenTense Time Server

Source: http://www.bytefusion.com

PresenTense Time Server is an RFC standard multi-protocol windows timeserver supporting the NTP4 and SNTP standards. It synchronizes a PC to a primary time source such as an atomic clock on the Internet or an in-house GPS receiver and offers time services to clients on the local area network. The serial port supports leading GPS and Radio hardware clocks.

PresenTense Time Client

Source: http://www.bytefusion.com

PresenTense Time Client is a network time client. It synchronizes a PC system clock to a network timeserver. It supports e-mail notification with or without SMTP Authentication. Lan Time Analyzer can remotely manage syslog, and redundancy of event logs.

NTP Time Server Monitor

Source: http://www.meinberglobal.com

NTP Time Server Monitor for Windows configures and controls the local NTP service. It displays the status of the local NTP service, as well as external NTP services.

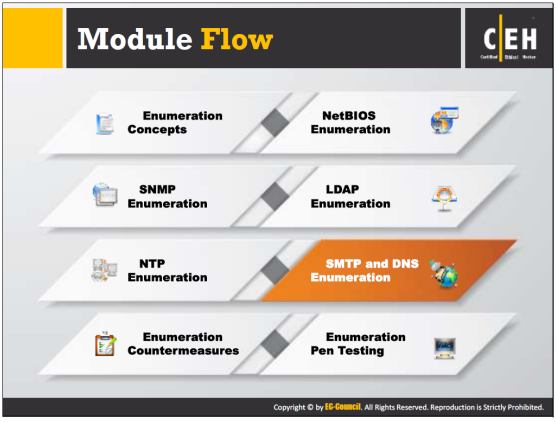
LAN Time Analyzer

Source: *http://www.bytefusion.com*

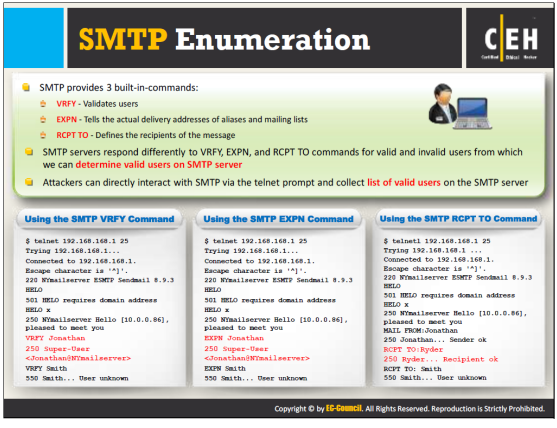
LAN Time Analyzer combines the ability to manage all the PresenTense time clients centrally with the ability to conduct complex error analysis of timeservers and clients.

Features:

- Remote administration of PresenTense time clients
- Verification of time clients through external measurements
- Real time analysis of nominal error on time clients
- Analysis of time server root dispersion
- Scan network for PresenTense Time Clients and PresenTense Time Servers

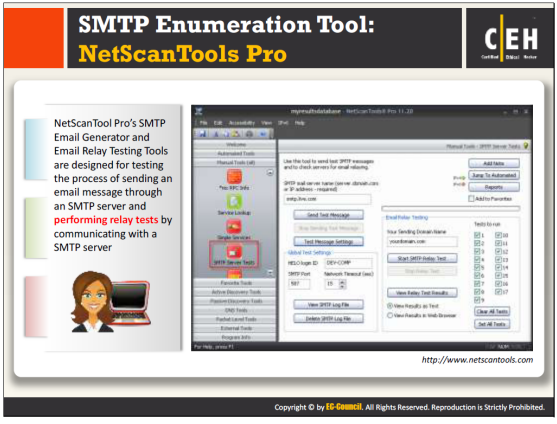


This section describes enumeration techniques to extract information related to network resources. It also covers DNS enumeration techniques that obtain information about DNS servers and the network infrastructure of the organization. The section discusses both SMTP and DNS enumeration techniques. This section will familiarize you with SMTP enumeration, how to get a list of valid users on the SMTP server, SMTP enumeration tools, DNS Zone Transfer Enumeration, etc.



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

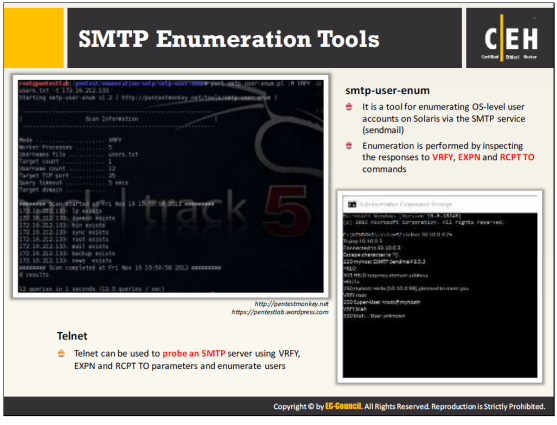
Administrators and pen testers can perform SMTP enumeration using command-line utilities such as telnet, netcat, etc. or by using tools such as Metasploit, Nmap, NetScanTools Pro, etc., to collect a list of valid users, delivery addresses, recipients of the message, etc.



NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server. It can extract all the common email header parameters including confirm/urgent flags. NetScanTools Pro supports SMTP Authentication, either basic or using STARTTLS with username and password for servers requiring it. This tool includes the ability to send email attachments. It can save the email session to a log file and then display the log file showing the communications between NetScanTools Pro and the SMTP server.

NetScanTools Pro's Email Relay Testing Tool performs relay testing by communicating with an SMTP server. The report includes a log of the communications between NetScanTools Pro and the target SMTP server. The relay test report displays as either text or as HTML in a browser.

Source: http://www.netscantools.com

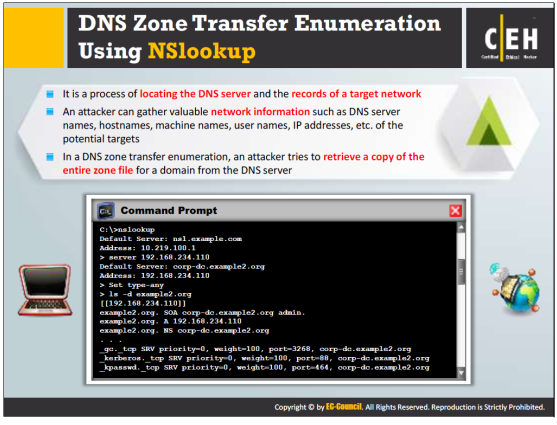


smtp-user-enum simply needs to be passed a list of users and at least one target running an SMTP service.

Usage: smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)

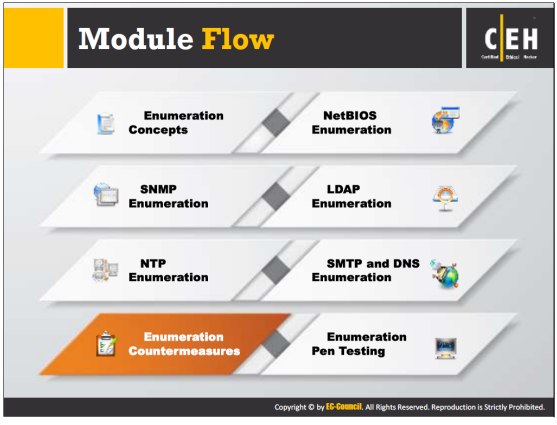
Options are:

-m n Maximum number of processes (default: 5)
-M mode Method to use for username guessing EXPN, VRFY or RCPT (default: VRFY)
-u user Check if user exists on remote system
-f addr From email address to use for "RCPT TO" guessing (default: user@example.com)
-D dom Domain to append to supplied user list to make email addresses (Default: none)
-U file File of usernames to check via smtp service
-t host Server host running smtp service
-T file File of hostnames running the smtp service
-p port TCP port on which smtp service runs (default: 25)
-d Debugging output
-t n Wait a maximum of n seconds for reply (default: 5)
-v Verbose
-h This help message

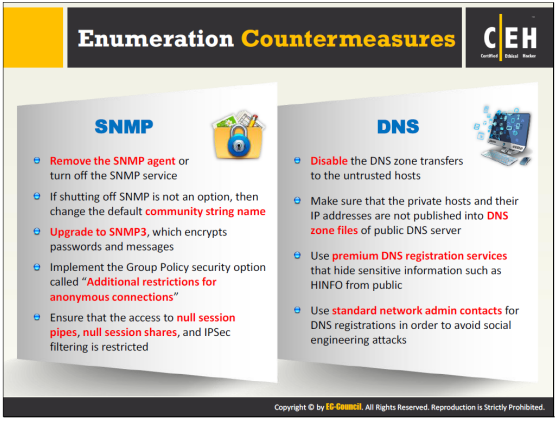


DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. The attacker performs DNS zone transfer enumeration to locate the DNS server and records of the target organization. Through this process, an attacker gathers valuable network information such as DNS server names, hostnames, machine names, user names, IP addresses, etc. of the potential targets. To perform DNS zone transfer enumeration, the attacker can use tools such as nslookup, DNSstuff, etc.

To perform a DNS zone transfer, the attacker sends a zone transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to you. This zone may contain a lot of information about the DNS zone network.



So far, we have described enumeration techniques and tools used to extract valuable information from the target. Now let us discuss countermeasures that can prevent attackers from enumerating sensitive information from the network or host. This section focuses on how to avoid information leakage through SNMP, DNS, SMTP, LDAP, and SMB enumeration.



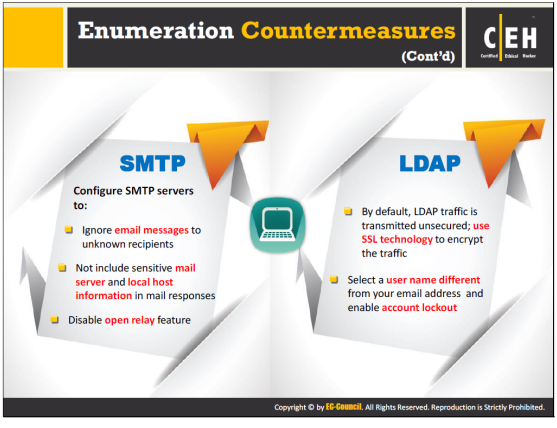
The following countermeasures can prevent information leakage through SNMP and DNS enumeration.

SNMP Enumeration Countermeasures

- Block access to TCP/UDP ports 161
- Do not install the management and monitoring Windows component unless it is required.
- Encrypt or authenticate using IPSEC

DNS Enumeration Countermeasures

- Prune DNS zone files to prevent revealing unnecessary information



The following countermeasures can prevent information leakage through SMTP and LDAP enumeration.

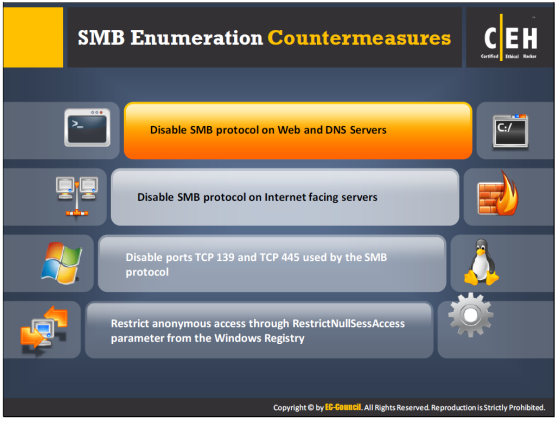
SMTP Enumeration Countermeasures

Configure SMTP servers to:

- Disable EXPN, VRFY, and RCPT TO commands, or restrict them to authentic users
- Ignore emails to unknown recipients by configuring SMTP servers

LDAP Enumeration Countermeasures

- Restrict the access to Active Directory by using software such as Citrix

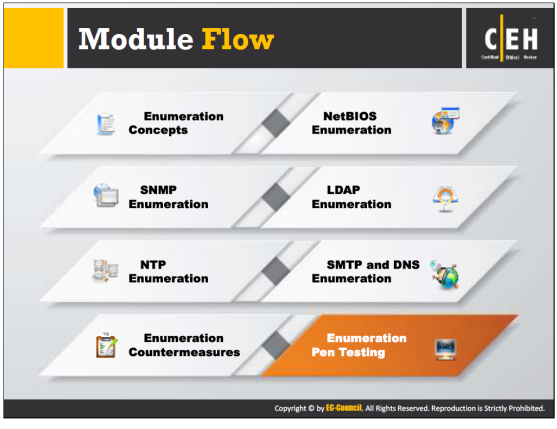


Common sharing services or other unused services may prove to be **doorways** for attackers to break into a network's security. **Server Message Block** (SMB) is a protocol that provides shared access to files, serial ports, printers, and communications between nodes on a network. If this service is running on a network, then there is a high risk of enumeration via SMB. Since web and DNS servers do not require this protocol, it is advisable to disable it on them. SMB protocol can be disabled by uninstalling the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** properties of **Network and Dial-up Connections**. On servers that are accessible from the internet, also known as bastion hosts, SMB can be disabled by uninstalling the same two properties of the **TCP/IP properties** dialog box. One other way of disabling SMB protocol on bastion hosts, without explicitly disabling it, is by blocking the ports which are used by the SMB service. These are TCP 139 and TCP 445 ports.

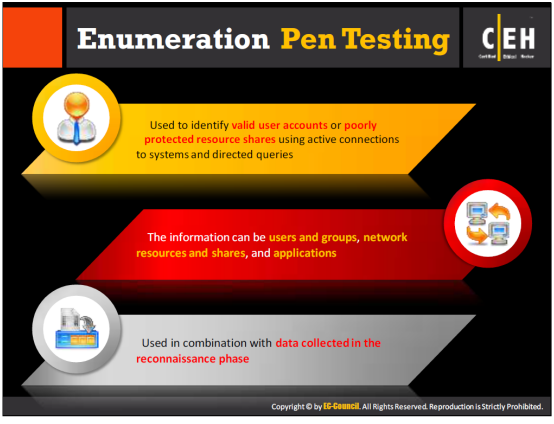
Since disabling SMB services is not always a feasible option, there are other countermeasures that can be taken against SMB enumeration. Windows registry can be configured to limit anonymous access from internet to just a specified set of files. These files and folders are specified in **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** settings. This configuration involves adding the RestrictNullSessAccess parameter to the registry key:

KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters

The RestrictNullSessAccess parameter takes binary values with 1 denoting enabled, and 0 denoting disabled. Setting this parameter to 1 or enabled restricts access of anonymous users to just the files specified in the **Network access** settings.

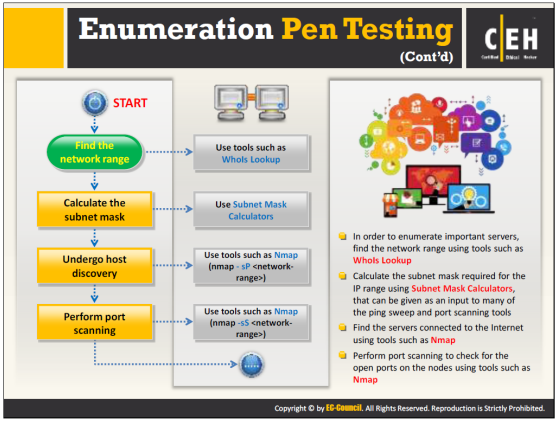


This section describes the importance of enumeration pen testing, the framework of pen testing steps, and the tools used to conduct pen testing.



Through enumeration, an attacker may gather sensitive information on organizations with weak security. That sensitive information can be used to hack and break into the organization's network, potentially resulting in huge loss in terms of information, service, or finance. To prevent these kinds of attacks, every organization must test its own security. Enumeration pen testing builds on the data collected in the reconnaissance phase.

A pen tester should conduct pen tests against various enumeration techniques in order to check if the target network is revealing any sensitive information that may help an attacker in performing an attack. This may reveal sensitive information such as user accounts, IP address, email contacts, DNS, network resources and shares, application information, etc. The pen tester should try to discover as much information as possible regarding the target. This helps to determine the vulnerabilities/weaknesses in the target organization's security.



A pen tester should perform all possible enumeration techniques to enumerate as much information as possible about the target. To ensure the full scope of the test, enumeration pen testing includes a series of steps to provide information.

Step 1: Find the network range

Find the network range using tools such as Whois Lookup. Finding network range helps in enumerating important servers in the target network.

Step 2: Calculate the subnet mask

Calculate the subnet mask required for the IP range using tools such as Subnet Mask Calculator. The calculated subnet mask can serve as an input to many of the ping sweep and port scanning tools for further enumeration, which includes discovering hosts and open ports.

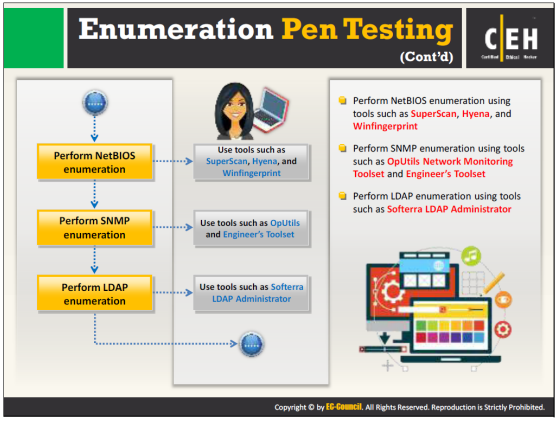
Step 3: Undergo host discovery

Find the important servers connected to the Internet using tools such as Nmap. Use the Nmap syntax to find the servers connected to Internet is as follows: **nmap - sP <network-range>**. In place of the network range, enter the network range value obtained in the first step.

Step 4: Perform port scanning

Find any open ports and close them if they are not required. Open ports are doorways for an attacker to break into a target's security perimeter. Therefore, perform port scanning to check

for the open ports on the nodes. Pen testers and security auditors use tools such as Nmap to perform port scanning.



Step 5: Perform NetBIOS enumeration

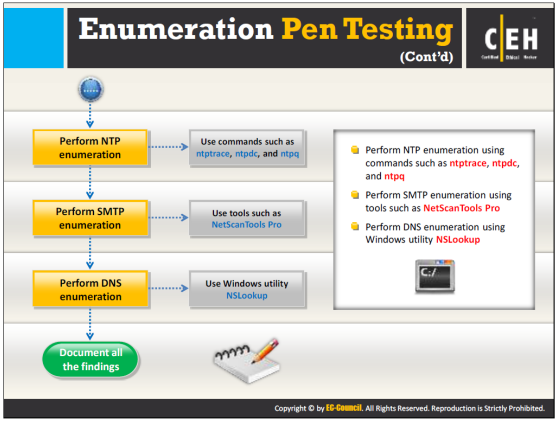
Perform NetBIOS enumeration to identify the network devices over TCP/IP and to obtain a list of computers that belong to a domain, a list of shares on individual hosts, and policies and passwords. Tools such as SuperScan, Hyena, and WinFingerprint can perform NetBIOS enumeration.

Step 6: Perform SNMP enumeration

Perform SNMP enumeration by querying the SNMP server in the network. The SNMP server may reveal information about user accounts and devices. Tools such as OpUtils Network Monitoring Toolset and Engineer's Toolset can perform SNMP enumeration.

Step 7: Perform LDAP enumeration

Perform LDAP enumeration by querying the LDAP service. Enumerating LDAP service provides valid user names, departmental details, and address details. An attacker can use this information to perform social engineering and other kinds of attacks. Tools such as Softerra LDAP Administrator can perform LDAP enumeration.



Step 8: Perform NTP enumeration

Perform NTP enumeration to extract information such as the host connected to an NTP server, client IP address, OS running on client systems, etc. Commands such as `ntptrace`, `ntpdc`, and `ntpq` can obtain this information.

Step 9: Perform SMTP enumeration

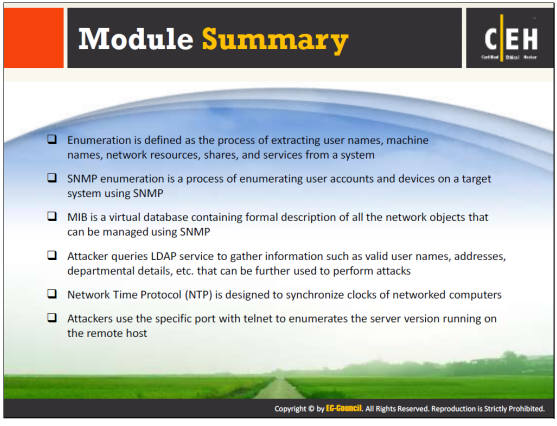
Perform SMTP enumeration to determine valid users on the SMTP server. Tools such as NetScanTools Pro can query the SMTP server for this information.

Step 10: Perform DNS enumeration

Perform DNS enumeration to locate all the DNS servers and their records. The DNS servers provide information such as system names, user names, IP addresses, etc. The Windows utility nslookup can extract this information.

Step 11: Document all the findings

The last step is to document all the findings obtained during the enumeration pen testing. Analyze the results and suggest countermeasures for the client to improve their security.



This module completes with an overview discussion of fundamental enumeration concepts. In the next module, we will see how attackers as well as ethical hackers and pen testers attempt system hacking based on the information collected about a target of evaluation from footprinting, scanning, and enumeration phases.