



Module 04

Enumeration

This page is intentionally left blank.

Enumeration

Module Objectives

CEH

- Understanding Enumeration Concepts
- Understanding Different Techniques for NetBIOS Enumeration
- Understanding Different Techniques for SNMP Enumeration
- Understanding Different Techniques for LDAP and NTP Enumeration
- Understanding Different Techniques for SMTP and DNS Enumeration
- Understanding Other Enumerations such as IPsec, VoIP, RPC, and Linux/Unix enumeration
- Understanding Different Enumeration Countermeasures
- Overview of Enumeration Pen Testing

Module Objectives

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

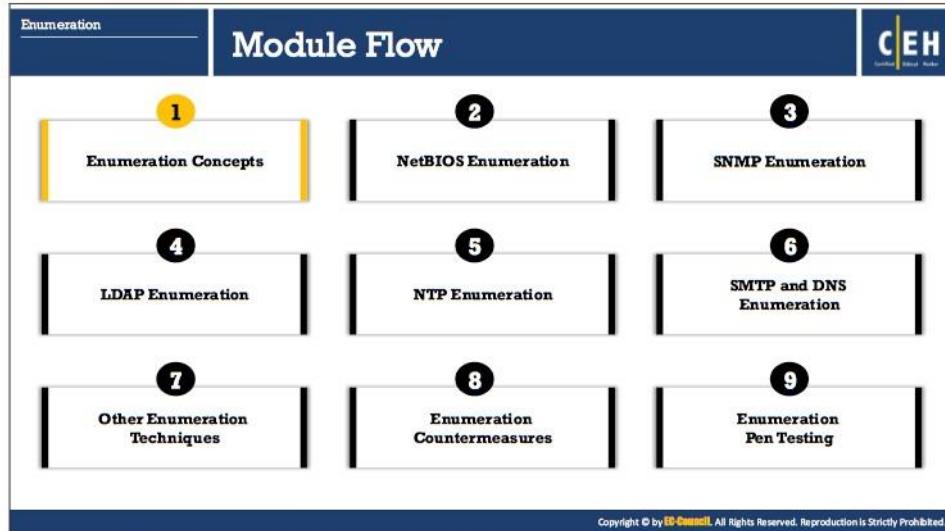
Module Objectives

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, DNS, IPsec, VoIP, RPC, and Linux/Unix 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.

At the end of this module, you will be able to:

- Describe the enumeration concepts
- Explain different techniques for NetBIOS enumeration
- Explain different techniques for SNMP enumeration
- Explain different techniques for LDAP enumeration
- Explain different techniques for NTP enumeration
- Explain different techniques for SMTP and DNS enumeration
- Explain other enumerations such as IPsec, VoIP, RPC, and Linux/Unix enumeration
- Apply enumeration countermeasures
- Perform enumeration penetration testing



Enumeration Concepts

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
Enumeration Concepts

What is Enumeration?

CEH

In the enumeration phase, attacker **creates active connections with system** and **performs directed queries** to gain more information about the target

Attackers use the extracted information to **identify points of system attack** and **perform password attacks** to gain unauthorized access to information system resources

Enumeration techniques are conducted in an **intranet environment**

Information Enumerated by Intruders

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and FQDN details
- Machine names
- Users and groups
- Applications and banners

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

What is Enumeration?

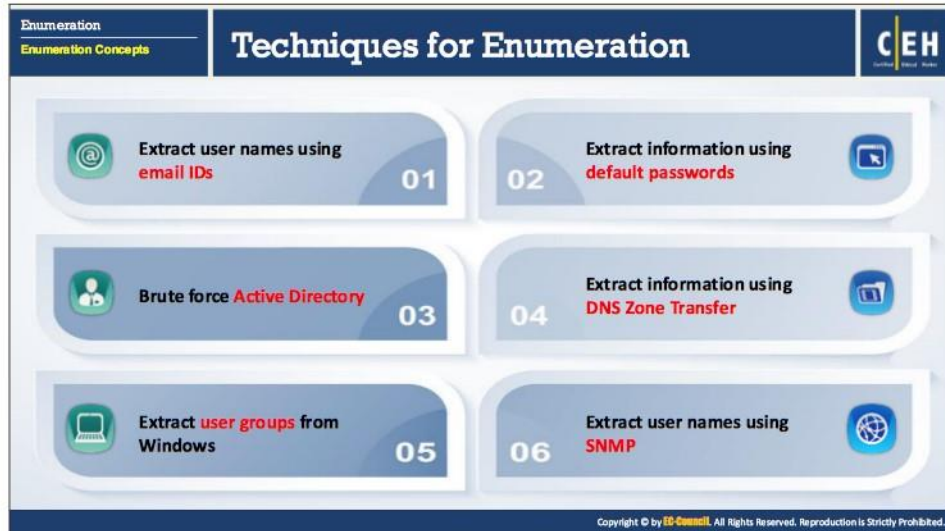
Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system or network. In the enumeration phase, attacker creates active connections with system and performs directed queries to gain more information about the target. The attackers use the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

Enumeration allows you to collect following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and FQDN details
- Machine names
- Users and groups
- Applications and banners

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.



Techniques for 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 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.

The infographic is titled "Services and Ports to Enumerate" and is part of the "Enumeration" section under "Enumeration Concepts". It lists 13 services and their associated ports, organized into two columns. Each entry includes a small icon representing the service and its name.

Port	Service
TCP/UDP 53	Domain Name System (DNS) Zone Transfer
TCP/UDP 135	Microsoft RPC Endpoint Mapper
UDP 137	NetBIOS Name Service (NBNS)
TCP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP/UDP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP/UDP 3268	Global Catalog Service
TCP 25	Simple Mail Transfer Protocol (SMTP)
TCP/UDP 162	SNMP Trap
UDP 500	ISAKMP/Internet Key Exchange (IKE)
TCP/UDP 5060, 5061	Session Initiation Protocol (SIP)

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

Services and Ports to Enumerate

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) 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 and 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. use 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 end point is the protocol port on which the server listens for the client's remote procedure calls. RPC end point 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 end point mapper that listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC End point Mapper process on a server, in order to launch a Denial of Service (DoS) attack.

- **UDP137: 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.

- **TCP139: 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	VERFY<string>
Expand	EXPN<string>
Help	HELP[<string>]
Quit	QUIT

TABLE 4.1: SMTP commands and their respective syntax

- **TCP/UDP 162: SNMP Trap**

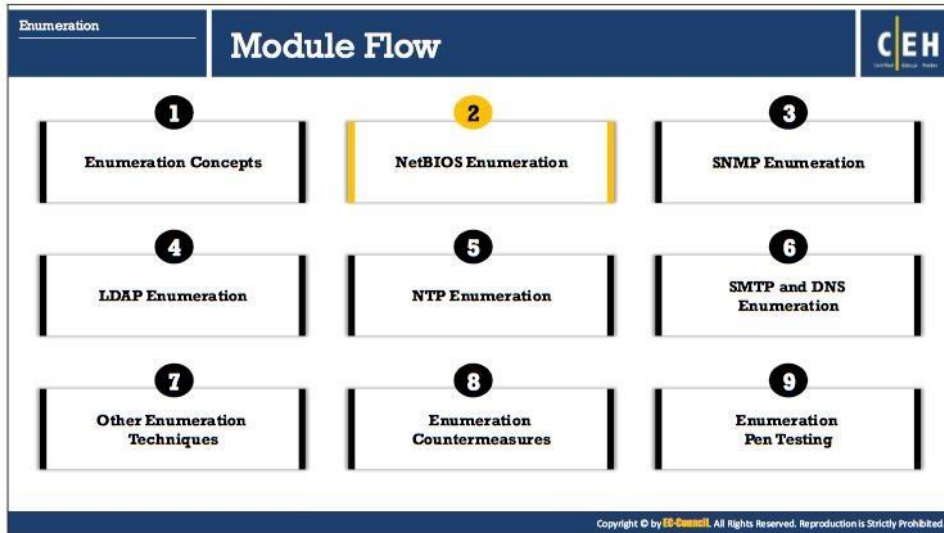
Simple Network Management Protocol Trap (SNMP Trap) uses TCP/UDP port 162 to receive notifications such as optional variable bindings, sysUpTime value, etc., from agent to manager.

- **UDP 500: ISAKMP/Internet Key Exchange (IKE)**

Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPsec protocol suite. It uses UDP port 500 to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment.

- **TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)**

Session Initiation Protocol (SIP) is a protocol used in the applications of Internet telephony for voice and video calls. It typically uses TCP/UDP port 5060 (non-encrypted signaling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other end points.



NetBIOS Enumeration

- NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP, 15 characters are used for the **device name** and the 16th character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts in the network
- Policies and passwords

NetBIOS Name List

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

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

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

Enumeration
NetBIOS Enumeration

NetBIOS Enumeration (Cont'd)

Nbtstat utility in Windows displays NetBIOS over **TCP/IP** (NetBT) **protocol statistics**, **NetBIOS name tables** for both the local and remote computers, and the **NetBIOS name cache**

Run nbtstat command "nbtstat.exe -c" to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses

Run nbtstat command "nbtstat.exe -a <IP address of the remote machine>" to get the NetBIOS name table of a remote computer

<https://technet.microsoft.com>
 Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NetBIOS Enumeration

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.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts in the network
- Policies and passwords

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.

NetBIOS name list:

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

TABLE 4.2: NetBIOS Name List

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

Nbtstat Utility

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

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name resolution problems. The `nbtstat` command removes and corrects preloaded entries using a number of case-sensitive switches. 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
<code>-a RemoteName</code>	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer.
<code>-A IPAddress</code>	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.
<code>-c</code>	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.
-x	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 4.3: Nbtstat parameters and their respective functions

Nbtstat Examples:

- Run nbtstat command “**nbtstat.exe -c**” to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses

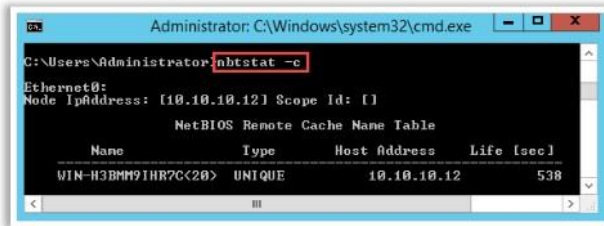


FIGURE 4.1: Nbtstat command to obtain the contents of the NetBIOS name

- Run nbtstat command “**nbtstat.exe -a <IP address of the remote machine>**” to get the NetBIOS name table of a remote computer

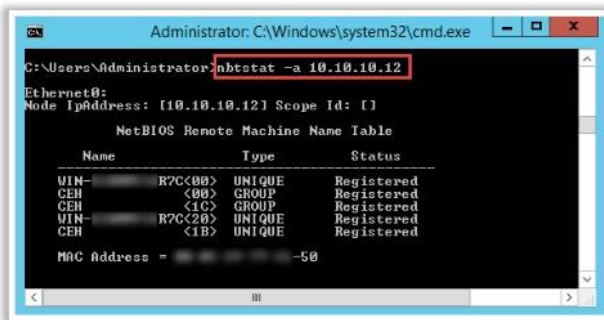


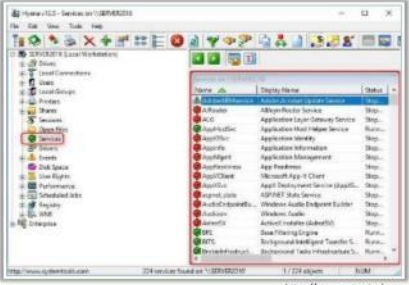
FIGURE 4.2: Nbtstat command to obtain the name table of a remote system

Enumeration

NetBIOS Enumeration Tools

Hyena

- Hyena is a GUI product for managing and securing **Microsoft operating systems**. It shows **shares** and **user logon names** for Windows servers and domain controllers
- It displays **graphical representation** of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.



Nsauditor Network Security Auditor
<https://www.nsauditor.com>

NetScanTools Pro
<https://www.netscantools.com>

SoftPerfect Network Scanner
<https://www.softperfect.com>

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

NetBIOS Enumerator
<http://hstenum.sourceforge.net>

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

NetBIOS Enumeration Tools

NetBIOS enumeration tools explore and scan the network within a given range of IP addresses and lists of computers to identify security loop holes or flaws present in networked systems. These tools also enumerate OS, users, groups, SIDs, password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks and security event logs.

- **Hyena**

Source: <https://www.systemtools.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 log on names for Windows servers and domain controllers.

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

Features:

- **Active Task Matching Options** - Added Key match option to Active Task when performing Active Directory update tasks. The new key option allows for any unique directory attribute to be used as a 'match' field when updating directory objects.
- **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.

Some of the enumeration tools are listed below:

- Nsauditor Network Security Auditor (<https://www.nsauditor.com>)
- NetScanTools Pro (<https://www.netscantools.com>)
- SoftPerfect Network Scanner (<https://www.softperfect.com>)
- SuperScan (<https://www.mcafee.com>)
- NetBIOS Enumerator (<http://nbtenum.sourceforge.net>)
- Nbtscan (<http://www.unixwiz.net>)
- IP Tools (<https://www.ks-soft.net>)
- MegaPing (<http://www.magnetosoft.com>)

The infographic is titled "Enumerating User Accounts" and is part of a "NetBIOS Enumeration" section. It lists ten PsTools commands in two columns:

- PsExec** - execute processes remotely
- PsFile** - shows files opened remotely
- PsGetSid** - display the SID of a computer or a user
- Pskill** - kill processes by name or process ID
- PsInfo** - list information about a system
- PsList** - list detailed information about processes
- PsLoggedOn** - see who's logged on locally and via resource sharing
- PsLogList** - dump event log records
- PsPasswd** - changes account passwords
- PsShutdown** - shuts down and optionally reboots a computer

Source: <https://docs.microsoft.com>
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerating User Accounts

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

Enumerating user accounts using PsTools suite helps to control and manage remote systems from the command line.

Commands for enumerating user accounts include:

- **PsExec**

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] [-n s] [-r servicename] [-h] [-l] [-s] [-e] [-x] [-I [session]] [-c [-f|-v]] [-w directory] [-d] [-<priority>] [-a n,n,...] cmd [arguments]

- **PsFile**

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**

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**

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**

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**

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**

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**

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**

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 pswd]]] Username [NewPassword]

- **PsShutdown**

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 pswd]]] [-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"]

Enumeration
NetBIOS Enumeration

Enumerating Shared Resources Using Net View

Net View utility is used to obtain a list of all the **shared resources of remote host or workgroup**

Net View Commands

- `net view \\<computersname>`
- `net view /workgroup:<workgroupname>`

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>net view \\10.10.10.12
Shared resources at \\10.10.10.12

Share name Type Used as Comment
-----
NETLOGON Disk Logon server share
C$ Disk Logon server share
W$ Disk Logon server share
The command completed successfully.
C:\Users\Administrator>
```

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

Enumerating Shared Resources Using Net View

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:

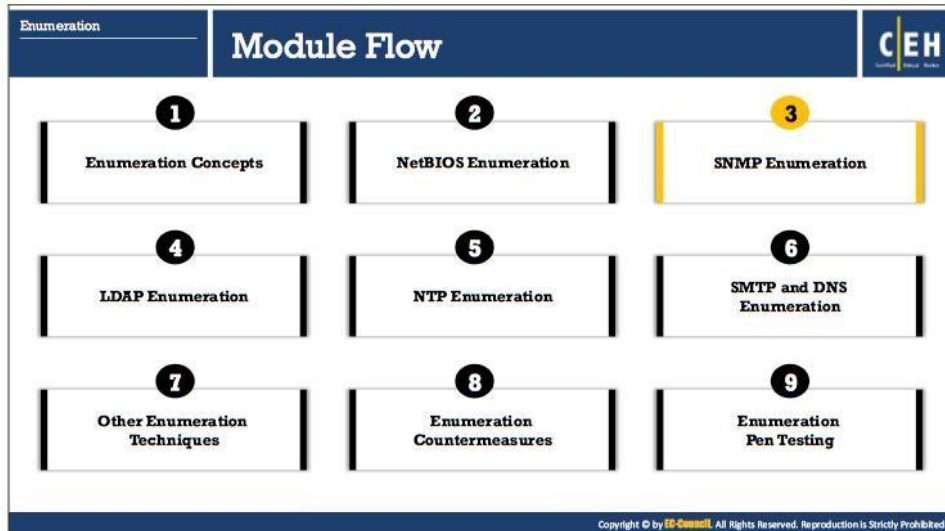
```
net view \\<computersname>
```

Where `<computersname>` 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




Enumeration


SNMP (Simple Network Management Protocol) Enumeration

CEH


- SNMP enumeration is a process of **enumerating user accounts and devices** on a target system using SNMP.
- SNMP consists of a **manager** and an **agent**; agents are embedded on every network device, and the manager is installed on a separate computer.



- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
 - Read community string:** It is public by default; allows viewing of device/system configuration
 - Read/write community string:** It is private by default; allows remote editing of configuration



- Attacker uses these **default community strings** to extract information about a device
- 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, traffic, etc.



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

SNMP Enumeration

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.

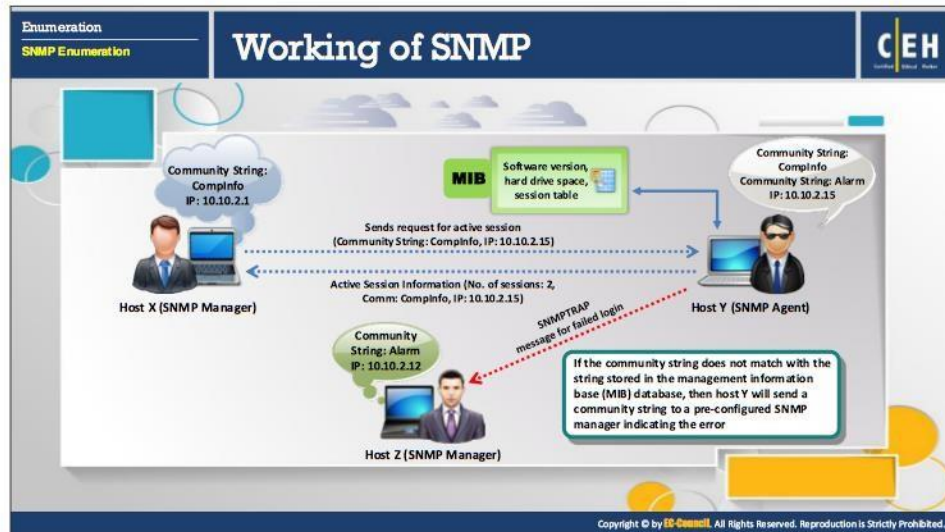
Almost all the network infrastructure devices such as routers, switches, etc. contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are the configuration variables accessible 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 (<http://www.wtcs.org>) and IP Network Browser (<https://www.solarwinds.com>).



Working of SNMP






SNMP uses a distributed 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.

Enumeration SNMP Enumeration	Management Information Base (MIB)	CEH
<input type="radio"/>	MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP	
<input type="radio"/>	The MIB database is hierarchical and each managed object in a MIB is addressed through Object Identifiers (OIDs)	
<input type="radio"/>	Two types of managed objects exist: <ul style="list-style-type: none">• Scalar objects that define a single object instance• Tabular objects that define multiple related object instances are grouped in MIB tables	
<input type="radio"/>	OID includes the type of MIB object such as counter, string, or address; access level such as not-accessible, accessible-for-notify, read-only, or read-write; size restrictions; and range information	
<input type="radio"/>	SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the OID numbers into a human-readable display	

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

Management Information Base (MIB)

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
- **LNMB2.MIB:** Contains object types for workstation and server services
- **WINS.MIB:** For Windows Internet Name Service

Enumeration
SNMP Enumeration

SNMP Enumeration Tools

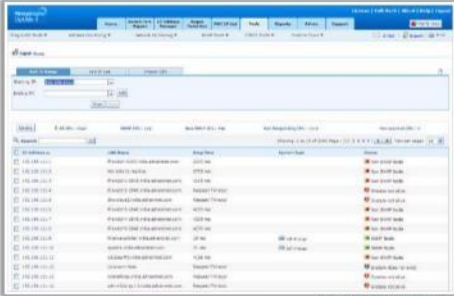


OpUtils


OpUtils with its integrated set of tools helps network engineers to **monitor, diagnose, and troubleshoot** their IT resources

Engineer's Toolset

Engineer's Toolset **performs network discovery** on a single subnet or a range of subnets using **ICMP and SNMP**



<https://www.manageengine.com>





<http://www.solarwinds.com>

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


Enumeration
SNMP Enumeration

SNMP Enumeration Tools (Cont'd)







Nsauditor Network Security Auditor
<https://www.nsauditor.com>




Spiceworks Network Monitor
<https://www.spiceworks.com>




NetScanTools Pro
<https://www.netcantools.com>




SoftPerfect Network Scanner
<https://www.softperfect.com>




Network Performance Monitor
<http://www.solarwinds.com>




SNMP Informant
<https://www.snmp-informant.com>




OIDVIEW SNMP MIB Browser
<http://www.oidview.com>



iReasoning MIB Browser
<http://iReasoning.com>



SNScan
<https://www.moftee.com>



SNMPCHECK
<http://www.nothink.org>

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

SNMP Enumeration Tools

SNMP enumeration tools are used to scan a single IP address or a range of IP addresses of SNMP enabled network devices in order to monitor, diagnose, and troubleshoot security threats.

- **OpUtils**

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

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

Features:

- **IP Address Management** - Scan IPv4 & IPv6 subnets in the network to identify the available and used IP Addresses.
- **Switch Port Management** - Scan all the switches in your network and map the switch ports to devices down to its physical location.
- **Detect Rogue Devices** – Identify the rogue device intrusions and block their access.
- **Network Tools** – Monitor the critical servers in the network for availability and alert for immediate attention.

▪ **Engineer's Toolset**

Source: <http://www.solarwinds.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.

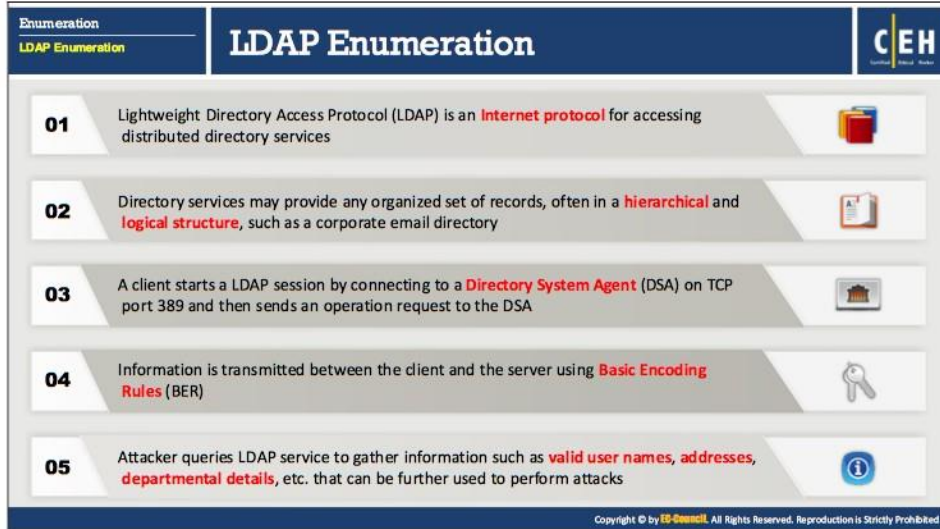
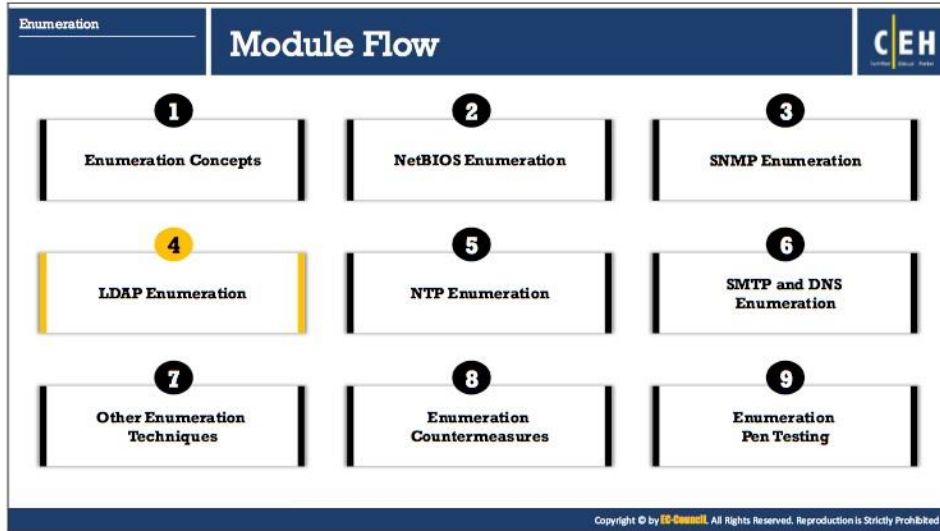
Features:

- **Automated network discovery**- Discover your entire network, including equipment, MAC to IP address relationships, Switch Port mapping, and more.
- **Real time monitoring and alerting**- Monitor and receive alerts in real time on network availability and health.
- **Powerful diagnostics**- Perform robust network diagnostics for faster troubleshooting and quick resolution of complex network issues.
- **Enhanced network security**- Simulate attacks on your network to identify security vulnerabilities.
- **Configuration and log management**- Configure devices on your network and troubleshoot any config issues with specialized tools.

Some of the SNMP enumeration tools include:

- Nsauditor Network Security Auditor (<https://www.nsauditor.com>)
- Spiceworks Network Monitor (<https://www.spiceworks.com>)

- NetScanTools Pro (<https://www.netscantools.com>)
- SoftPerfect Network Scanner (<https://www.softperfect.com>)
- Network Performance Monitor (<http://www.solarwinds.com>)
- SNMP Informant (<https://www.snmp-informant.com>)
- OiDVIEW SNMP MIB Browser (<http://www.oidview.com>)
- iReasoning MIB Browser (<http://ireasoning.com>)
- SNScan (<https://www.mcafee.com>)
- SNMPCHECK (<http://www.nothink.org>)
- Net-SNMP (<http://www.net-snmp.org>)
- Getif (<http://www.wtcs.org>)



LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All of these protocols carry valuable information about network resources along with the data. An external user who is able to enumerate that information by manipulating the protocols, can break into the network and may misuse the network resources. The 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 is an Internet protocol for accessing distributed directory services. 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. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory. 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.

The screenshot shows a webpage titled "LDAP Enumeration Tools" with a navigation menu for "Enumeration" and "LDAP Enumeration". The main content area is titled "Softerra LDAP Administrator" and includes a description: "Softerra LDAP Administrator provides a wide variety of features essential for LDAP development, deployment, and administration of directories". Below this is a screenshot of the Softerra LDAP Administrator interface, showing a user profile for "Franco Banucci" with details like "First Name: Franco", "Last Name: Banucci", and "Title: Training Manager". To the right of the main content are five tool recommendations, each with an icon and a link: "LDAP Admin Tool" (https://www.ldapsoft.com), "LDAP Account Manager" (https://www.ldap-account-manager.org), "LDAP Search" (http://securityxploded.com), "JXplorer" (http://www.jxplorer.org), and "Active Directory Explorer" (https://docs.microsoft.com). The page footer includes a copyright notice for EC-Council.

LDAP Enumeration Tools

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.

- **Softerra LDAP Administrator**

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

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. Additionally, it provides a wide variety of features essential for LDAP development, deployment, and administration of directories.

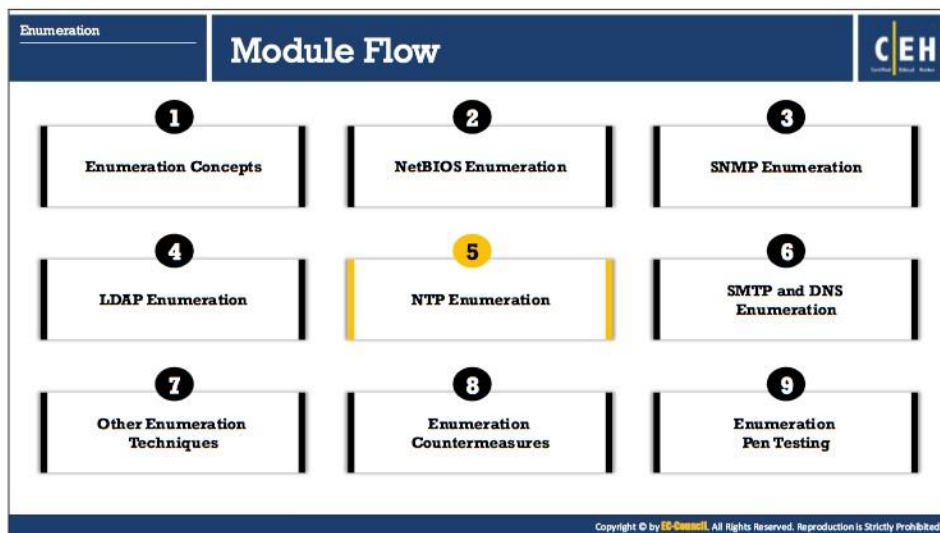
Features:

- 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.

Some of the LDAP enumeration tools are listed below:

- LDAP Admin Tool (<https://www.ldapsoft.com>)
- LDAP Account Manager (<https://www.ldap-account-manager.org>)
- LDAP Search (<http://securityxploded.com>)
- JXplorer (<http://www.jxplorer.org>)
- Active Directory Explorer (<https://docs.microsoft.com>)

- LDAP Admin (<http://www.ldapadmin.org>)
- LDAP Administration Tool (<https://sourceforge.net>)
- OpenLDAP (<https://www.openldap.org>)
- ad-ldap-enum (<https://github.com>)
- LEX - The LDAP Explorer (<http://www.ldapexplorer.com>)
- LDAP Browser/Editor (<https://www.novell.com>)



The slide features a vertical stack of four icons on the left: a clock, a building, a globe, and a server rack. To the right, there are four text blocks. A yellow callout box on the right contains a list of information gathered by an attacker. The CEH logo is in the top right corner.

Network Time Protocol (NTP) is designed to **synchronize clocks of networked computers**

It uses **UDP port 123** as its primary means of communication

NTP can maintain time to within **10 milliseconds (1/100 seconds)** over the public Internet

It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions

Attacker queries NTP server to gather valuable information such as:

- List of **hosts connected to NTP server**
- Clients IP addresses** in a network, their system names and OSs
- Internal IPs** can also be obtained if NTP server is in the demilitarized zone (DMZ)

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

NTP Enumeration

Administrators often overlook the Network Time Protocol (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 is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time to within 10 milliseconds (1/100 seconds) over the public Internet. It can achieve accuracies of 200 microseconds or better in local area networks under ideal conditions.

Attacker queries NTP server to gather valuable information such as:

- List of hosts connected to NTP server
- Clients IP addresses in a network, their system names and OSs
- Internal IPs can also be obtained if NTP server is in the DMZ

Enumeration
NTP Enumeration

NTP Enumeration Commands

CEH
Certified Ethical Hacker

- **ntptrace**
 - Traces a chain of NTP servers back to the primary source
 - `ntptrace [-vdn] [-r retries] [-t timeout] [server]`
- **ntpdc**
 - Monitors operation of the NTP daemon, ntpd
 - `ntpdc [-ilnps] [-c command] [host] [...]`
- **ntpq**
 - Monitors NTP daemon ntpd operations and determines performance
 - `ntpq [-inp] [-c command] [host] [...]`

ntpdc queries

ntpq: readlist query

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

NTP Enumeration Commands

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 4.4: ntpdate parameters and their respective functions

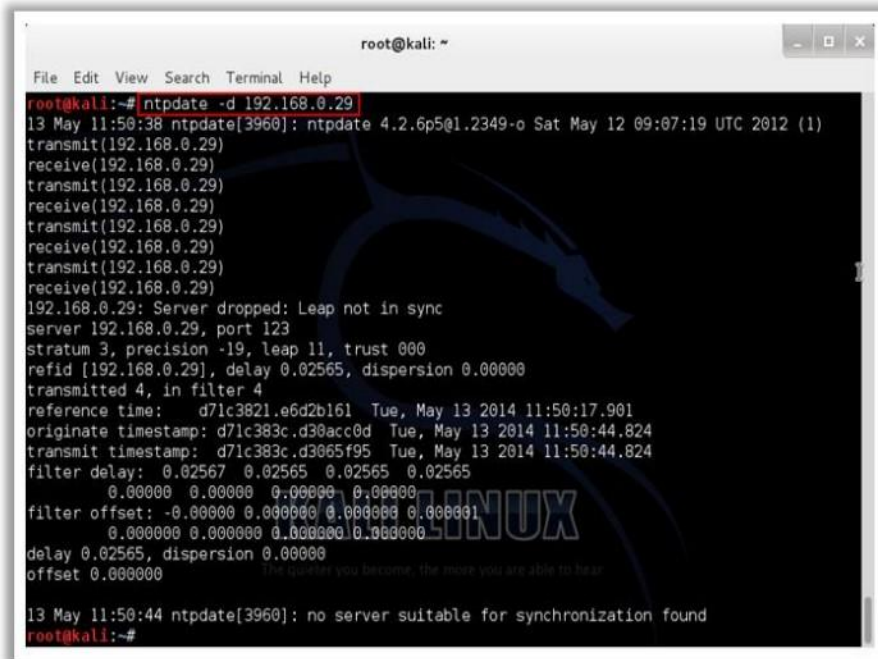


FIGURE 4.3: Screenshot of ntpdate command showing debugging information for a given IP

▪ **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]`

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

TABLE 4.5: ntptrace parameters and their respective functions

Example:

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

▪ **ntpd**

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

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

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

TABLE 4.6: 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]`

<code>-c</code>	Following argument is an interactive format command. Multiple -c options may be given
<code>-d</code>	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 4.7: ntpq parameters and their respective functions

Example:


```
ntpq> version  
ntpq 4.2.8p10@1.3728-o  
ntpq> host  
current host is localhost
```

Enumeration
NTP Enumeration

NTP Enumeration Tools



PRTG Network Monitor includes **SNTP Sensor monitors**, a Simple Network Time Protocol (SNTP) server that shows response time of the server and time difference in comparison to the local system time



Duration	0	Last Value	Minimum	Maximum	Settings
Difference	1	0 s	0 s	22 m 39 s	
Downtime	-4				
Response Time	0	28 msec	22 msec	121,113 msec	

NTP Enumeration Tools

- Nmap (<https://nmap.org>)
- Wireshark (<https://www.wireshark.org>)
- udp-proto-scanner (<https://labs.portcullis.co.uk>)
- NTP Time Server Monitor (<https://www.meinbergglobal.com>)

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

NTP Enumeration Tools

NTP enumeration tools are used to monitor working of NTP and SNTP servers present in the network and also help in the configuration and verification of connectivity from the time client to the NTP servers.

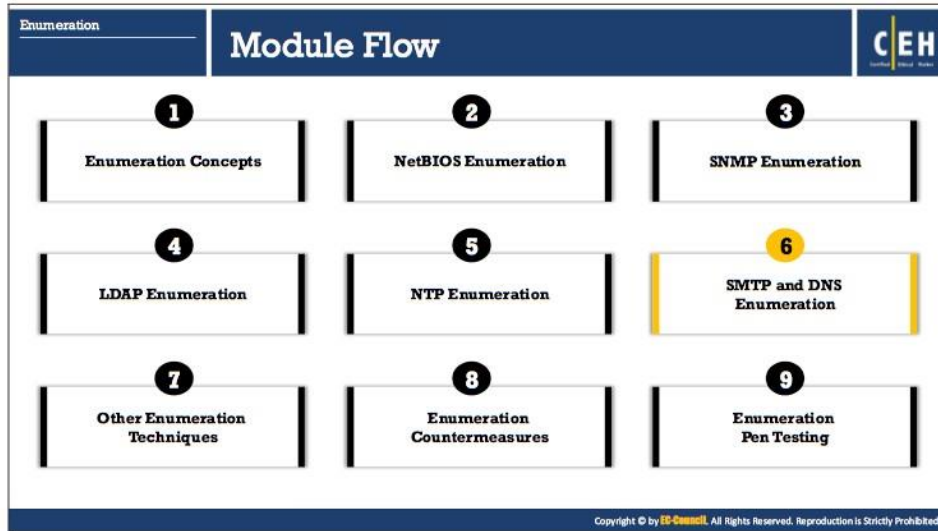
- **PRTG Network Monitor**

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

PRTG monitors all systems, devices, traffic and applications of the IT infrastructure using various technologies such as SNMP, WMI, SSH, etc. PRTG Network Monitor includes SNTP Sensor monitors, a Simple Network Time Protocol (SNTP) server that shows response time of the server and time difference in comparison to the local system time.

Some of the NTP enumeration tools include:

- Nmap (<https://nmap.org>)
- Wireshark (<https://www.wireshark.org>)
- udp-proto-scanner (<https://labs.portcullis.co.uk>)
- NTP Time Server Monitor (<https://www.meinbergglobal.com>)



SMTP and DNS Enumeration

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.

Enumeration
SMTP and DNS Enumeration

SMTP Enumeration

- SMTP provides 3 built-in-commands:
 - **VERFY** - Validates users
 - **EXPN** - Tells the actual delivery addresses of aliases and mailing lists
 - **RCPT TO** - Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can **determine valid users on SMTP server**
- Attackers can directly interact with SMTP via the telnet prompt and collect **list of valid users** on the SMTP server

Using the SMTP VRFY Command

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

Using the SMTP EXPN Command

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

Using the SMTP RCPT TO Command

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

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

SMTP Enumeration

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

SMTP provides 3 built-in-commands:

- **VERFY** - Validates users


```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```
- **EXPN** - Tells the actual delivery addresses of aliases and mailing lists


```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
```

```
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

- **RCPT TO** - Defines the recipients of the message

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

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server. Attackers can directly interact with SMTP via the telnet prompt and collect list of valid users on the SMTP server.

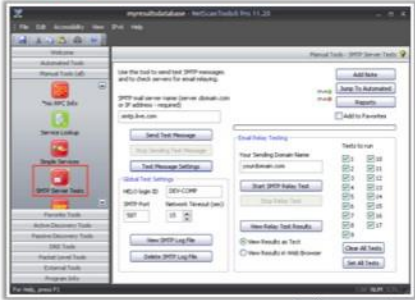
Administrators and pen testers can perform SMTP enumeration using command-line utilities such as telnet, netcat, etc. or by using tools such as Metasploit, Nmap, NetScanTools Pro, smtp-user-enum, etc., to collect a list of valid users, delivery addresses, recipients of the message, etc.

Enumeration
SMTP and DNS Enumeration

SMTP Enumeration Tools

NetScanTools Pro


- NetScanTools Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and **performing relay tests** by communicating with a SMTP server



<https://www.netscantools.com>

smtp-user-enum

- It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail)
- Enumeration is performed by inspecting the responses to **VRFY, EXPN, and RCPT TO** commands



<http://pentestmonkey.net>, <http://pentestlab.blog>

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

SMTP Enumeration Tools

SMTP enumeration tools are used to perform username enumeration. Attackers can use the usernames obtained from this enumeration to launch further attacks on other systems in the network.

- **NetScanTools Pro**

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

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.

- **smtp-user-enum**

Source: <http://pentestmonkey.net>

smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands. smtp-user-enum simply needs to be passed on to 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 for a maximum of n seconds for reply (default: 5)
- **-v** - Verbose
- **-h** - This help message

Some of the SMTP enumeration tools include:

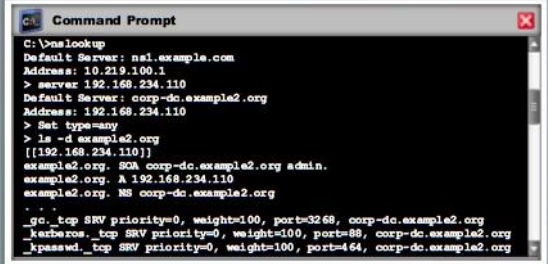
- Telnet (<https://technet.microsoft.com>)
- Vanquish (<https://github.com>)
- MX Toolbox (<https://mxttoolbox.com>)

Enumeration
SMTP and DNS Enumeration

DNS Enumeration Using Zone Transfer



- It is a process for **locating the DNS server** and the **records of a target network**
- An attacker can gather valuable **network information** such as DNS server names, host names, machine names, user names, IP addresses, etc. of the potential targets
- In DNS zone transfer enumeration, an attacker tries to **retrieve a copy of the entire zone file** for a domain from the DNS server



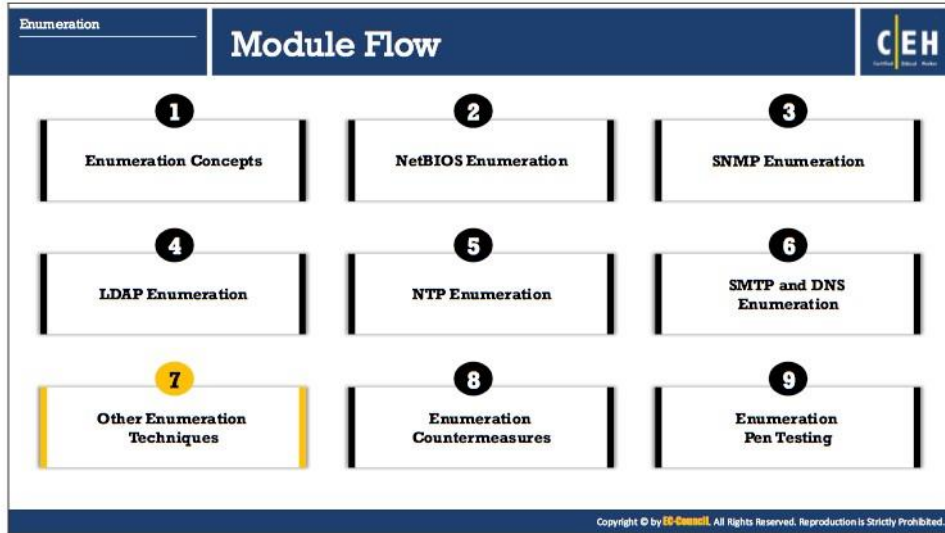
```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> Set type=any
> ls -d example2.org
[[192.168.234.110]]
example2.org. 90A corp-dc.example2.org admin.
example2.org. A 192.168.234.110
example2.org. NS corp-dc.example2.org
. . .
_gc._tcp SRV priority=0, weight=100, port=3268, corp-dc.example2.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.example2.org
_kpasswd._tcp SRV priority=0, weight=100, port=464, corp-dc.example2.org
```

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

DNS Enumeration Using Zone Transfer

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. In a DNS zone transfer enumeration, an attacker tries to retrieve a copy of the entire zone file for a domain from the DNS server. 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.




Other Enumeration Techniques

This section will familiarize you with IPsec, VoIP, RPC, and Unix/Linux user enumerations.


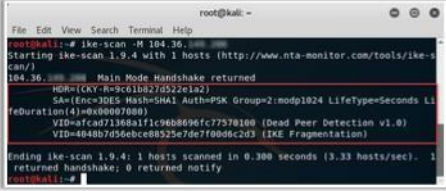
Enumeration

Other Enumeration Techniques

IPsec Enumeration



- IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange) to secure **communication between virtual private network (VPN) end points**
- Most IPsec based **VPNs use Internet Security Association and Key Management Protocol (ISAKMP)**, a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment
- A simple **scanning for ISAKMP at UDP port 500** can indicate the presence of a VPN gateway
- Attackers can probe further using a tool such as **ike-scan** to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA LifeDuration, etc.

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

IPsec Enumeration

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host to gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components like ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to secure communication between VPN end-points.

Most IPsec based VPNs use ISAKMP (Internet Security Association Key Management Protocol), a part of IKE, to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attacker can perform a simple direct scanning for ISAKMP at UDP port 500 with tools like Nmap, etc. to acquire the information related to the presence of a VPN gateway.

You can enter the following command to perform Nmap scan for checking the status of isakmp over port 500:

```
# nmap -sU -p 500 <target IP address>
```

Attackers can probe further using fingerprinting tools such as ike-scan to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA LifeDuration, etc. In this type of scan, specially crafted IKE packets with ISAKMP header are sent to the target gateway and the responses are recorded.

An initial IPsec VPN discovery with ike-scan tool is discussed below:

```
# ike-scan -M <target gateway IP address>
```

- **ike-scan**

Source: <https://github.com>

ike-scan discovers IKE hosts and can also fingerprint them using the retransmission backoff pattern.


ike-scan can perform the following functions:

- **Discovery:** Determine which hosts in a given IP range are running IKE. This is done by displaying those hosts which respond to the IKE requests sent by ike-scan.
- **Fingerprinting:** Determine which IKE implementation the hosts are using, and in some cases determine the version of software that they are running. This is done in two ways: firstly by UDP backoff fingerprinting which involves recording the times of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns; and secondly by Vendor ID fingerprinting which compares Vendor ID payloads from the VPN servers against known vendor id patterns.
- **Transform Enumeration:** Find which transform attributes are supported by the VPN server for IKE Phase-1 (e.g. encryption algorithm, hash algorithm, etc.).
- **User Enumeration:** For some VPN systems, discover valid VPN usernames.
- **Pre-Shared Key Cracking:** Perform offline dictionary or brute-force password cracking for IKE Aggressive Mode with Pre-Shared Key authentication. This uses ike-scan to obtain the hash and other parameters, and psk-crack (which is part of the ike-scan package) to perform the cracking.

Enumeration

Other Enumeration Techniques

VoIP Enumeration



- VoIP uses **SIP (Session Initiation Protocol) protocol** to enable voice and video calls over an IP network
- SIP service generally uses **UDP/TCP ports 2000, 2001, 5050, 5061**
- VoIP enumeration provide sensitive information such as **VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones User-agent IP addresses and user extensions**
- This information can be used to launch various VoIP attacks such as **Denial-of-Service (DoS), Session Hijacking, Caller ID spoofing, Eavesdropping, Spaming over Internet Telephony (SPIT), VoIP phishing (Vishing)**, etc.

```

root@kali ~# nmap 192.168.0.1/24
Nmap scan report for 192.168.0.1
Host: 192.168.0.1
OS: Linux 3.10
Device: User Agent
SIP Device
-----
| Fingerprint |
|-----|
| 192.168.0.187:5060 | Grandstream GXP1620 1.0.4.33 | disabled |
| 192.168.0.87:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.169:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.54:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.110:5060 | Grandstream GXP1620 1.0.2.27 | disabled |

```

```

root@kali ~# nmap --script=auxiliary/scanner/sip/sipoptions 192.168.0.1/24
Nmap scan report for 192.168.0.1/24
Host: 192.168.0.1/24
OS: Linux 3.10
Device: User Agent
SIP Device
-----
| Fingerprint |
|-----|
| 192.168.0.187:5060 | Grandstream GXP1620 1.0.4.33 | disabled |
| 192.168.0.87:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.169:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.54:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.110:5060 | Grandstream GXP1620 1.0.2.27 | disabled |

```

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

VoIP Enumeration

VoIP is the advanced technique that has replaced traditional PSTN in both corporate and home environments. VoIP uses internet infrastructure to establish the connection for voices, data also travels on the same network; however, VoIP is vulnerable to TCP/IP attack vectors. SIP (Session Initiation Protocol) is one of the protocols used by VoIP in performing voice calls, video calls, etc. over an IP network. This SIP service generally uses UDP/TCP ports 2000, 2001, 5050, 5061.

Attackers use Svmmap and Metasploit tools to perform VoIP enumeration. VoIP enumeration provide sensitive information such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones User-agent IP addresses and user extensions, etc. to the attacker. This information can be used to launch various VoIP attacks such as Denial-of-Service (DoS), Session Hijacking, Caller ID spoofing, Eavesdropping, Spaming over Internet Telephony (SPIT), VoIP phishing (Vishing), etc.

- **Svmmap**

Source: <https://github.com>

Svmmap is a free and Open Source scanner to identify sip devices and PBX servers on a target network. It can also be helpful for systems administrators when used as a network inventory tool. Svmmap was designed to be faster than the competition by specifically targeting SIP over UDP.

Svmmap can:

- Identify SIP devices and PBX servers on default and non-default ports
- Scan large ranges of networks

- Scan just one host on different ports, looking for a SIP service on that host or just multiple hosts on multiple ports
- Take previous scan results as input, allowing you to only scan known hosts running SIP
- Use different scanning methods (make use of REGISTER instead of OPTIONS request)
- Get all the phones on a network to ring at the same time (using INVITE as method)
- Randomly scan internet ranges
- Resume previous scans

Enumeration
Other Enumeration Techniques

RPC Enumeration

- Remote Procedure Call (RPC) allows client and server to communicate in **distributed client/server programs**
- Enumerating RPC endpoints enable attackers to **identify any vulnerable services** on these service ports

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

RPC Enumeration

RPC (Remote Procedure Call) is a technology used for creating distributed client/server programs. RPC allows client and server to communicate in distributed client/server programs. It is an inter-process communication mechanism, which enables data exchange in between different processes. In general, RPC consists of components like client, server, endpoint, endpoint mapper, client stub and server stub along with various dependencies.

The portmapper service listens on TCP and UDP port 111 in order to detect the endpoints and present clients details of listening RPC services. Enumerating RPC endpoints enable attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan high port ranges to identify RPC services that are open to direct attack.

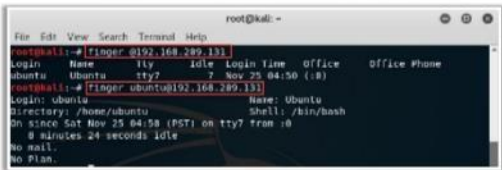
You can use the following Nmap scan commands to identify the RPC service running on the network.

```
# nmap -sR <target IP/network>
```

```
# nmap -T4 -A <target IP/network>
```

Additionally, you can also use tools like NetScanTools Pro to capture the RPC information of the target network.

Enumeration		Unix/Linux User Enumeration		CEH	
Other Enumeration Techniques					
rusers	<ul style="list-style-type: none">Displays a list of users who are logged on to remote machines or machines on local network Syntax: <code>/usr/bin/rusers [-a] [-l] [-u] [-h] [-i] [Host ...]</code>				
rwho	<ul style="list-style-type: none">Displays a list of users who are logged in to hosts on the local network Syntax: <code>rwho [-a]</code>				
finger	<ul style="list-style-type: none">Displays information about system users such as user's login name, real name, terminal name, idle time, login time, office location and office phone numbers Syntax: <code>finger [-l] [-m] [-p] [-a] [user ...] [user@host ...]</code>				



```
root@kali:~# finger ubuntu192.168.289.131
Login: ubuntu          Name: ubuntu
Directory: /home/ubuntu      Shell: /bin/bash
ln since Sat Nov 25 04:58 (PST) on tty7 from :0
  0 minutes 24 seconds idle
no mail.
no plan.
```

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

Unix/Linux User Enumeration

One of the important step for conducting an enumeration is to perform Unix/Linux user enumeration. Unix/Linux user enumeration provides list of users along with details like user name, host name, start date and time of each session, etc.

You can use following command line utilities to perform UNIX / Linux user enumeration:

- **rusers**

rusers displays a list of users who are logged on to remote machines or machines on local network. It displays output similar to who, but for the hosts/systems on the local network.

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

Where,

- **-a:** Gives a report for a machine even if no users are logged in
- **-h:** Sorts alphabetically by host name
- **-l:** Gives a longer listing similar to the who command
- **-u:** Sorts by number of users
- **-i:** Sorts by idle time

- **rwho**

rwho displays a list of users who are logged in to hosts on the local network. It produces output similar to who command which contains information about user name, host name, and start date and time of each session for all machines on the local network running the rwho daemon.

Syntax: `rwho [-a]`

where,

- **-a:** Includes all users. Without this flag, users whose sessions are idle an hour or more are not included in the report.

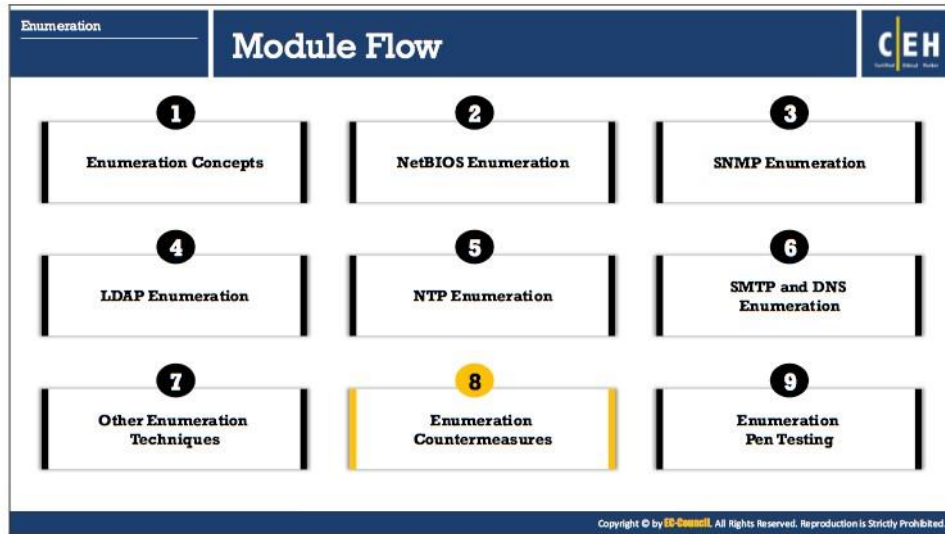
- **finger**

finger displays information about system users such as user's login name, real name, terminal name, idle time, login time, office location and office phone numbers.

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

Where,

- **-s:** Displays user's login name, real name, terminal name, idle time, login time, office location and office phone number.
- **-l:** Produces a multi-line format displaying all of the information described for the -s option as well as the user's home directory, home phone number, login shell, mail status, and the contents of the files ``.plan`` ``.project`` ``.pgpkey`` and ``.forward`` from the user's home directory.
- **-p:** Prevents the -l option of finger from displaying the contents of the ``.plan`` ``.project`` and ``.pgpkey`` files.
- **-m:** Prevent matching of user names.



Enumeration Countermeasures

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, DNS, SMTP, LDAP, and SMB enumeration.

Enumeration
Enumeration Countermeasures

Enumeration Countermeasures

CEH

SNMP

- Remove the **SNMP agent** or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default **community string names**
- Upgrade to **SNMP3**, which encrypts passwords and messages
- Implement the Group Policy security option called **"Additional restrictions for anonymous connections"**
- Ensure that the access to **null session pipes**, **null session shares**, and IPSec filtering is restricted

DNS

- Disable the DNS zone transfers to the untrusted hosts
- Make sure that the private hosts and their IP addresses are not published in **DNS zone files** of public DNS server
- Use **premium DNS registration services** that hide sensitive information such as host information (HINFO) from public
- Use **standard network admin contacts** for DNS registrations in order to avoid social engineering attacks

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

Enumeration
Enumeration Countermeasures

Enumeration Countermeasures (Cont'd)

CEH

SMTP

Configure SMTP servers to:

- Ignore **email messages** to unknown recipients
- Not to include sensitive **mail server** and **local host information** in mail responses
- Disable **open relay** feature
- Limit the number of **accepted connections** from a source in order to prevent brute force attacks

LDAP

- By default, LDAP traffic is transmitted unsecured; use **SSL or STARTTLS technology** to encrypt the traffic
- Select a **user name different** from your email address and enable **account lockout**

SMB

- Disable SMB protocol on **Web and DNS Servers**
- Disable SMB protocol on **Internet facing servers**
- Disable ports **TCP 139** and **TCP 445** used by the SMB protocol
- Restrict anonymous access through **RestrictNullSessAccess** parameter from the **Windows Registry**

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

SNMP Enumeration Countermeasures

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default community string names
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"

- Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted
- 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

- Disable the DNS zone transfers to the untrusted hosts
- Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
- Use premium DNS registration services that hide sensitive information such as host information (HINFO) from public
- Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks
- Prune DNS zone files to prevent revealing unnecessary information

SMTP Enumeration Countermeasures

Configure SMTP servers to:

- Ignore email messages to unknown recipients
- Not to include sensitive mail server and local host information in mail responses
- Disable open relay feature
- Limit the number of accepted connections from a source in order to prevent brute force attacks
- 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

- By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic
- Select a user name different from your email address and enable account lockout
- Restrict the access to Active Directory by using software such as Citrix

SMB Enumeration Countermeasures

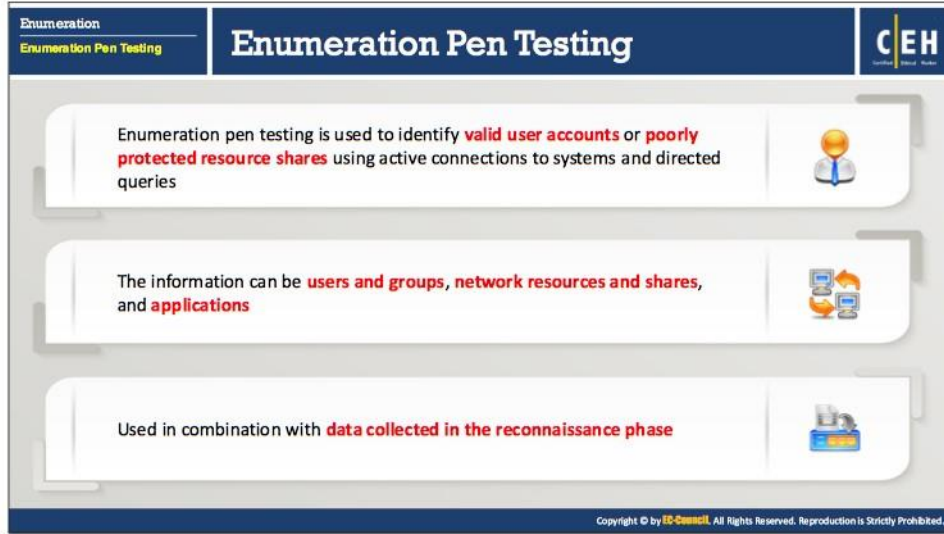
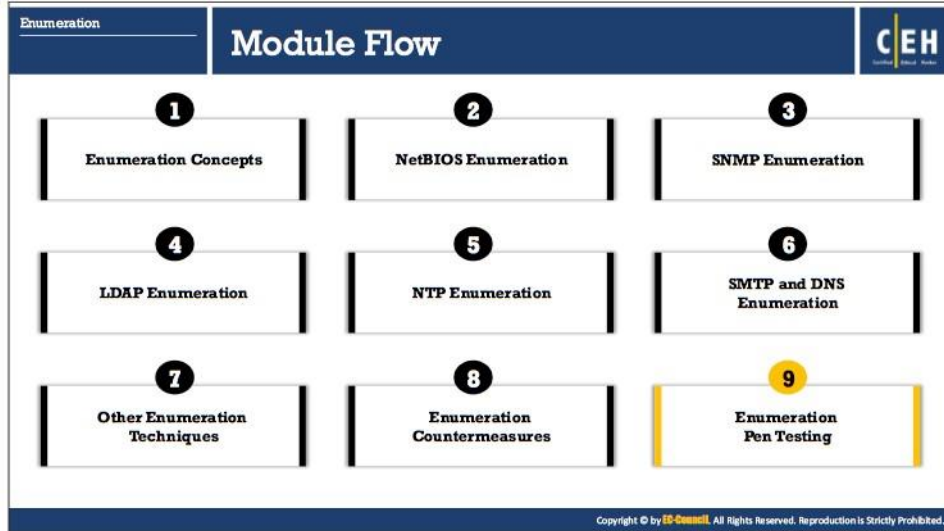
Common sharing services or other unused services may prove to be doorways for attackers to break into a network's security. **Server Message Block (SMB)** is a protocol that provides shared access to files, serial ports, printers, and communications between nodes on a network. If this service is running 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

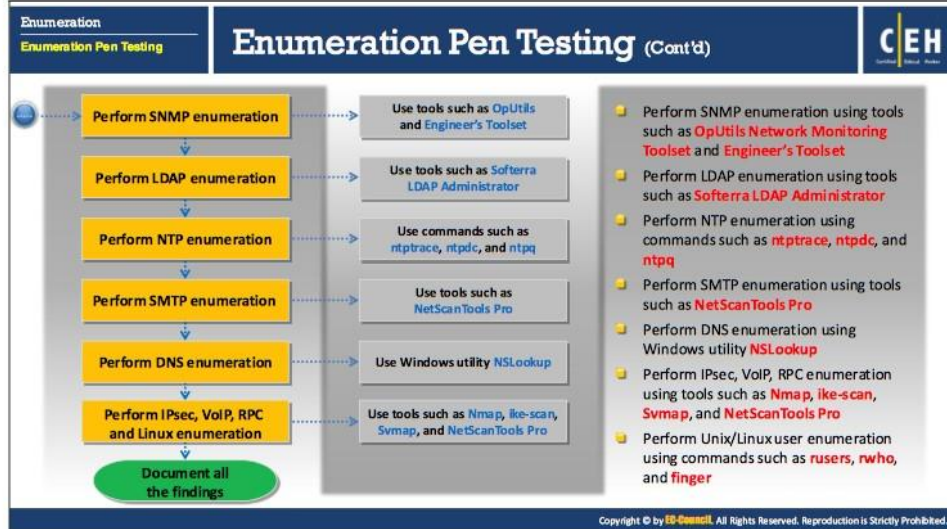
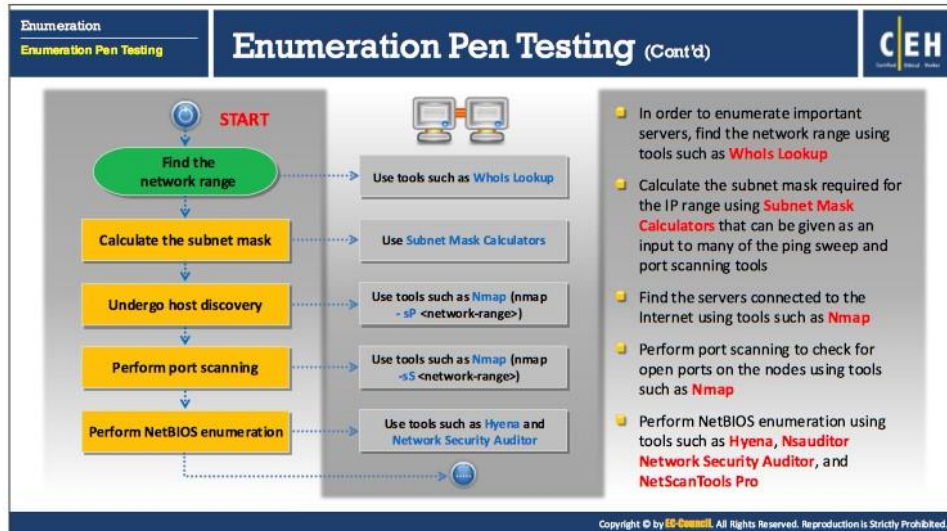
be disabled by uninstalling the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** properties of **Network and Dial-up Connections**. On servers that are accessible from the internet, also known as bastion hosts, SMB can be disabled by uninstalling the same two 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.





Enumeration Pen Testing

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. It is used to identify valid user accounts or poorly protected resource shares using active connections to systems and directed queries.

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 Hyena, Nsauditor Network Security Auditor, and NetScanTools Pro 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 10: Perform IPsec, VoIP, VPN and Linux enumeration**

Perform IPsec enumeration to extract information about encryption and hashing algorithm, authentication type, key distribution algorithm, SA LifeDuration, etc. Tools such as ike-scan and Nmap can extract this information.

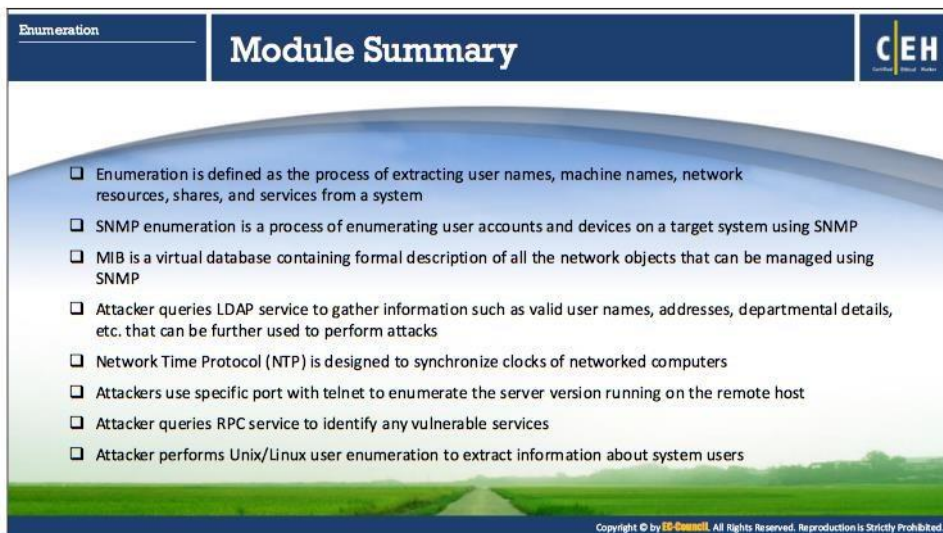
Perform VoIP enumeration to extract information about VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones User-agent IP addresses and user extensions, etc. Use tool such as Svmmap and Metasploit to collect this information.

Perform RPC enumeration to identify any vulnerable services on the RPC service ports. Use tools such as Nmap and NetScan Tools Pro to extract this information.

Perform Unix/Linux user enumeration to extract information about system users. Commands such as `rusers`, `rwho`, and `finger` can obtain 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.



The slide features a dark blue header with the word "Enumeration" on the left and the "CEH" logo on the right. The main content area has a light blue background with a white curved top and a green landscape at the bottom. A list of eight items, each preceded by a square checkbox, is displayed. A small copyright notice is visible at the bottom right of the slide.

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system
- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP
- MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers
- Attackers use specific port with telnet to enumerate the server version running on the remote host
- Attacker queries RPC service to identify any vulnerable services
- Attacker performs Unix/Linux user enumeration to extract information about system users

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

Module Summary

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 perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.