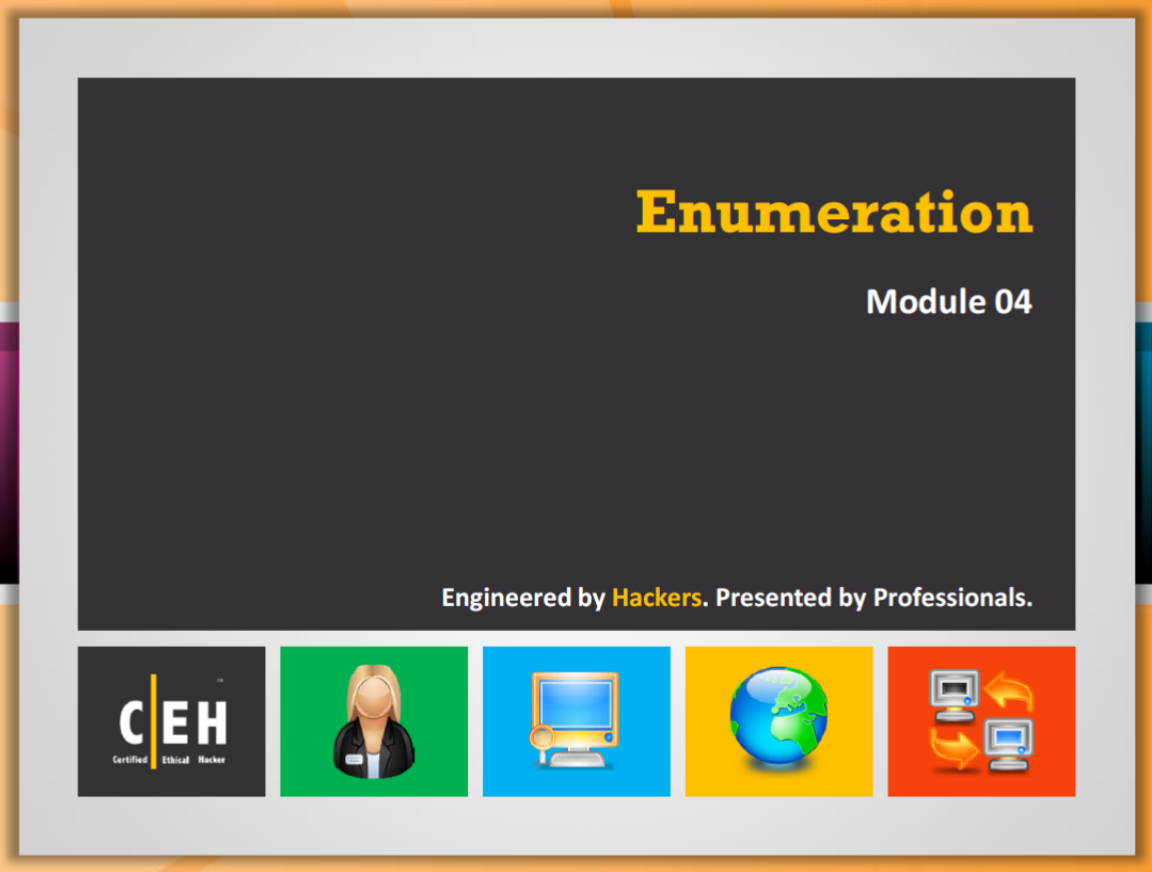
Enumeration

Module 04



Ethical Hacking and Countermeasures v8

Module 04: Enumeration

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security News

Hackers Attack US Weather Service

Source: http://www.theaustralian.com.au

The US National Weather Service computer network was hacked with a group from Kosovo claiming credit and posting sensitive data, security experts said recently.

Data released by the **Kosovo Hackers Security** group includes directory structures, sensitive files from the web server, and other data that could enable later access, according to Chrysostomos Daniel of the security firm Acunetix.

"The hacker group stated that the attack is a protest against the US policies that target Muslim countries," Daniel said.

Moreover, the attack was a payback for hacker attacks against nuclear plants in Muslim countries, according to a member of the hacking group who said, "They hack our nuclear plants using **STUXNET** and **FLAME-like malwares**, they are bombing us 24-7, we can't sit silent -- hack to payback them."

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Paul Roberts, writing on the Sophos Naked Security blog, said the leaked information includes a list of administrative account names, which could open the hacked servers to subsequent "**brute force attacks**."

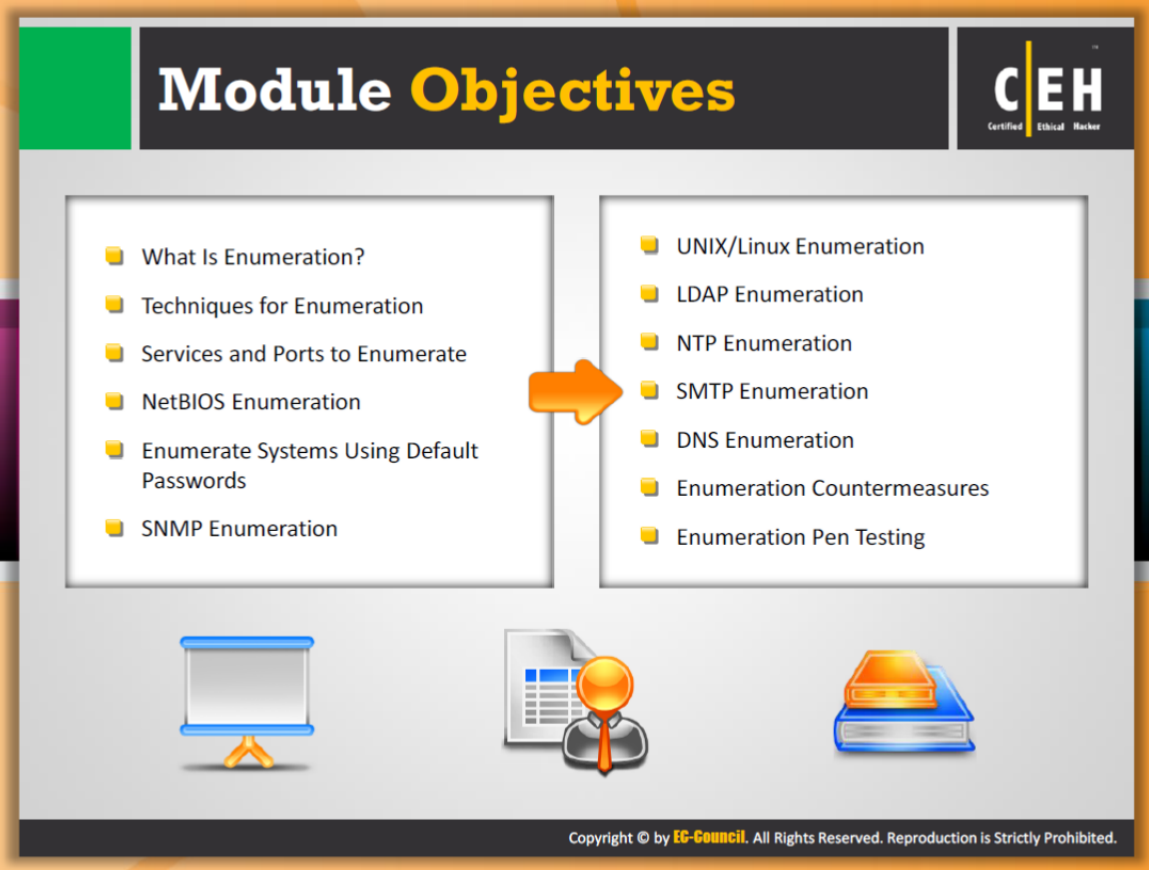
"Little is known about the group claiming responsibility for the attack," he said.

"However, they allege that the weather.gov hack was just one of many US government hacks the group had carried out and that more releases are pending."

© 2011 CBS Interactive. All rights reserved.

http://www.theaustralian.com.au/australian-it/hackers-attack-us-weather-service/story-e6frgakx-1226499796122

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

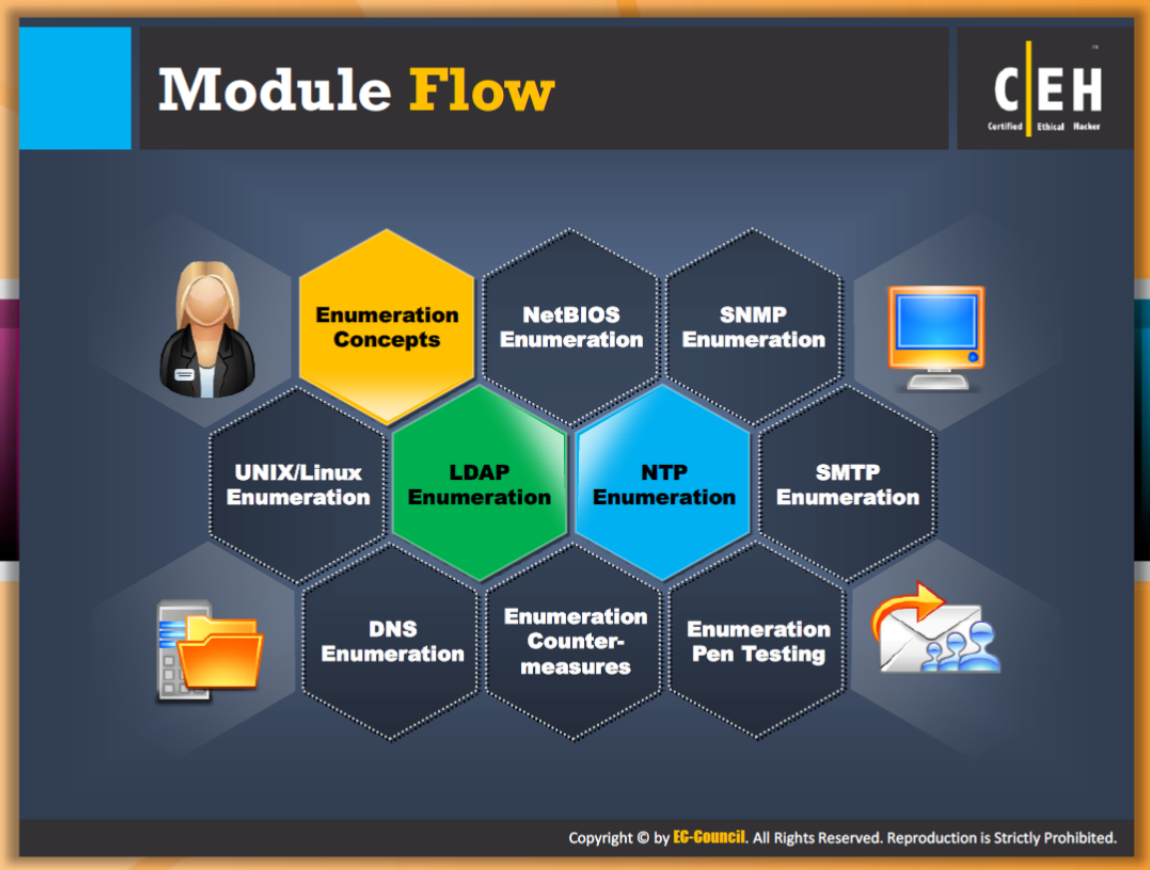


Module Objectives

In the previous modules, you learned about **foot printing** and **scanning networks**. The next phase of penetration testing is enumeration. As a pen tester, you should know the purpose of performing enumeration, techniques used to perform enumeration, where you should apply **enumeration**, what information you get, enumeration tools, and the countermeasures that can make **network security** stronger. All these things are covered in this module. This module will familiarize you with the following:

- What Is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- Enumerate Systems Using Default Passwords
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



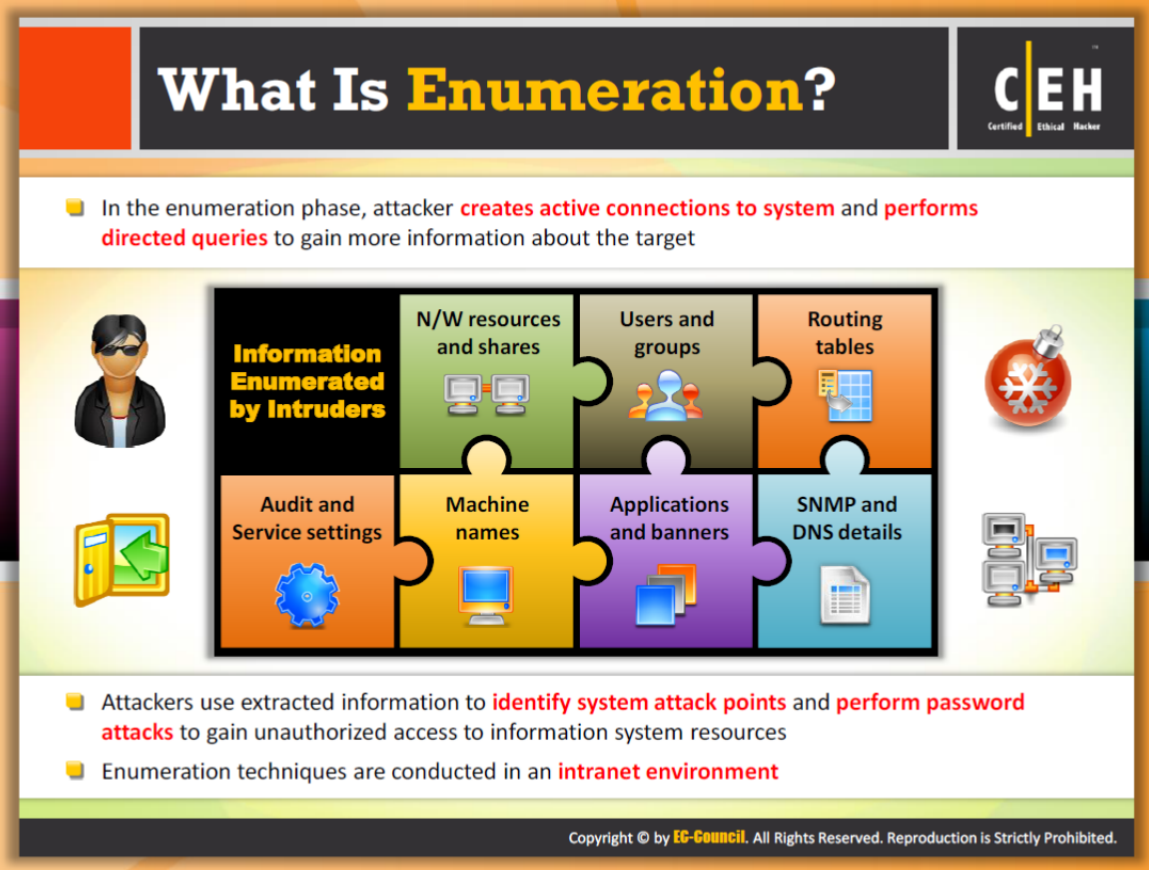
Module Flow

In order to make you better understand the concept of enumeration, we have divided the module into various sections. Each section deals with different services and ports to enumerate. Before beginning with the actual enumeration process, first we will discuss enumeration concepts.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section briefs you about what enumeration is, enumeration techniques, and services and ports to enumerate.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Is Enumeration?

Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. In the **enumeration phase**, the attacker creates active connections to the system and performs directed queries to gain more information about the target. The attacker uses the gathered information to identify the vulnerabilities or weak points in system security and then tries to exploit them. Enumeration techniques are conducted in an **intranet environment**. It involves making active connections to the target system. It is possible that the attacker stumbles upon a remote IPC share, such as **IPC$ in Windows**, that can be probed with a null session allowing shares and accounts to be enumerated.

The previous modules highlighted how the attacker gathers necessary information about the target without really getting on the wrong side of the **legal barrier**. The type of information enumerated by attackers can be loosely grouped into the following categories:

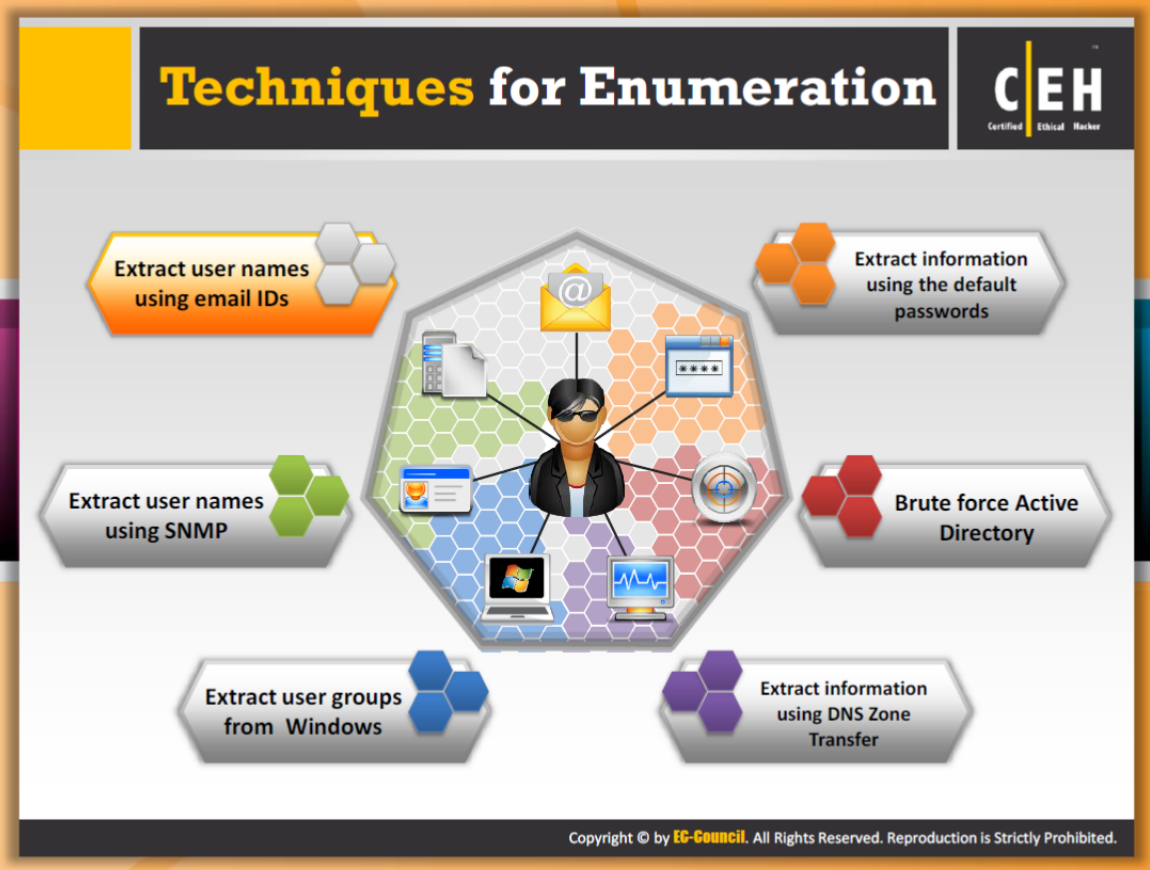
Information Enumerated by Intruders:

- Network resources and shares
- Users and groups

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Routing tables
- Auditing and service settings
- Machine names
- Applications and banners
- SNMP and DNS details

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Techniques for Enumeration

In the enumeration process, an **attacker collects data** such as network users and group names, routing tables, and Simple Network Management Protocol (SNMP) information. This module explores possible ways an attacker might enumerate a target network, and what countermeasures can be taken.

The following are the different enumeration techniques that can be used by **attackers**:

Extract user names using email IDs

In general, every email ID contains two parts; one is **user name** and the other is **domain name**. The structure of an email address is username@domainname. Consider abc@gmail.com; in this email ID "abc" (characters preceding the '@' symbol) is the user name and "gmail.com" (characters proceeding the '@' symbol) is the domain name.

Extract information using the default passwords

Many online resources provide lists of default passwords assigned by the manufacturer for their products. Often users forget to change the default passwords provided by the **manufacturer or developer** of the product. If users don't change their passwords for a long time, then attackers can easily enumerate their data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Brute force Active Directory

Microsoft Active Directory is susceptible to a user name enumeration weakness at the time of user-supplied input verification. This is the consequence of design error in the application. If the "**logon hours**" feature is enabled, then attempts to the service authentication result in varying error messages. Attackers take this advantage and exploit the weakness to enumerate valid user names. If an attacker succeeds in revealing valid user names, then he or she can conduct a **brute-force attack** to reveal respective passwords.

Extract user names using SNMP

Attackers can easily guess the “strings” using this SNMP API through which they can extract required user names.

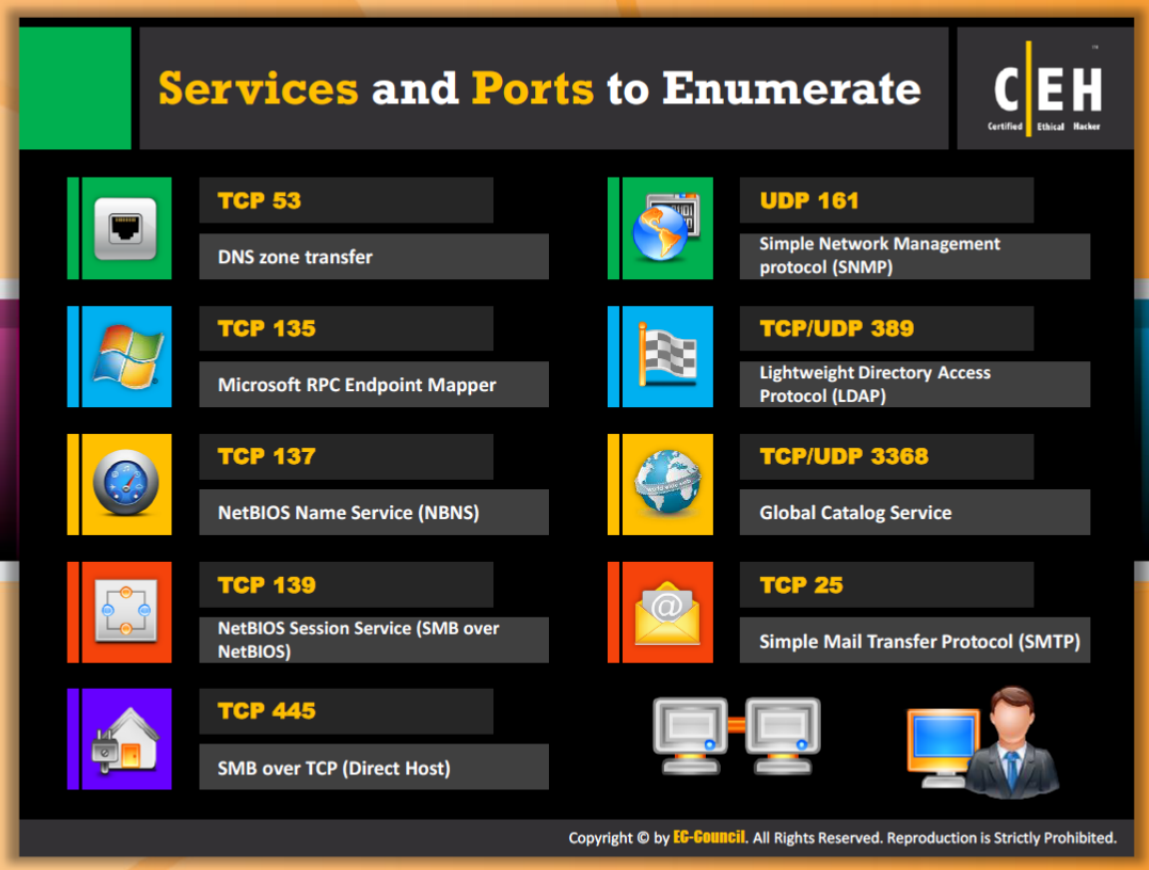
Extract user groups from Windows

These extract user accounts from specified groups and store the results and also verify if the **session accounts** are in the group or not.

Extract information using DNS Zone Transfer

DNS zone transfer reveals a lot of valuable information about the particular zone you request. When a DNS zone transfer request is sent to the DNS server, the server transfers its DNS records containing information such as DNS zone transfer. An attacker can get valuable topological information about a target’s internal network using DNS zone transfer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Services and Ports to Enumerate

TCP 53: DNS zone transfer

DNS zone transfer relies on **TCP 53 port** rather than **UDP 53**. If TCP 53 is in use then it means that DNS zone transfer is in process. The TCP protocol helps to maintain a consistent DNS database between DNS servers. This communication occurs only between DNS servers. DNS servers always use TCP protocol for the zone transfer. The connection established between DNS servers transfers the zone data and also helps both source and destination DNS servers to ensure the data consistency by means of **TCP ACK bit**.

TCP 135: Microsoft RPC Endpoint Mapper

The **RPC port 135** is used in client/server applications to exploit message services. To stop the popup you will need to filter port 135 at the firewall level. When trying to connect to a service, you go through this mapper to discover where it is located.

TCP 137: NetBIOS Name Service (NBNS)

NBNS, also known as Windows Internet Name Service (WINS), provides name resolution service for computers running **NetBIOS**. NetBIOS Name Servers maintain a database

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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. The name service is usually the first service that will be attacked.

TCP 139: NetBIOS Session Service (SMB over NetBIOS)

NetBIOS session service is used to set up and tear down sessions between NetBIOS-capable computers.

Sessions are established by exchanging packets. The computer establishing the session attempts to make a TCP connection to port 139 on the computer with which the session is to be established. If the connection is made, the computer establishing the session then sends over the connection a "Session Request" packet with the NetBIOS names of the application establishing the session and the NetBIOS name to which the session is to be established. The computer with which the session is to be established will respond with a "Positive Session Response," indicating that a session can be established or a "**Negative Session Response**," indicating that no session can be established.

TCP 445: SMB over TCP (Direct Host)

By using TCP port 445 you can directly access the TCP/IP MS Networking without the help of a **NetBIOS layer**. You can only get this service in recent versions of Windows, such as Windows2K/XP. File sharing in Windows2K/XP can be done only by using Server Message Block (SMB) protocol. You can also run SMB directly over TCP/IP in Windows 2K/XP without using the help of **extra layer** of NetBT. They use TCP port 445 for this purpose.

UDP 161: Simple Network Management protocol (SNMP)

You can use the SNMP protocol for various devices and applications (including firewalls and routers) to communicate logging and management information with **remote monitoring applications**. SNMP agents listen on UDP port 161; asynchronous traps are received on port 162.

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

You can use LDAP (Lightweight Directory Access Protocol) Internet protocol, used my **MS Active Directory**, as well as some email programs to look up contact information from a server. Both Microsoft Exchange and NetMeeting install an LDAP server on this port.

TCP/UDP 3368: Global Catalog Service

You can use TCP port 3368, which uses one of the main protocols in TCP/IP a connection-oriented protocol networks; it requires three-way handshaking to set up end-to-end communications. Only then a connection is set up to user data and can be sent bi-directionally over the connection. TCP guarantees delivery of **data packets** on port 3368 in the same order in which they were sent.

You can use UDP port 3368 for **non-guaranteed communication**. It provides an unreliable service and datagrams may arrive duplicated, out of order, or missing without notice and error

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

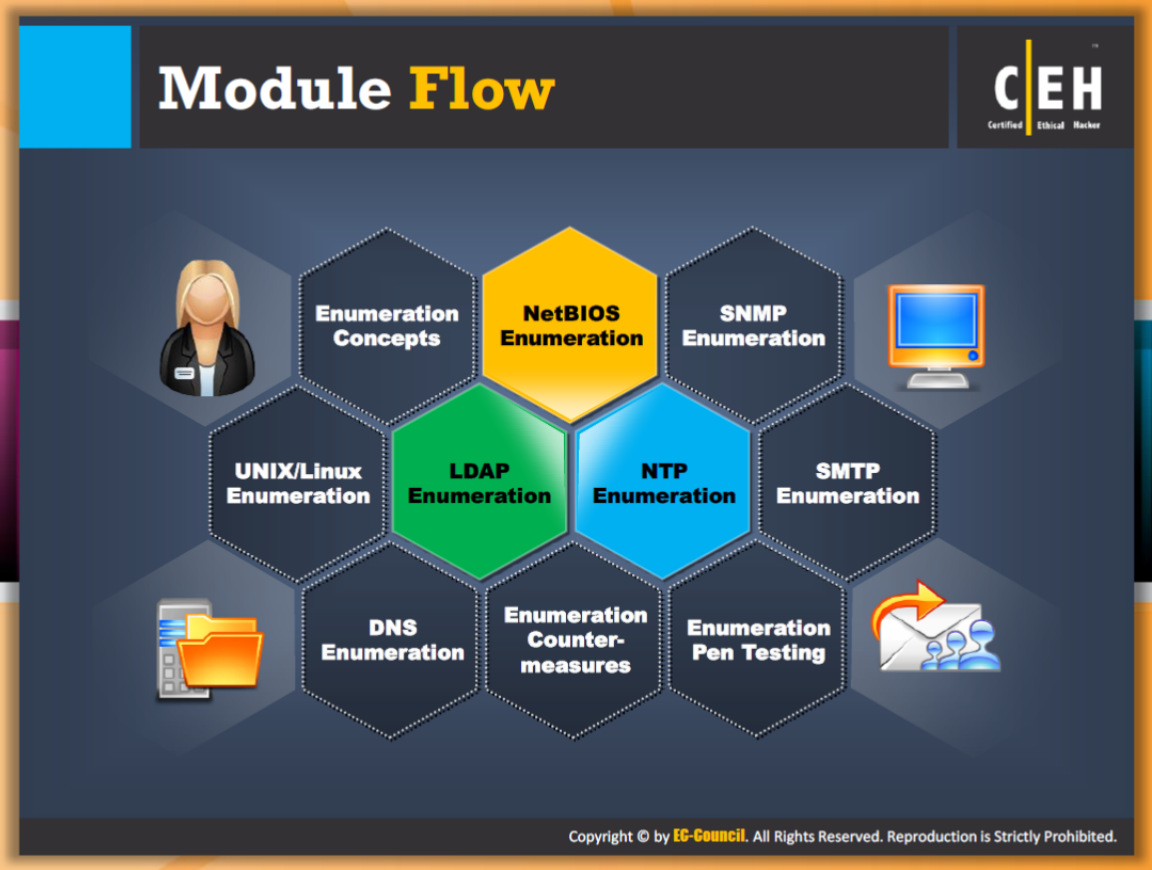
Checking and correction is not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.

UDP (User Datagram Protocol) is a minimal **message-oriented Transport Layer protocol**. Examples that often use UDP include voice over IP (VoIP), streaming media, and real-time multiplayer games.

TCP 25: Simple Mail Transfer Protocol (SMTP)

SMTP allows moving email across the Internet and across your local network. It runs on the connection-oriented service provided by **Transmission Control Protocol** (TCP), and it uses well-known port number 25. Telnet to port 25 on a remote host; this technique is sometimes used to test a remote system's SMTP server but here you can use this command-line technique to illustrate how mail is delivered between systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed enumeration concepts and the resources that give valuable information through enumeration; now it's time to put them into practice. If you are trying to enumerate information of a target network, then NetBIOS is the first place from where you should try to extract as much information as possible.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section describes **NetBIOS enumeration** and the information you can extract through enumeration, as well as NetBIOS enumeration tools.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 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 on 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 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.

NetBIOS Enumeration

The first step in enumerating a Windows machine is to take advantage of the NetBIOS API. NetBIOS stands for Network Basic Input Output System. IBM, in association with Sytek, developed NetBIOS. It was developed as an **Application Programming Interface (API)**, originally to facilitate the access of LAN resources by the client's software. The 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 and shares of the individual hosts on the network
- Policies and passwords

If an attacker finds a Windows OS with **port 139 open**, he or she would be interested in checking what resources he or she can access, or view, on the remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. Using these techniques, the attacker can launch two types of attacks on a **remote computer**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

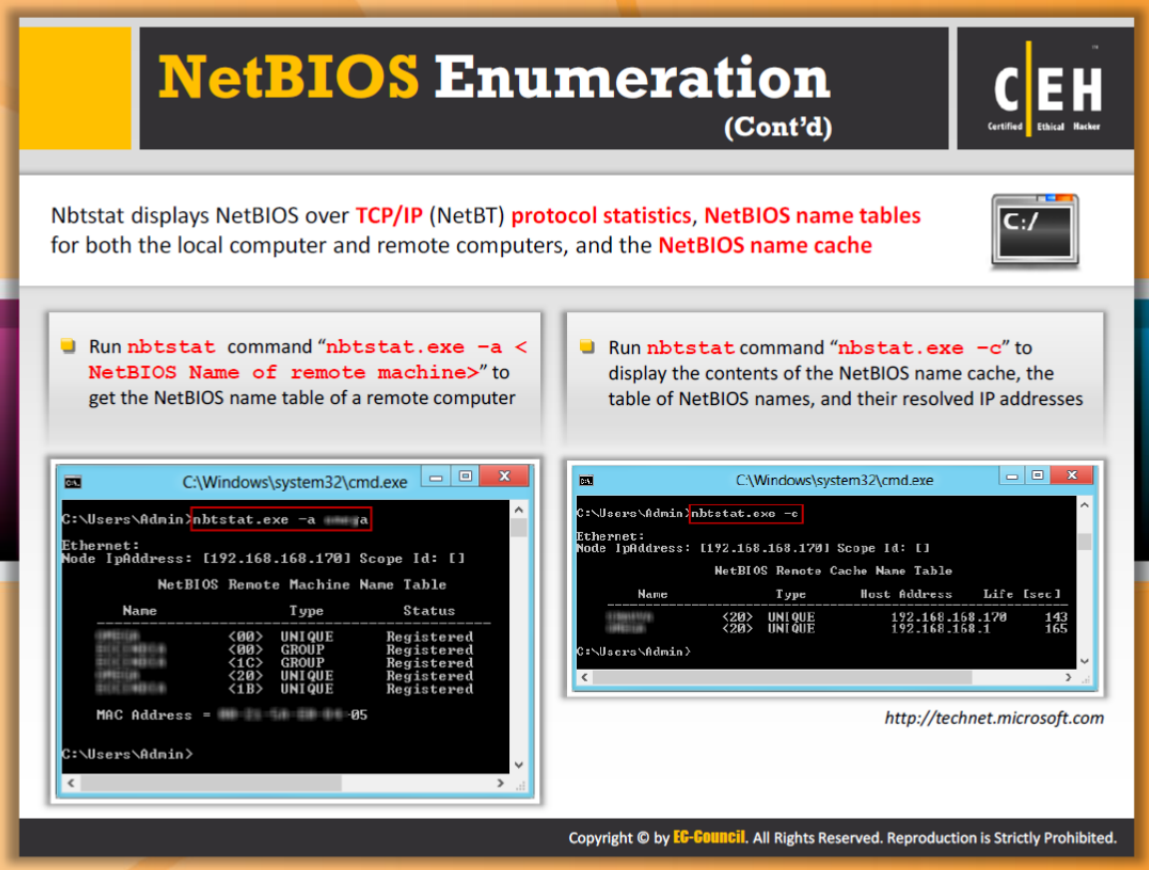
that has NetBIOS. The attacker can choose to read/write to a remote computer system, depending on the availability of shares, or launch a denial-of-service.

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 PDC for that domain

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration (Cont'd)

Source: http://technet.microsoft.com

Nbtstat displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer 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). Used without parameters, Nbtstat displays help.

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

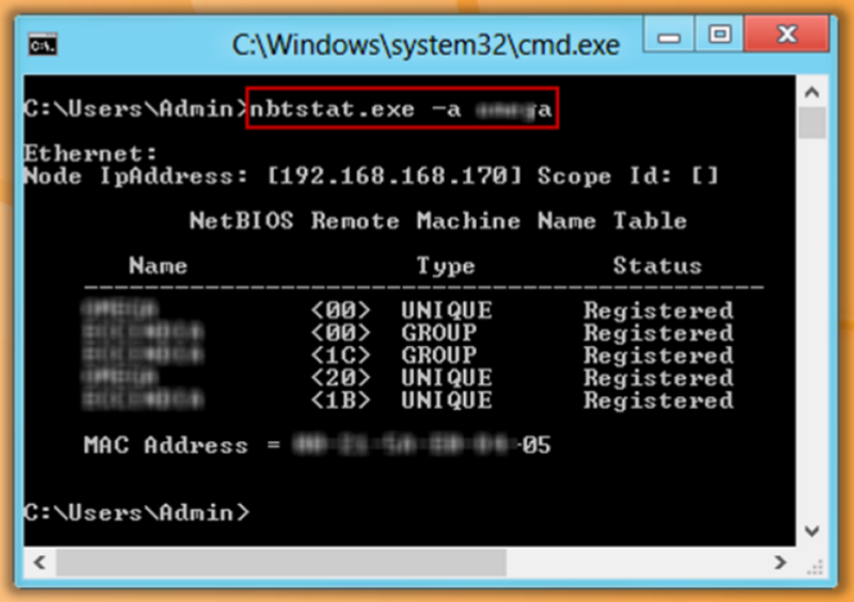


FIGURE 4.1: Enumeration Screenshot

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

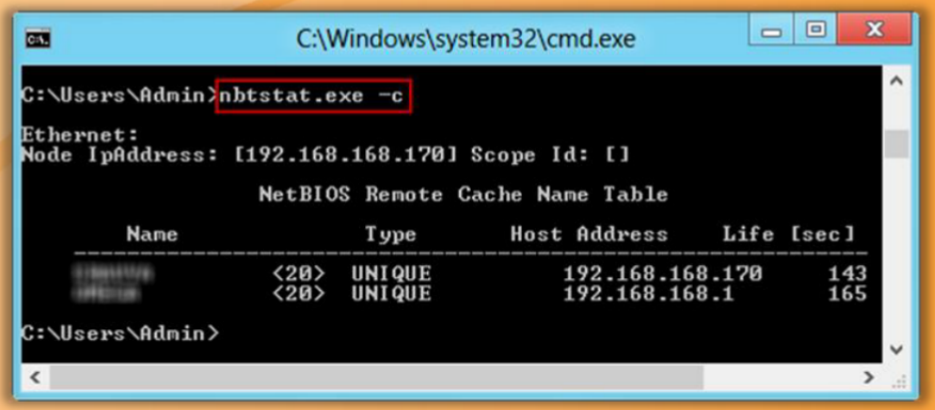
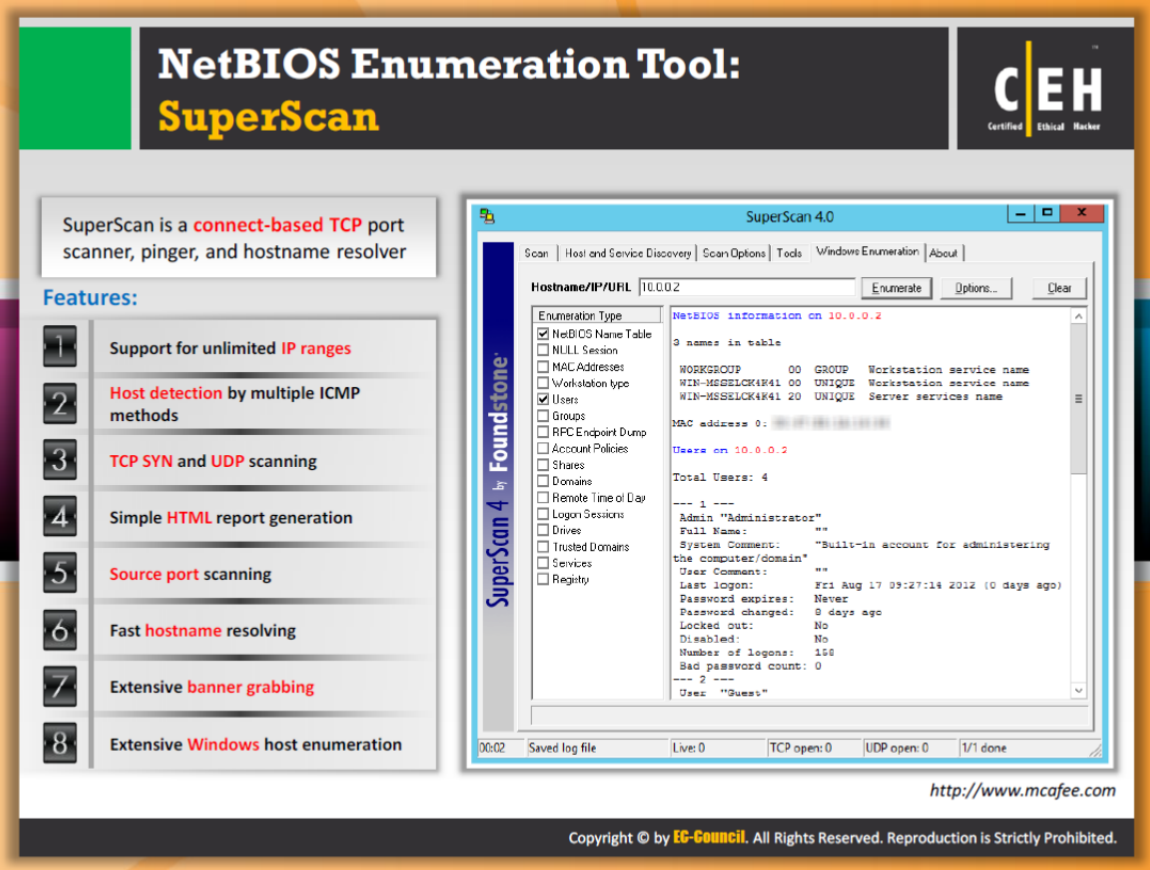


FIGURE 4.2: Enumeration Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration Tool: SuperScan

Source: http://www.mcafee.com

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver. It performs ping sweeps and scans any IP range with **multithreading** and asynchronous techniques. You can restore some functionality by running the following at the Windows command prompt before stating SuperScan:

- Support for unlimited IP ranges
- Host detection using multiple ICMP methods
- TCP SYN , UDP, and source port scanning
- Hostname resolving
- IP and port scan order randomization
- Extensive Windows host enumeration capability
- Extensive banner grabbing
- Source port scanning
- Simple HTML report generation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

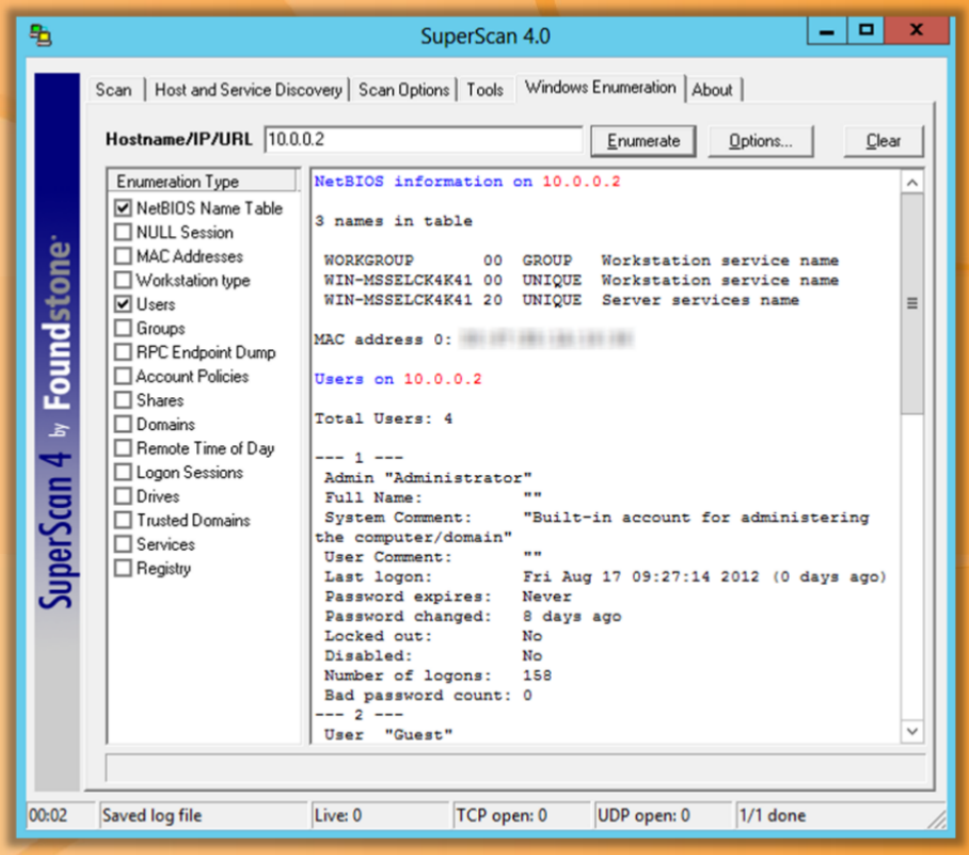
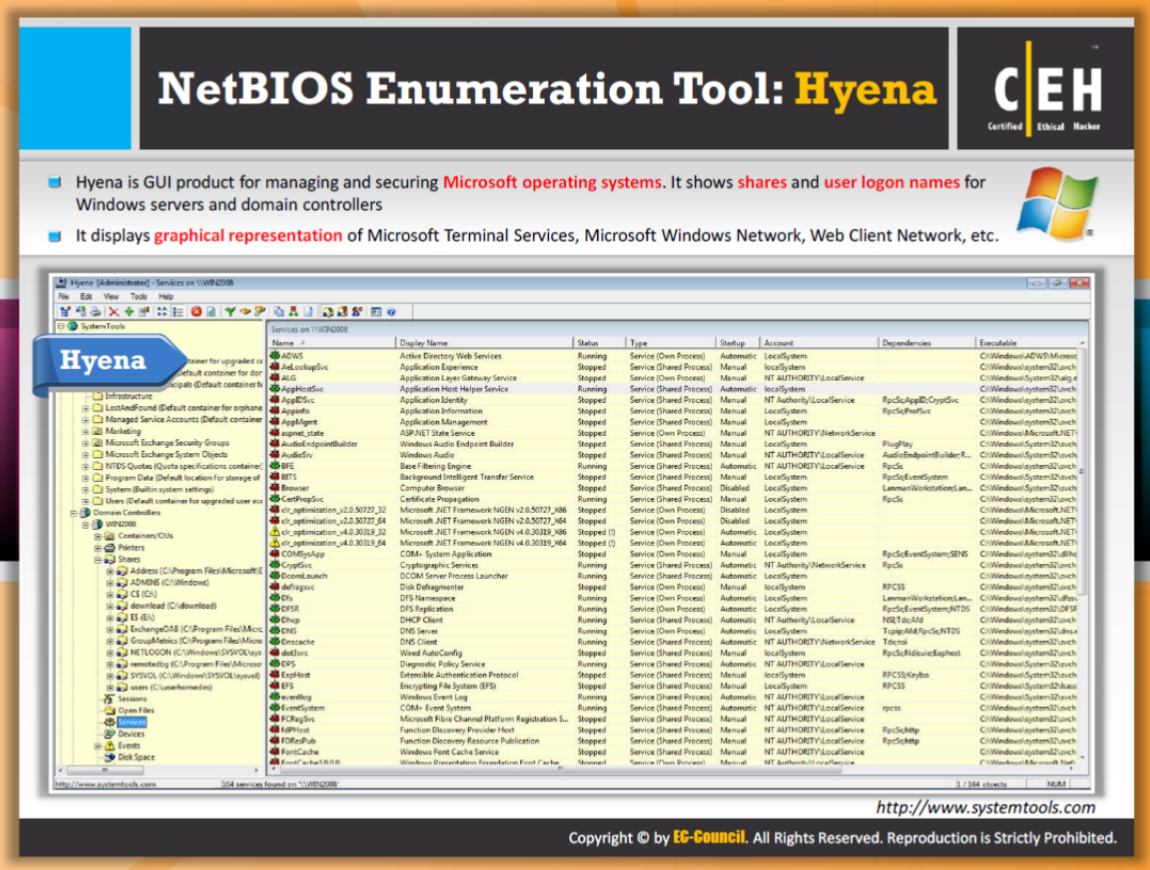


FIGURE 4.3: SuperScan Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration Tool: Hyena

Source: http://www.systemtools.com

Hyena is **GUI product** for managing and securing any Windows operating system such as Windows NT, Windows 2000, Windows XP/Vista, Windows 7, or Windows Server 2003/2008 installation. It uses an **Explorer-style** interface for all operations and to manage users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing. It shows shares and **user logon names** for Windows servers and domain controllers.

It displays a graphical representation of the web client network, Microsoft terminal services, and Windows network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

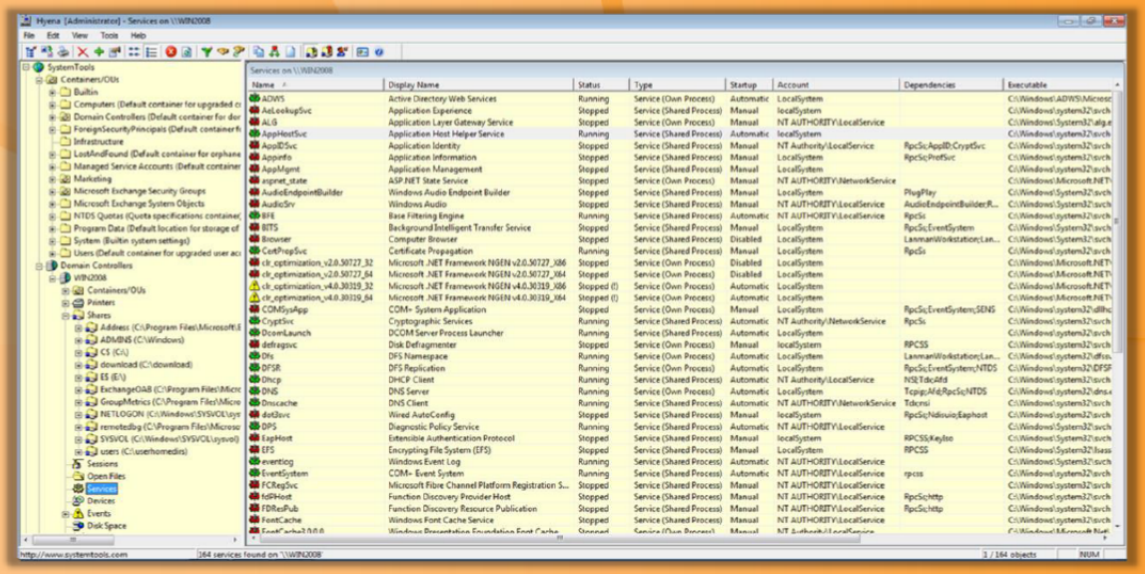
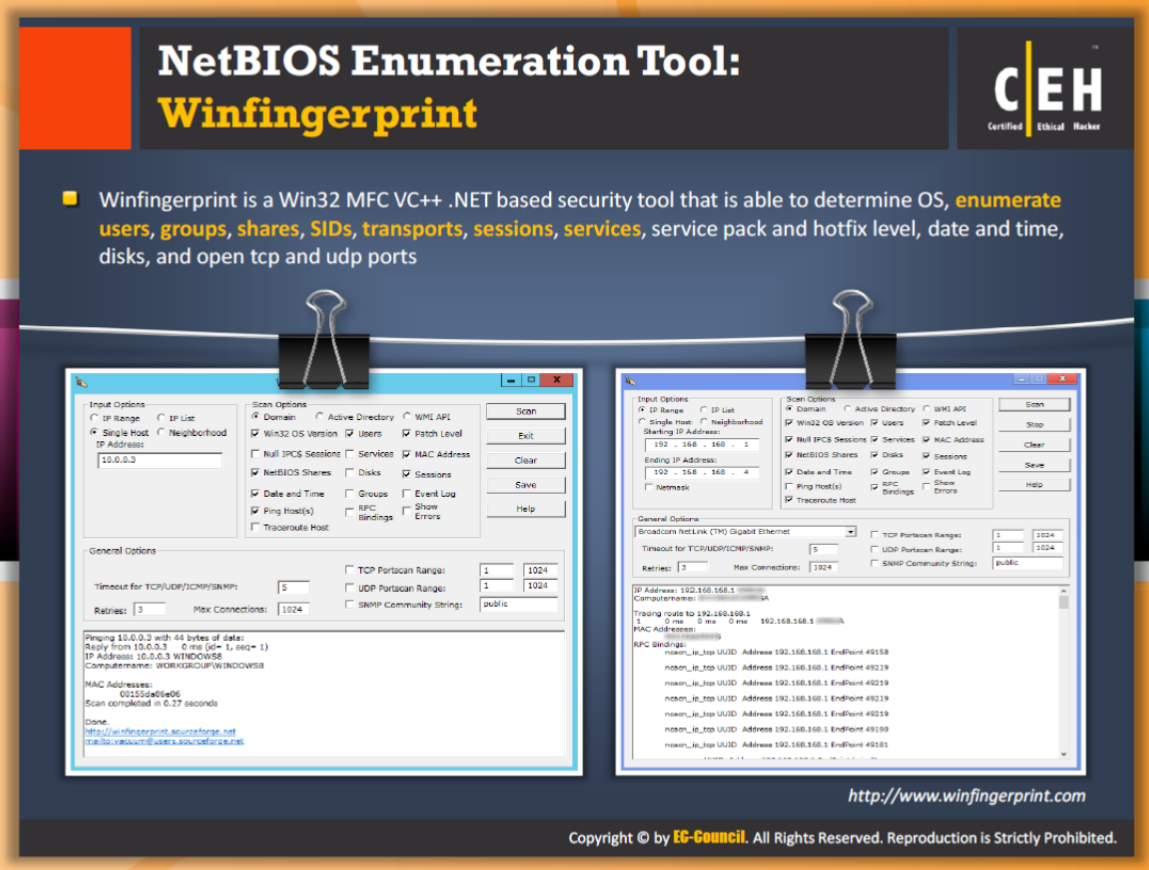


FIGURE 4.4: Hyena Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

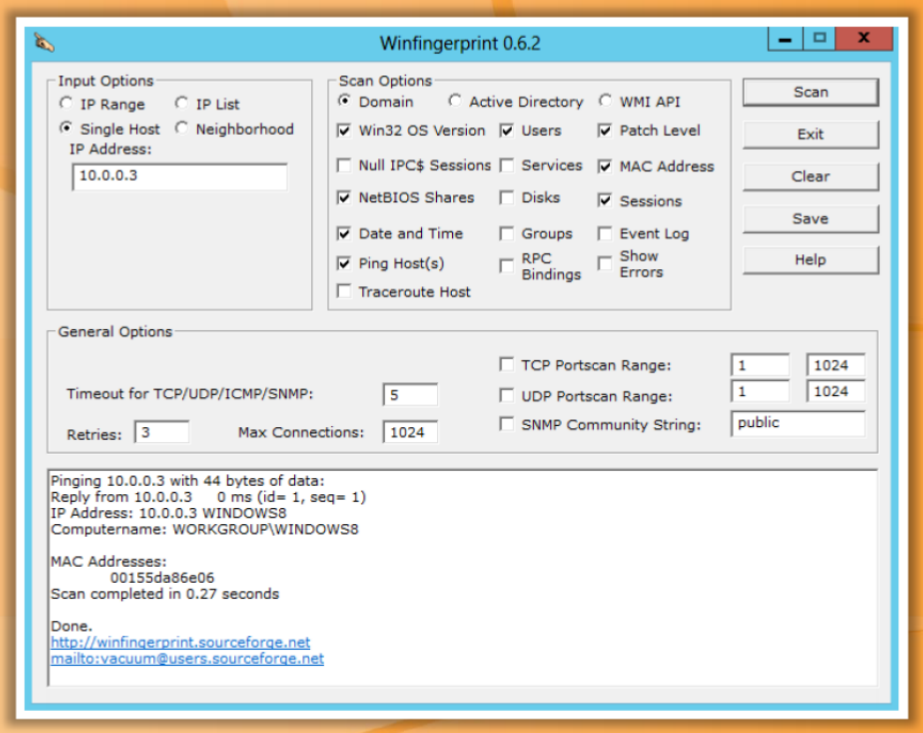


NetBIOS Enumeration Tool: WinFingerprint

Source: http://www.winfingerprint.com

WinFingerprint is an administrative network resource scanner that allows you to **scan machines** on your LAN and returns various details about each host. This includes NetBIOS shares, disk information, services, users, groups, and more. **WinFingerprint** is an administrative network resource scanner that allows you to scan machines on your LAN and returns various details about each host. This includes NetBIOS shares, disk information, services, users, groups, and more. You can choose to perform a passive scan or interactively explorer network shares, map network drives, browse **HTTP/FTP sites** and more. Scans can be run on a single host or the entire network neighborhood.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



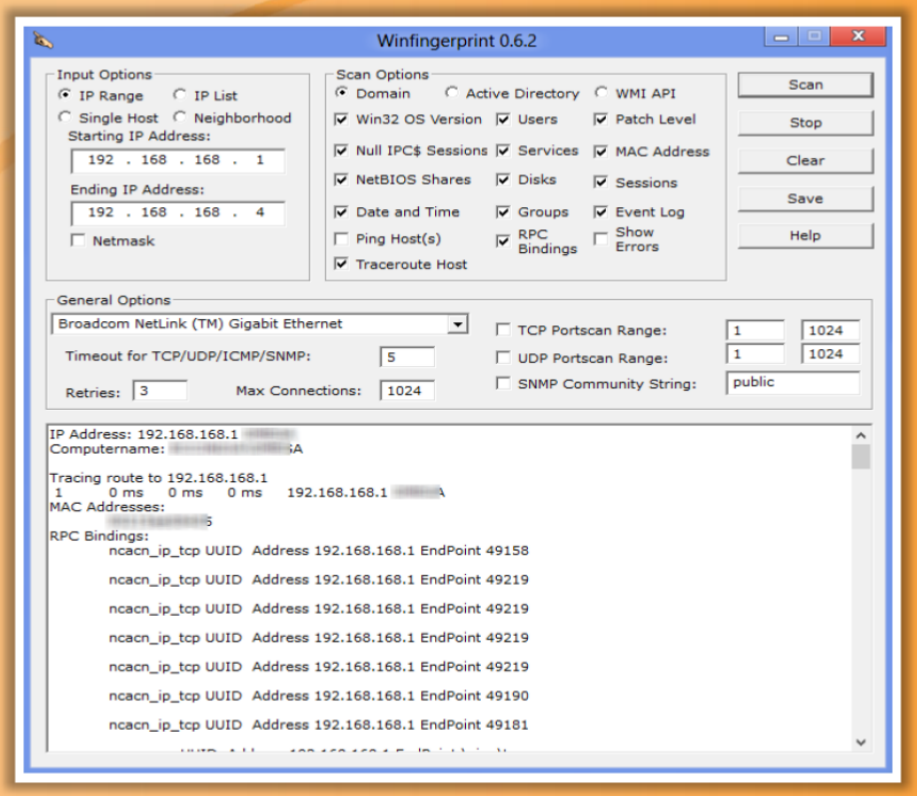
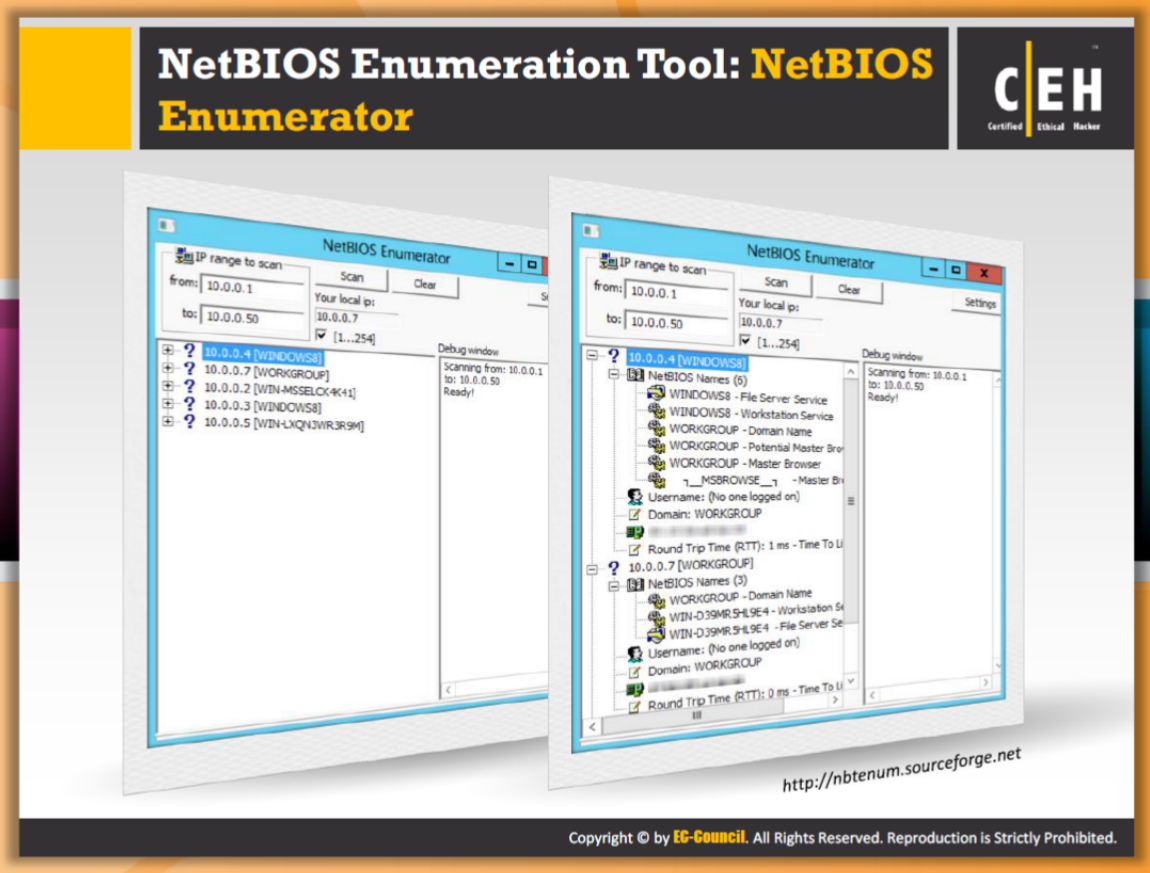


FIGURE 4.5: Winfingerprint Screenshots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NetBIOS Enumeration Tool: NetBIOS Enumerator

Source: http://nbtenum.sourceforge.net

This application is recommended when you want to determine how to use remote network support and how to deal with some other interesting web techniques, such as **SMB**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

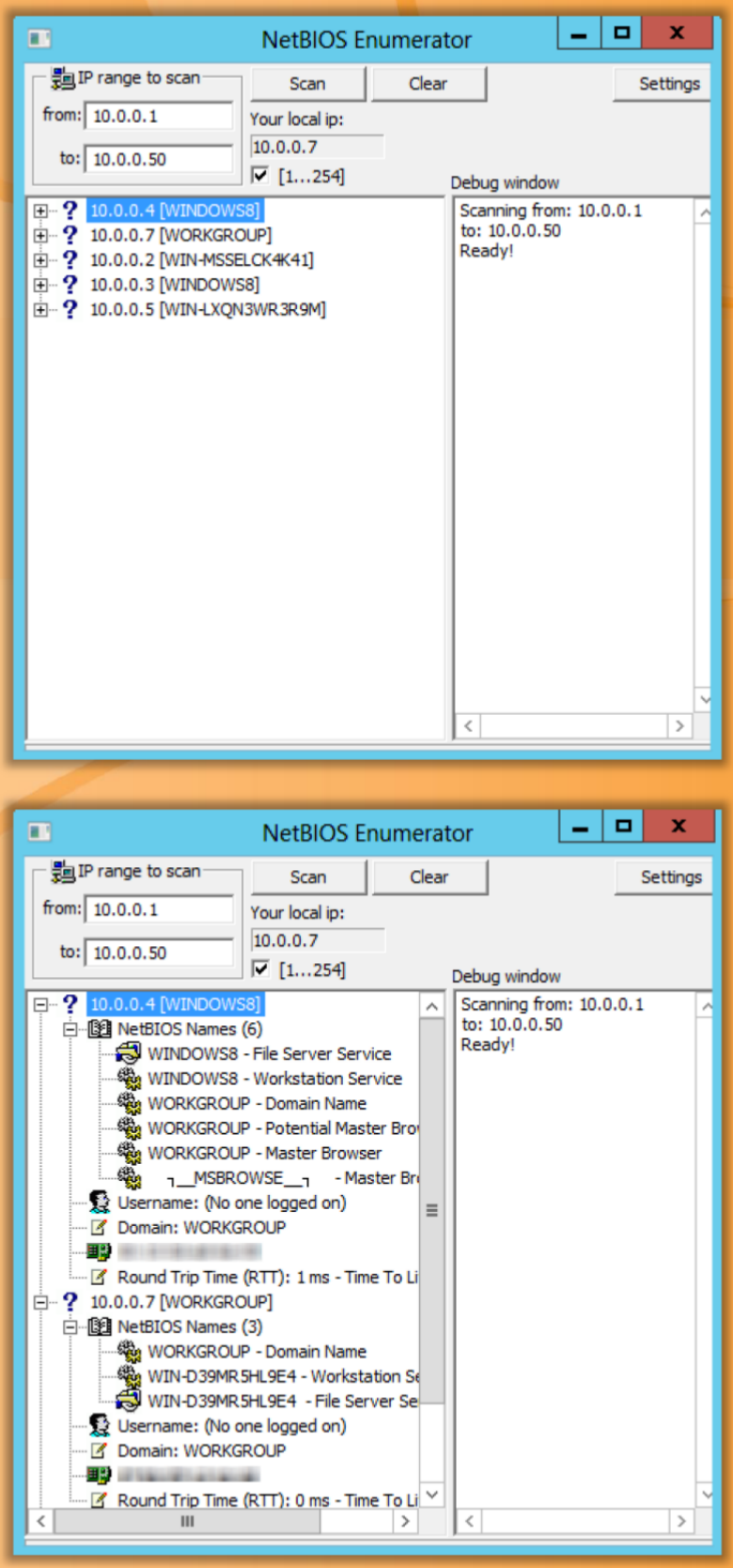
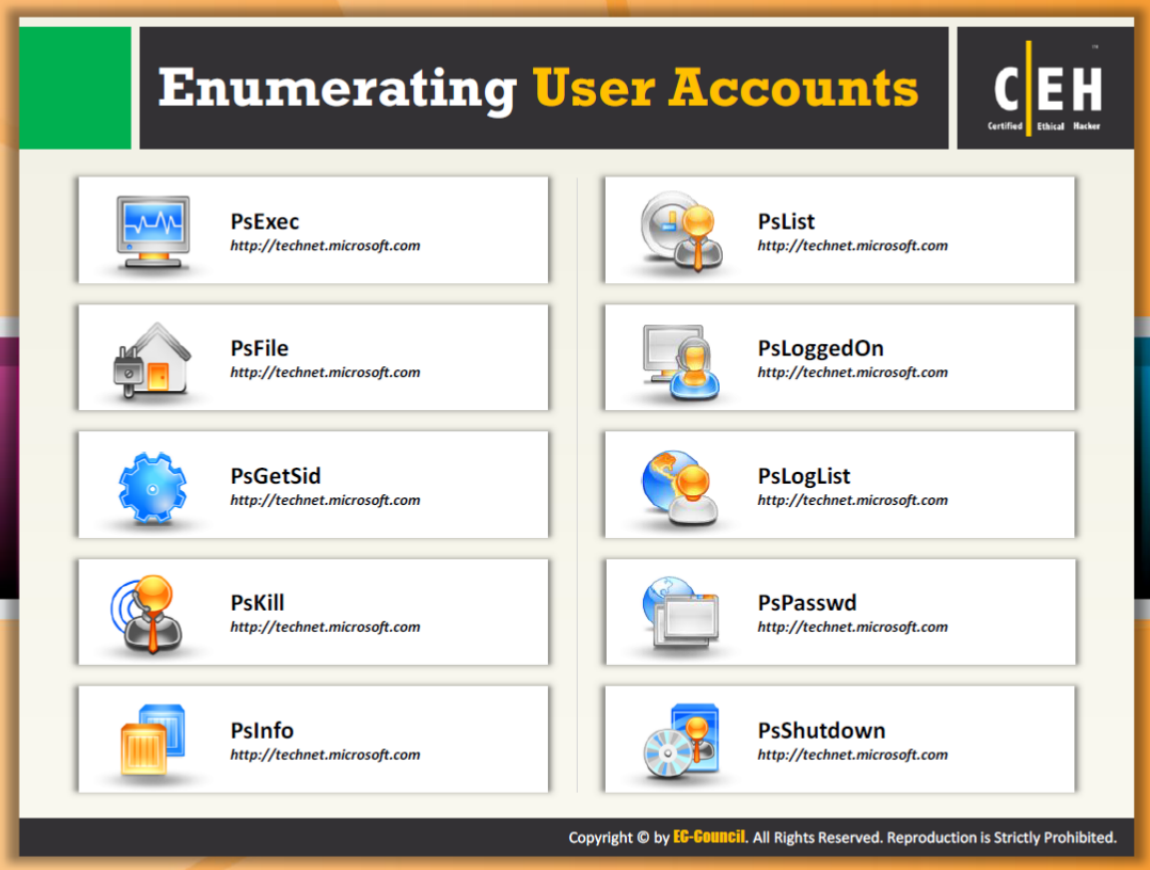


FIGURE 4.6: Enumeration Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerating User Accounts

PsExec

Source: http://technet.microsoft.com

PsExec is a command-line tool used for telnet-replacement that lets you execute processes on other systems and console applications, without having to manually install client software. When you use a specific user account, **PsExec** passes credentials in the clear to the remote workstation, thus exposing the credentials to anyone who happens to be listening in.

PsFile

Source: http://technet.microsoft.com

PsFile is a command-line utility that shows a list of files on a system that is opened remotely, and it also allows you to 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 that are open by remote systems. Typing a command followed by "- " displays information on the **syntax** for the command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PsGetSid

Source: http://technet.microsoft.com

PsGetsid allows you to translate SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also allows you to see the **SIDs** of user accounts and translates a SID into the name that represents it and works across the network so that you can query SIDs remotely.

PsKill

Source: http://technet.microsoft.com

PsKill is a kill utility that can kill processes on **remote systems** and terminate processes on the local computer. You don't need to install any client software on the target computer to use PsKill to terminate a remote process.

PsInfo

Source: http://technet.microsoft.com

PsInfo is a command-line tool that gathers key information about the local or remote Windows **NT/2000** system, 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.

PsList

Source: http://technet.microsoft.com

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

PsLoggedOn

Source: http://technet.microsoft.com

PsLoggedOn is an applet that displays local and remote logged users. If you specify a user name instead of a computer, the **PsLoggedOn** tool searches all the computers in the network neighborhood and tells you if the user is currently logged on PsLoggedOn's definition of a locally logged on user is one that has their profile loaded into the Registry, so PsLoggedOn determines who is logged on by scanning the keys under the HKEY_USERS key.

PsLogList

Source: http://technet.microsoft.com

The default behavior of PsLogList is to show the contents of the **System Event Log** on the local computer, with visually-friendly formatting of Event Log records. Command-line options let you

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

view logs on different computers, use a different account to view a log, or to have the output formatted in a string-search friendly way.

PsPasswd

Source: http://technet.microsoft.com

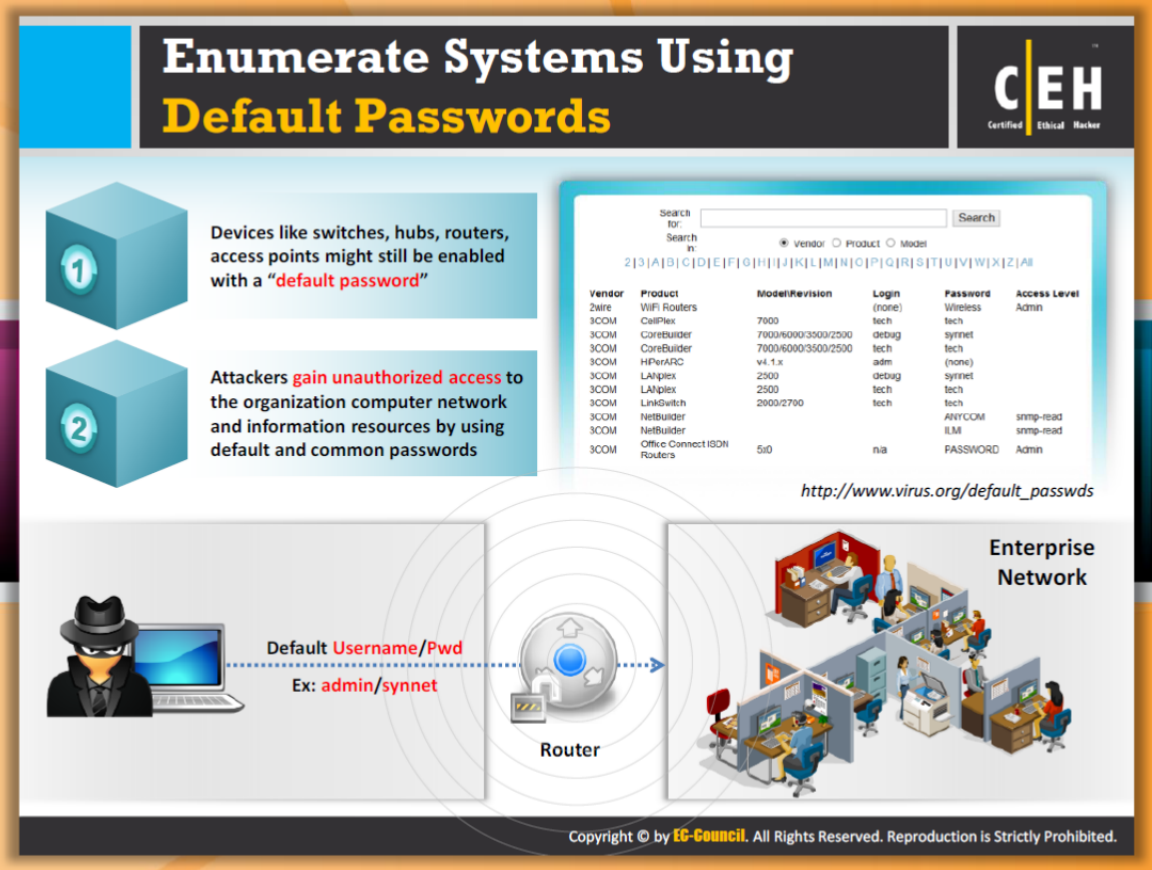
sPasswd is a tool that enables the administrator to create batch files that run PsPasswd on the network of computers to change the administrator password as a part of standard security practice.

PsShutdown

Source: http://technet.microsoft.com

PsShutdown is a command-line tool that allows you to remotely shut down the PC in networks. It can log off the console user or lock the console (locking requires Windows 2000 or higher). It does not require any manual installation of client **software**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerate Systems Using Default Passwords

Source: http://www.defaultpassword.com

Devices such as switches, hubs, routers, and access points usually come with "**default passwords**." Not only network devices but also a few local and online applications have built-in default passwords. These passwords are provided by vendors or application programmers during development of the product. Most users use these applications or devices without changing the default passwords provided by the vendor or the programmer. If you do not change these default passwords, then you might be at **risk** because lists of default passwords for many products and applications are available online. Once such example is http://www.virus.org/default_passwds; it provides verified default login/password pairs for common networked devices. The logins and passwords contained in this database are either set by default when the hardware or software is first installed or are in some cases **hardcoded** into the hardware or software.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Search for: Search

Search In: Vendor Product Model

2|3|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Z|All

Vendor	Product	Model\Revision	Login	Password	Access Level
2wire	WiFi Routers		(none)	Wireless	Admin
3COM	CellPlex	7000	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	tech	tech	
3COM	HiPerARC	v4.1.x	adm	(none)	
3COM	LANplex	2500	debug	synnet	
3COM	LANplex	2500	tech	tech	
3COM	LinkSwitch	2000/2700	tech	tech	
3COM	NetBuilder			ANYCOM	snmp-read
3COM	NetBuilder			ILMI	snmp-read
3COM	Office Connect ISDN Routers	5x0	n/a	PASSWORD	Admin

FIGURE 4.7: Enumeration Screenshot

Attackers take advantage of these default passwords and the online resources that provide default passwords for various products and application. Attackers gain **unauthorized** access to the organization computer network and information resources by using default and common passwords.

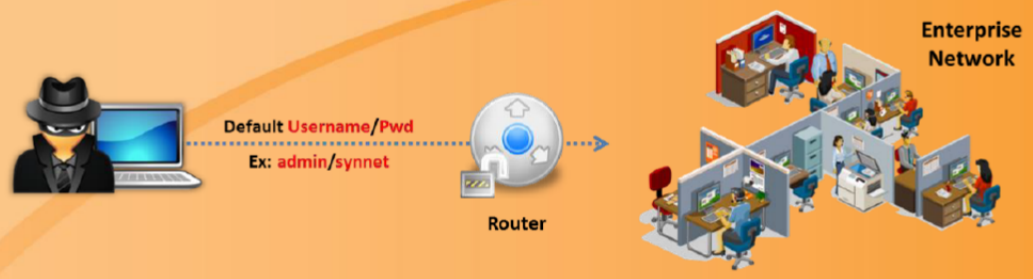
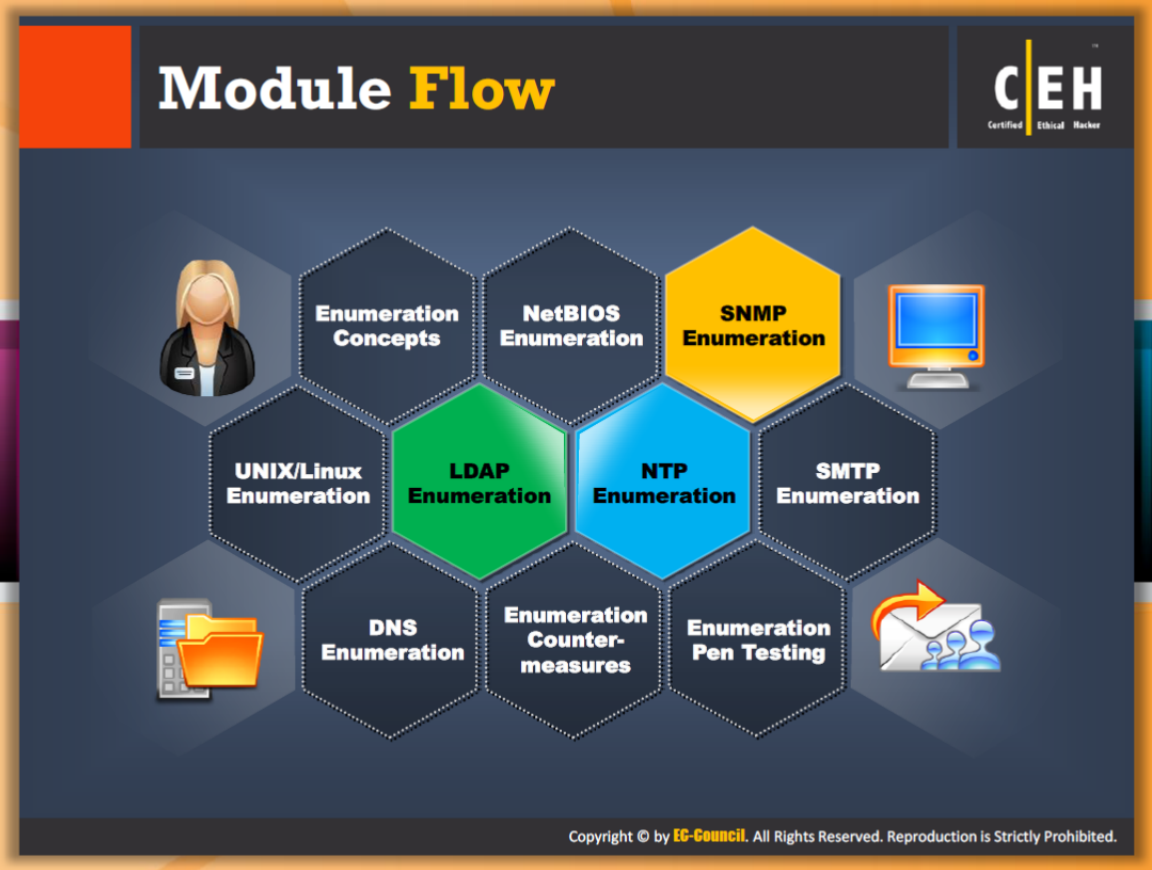


FIGURE 4.8: Enumeration Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

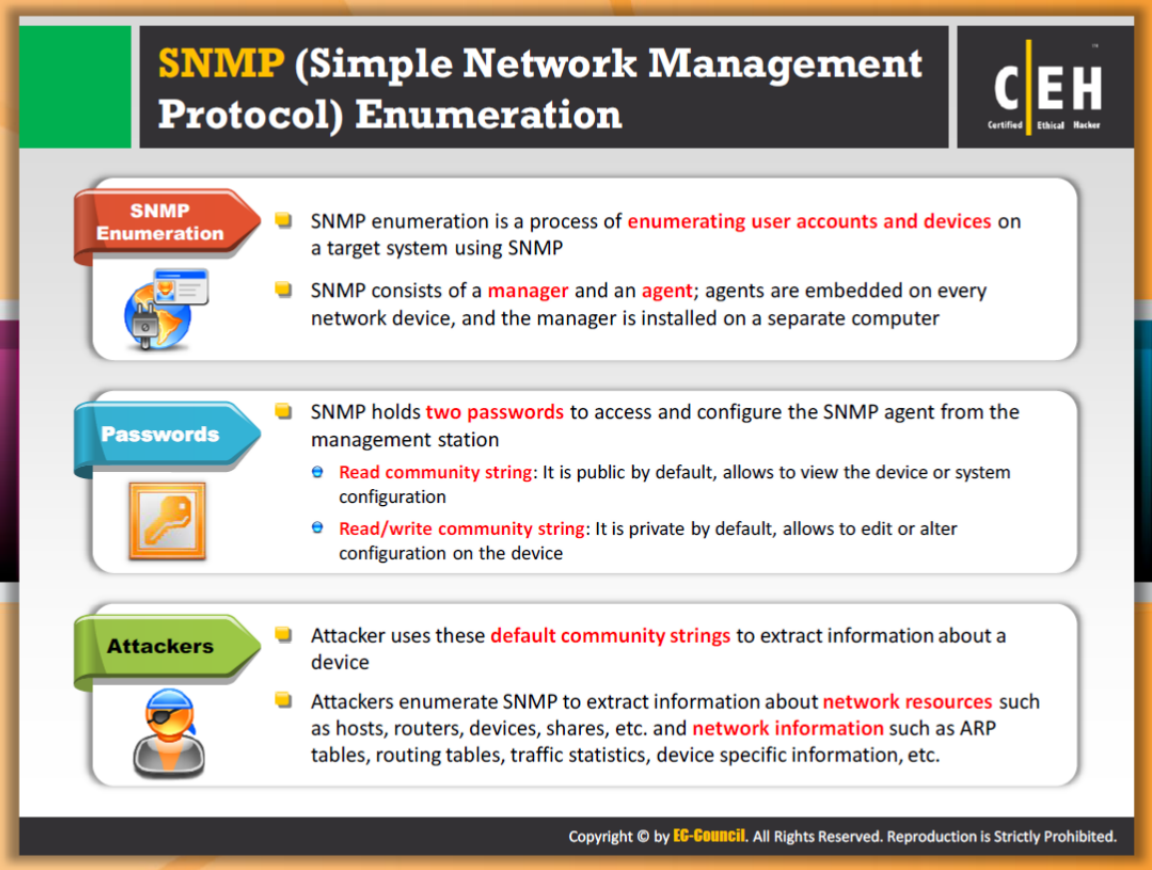


Module Flow

This section describes the **UNIX/Linux commands** that can be used for enumeration and Linux enumeration tools.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SNMP (Simple Network Management Protocol) Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP, and is used to maintain and manage 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 enumerating the user's accounts and devices on a target computer using SNMP. Two types of software components are employed by SNMP for communicating. They are the SNMP agent and SNMP management station. The **SNMP agent** is located on the networking device whereas the SNMP management station is communicated 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 the requests to the agent; after receiving the request the agent sends back the replies. Both requests and replies are the configuration variables accessible by the agent software. Requests are also sent by SNMP management stations for setting values to some variables. Trap let the management station know if anything has happened at the agent's side such as a reboot or **interface failure** or any other abnormal event.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP contains two passwords that you can use for configuring as well as for accessing the SNMP agent from the management station.

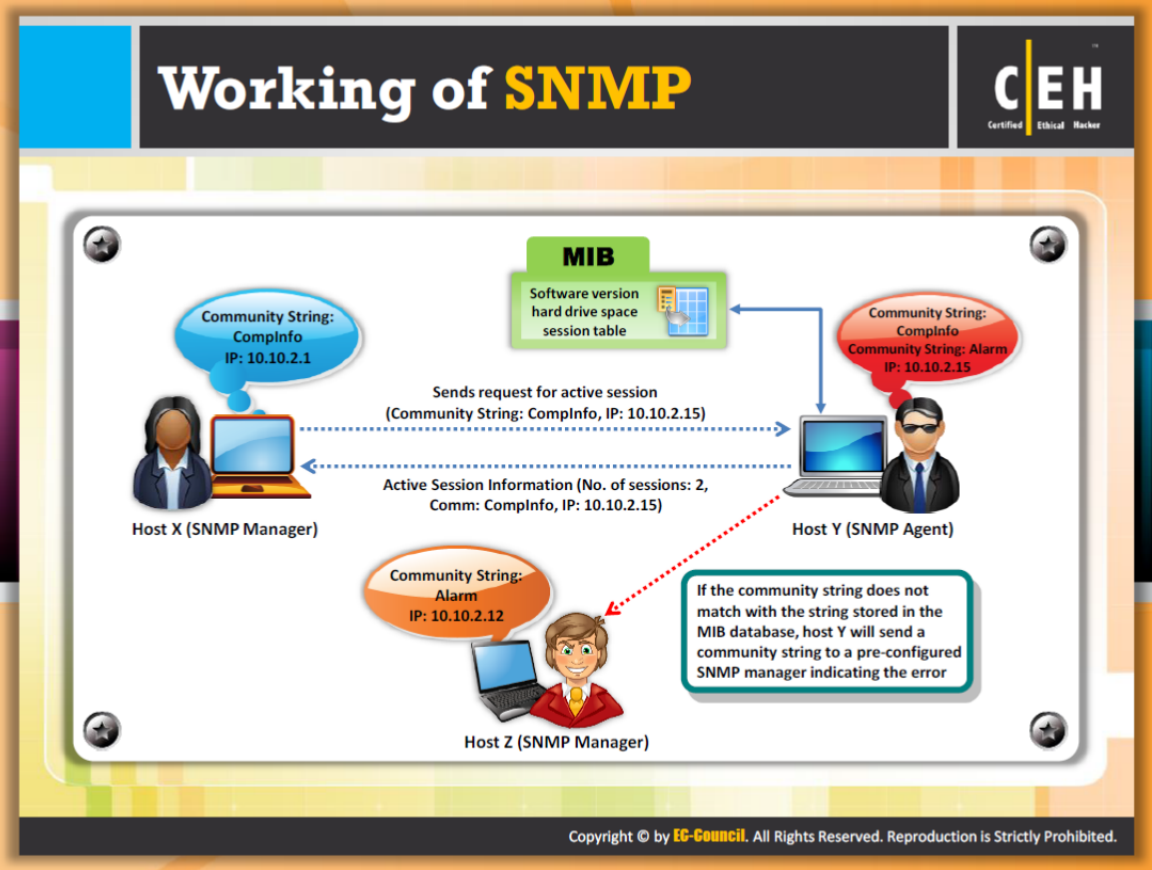
The two SNMP passwords are:

- **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 the community strings are left at the default setting, attackers take the opportunity and find the loopholes in it. Then, the attacker can uses these default passwords for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, device specific information, and traffic statistics.

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of SNMP

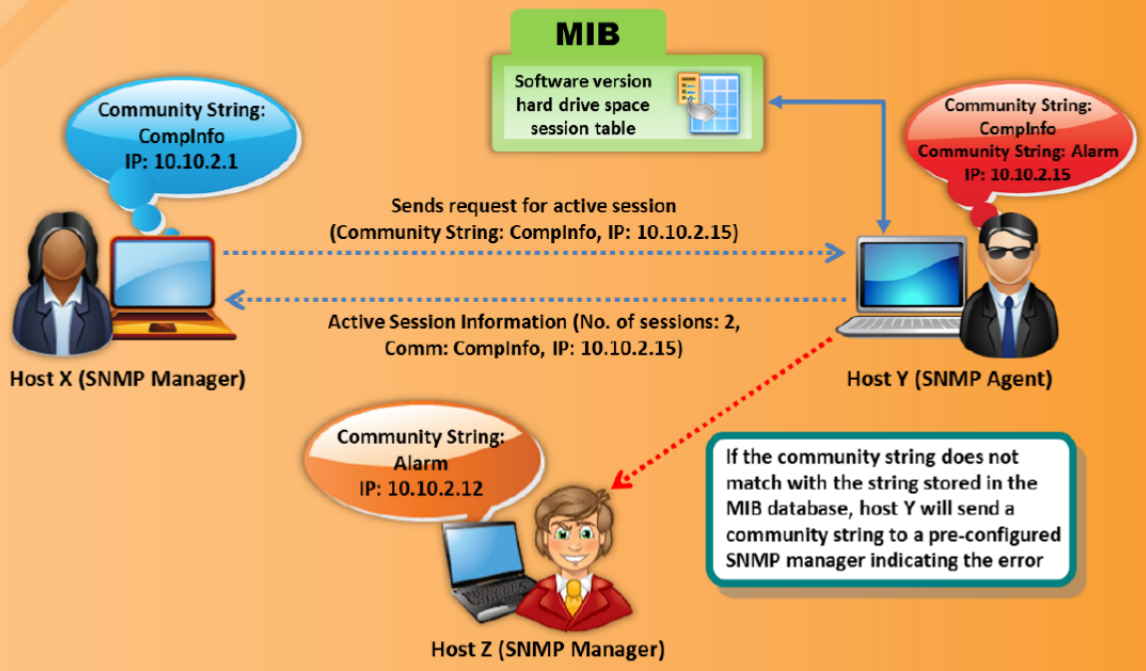
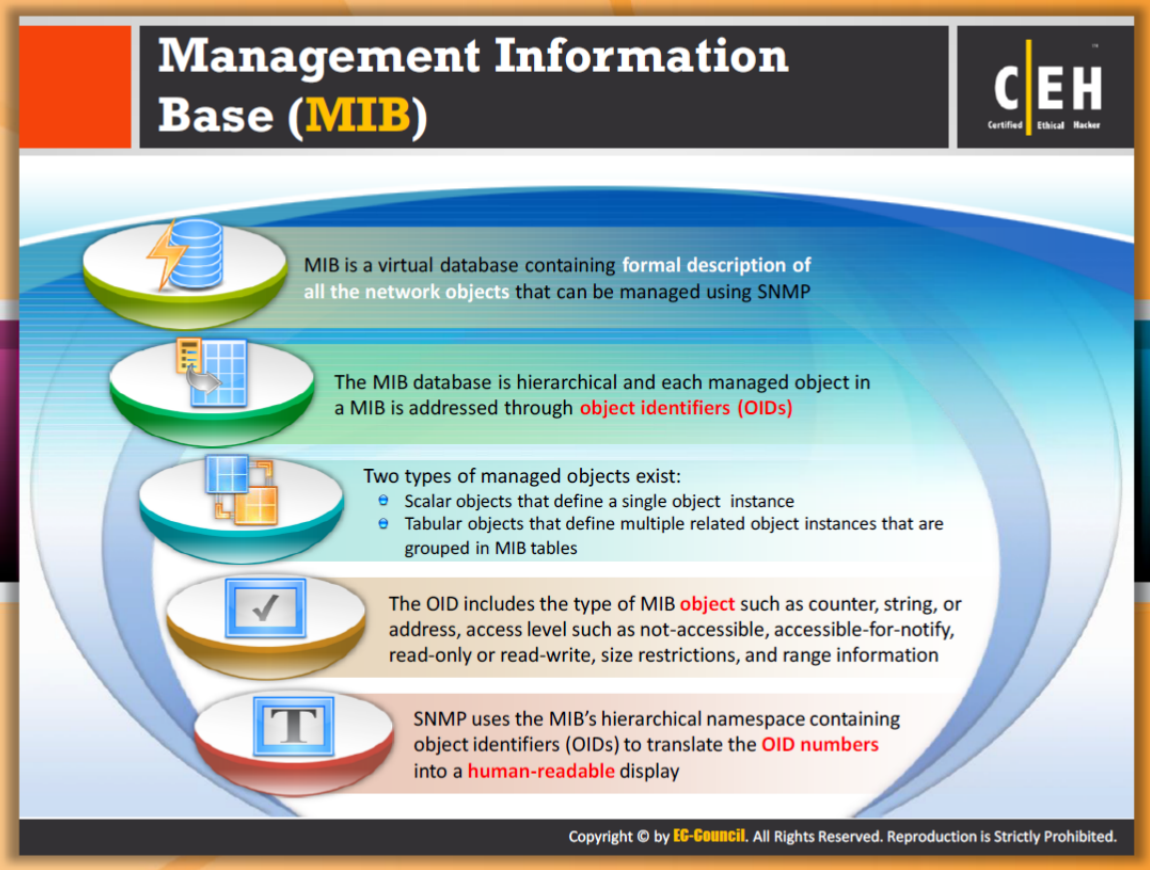


FIGURE 4.9: SNMP Screenshot

Ethical Hacking and Countermeasures 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 can be managed using SNMP. MIB is the 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 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 group of related object instances. The object identifiers include the object's type such as counter, string, or address, access level such as read or read/write, size restrictions, and range information. MIB is used as a codebook by the SNMP manager for converting the OID numbers into a human-readable display.

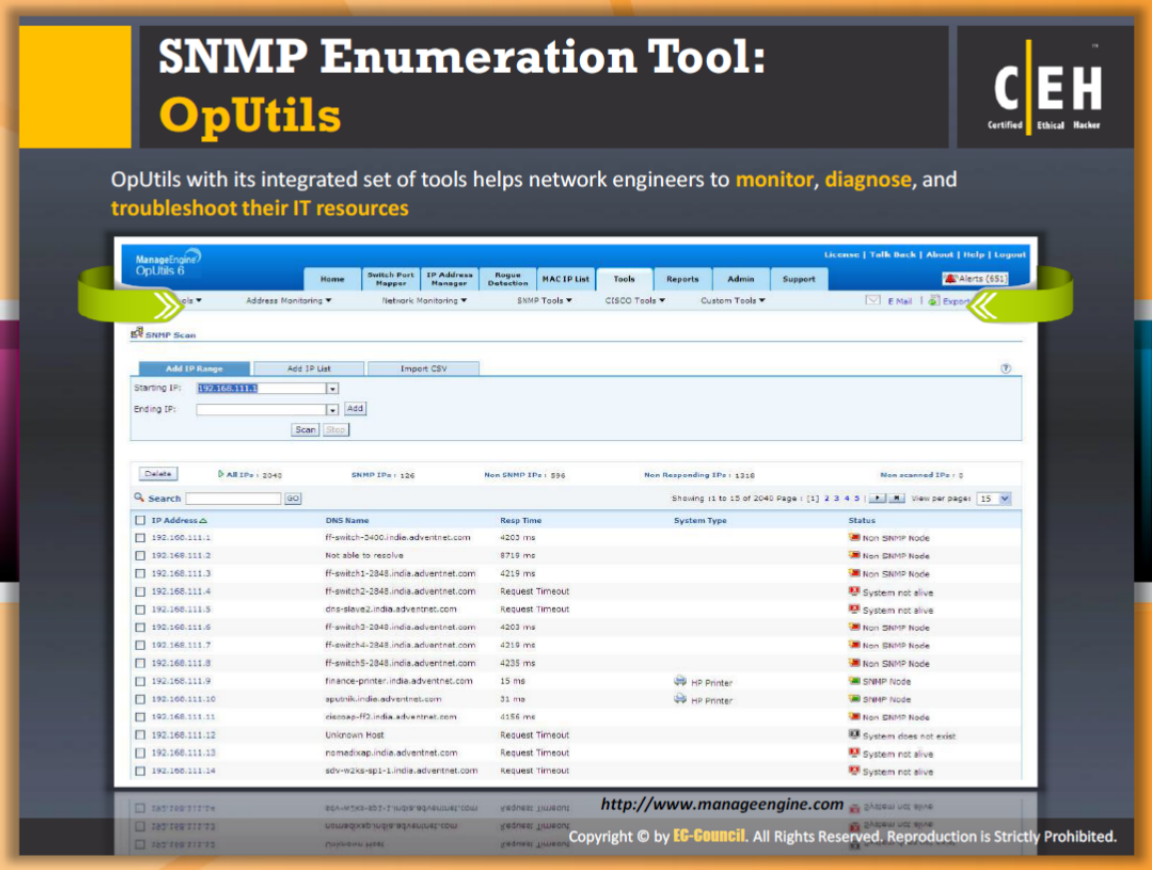
The contents of the MIB can be accessed and viewed using a web browser either by entering the IP address and Lseries.mib or by entering DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.

Microsoft provides the list of MIBs that are installed with the SNMP Service in the Windows resource kit. The major ones are:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SNMP Enumeration Tool: OpUtils

Source: http://www.manageengine.com

OpUtils is a collection of tools using which network engineers can monitor, diagnose, and troubleshoot their **IT resources**. You can monitor the availability and other activities of critical devices, detect unauthorized network access, and manage IP addresses. It allows you to create a custom SNMP tools through which you can **monitor MIB nodes**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

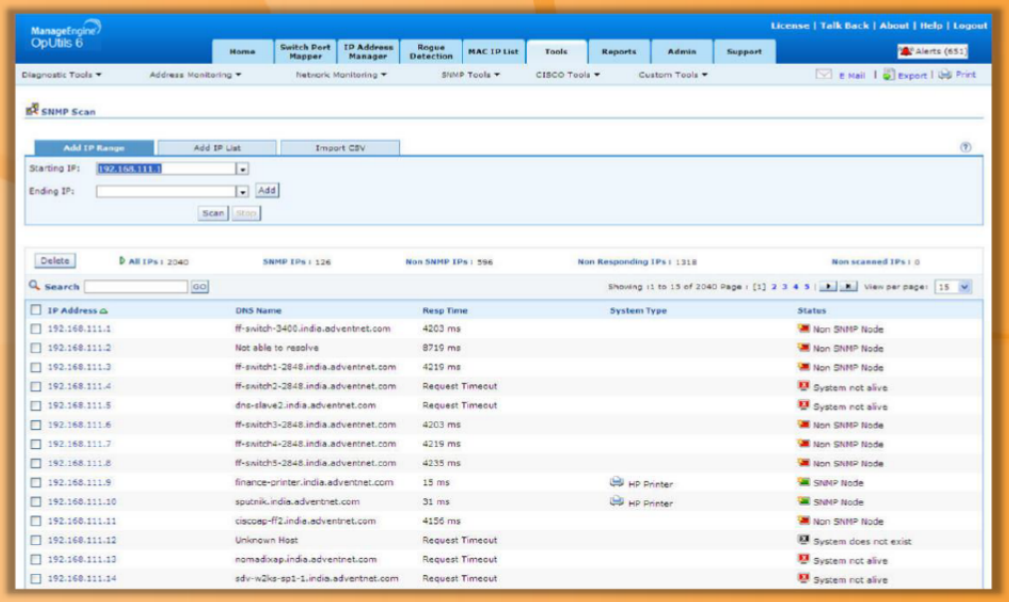
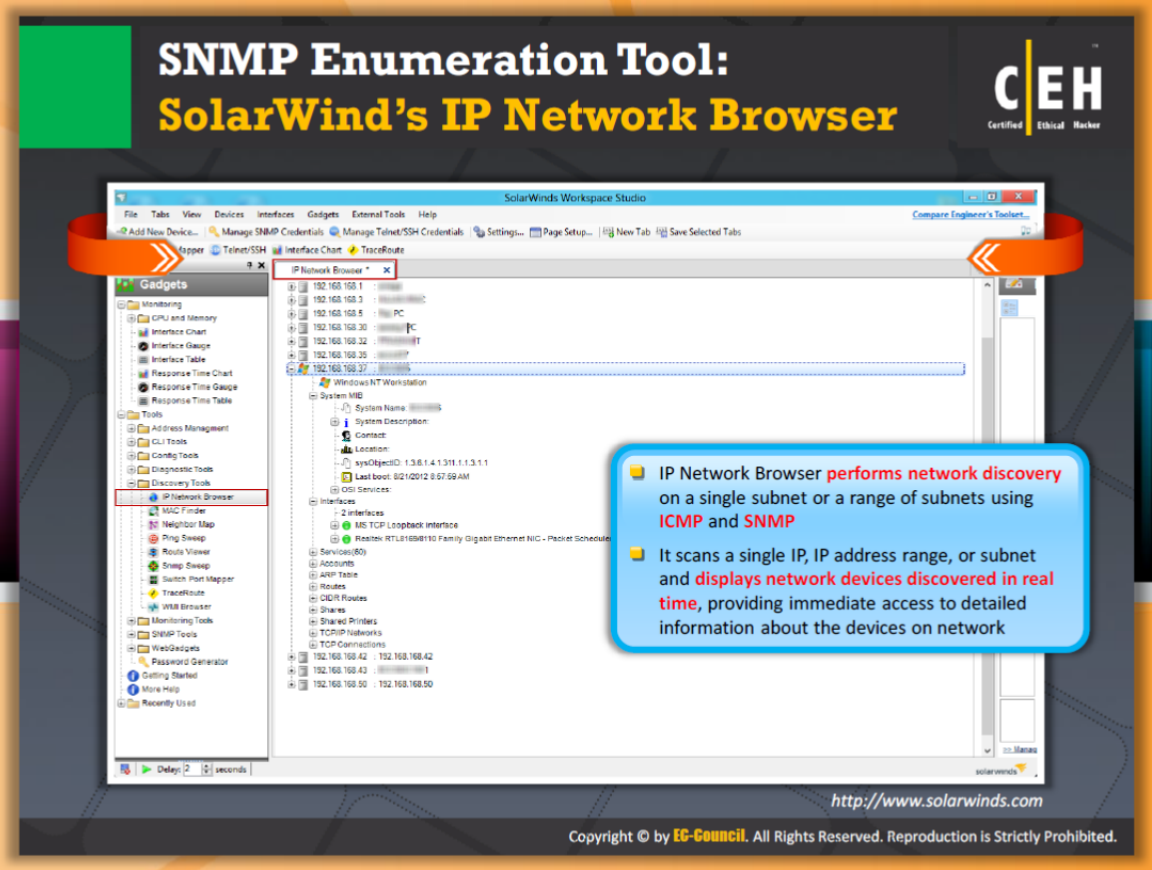


FIGURE 4.10: Oputils Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SNMP Enumeration Tool: SolarWind's IP Network Browser

Source: http://www.solarwinds.com

IP Network Browser from SolarWinds is a network discovery application. It collects information via ICMP and SNMP locally or on a remote network. It scans a single IP, IP address range, or subnet and displays network devices as they are discovered in real time, providing you with immediate access to detailed information about the devices on your network. It is easy for the attacker to discover information about the target network after performing scanning of the entire subnet. Using IP Network Browser, an attacker can gather information from a poorly configured Windows system. The information that can be gathered includes server name, operating system version, SNMP contact and location information, list of services and network interfaces, list of all user accounts, machine date/time, etc.

For example, on a Cisco router, **Solar Winds IP** Network Browser will determine the current IOS version and release, as well as identify which cards are installed into which slots, the status of each port, and ARP tables. When the IP Network Browser discovers a Windows server, it returns information including interface status, bandwidth utilization, services running, and even details of software that is installed and running.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

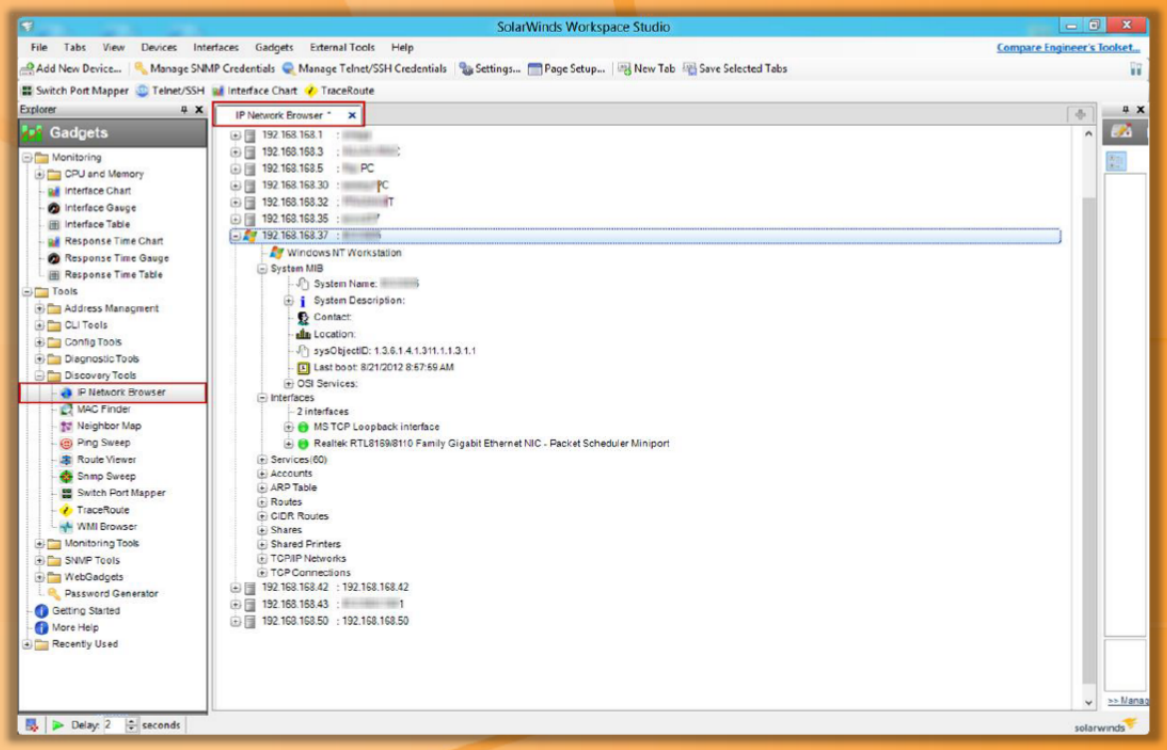
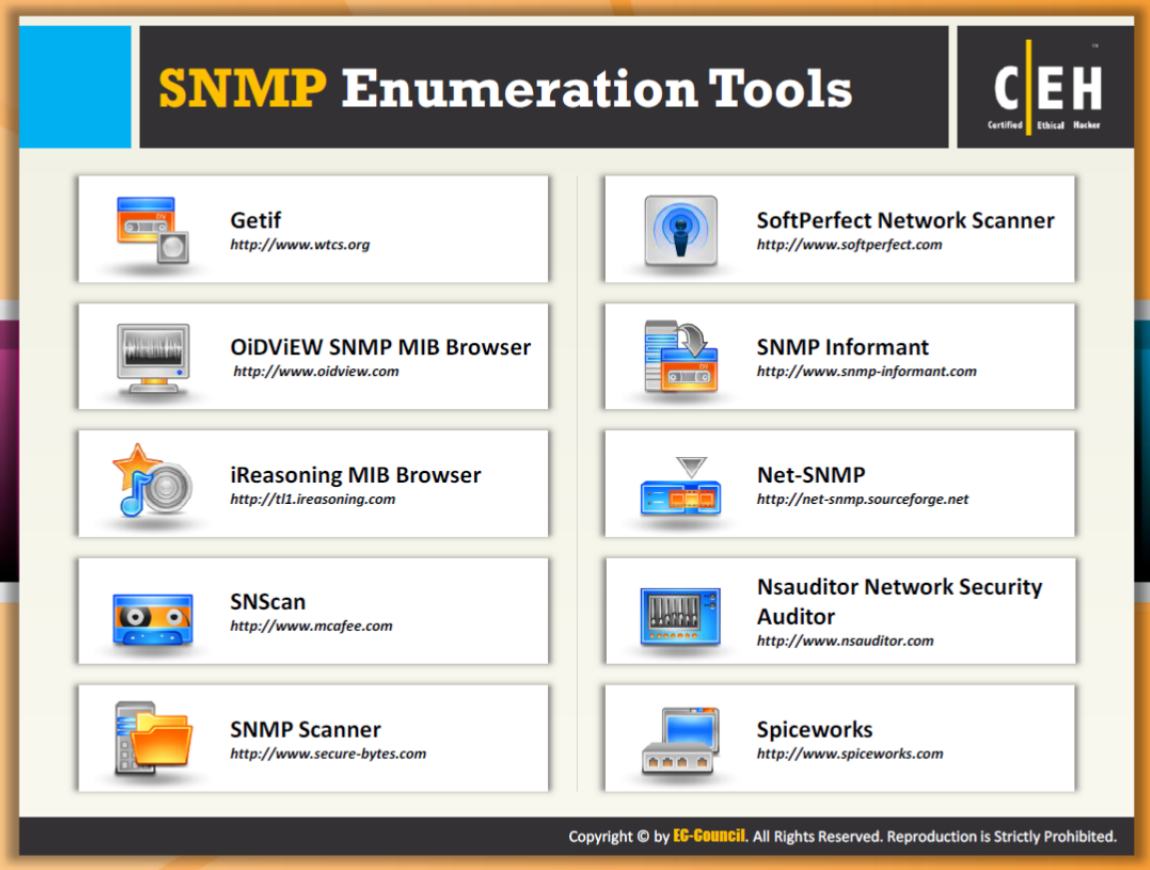


FIGURE 4.11: SNMP Enumeration Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

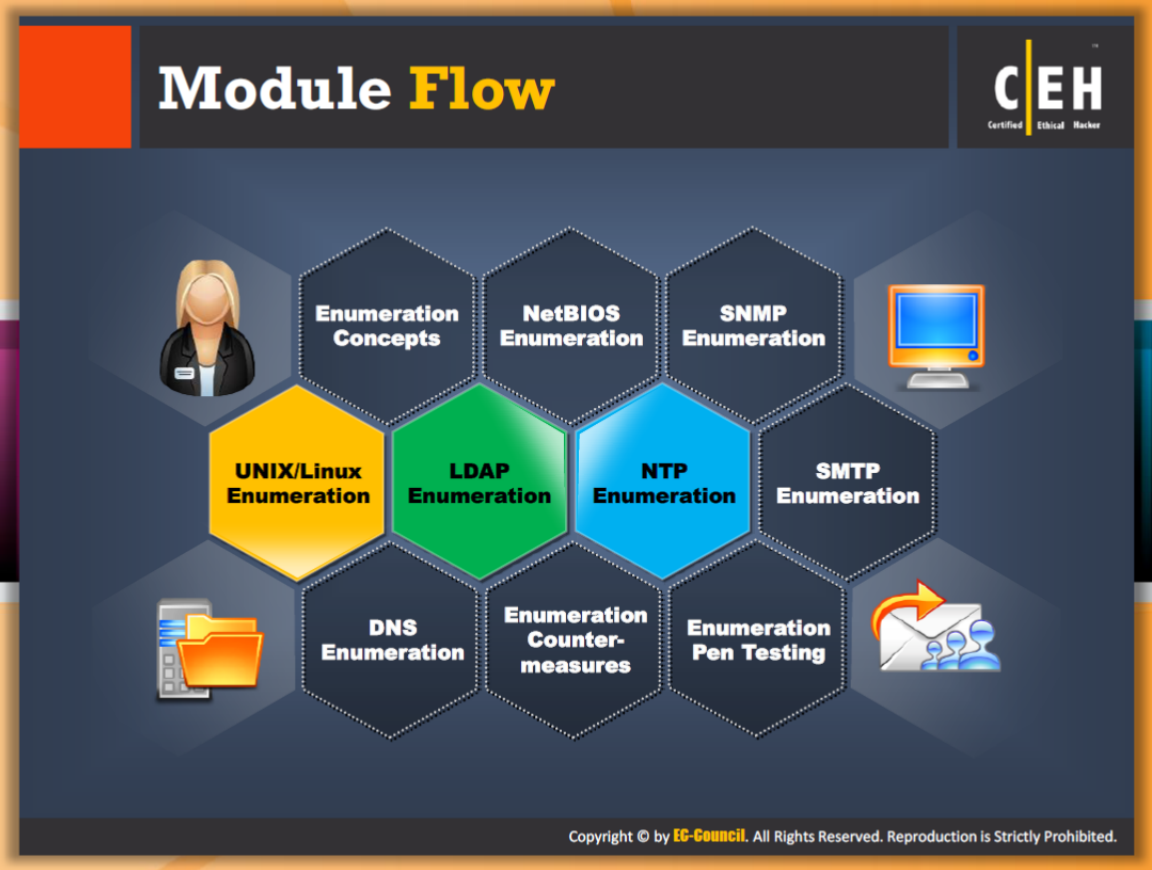


SNMP Enumeration Tools

In addition to OpUtils and **SolarWind's IP Network Browser**, a few more SNMP tools are listed as follows:

- Getif available at http://www.wtcs.org
- OiDViEW SNMP MIB Browser available at http://www.oidview.com
- iReasoning MIB Browser available at http://tl1.ireasoning.com
- SNScan available at http://www.mcafee.com
- SNMP Scanner available at http://www.secure-bytes.com
- SoftPerfect Network Scanner available at http://www.softperfect.com
- SNMP Informant available at http://www.snmp-informant.com
- Net-SNMP available at http://net-snmp.sourceforge.net
- Nsauditor Network Security Auditor available at http://www.nsauditor.com
- Spiceworks available at http://www.spiceworks.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

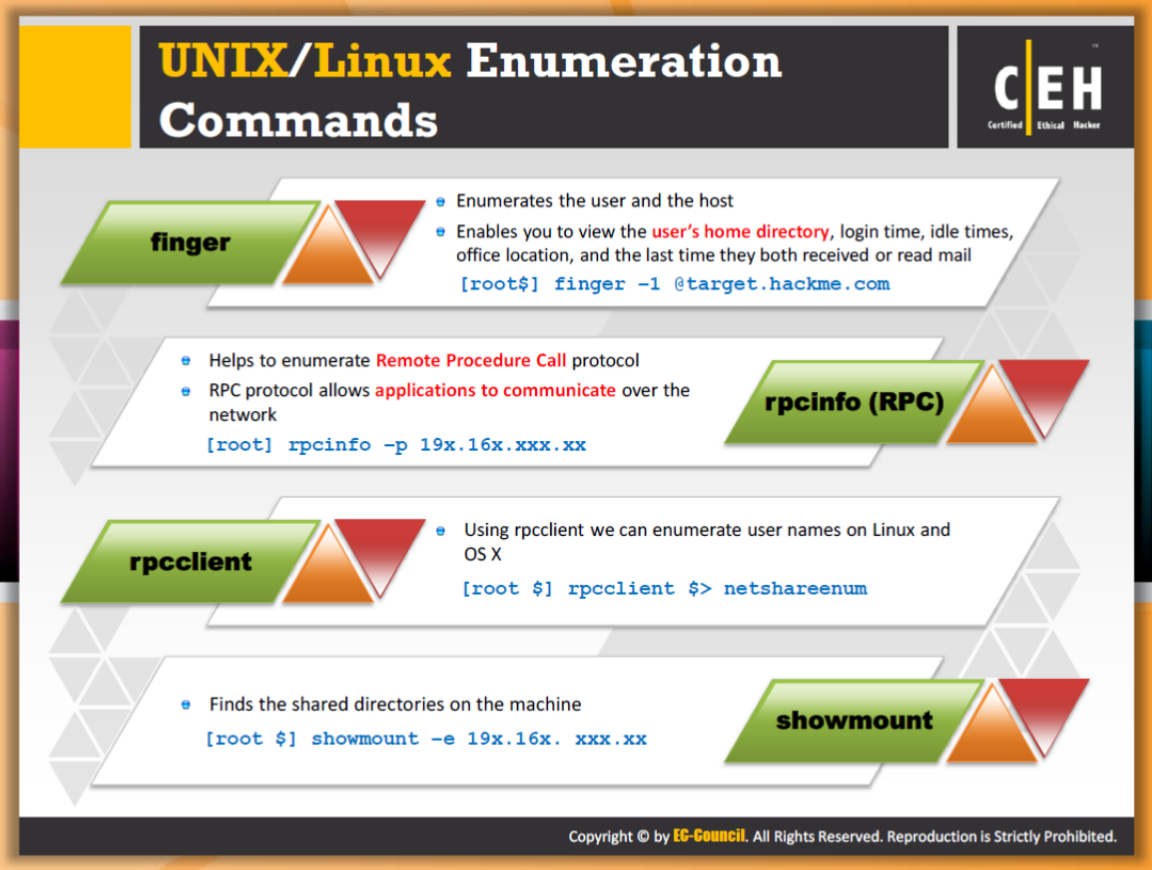


Module Flow

This section describes the **UNIX/Linux commands** that can be used for enumeration and Linux enumeration tools.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



UNIX/Linux Enumeration Commands

Commands used to enumerate UNIX network resources are as follows: showmount, finger, rpcinfo (RPC), and rpcclient.

Finger:

The **finger command** is used for enumerating the users on the remote machine. It enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail.

The syntax for finger is:

finger [-b] [-f] [-h] [-i] [-l] [-m] [-p] [-q] [-s] [-w] [username]

Options:

-b	Suppresses printing the user's home directory and shell in a long format printout.
-f	Suppresses printing the header that is normally printed in a non-long format printout.
-h	Suppresses printing of the .project file in a long format printout.
-l	Forces "idle" output format, which is similar to short format except that only the login name, terminal, login time, and idle time are printed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-l	Forces long output format.
-m	Matches arguments only on the user's name.
-p	Suppresses printing of the .plan file in a long format printout.
-q	Forces quick output format, which is similar to short format except that only the login name, terminal, and login time are printed.
-s	Forces short output format.
-w	Suppresses printing the full name in a short format printout.

For example, if the command root$] finger –1 @target.hackme.com is executed, then you can get the list of users on the target host.

rpcinfo (RPC)

rpcinfo (RPC) helps you to enumerate Remote Procedure Call protocol. This in turn allows the applications to communicate over the network.

The syntax for rpcinfo follows:

```
rpcinfo [-m | -s ] [ host ]
rpcinfo -p [ host ]
rpcinfo -T transport host prognum [ versnum ]
rpcinfo -l [ -T transport ] host prognum versnum
rpcinfo [ -n portnum ] -u host prognum [ versnum ]
rpcinfo [ -n portnum ] -t host prognum [ versnum ]
rpcinfo -a serv_address -T transport prognum [ versnum ]
rpcinfo -b [ -T transport ] prognum versnum
rpcinfo -d [ -T transport ] prognum versnum
```

Options:

-m	Displays a table of statistics of rpcbind operations on the given host. The table shows statistics for each version of rpcbind (versions 2, 3 and 4), giving the number of times each procedure was requested and successfully serviced, the number and type of remote call requests that were made, and information about RPC address lookups that were handled. This is useful for monitoring RPC activities on the host.
-s	Displays a concise list of all registered RPC programs on host. If host is not specified, it defaults to the local host.
-p	Probes rpcbind on host using version 2 of the rpcbind protocol, and display a list of all registered RPC programs. If host is not specified, it defaults to the local host. Note that version 2 of the rpcbind protocol was previously known as the portmapper protocol.
-t	Makes a RPC call to procedure 0 of prognum on the specified host using TCP, and report whether or not a response was received. This option is made obsolete by the -T option as shown in the third synopsis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-l	Displays a list of entries with a given prognum and versnum on the specified host. Entries are returned for all transports in the same protocol family as that used to contact the remote rpcbind.
-b	Makes a RPC broadcast to procedure 0 of the specified prognum and versnum and report all hosts that respond. If transport is specified, it broadcasts its request only on the specified transport. If broadcasting is not supported by any transport, an error message is printed. Use of broadcasting should be limited because of the potential for adverse effect on other systems.
-d	Deletes registration for the RPC service of the specified prognum and versnum. If transport is specified, unregister the service on only that transport; otherwise, unregister the service on all the transports on which it was registered. Only the owner of a service can delete a registration, except the superuser, who can delete any service.
-u	Makes an RPC call to procedure 0 of prognum on the specified host using UDP, and report whether or not a response was received. This option is made obsolete by the -T option as shown in the third synopsis.

-a serv_address	Uses serv_address as the (universal) address for the service on transport to ping procedure 0 of the specified prognum and report whether or not a response was received. The -T option is required with the -a option. If versnum is not specified, rpcinfo tries to ping all available version numbers for that program number. This option avoids calls to remote rpcbind to find the address of the service. The serv_address is specified in universal address format of the given transport.
-n portnum	Uses portnum as the port number for the -t and -u options instead of the port number given by rpcbind. Use of this option avoids a call to the remote rpcbind to find out the address of the service. This option is made obsolete by the -a option.
-T transport	Specifies the transport on which the service is required. If this option is not specified, rpcinfo uses the transport specified in the NETPATH environment variable, or if that is unset or NULL, the transport in the netconfig database is used. This is a generic option, and can be used in conjunction with other options as shown in the SYNOPSIS.
Host	Specifies host of rpc information required.

For example, if the command [root] rpcinfo –p 19x.16x.xxx.xx is executed, then you can get the rpc information of the host you are currently connected to.

rpcclient

rpcclient is used to enumerate usernames on Linux and OS X.

The syntax for rpcclient follows:

rpcclient [-A authfile] [-c <command string>] [-d debuglevel] [-h] [-l logdir] [-N] [-s <smb config file>] [-U username[%password]] [-W workgroup] [-I destinationIP] {server}

Options:

-c	Execute semicolon-separated commands.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-I	IP address is the address of the server to connect to. It should be specified in standard "a.b.c.d" notation.
Z`-p	This number is the TCP port number used when making connections to the server. The standard TCP port number for an SMB/CIFS server is 139, which is the default.
-d	debuglevel is an integer from 0 to 10. The default value if this parameter is not specified is 0.
-V	Prints the program version number.
-s	The file specified contains the configuration details required by the server.
-l	Base directory name for log/debug files. The extension ".progname" will be appended (e.g. log.smbclient, log.smbd, etc...). The log file is never removed by the client.
-N	If specified, this parameter suppresses the normal password prompt from the client to the user. This is useful when accessing a service that does not require a password.
-A	This option allows you to specify a file from which to read the username and password used in the connection.
-U	Sets the SMB user name or user name and password.
-W	Set the SMB domain of the use rname.
-h	Print a summary of command-line options.

For example, if the command root $] rpcclient $> netshareenum is executed, then it displays all the user names.

showmount

showmount identifies and lists the shared directories available on a system. The clients that are remotely mounted on a file system from a host are listed by showmount. mountd is an RPC server that replies to the **NFS access information** and file system mount requests. The mountd server on the host maintains the obtained information. The file /etc/rmtab saves the information from **crashing**. The default value for the host is the value returned by hostname (1).

The syntax for the mountd: `/usr/lib/nfs/mountd [-v] [-r]`

The syntax for Showmount: `/usr/sbin/showmount [-ade] [hostname]`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Options:

-a	Print all remote mounts in the format.
-d	List directories that have been remotely mounted by clients.
-e	Print the list of shared file systems.

For example, if the command [root $] showmount –e 19x.16x. xxx.xx is executed, then it displays the list of all shared directories that are mounted by a host.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Linux Enumeration Tool: Enum4linux

```
sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 20(

----- Target information -----
Target ........... 192.168.2.55
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 ------
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008
```

http://labs.portcullis.co.uk

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

Linux Enumeration Tool: Enum4linux

Source: http://labs.portcullis.co.uk

Enum4linux is a tool that allows you to enumerate information from **samba**, as well as Windows systems.

Features:

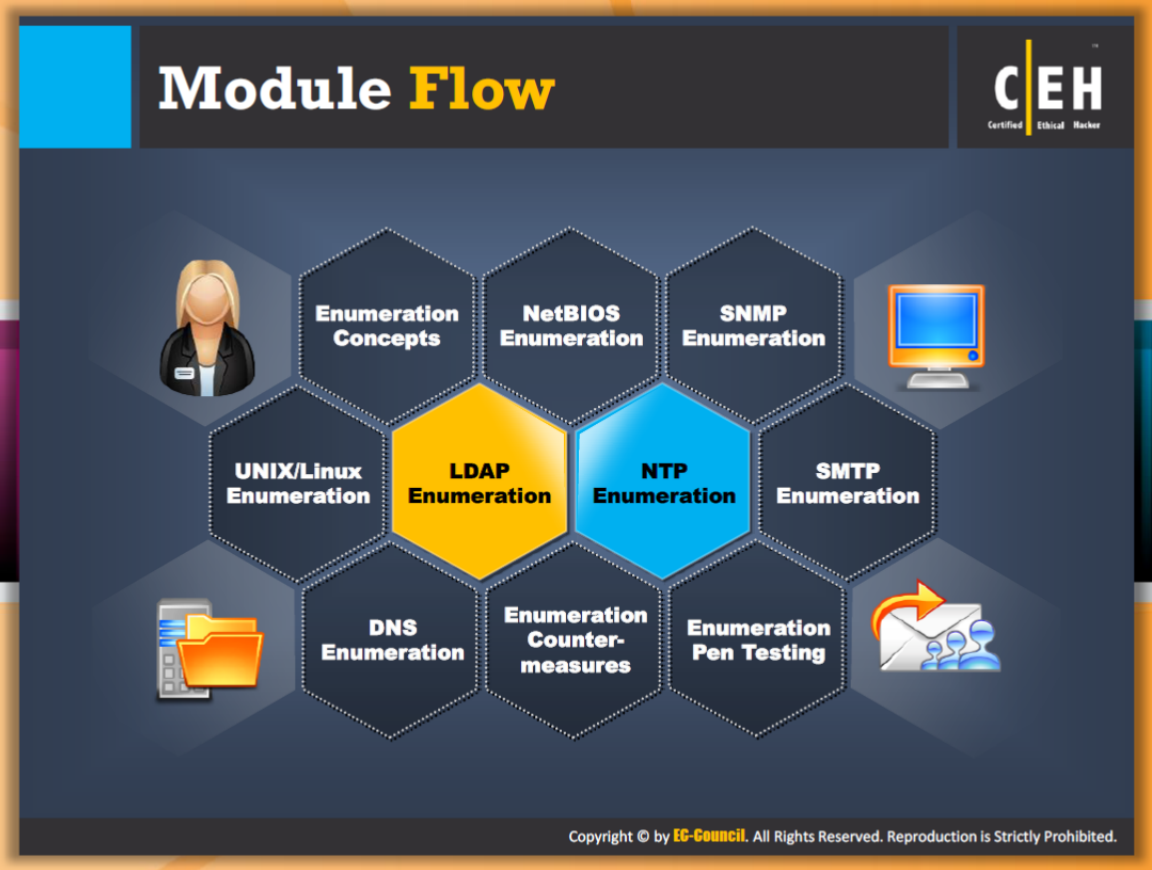
- RID Cycling (When RestrictAnonymous is set to 1 on Windows 2000)
- User Listing (When RestrictAnonymous is set to 0 on Windows 2000)
- Listing of Group Membership Information
- Share Enumeration
- Detecting if host is in a Workgroup or a Domain
- Identifying the remote Operating System
- Password Policy Retrieval (using polenum)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 20(

----- Target information -----
Target ........... 192.168.2.55
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 ------
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008
```

FIGURE 4.11: Enum4linux Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



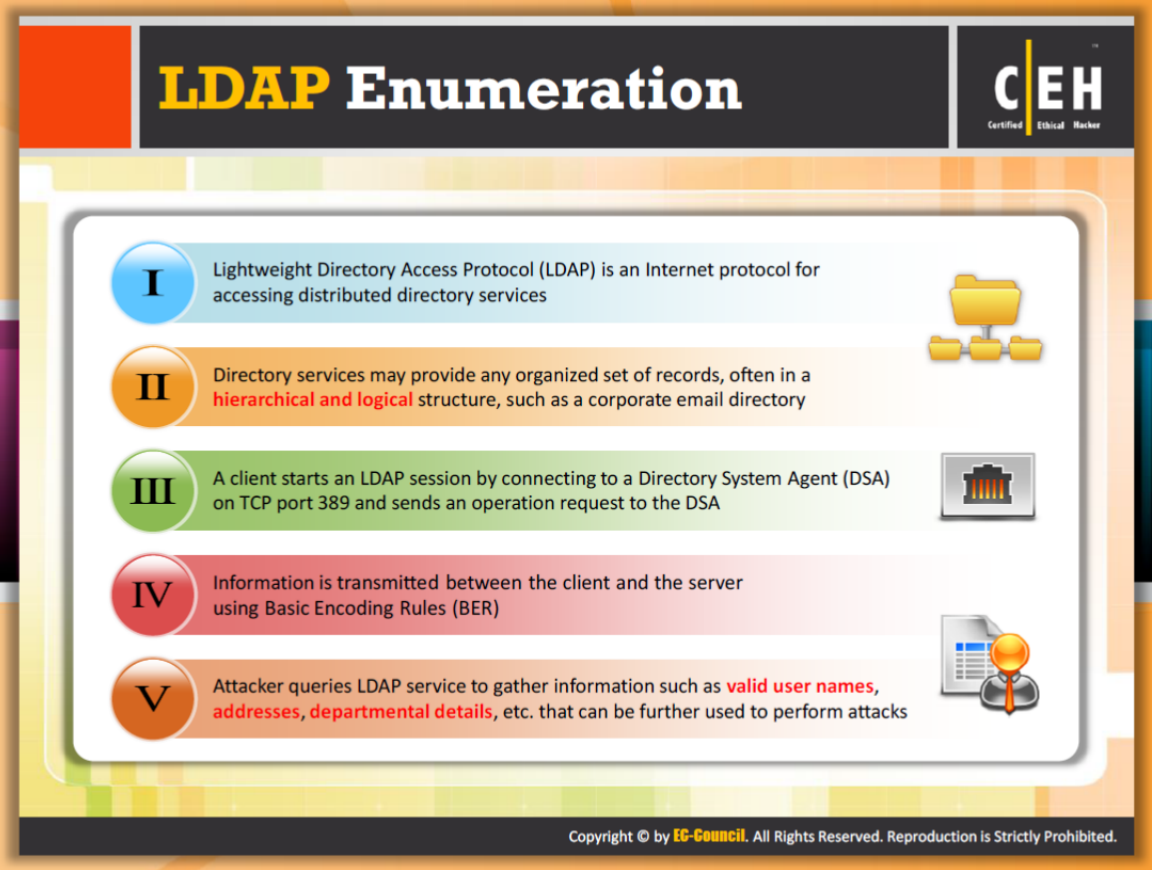
Module Flow

To enable communication and manage data transfer between network resources, various protocols are employed. All these protocols carry valuable information about network resources along with the data to be transferred. If any external user is able to enumerate that information by manipulating the protocols, then he or she can break into the network and may misuse the network resources. LDAP is one such protocol intended to access the directory listings.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section focuses on LDAP enumeration and LDAP enumeration tools

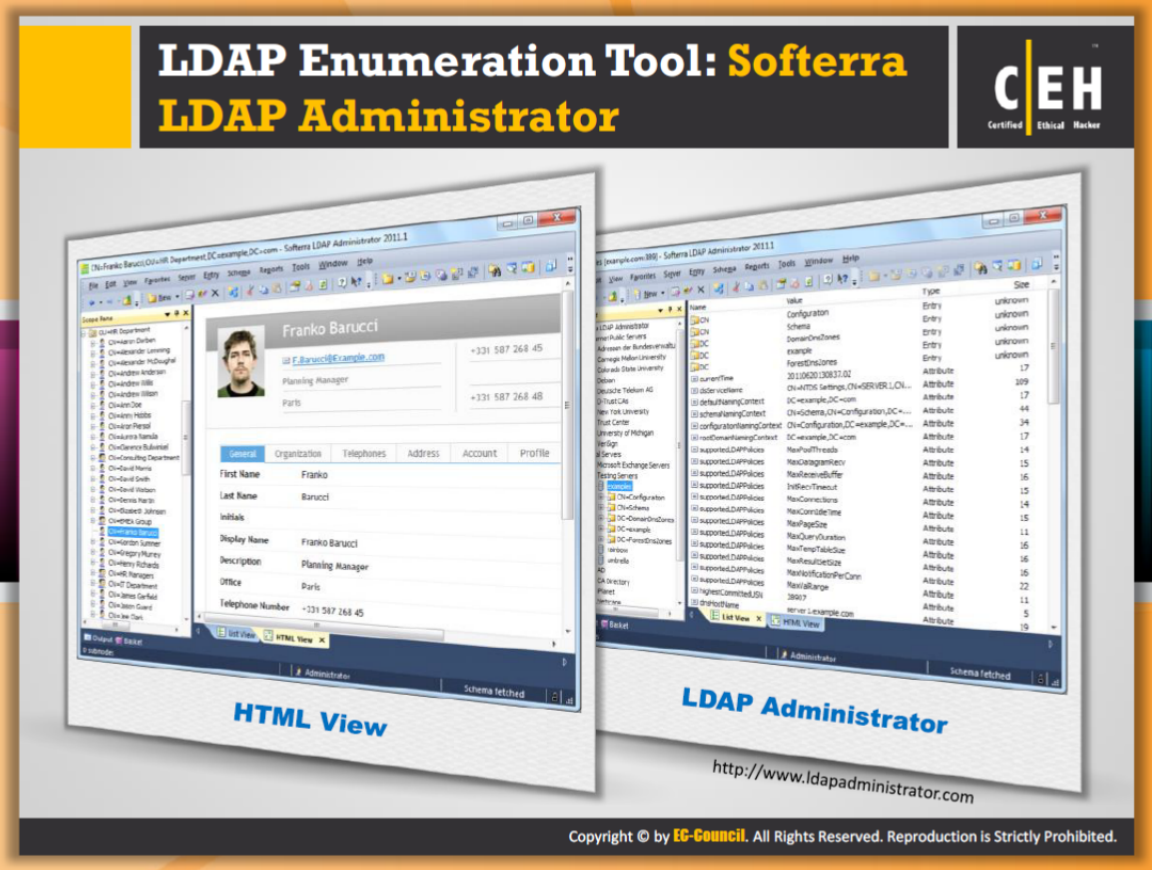
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LDAP Enumeration

The Lightweight Directory Access Protocol (LDAP) is used to access directory listings within an Active Directory or from other directory services. A directory is compiled in hierarchical or logical form, slightly like the levels of management and employees in a company. It is suitable to attach with the Domain Name System (DNS) to allow quick lookups and fast resolution of queries. It usually runs on the port 389 and other similar protocols. You can anonymously query the LDAP service. The query will disclose sensitive information such as user names, addresses, departmental details, server names, etc., which can be used by the attacker for launching the attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LDAP Enumeration Tool: Softerra LDAP Administrator

Source: http://www.ldapadministrator.com

Softerra LDAP Administrator is a **LDAP administration tool** that allows you to work with LDAP servers such as Active Directory, Novell Directory Services, Netscape/iPlanet, etc. It generates customizable directory reports with information necessary for effective monitoring and audit.

Features:

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

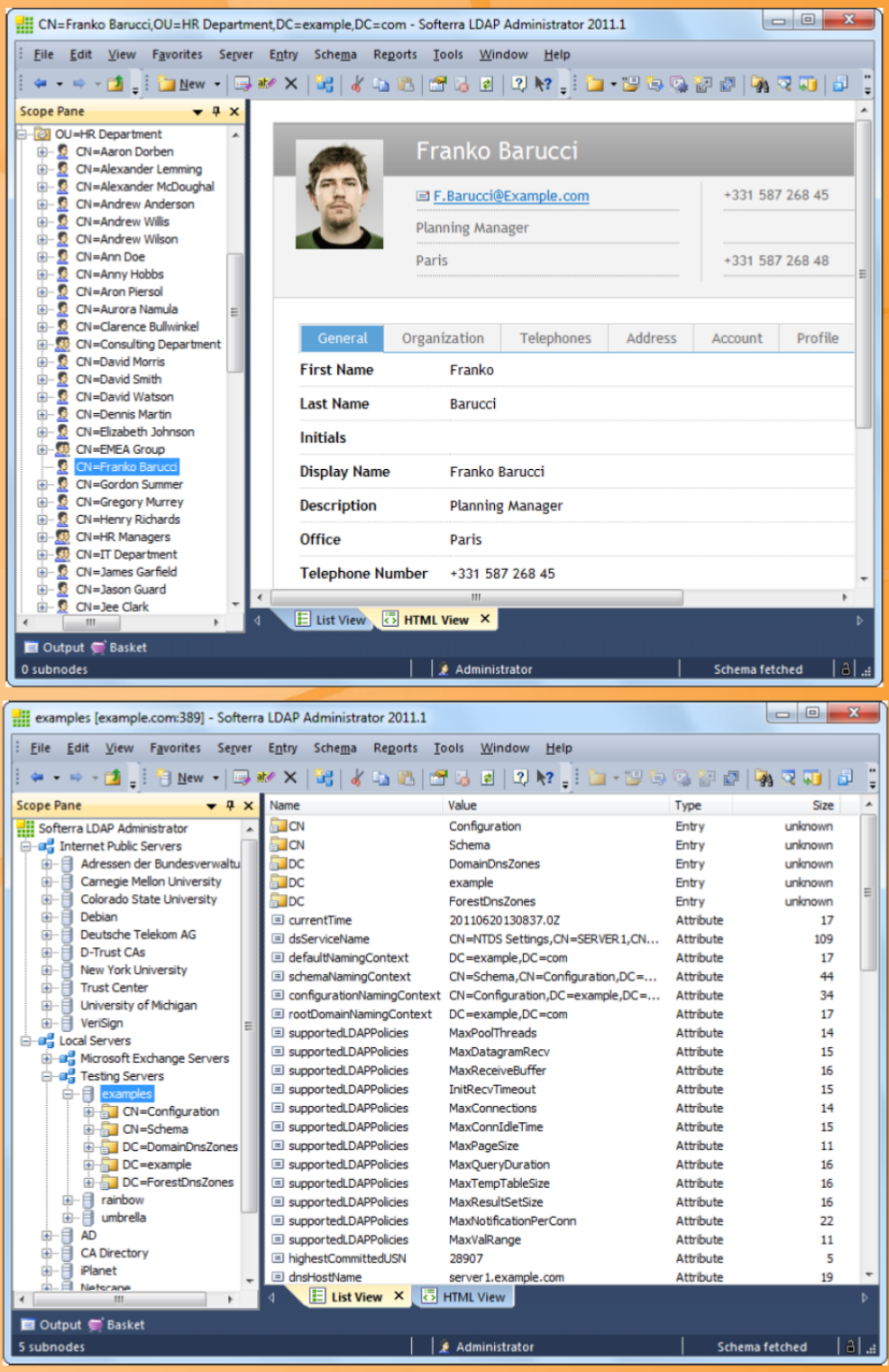
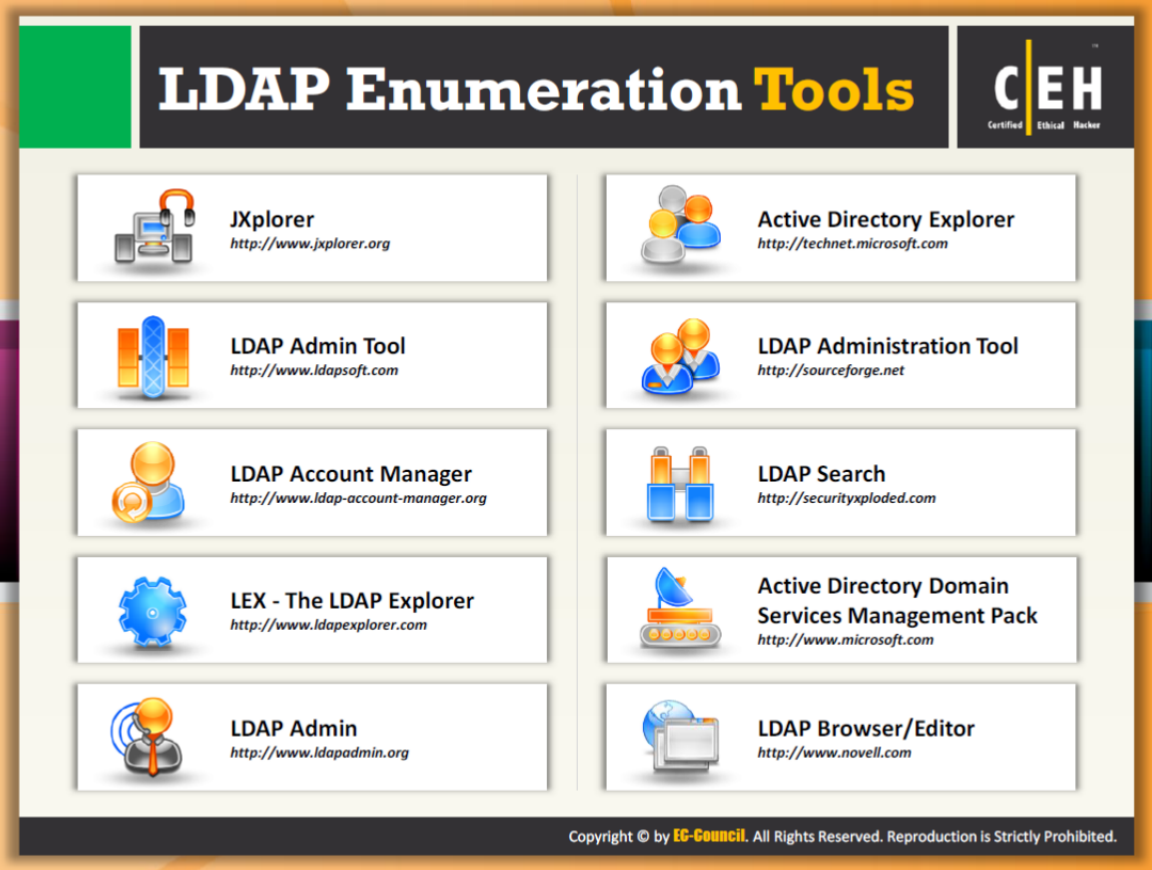


FIGURE 4.12: Softerra LDAP Administrator tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



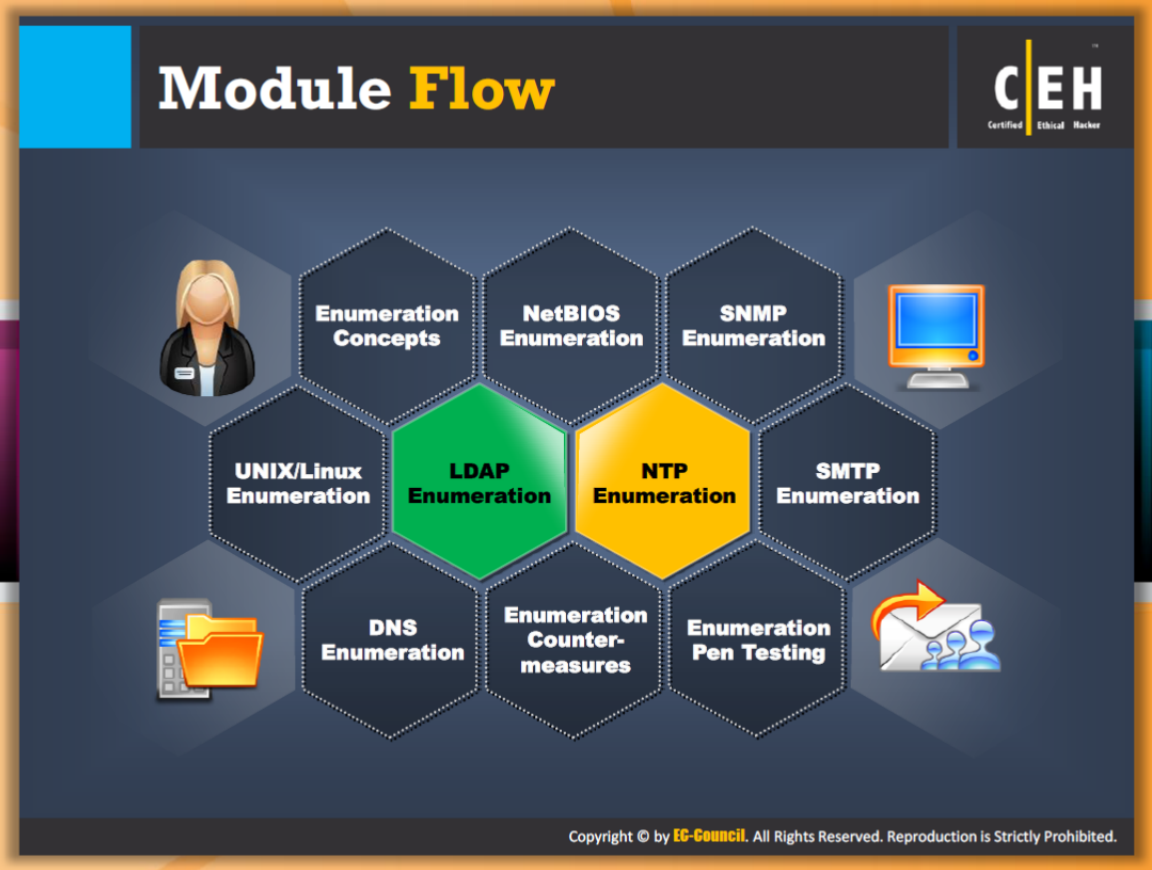
LDAP Enumeration Tools

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

A few LDAP enumeration tools are listed as follows:

- JXplorer available at http://www.jxplorer.org
- LDAP Admin Tool available at http://www.ldapsoft.com
- LDAP Account Manager available at http://www.ldap-account-manager.org
- LEX - The LDAP Explorer available at http://www.ldapexplorer.com
- LDAP Admin available at http://www.ldapadmin.org
- Active Directory Explorer available at http://technet.microsoft.com
- LDAP Administration Tool available at http://sourceforge.net
- LDAP Search available at http://securityxploded.com
- Active Directory Domain Services Management Pack available at http://www.microsoft.com
- LDAP Browser/Editor available at http://www.novell.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



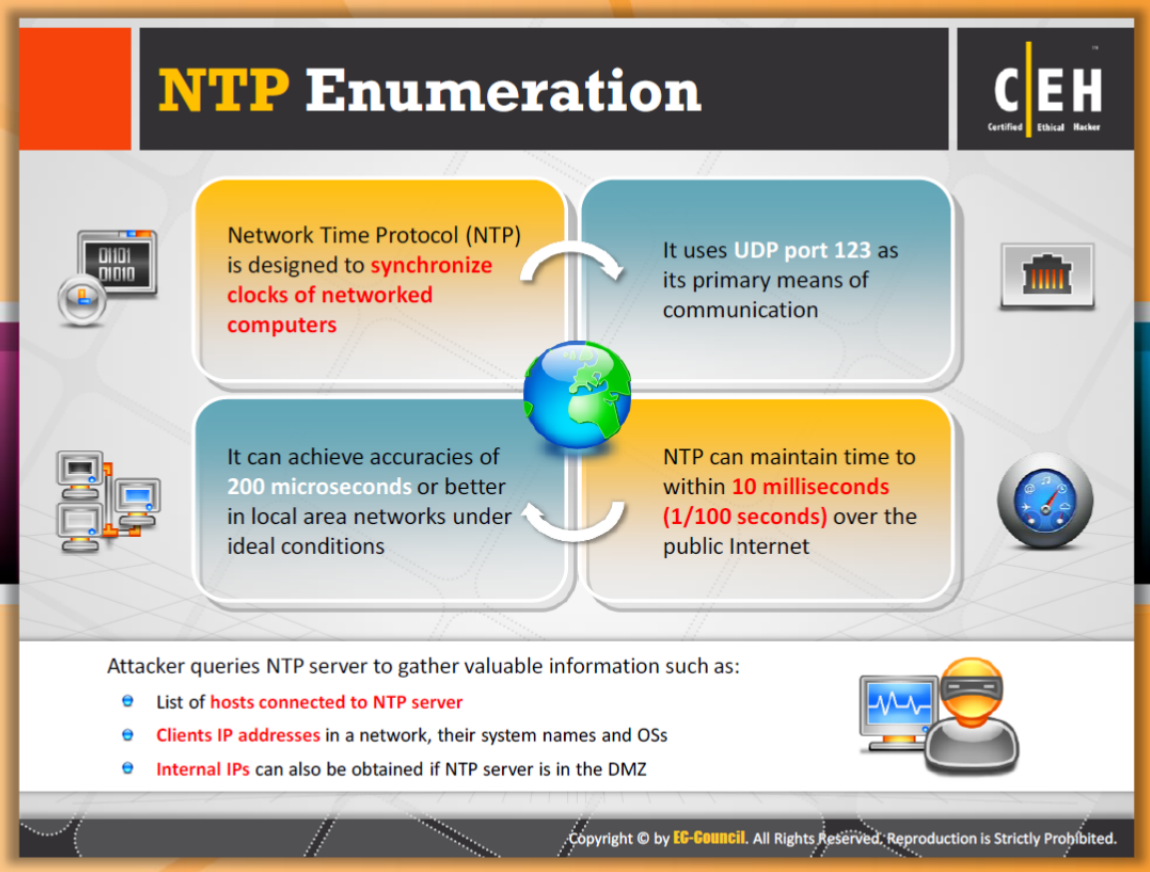
Module Flow

Often, the NTP server is overlooked in terms of security. But, if queried properly, it can also provide a lot of valuable network information to the attackers. Therefore, it is necessary to test what information an attacker can enumerate about your network through NTP enumeration.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section describes what is NTP, what information can be extracted through NTP enumeration, and NTP enumeration commands

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

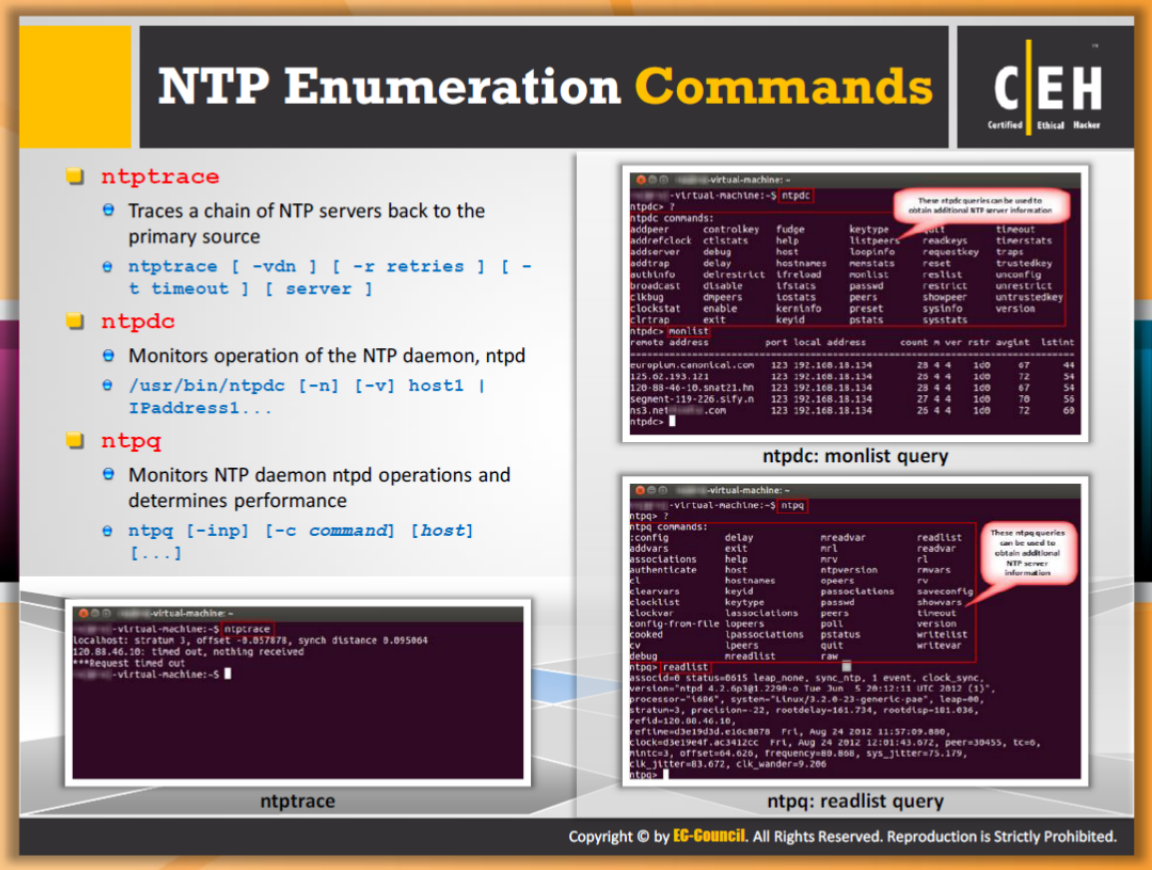


NTP Enumeration

Before beginning with NTP enumeration, let's first discuss what NTP is. NTP is a network protocol designed to synchronize clocks of networked computer systems. NTP is important when using Directory Services. It uses **UDP port 123** as its primary means for 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.

Through NTP enumeration, you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client systems in a network. All this information can be enumerated by querying the NTP server. If the **NTP server** is in the DMZ, then it can also be possible to obtain internal IPs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTP Enumeration Commands

NTP enumeration can be performed using the **NTP suite command-line tool**. NTP Suite is used for querying the NTP server to get desired information from the NTP. This command-line tool includes the following commands:

- `ntptrace`
- `ntpdc`
- `ntpq`

These commands will help you extract the data from the NTP protocol used in the **target network**.

ntptrace:

This command helps you determine from where the NTP server updates its time and traces the chain of NTP servers from a given host back to the prime source.

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

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
192.168.0.1: stratum 2, offset 0.0114273, synch distance 0.115554
192.168.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```

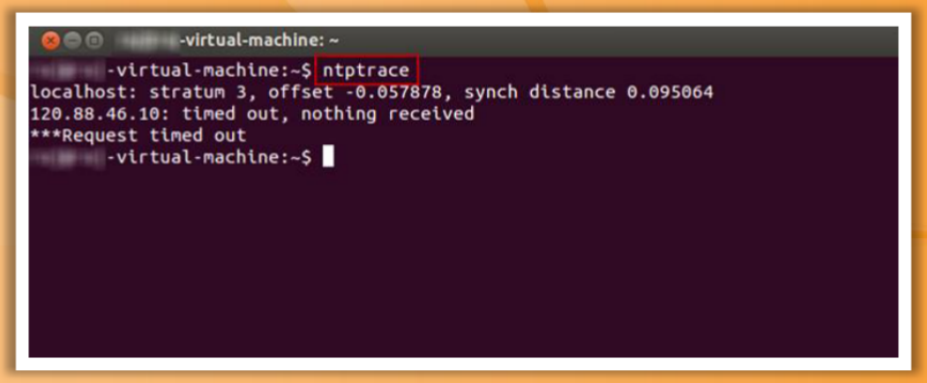


FIGURE 4.13: NTP Enumeration Tool Screenshot

ntpdc:

This command will help you to query the **ntpd** daemon about its current state and to request changes in that state.

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

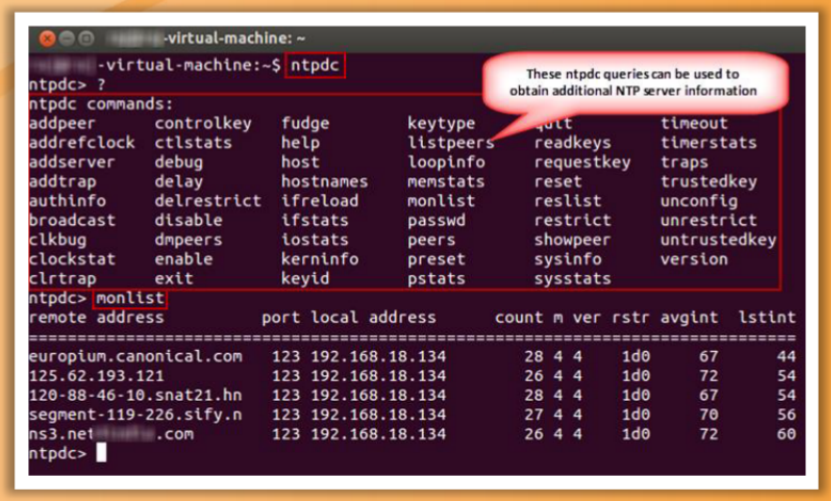


FIGURE 4.14: NTP Enumeration Tool Screenshot

ntpq:

This command will help you to monitor NTP daemon **ntpd** operations and determine performance.

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


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

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

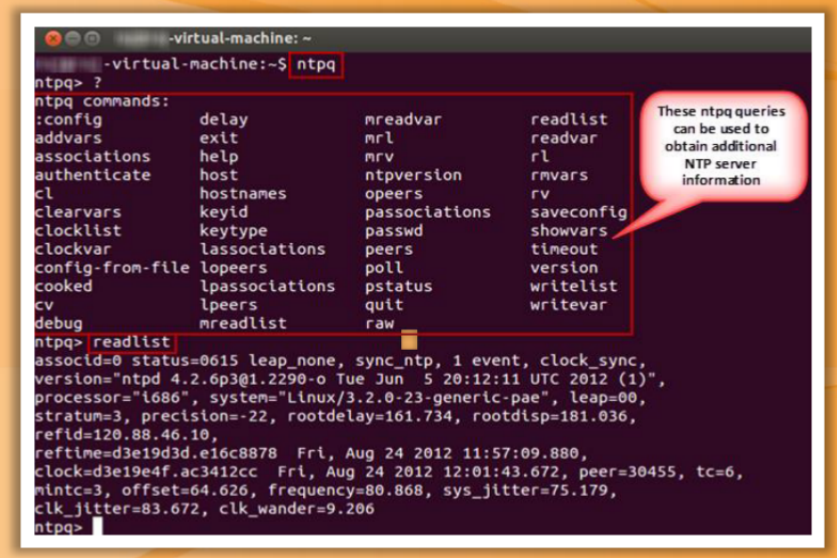
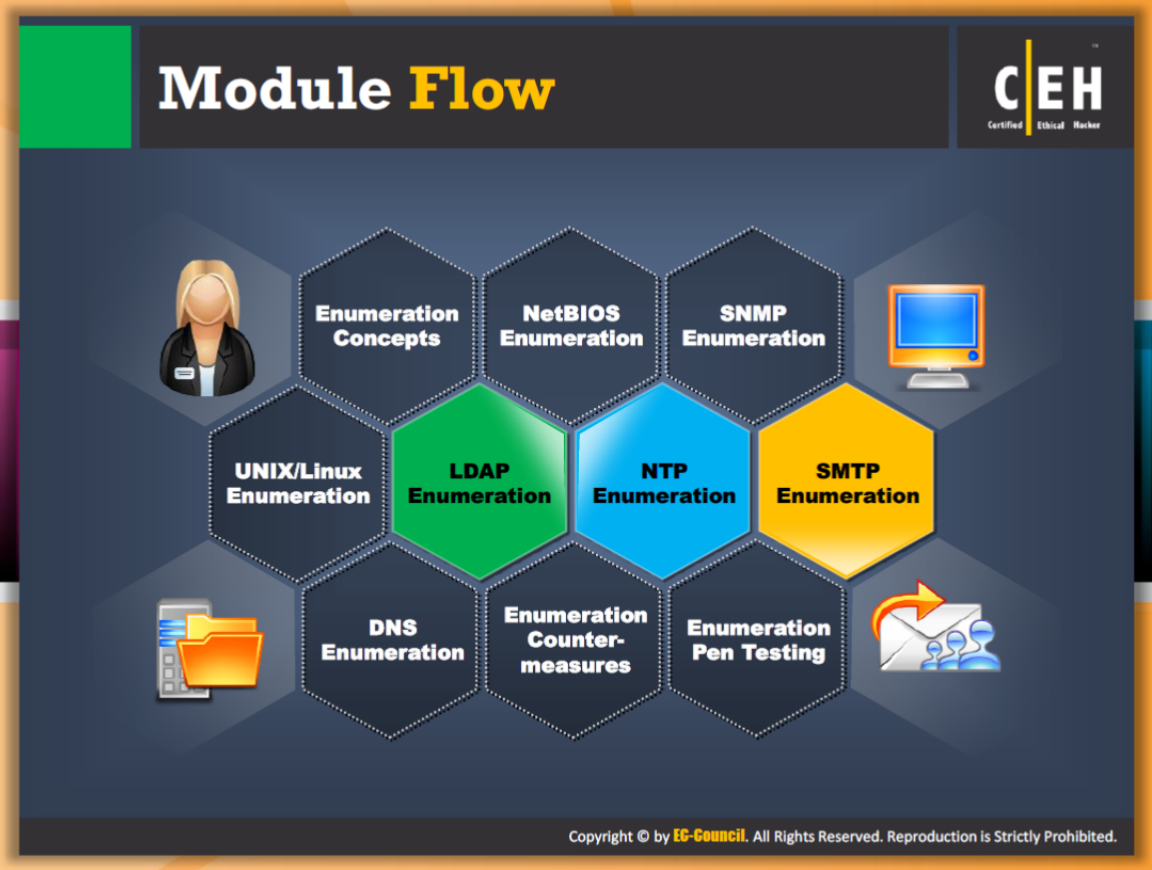


FIGURE 4.15: NTP Enumeration Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



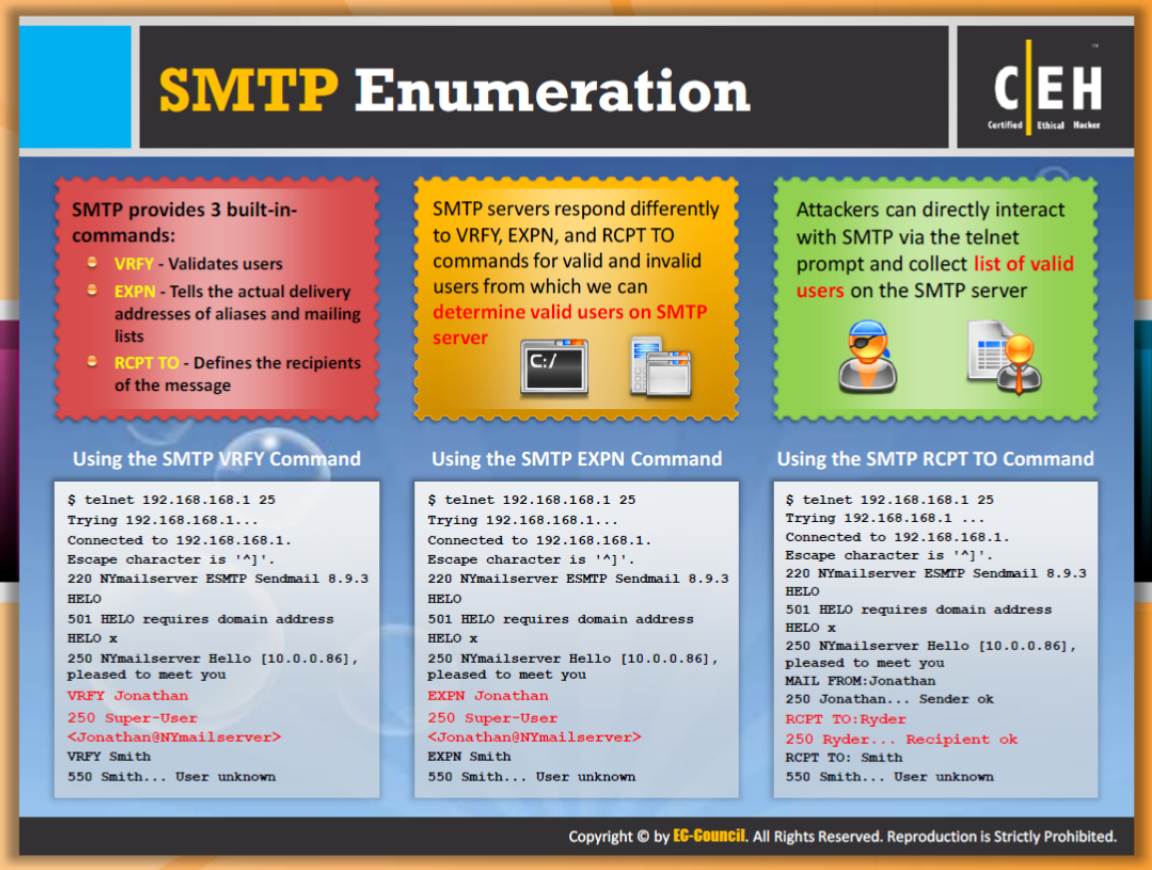
Module Flow

So far, we discussed what enumeration is and enumeration techniques to extract information related to network resources. Now it's time to discuss an enumeration technique that can extract information related to valid users on SMTP server, i.e., SMTP enumeration

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section will familiarize you with how to get a list of valid users on the SMTP server and the tools that can test the process of sending email through the SMTP server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMTP Enumeration

SMTP Enumeration allows you to determine valid users on the SMTP server. This is accomplished with the help of three **built-in SMTP commands**. The three commands are:

- **VRFY** - This command is used for validating users
- **EXPN** - This command tells the actual delivery address of aliases and mailing lists
- **RCPT TO** - It defines the recipients of the message

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users. Thus, by observing the SMTP server response to these commands, one can easily determine valid users on the SMTP server.

The attacker can also directly communicate with the **SMTP server** though the **telnet prompt** as follows:

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 '^]'.
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
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
```

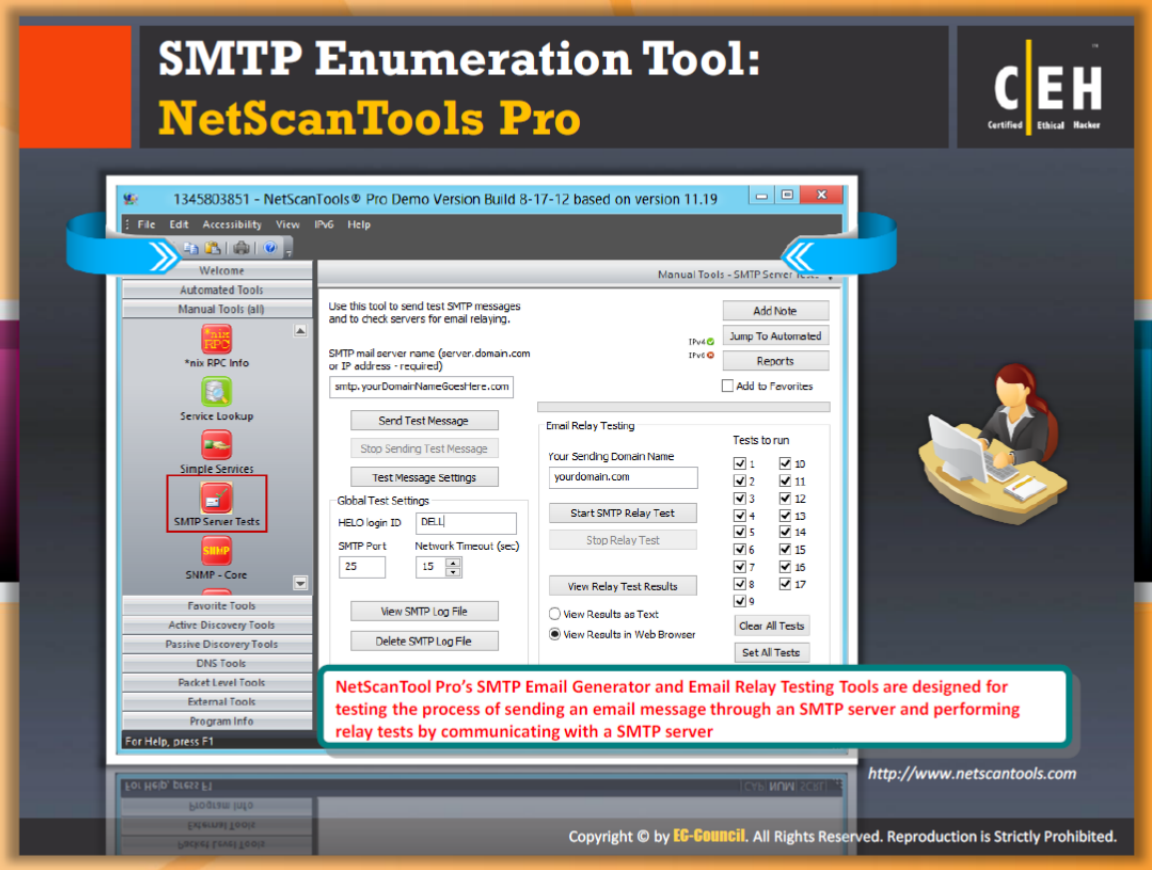
Using the SMTP EXPN Command

```
$ 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:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMTP Enumeration Tool: NetScanTools Pro

Source: http://www.netscantools.com

NetScanTool Pro's SMTP Email Generator tool allows you to test the process of sending an email message through an SMTP server. You can extract all the common email header parameters including confirm/urgent flags. You can log the **email session** to the log file and then view the log file showing the communications between NetScanTools Pro and the SMTP server.

NetScanTool Pro's Email Relay Testing Tool allows you to perform relay test by communicating with an SMTP server. The report includes a log of the communications between NetScanTools Pro and the target SMTP server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

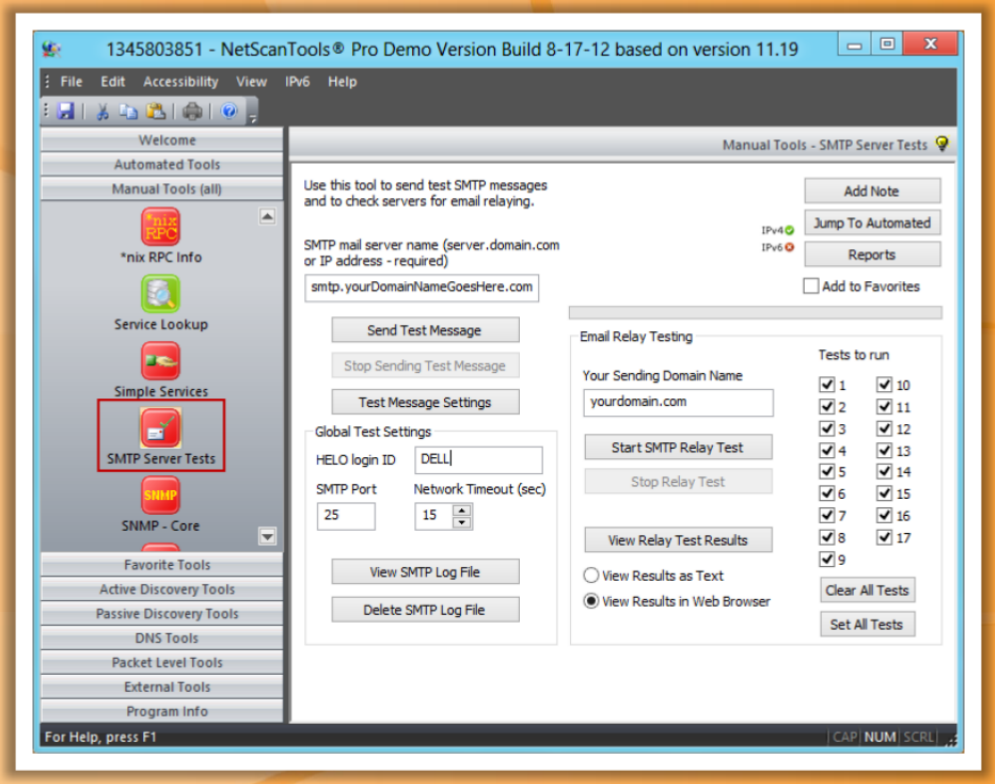
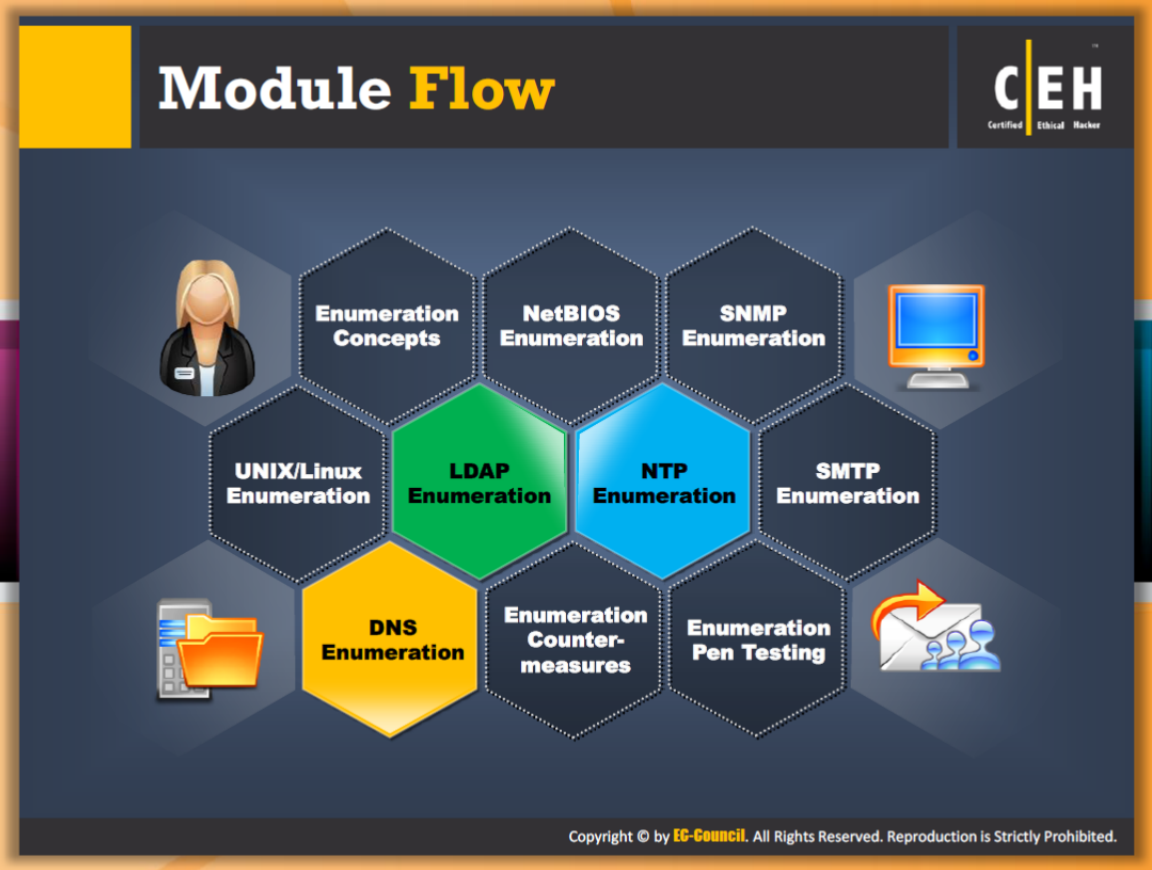


FIGURE 4.1: NetScanTools Pro Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed enumeration concepts, how to enumerate NetBIOS, SNMP, UNIX/Linux, LDAP, NTP, SMTP, and what information you can get from those enumeration processes. Now we will discuss DNS enumeration and the information you can get from it.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section describes DNS zone transfer enumeration and tools that can be used to extract DNS records.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNS Zone Transfer Enumeration Using NSLookup

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

Command Prompt

```
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. SOA 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 Zone Transfer Enumeration Using nslookup

The **attacker performs DNS zone transfer enumeration** for locating 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, and IP addresses of potential targets. To perform DNS zone transfer enumeration, you can use tools such as nslookup, DNSstuff, etc. These tools enable you to extract the same information that an attacker gathers from the DNS servers of **target organization**.

To perform a DNS zone transfer, you need to send 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.

To perform a DNS zone transfer, you need to send a zone transfer request to the DNS server pretending to be a client. In reply to your request, the DNS server transfers DNS records containing a lot of valuable network information, including IP address.

The following screenshot shows how to perform **DNS zone** transfer using nslookup:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

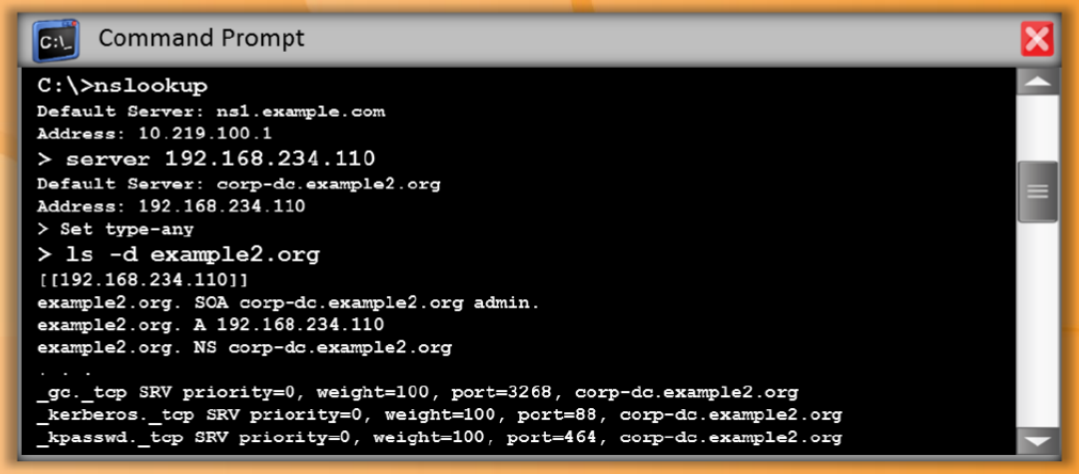
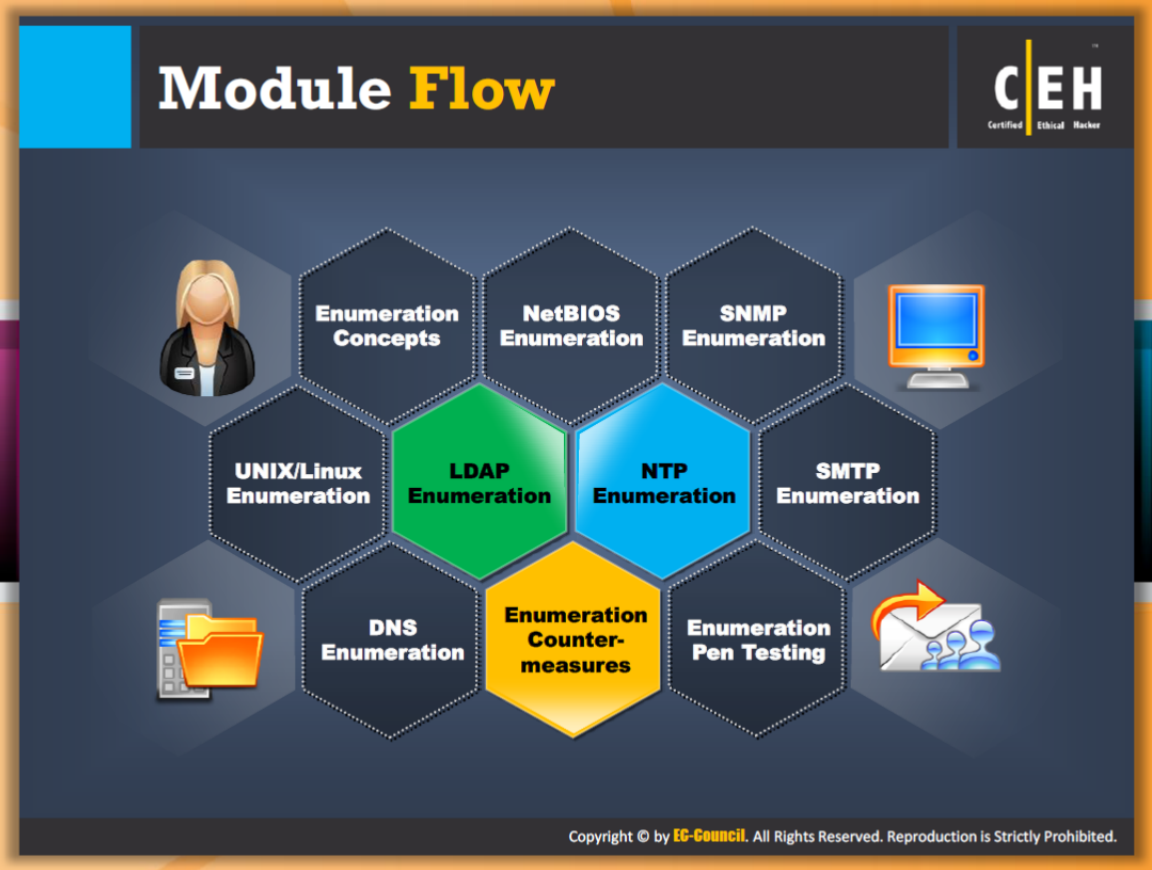


FIGURE 4.17: DNS zone Transfer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



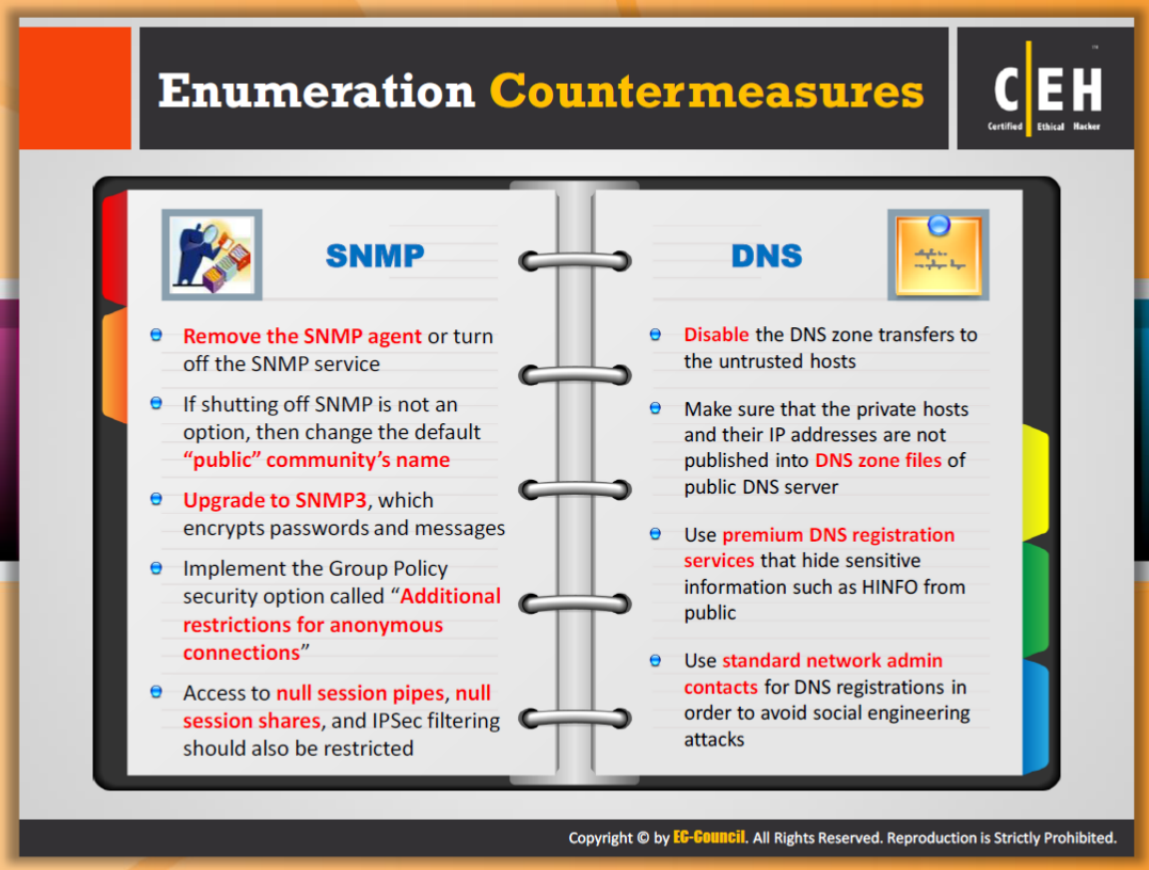
Module Flow

So far, we have discussed what enumeration is, how to perform various types of enumeration, and what type of information an attacker can extract through enumeration. Now it's time to examine the countermeasures that can help you to keep attackers away from enumerating sensitive information from your network or host.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section focuses on how to avoid **information leakage** through SNMP, DNS, SMTP, LDAP, and SMB.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumeration Countermeasures

You can apply the following countermeasures to prevent information leakage through various types of enumeration.

SNMP Enumeration Countermeasures:

- Remove the SNMP agent or turn off the SNMP service from your system.
- If shutting off **SNMP** is not an option, then change the default "public" community's name.
- Upgrade to **SNMP3**, which encrypts passwords and messages.
- Implement the Group Policy security option called "Additional restrictions for anonymous connections."
- Restrict access to null session pipes, null session shares, and IPSec filtering.
- Block access to **TCP**/**UDP** ports 161.
- Do not install the management and monitoring Windows component unless it is required.

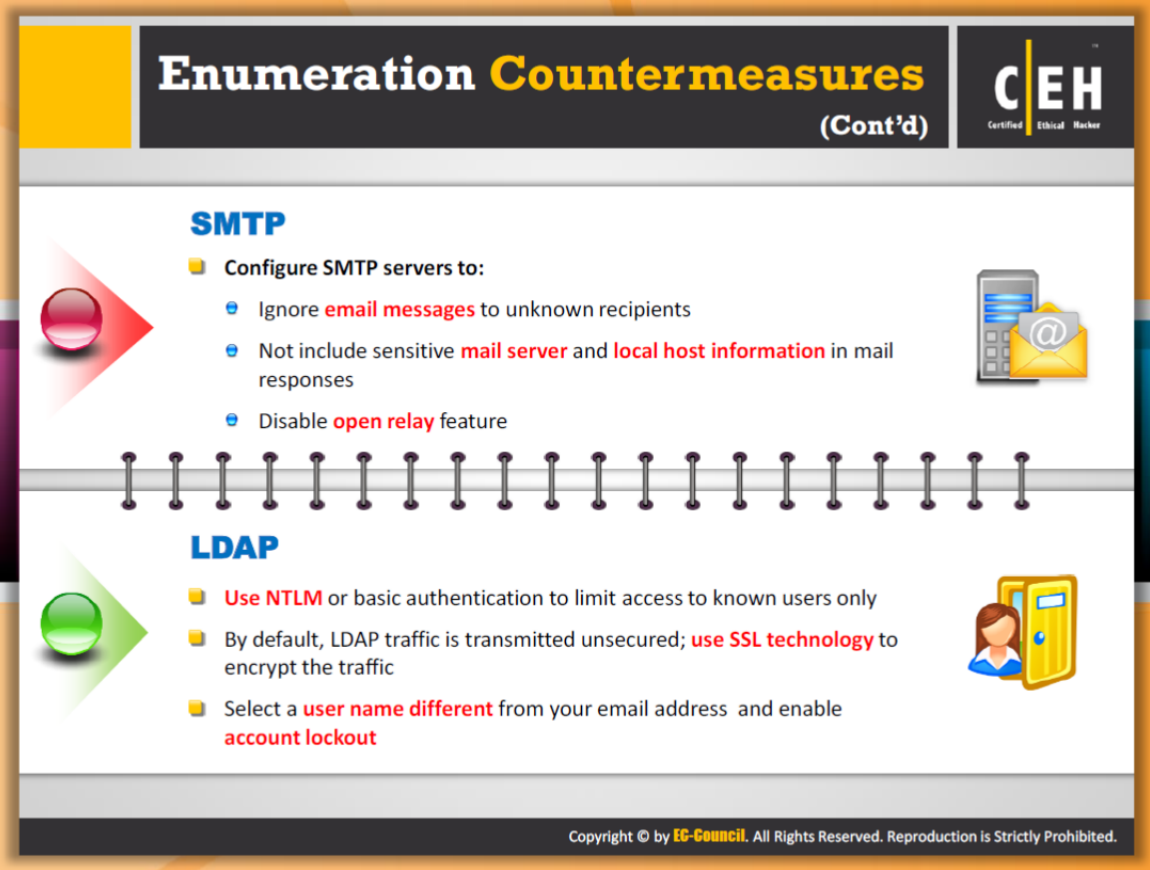
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Encrypt or authenticate using **IPSEC**.

DNS Enumeration Countermeasures:

- Configure all name servers not to send DNS zone transfers to unreliable hosts.
- Check the publicly accessible DNS server's DNS zone files and ensure that the IP addresses in these files are not referenced by non-public hostnames.
- Make sure that the DNS zone files do not contain HINFO or any other records.
- Provide standard network administration contact details in Network Information Center Databases. This helps to avoid war-dialing or social engineering attacks.
- Prune **DNS zone files** to prevent revealing unnecessary information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumeration Countermeasures (Cont'd)

SMTP:

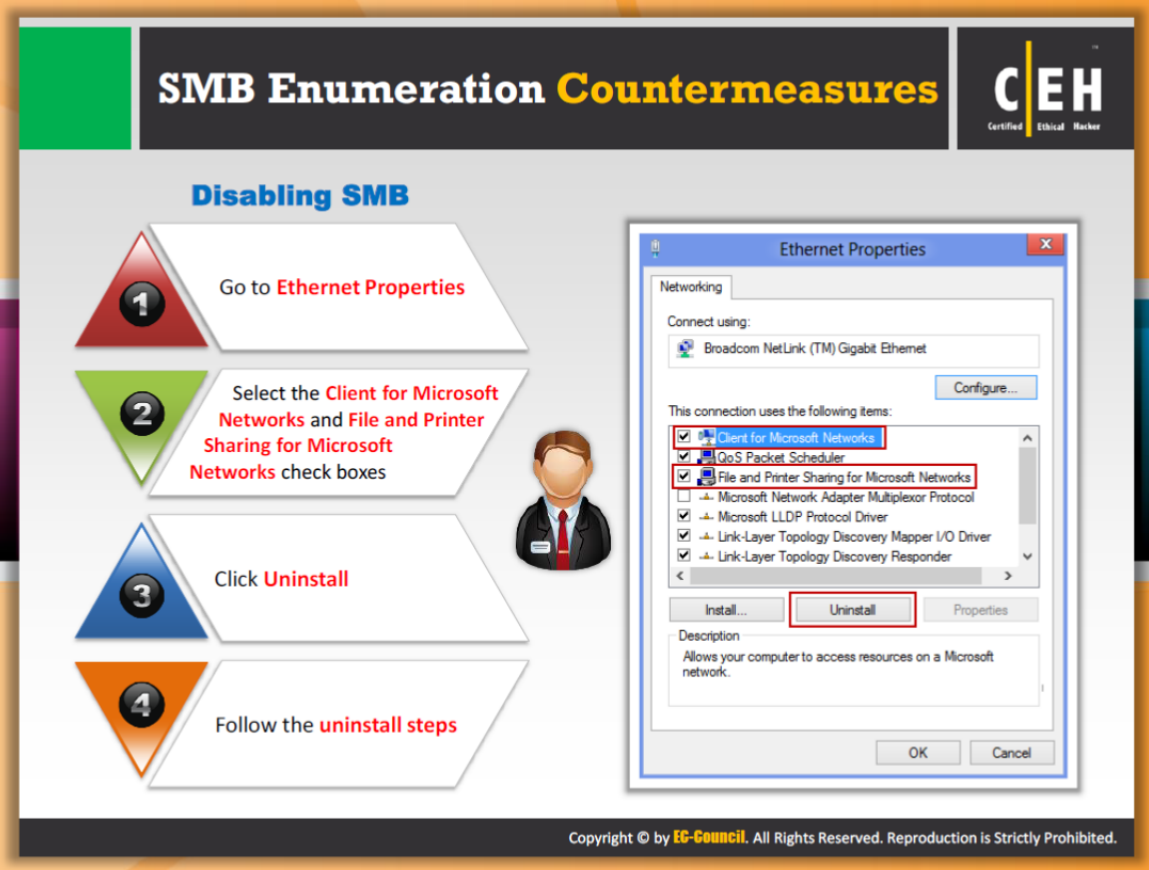
Configure SMTP servers to:

- Ignore email messages to unknown recipients.
- Not include sensitive mail server and local host information in mail responses.
- Disable open relay feature Ignore emails to unknown recipients by configuring SMTP servers.

LDAP:

- Use **NTLM** or basic authentication to limit access to known users only.
- By default, **LDAP** traffic is transmitted unsecured; use SSL technology to encrypt the traffic.
- Select a user name different from your **email address** and enable account lockout.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SMB Enumeration Countermeasures

Common sharing services or other unused services may prove to be **doorways** for attackers to break into your security. Therefore, you should disable these services to avoid information leakage or other types of attacks. If you don't disable these services, then you can be vulnerable enumeration. **Server Message Block** (SMB) is a service intended to provide shared access to files, serial ports, printers, and communications between nodes on a network. If this service is running on your network, then you will be at high risk of getting **attacked**.

Therefore, you should disable it if not necessary, to prevent enumeration. Steps to disable SMB:

1. Go to **Ethernet Properties**.
2. Select the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** check boxes.
3. Click **Uninstall**.
4. Follow the uninstall steps.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

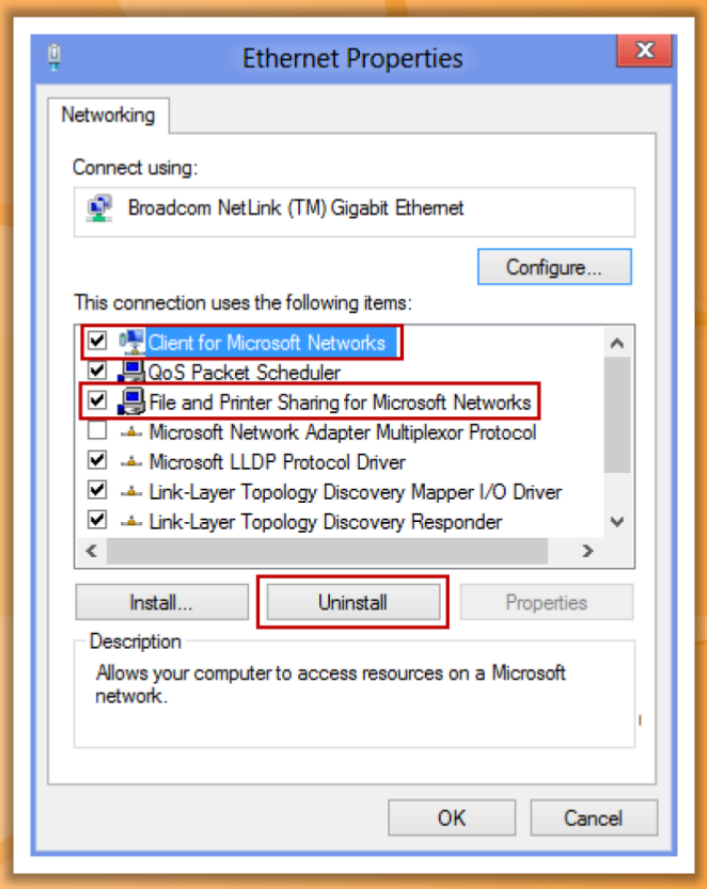
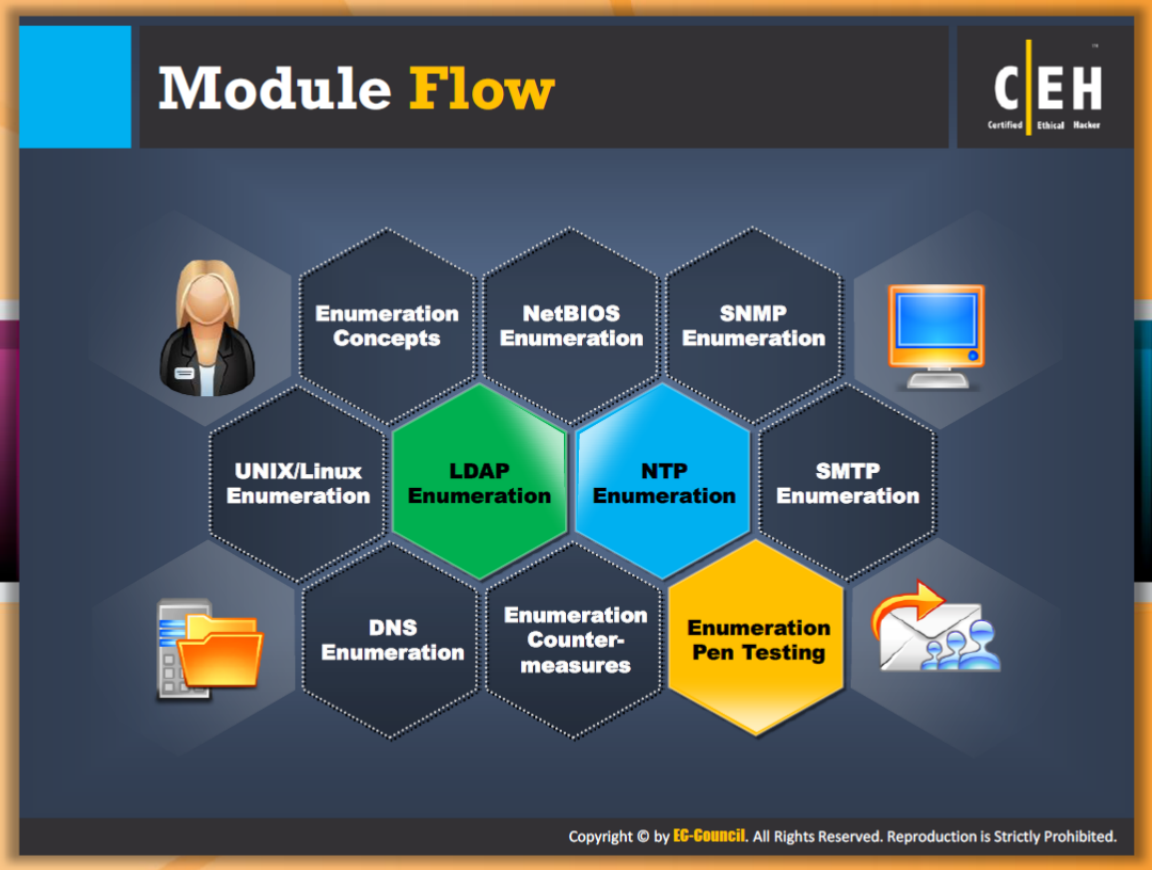


FIGURE 4.18: Ethernet properties Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

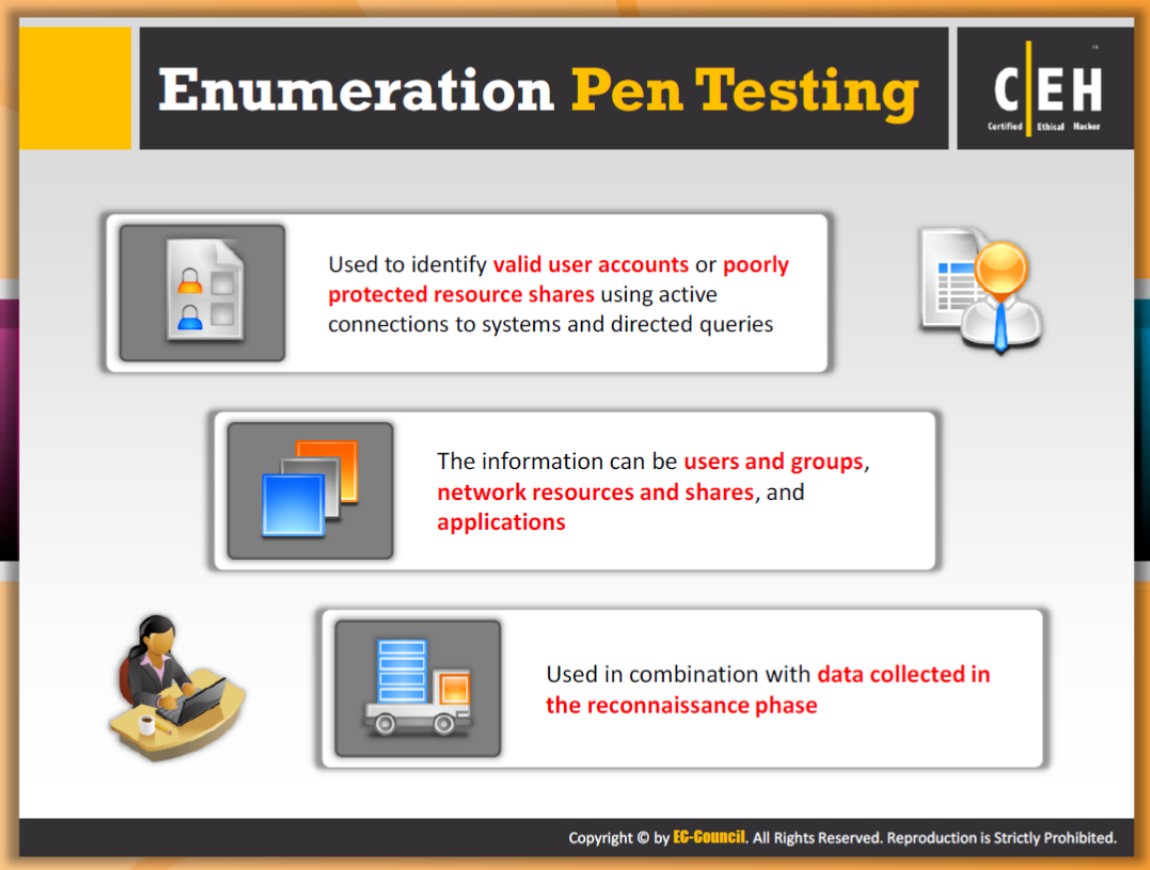


Module Flow

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

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

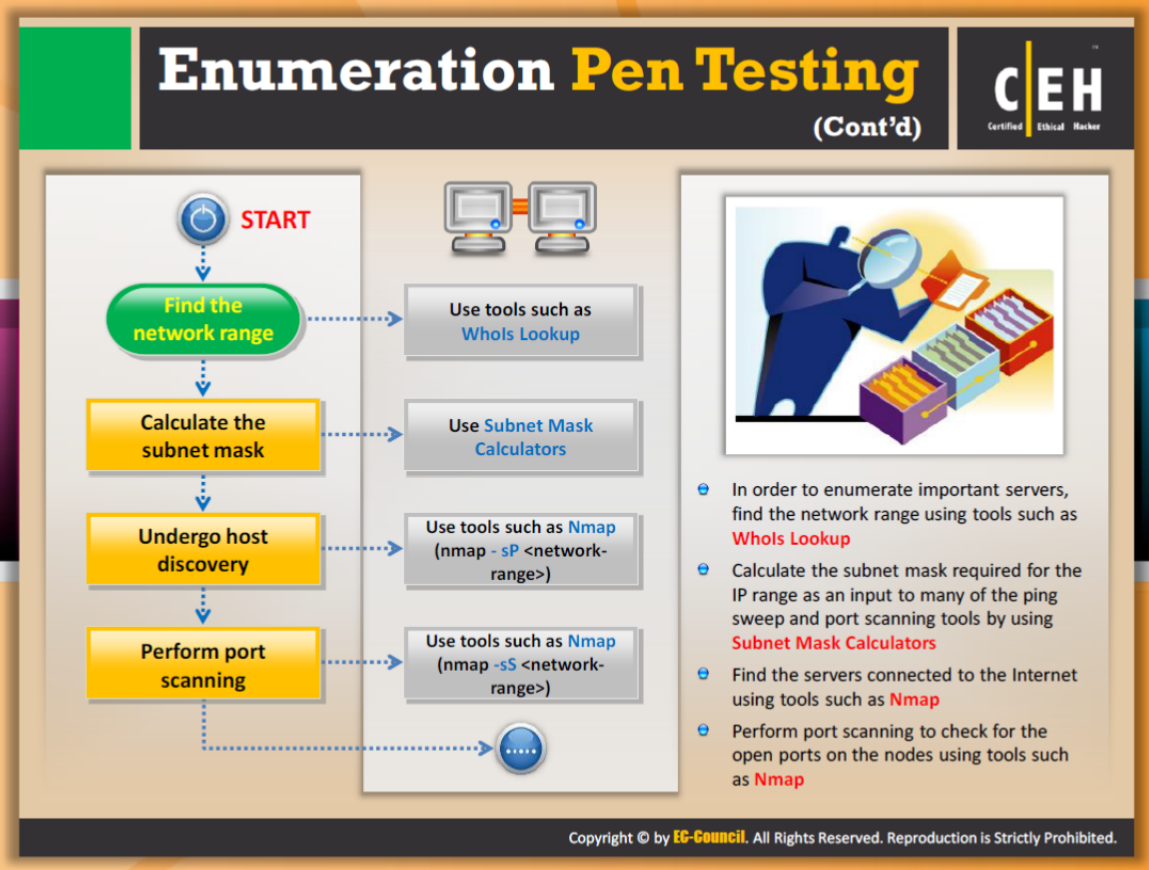


Enumeration Pen Testing

Through enumeration, an attacker may gather **sensitive information** of organizations if the security is not strong. He or she may then use that sensitive information to hack and break into the organization's network. If an attacker breaks into the organization, then the organization **potentially faces** huge losses in terms of information, service, or finance. Therefore, to avoid these kinds of attacks, every organization must test its own security. Testing the security of an organization legally against enumeration is called enumeration pen testing. Enumeration pen testing is conducted with the help of the data collected in the **reconnaissance phase.**

As a pen tester, conduct enumeration penetration tests to check whether the target network is revealing any sensitive information that may help an attacker to perform a **well-planned attack**. Apply all types of enumeration techniques to gather sensitive information such as user accounts, IP address, email contacts, DNS, network resources and shares, application information, and much more. Try to discover as much information as possible regarding the target. This helps you determine the **vulnerabilities**/**weaknesses** in the target organization's security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumeration Pen Testing (Cont'd)

You should conduct 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 is divided into steps. This **penetration test** includes a series of steps to obtain desired information.

Step1: Find the network range

If you want to break into an **organization's network**, you should know the network range first. This is because if you know the network range, then you can mask yourself as a user falling within the range and then try to access the network. So the first step in enumeration pen testing is to obtain information about network range. You can find the network range of target organization with the help of tools such as **WhoIs** Lookup.

Step 2: Calculate the subnet mask

Once you find the network rage of the target network, then calculate the subnet mask required for the IP range using tools such as **Subnet Mask** Calculator. You can use the calculated subnet mask as an input to many of the ping sweep and port scanning tools for further enumeration, which includes discovering hosts and open ports.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

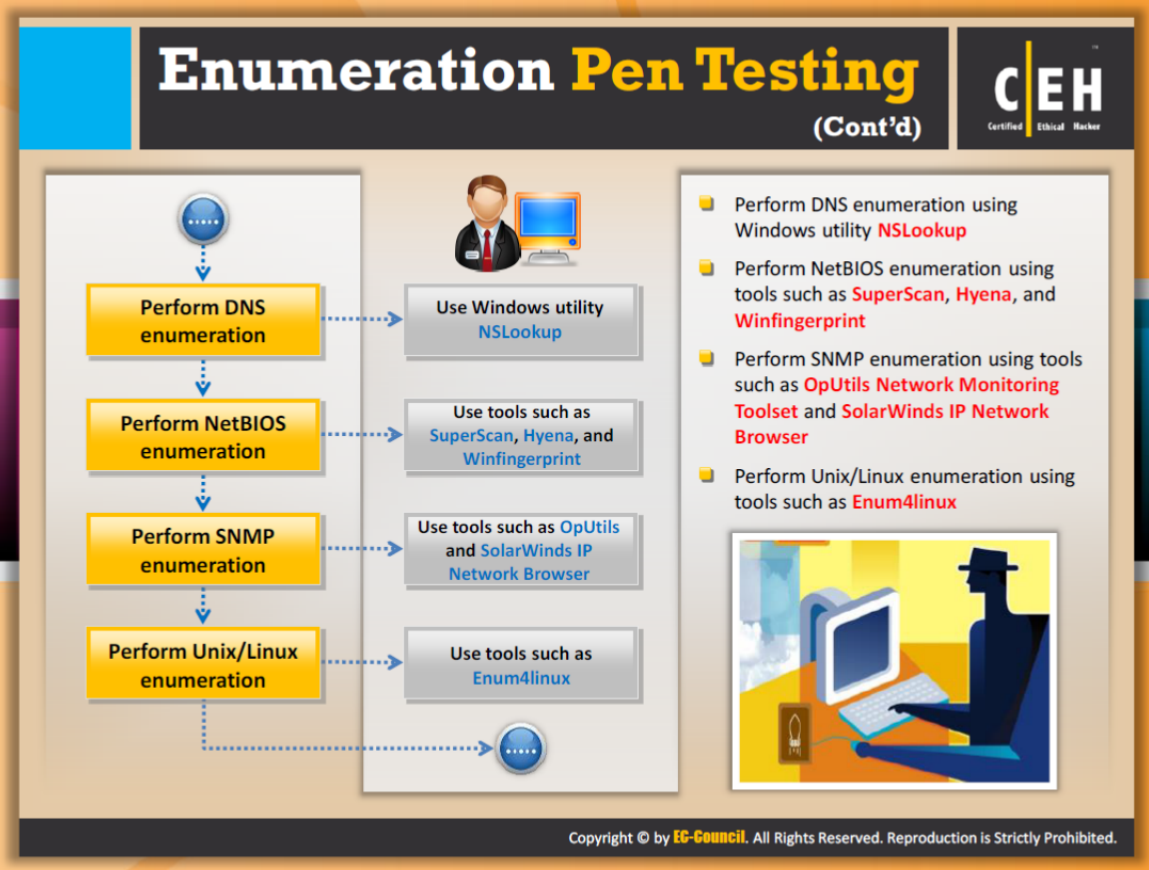
Step 3: Undergo host discovery

Find the important servers connected to the Internet using tools such as Nmap. 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

It is very important to discover the open ports and close them if they are not required. This is because open ports are the 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. This can be accomplished with the help of tools such as **Nmap**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumeration Pen Testing (Cont'd)

Step 5: 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. You can extract all this information with the help of the Windows utility **nslookup**.

Step 6: 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**. You can perform NetBIOS enumeration with the help of tools such as SuperScan, Hyena, and WinFingerprint.

Step 7: Perform SNMP enumeration

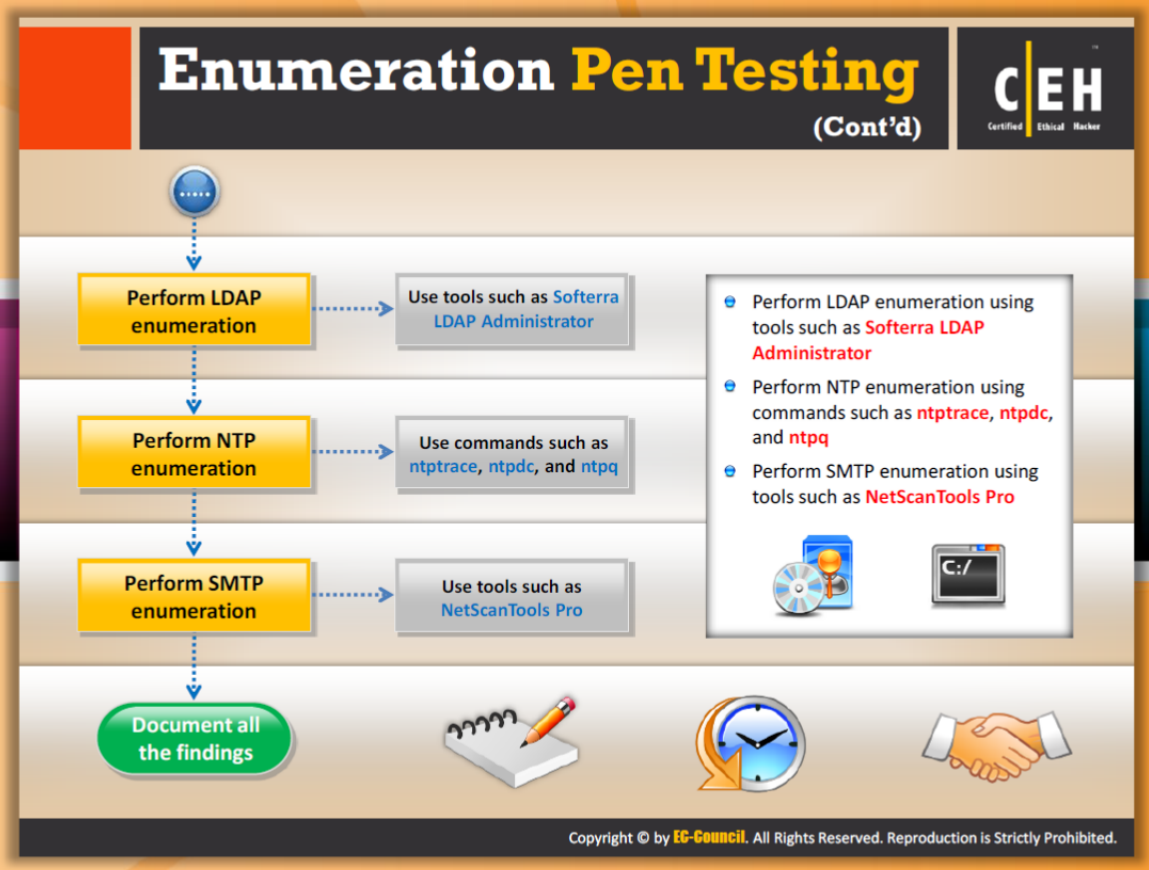
Perform SNMP enumeration by querying the SNMP server in the network. The SNMP server may reveal information about user accounts and devices. You can perform SNMP enumeration using tools such as **OpUtils** and **SolarWinds** IP Network Browser.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Perform Unix/Linux enumeration

Perform Unix/Linux enumeration using tools such as Enum4linux. You can use commands such as `Showmount`, `Finger`, `rpfinfo` (RPC), and `rpcclient` etc.to enumerate UNIX network resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumeration Pen Testing (Cont'd)

Step 9: Perform LDAP enumeration

Perform LDAP enumeration by querying the LDAP service. By querying the LDAP service you can enumerate valid user names, departmental details, and address details. You can use this information to perform social engineering and other kinds of attacks. You can perform LDAP enumeration using tools such as Softerra LDAP Administrator.

Step 10: Perform NTP enumeration

Perform NTP enumeration to extract information such as host connected to NTP server, client IP address, OS running of client systems, etc. You can obtain this information with the help of commands such as ntptrace, ntpdc, and ntpq.

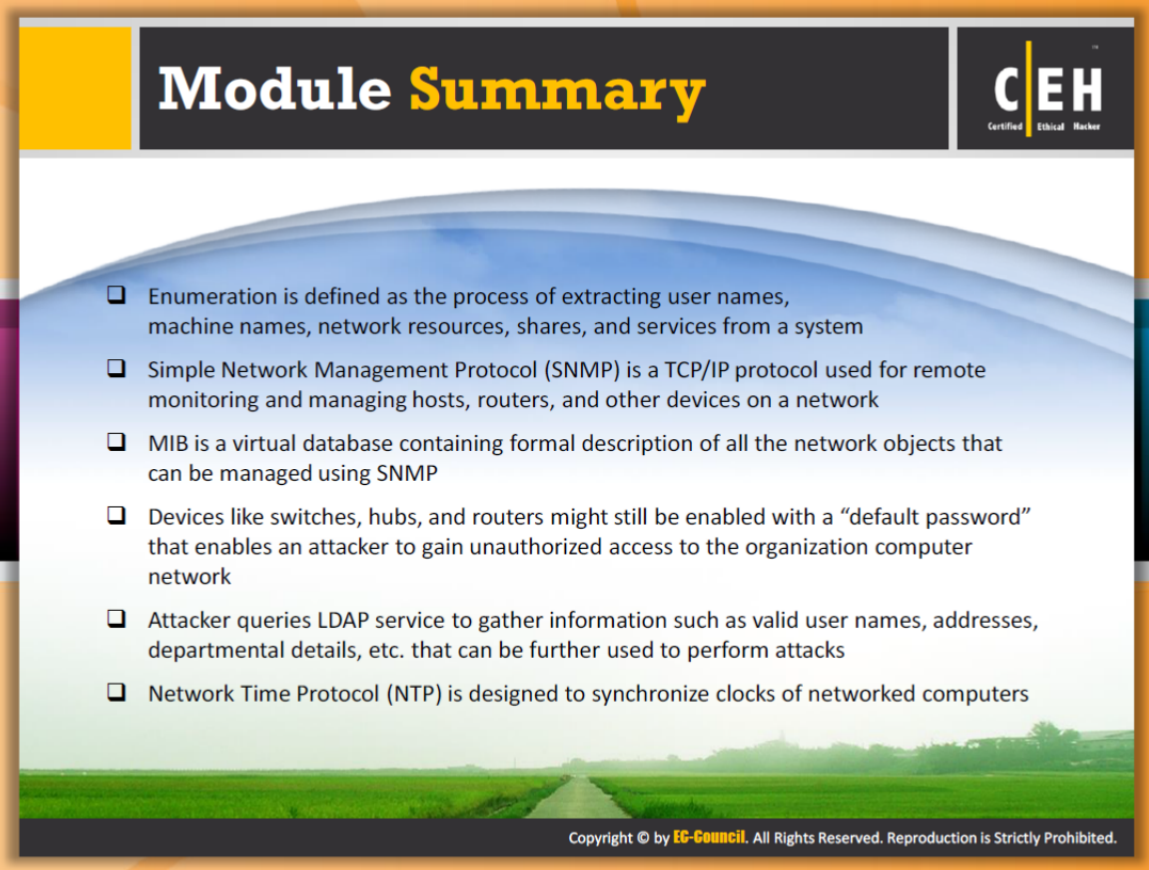
Step 11: Perform SMTP enumeration

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

Step 12: Document all the findings

The last step in every pen test is documenting all the findings obtained during the test. You should analyze and suggest countermeasures for your client to improve their security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

- Enumeration is defined as the process of extracting usernames, machine names, network resources, shares, and services from a system.
- Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for remote monitoring and managing hosts, routers, and other devices on a network.
- MIB is a virtual database containing formal description of all the network objects that can be managed using **SNMP**.
- Devices like switches, hubs, and routers might still be enabled with a "**default password**" that enables an attacker to gain unauthorized access to the organization computer network.
- Attacker queries LDAP service to gather information such as valid usernames, addresses, departmental details, etc. that can be further used to perform attacks.
- **Network Time Protocol (NTP)** is designed to synchronize clocks of networked computers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.