Enumeration

Module 04

Unmask the Invisible Hacker.

Module Objectives

- Understanding Enumeration Concepts
- Understanding Different Techniques for NetBIOS Enumeration
- Understanding Different Techniques for SNMP Enumeration
- Understanding Different Techniques for LDAP Enumeration

- Understanding Different Techniques for NTP Enumeration
- Understanding Different Techniques for SMTP and DNS Enumeration
- Enumeration Countermeasures
- Overview of Enumeration Pen Testing

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

What is Enumeration?

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

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

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

Information Enumerated by Intruders


Network resources


Network shares


Routing tables


Audit and service settings


SNMP and DNS details


Machine names


Users and groups


Applications and banners

Techniques for Enumeration

C|EH Certified Ethical Hacker

01 Extract user names using email IDs

02 Extract information using the default passwords

03 Extract user names using SNMP

04 Brute force Active Directory

05 Extract user groups from Windows

06 Extract information using DNS Zone Transfer

Services and Ports to Enumerate

C|EH Certified Ethical Hacker

TCP/UDP 53

DNS Zone Transfer

TCP/UDP 135

Microsoft RPC Endpoint Mapper

UDP 137

NetBIOS Name Service (NBNS)

TCP 139

NetBIOS Session Service (SMB over NetBIOS)

TCP/UDP 445

SMB over TCP (Direct Host)

UDP 161

Simple Network Management protocol (SNMP)

TCP/UDP 389

Lightweight Directory Access Protocol (LDAP)

TCP/UDP 3268

Global Catalog Service

TCP 25

Simple Mail Transfer Protocol (SMTP)

TCP/UDP 162

SNMP Trap

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

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 in the network
- Policies and passwords

NetBIOS Name List

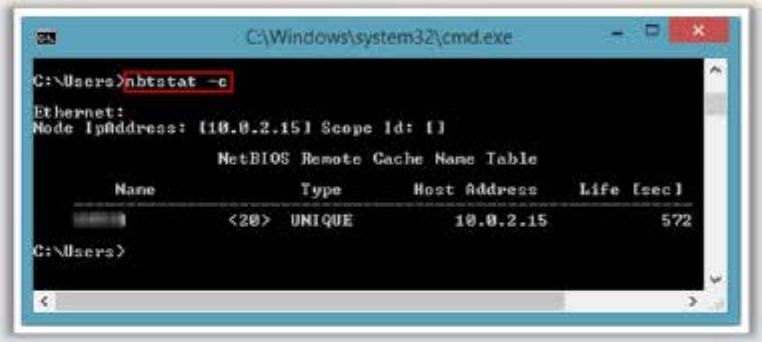
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running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

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

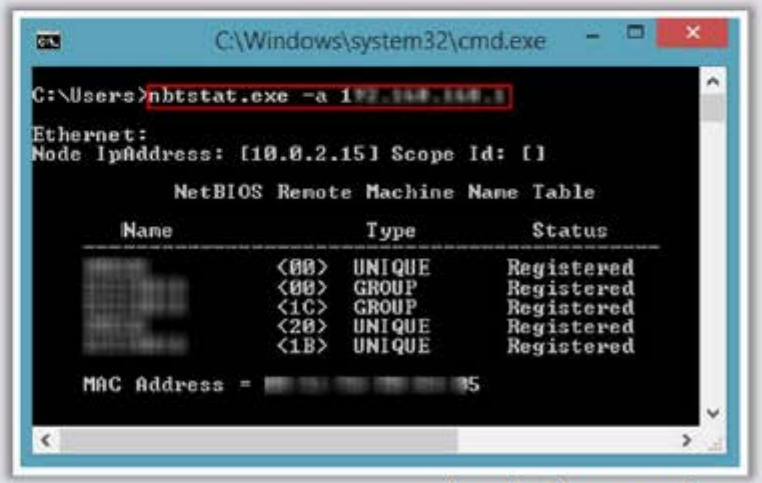
NetBIOS Enumeration (Cont'd)

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

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



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



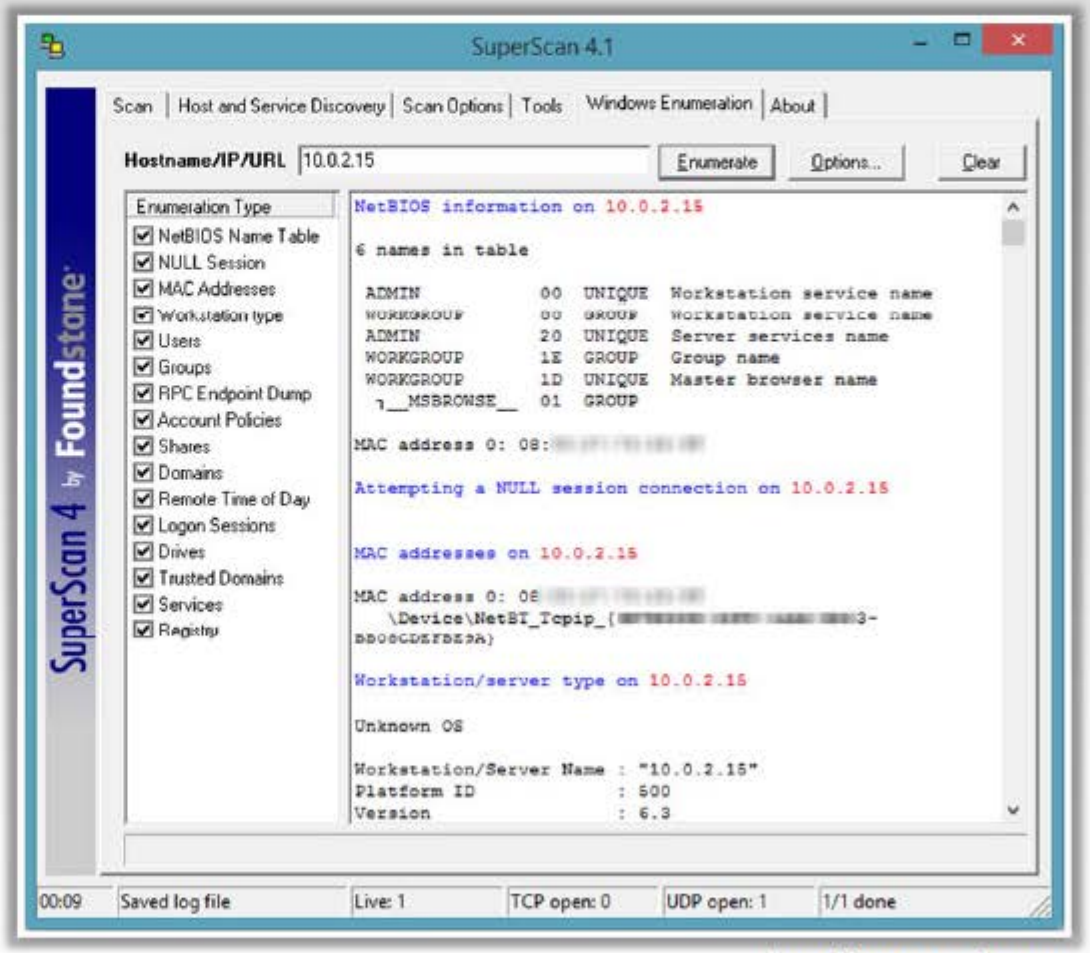
http://technet.microsoft.com

NetBIOS Enumeration Tool: SuperScan

SuperScan is a **connect-based TCP** port scanner, pinger, and hostname resolver

Features:

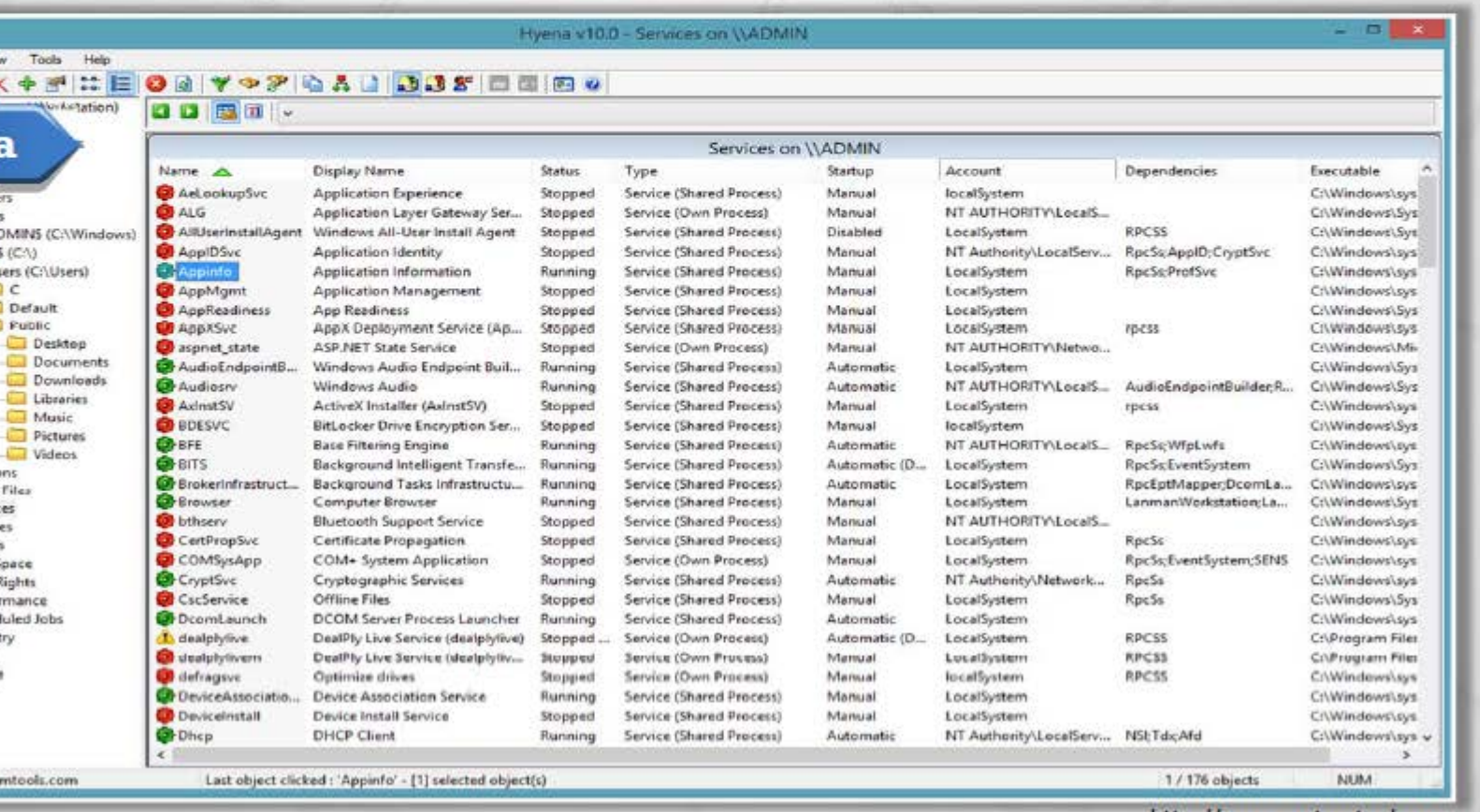
1. Support for unlimited IP ranges
2. Host detection by multiple ICMP methods
3. TCP SYN and UDP scanning
4. Simple HTML report generation
5. Source port scanning
6. Hostname resolving
7. Banner grabbing
8. Windows host enumeration



http://www.mcafee.com

NetBIOS Enumeration Tool: Hyena

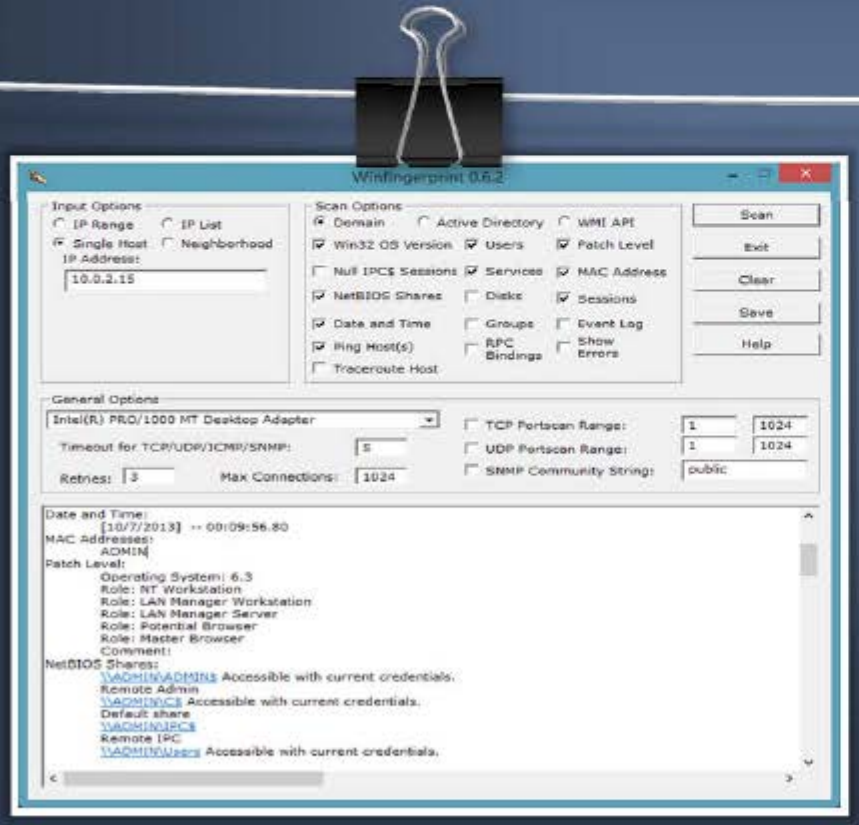
- Hyena is a GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Windows servers and domain controllers
- It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.

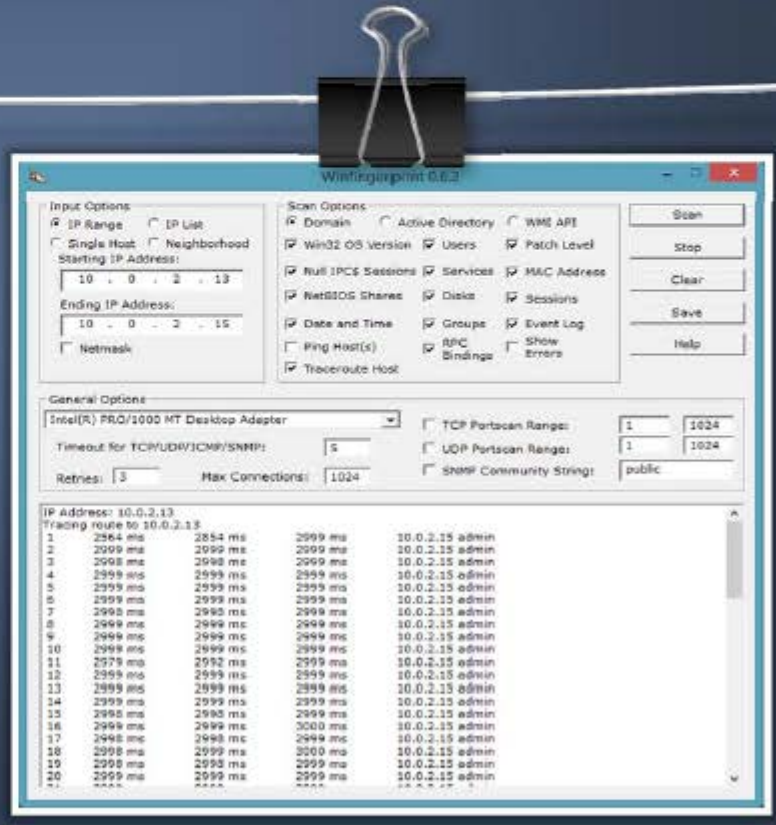


http://www.systemtools.com

NetBIOS Enumeration Tool: Winfingerprint

Winfingerprint determines OS, **enumerate users**, **groups**, **shares**, **SIDs**, **transports**, **sessions**, **services**, service pack and hotfix level, date and time, disks, and open TCP and UDP ports

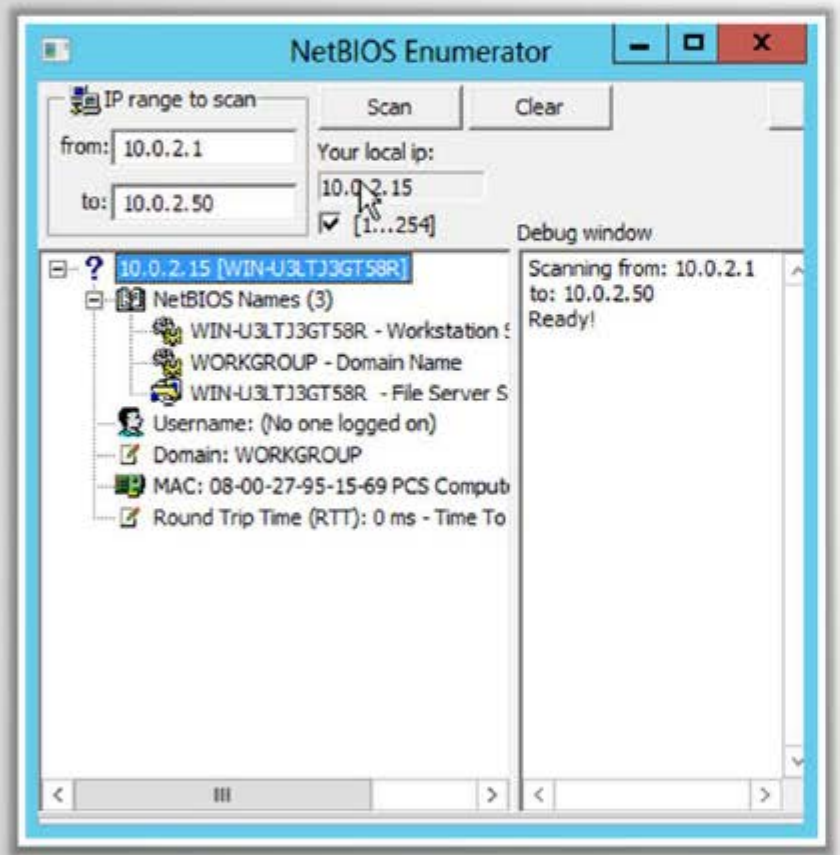




http://www.winfingerprint.com

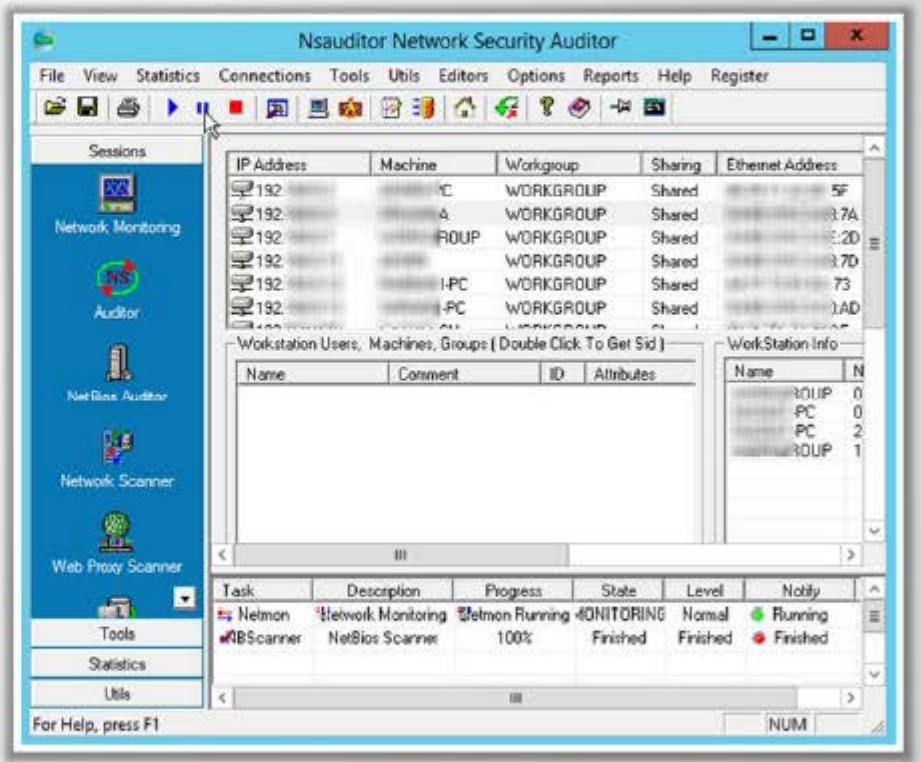
NetBIOS Enumeration Tools: NetBIOS Enumerator and Nsauditor Network Security Auditor

NetBIOS Enumerator



http://nbtenum.sourceforge.net

Nsauditor Network Security Auditor



http://www.nsauditor.com

Enumerating User Accounts

PsExec
http://technet.microsoft.com

PsList
http://technet.microsoft.com

PsFile
http://technet.microsoft.com

PsLoggedOn
http://technet.microsoft.com

PsGetSid
http://technet.microsoft.com

PsLogList
http://technet.microsoft.com

PsKill
http://technet.microsoft.com

PsPasswd
http://technet.microsoft.com

PsInfo
http://technet.microsoft.com

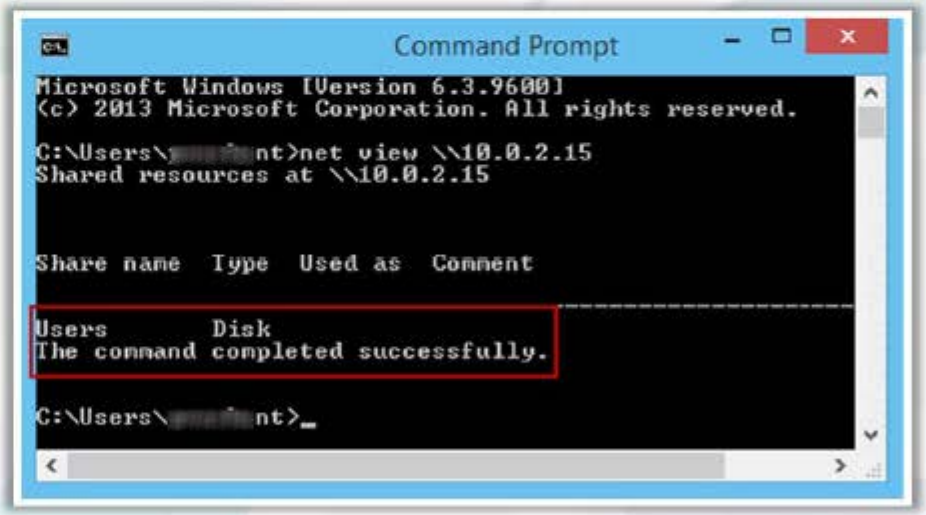
PsShutdown
http://technet.microsoft.com

Enumerating Shared Resources Using Net View

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

Net View Commands

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



Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

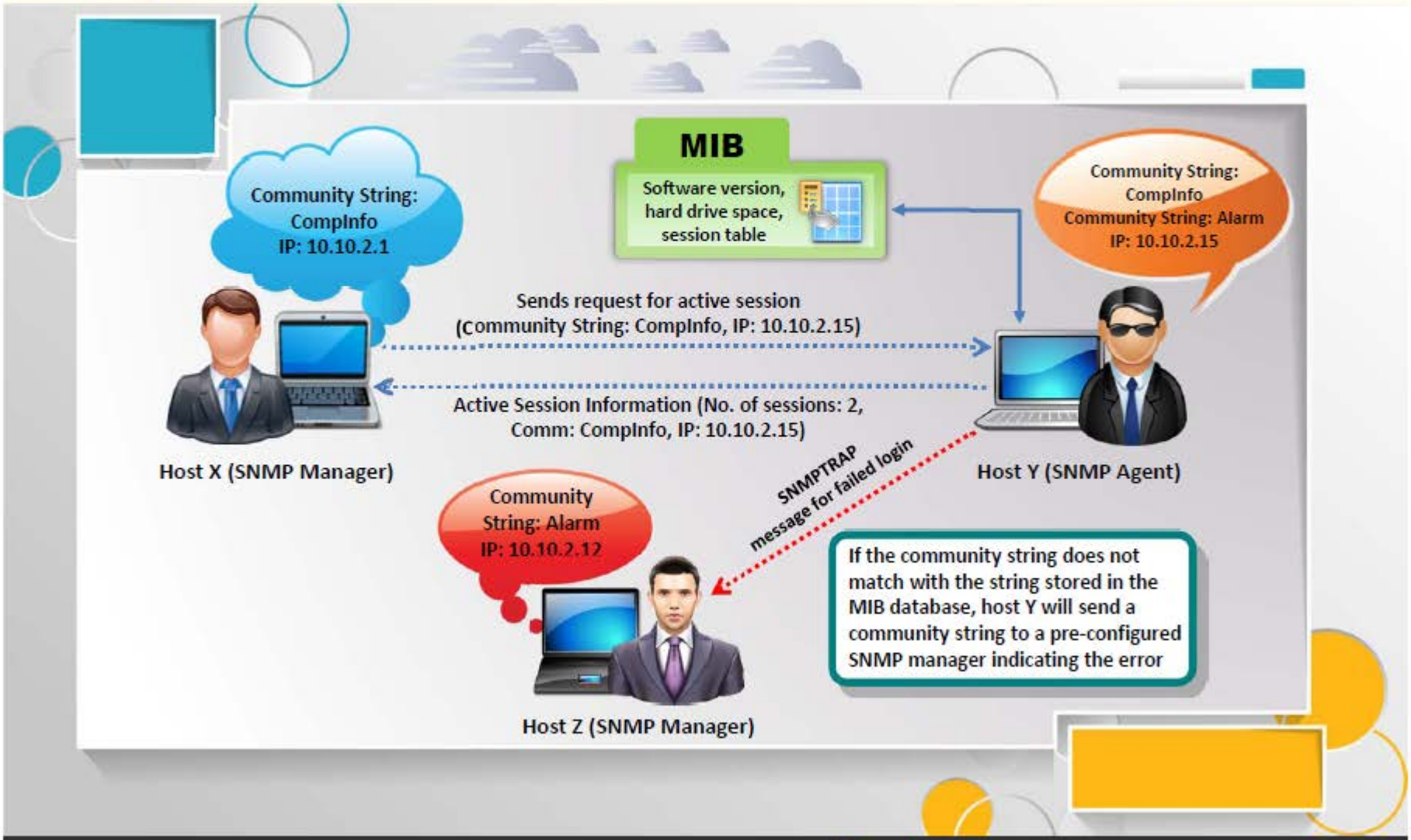
SNMP (Simple Network Management Protocol) Enumeration

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

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

- Attacker uses these **default community strings** to extract information about a device
- Attackers enumerate SNMP to extract information about **network resources** such as hosts, routers, devices, shares, etc. and **network information** such as ARP tables, routing tables, traffic , etc.

Working of SNMP



Management Information Base (MIB)

- MIB is a virtual database containing **formal description of all the network objects** that can be managed using SNMP

- The MIB database is hierarchical and each managed object in a MIB is addressed through **Object Identifiers (OIDs)**

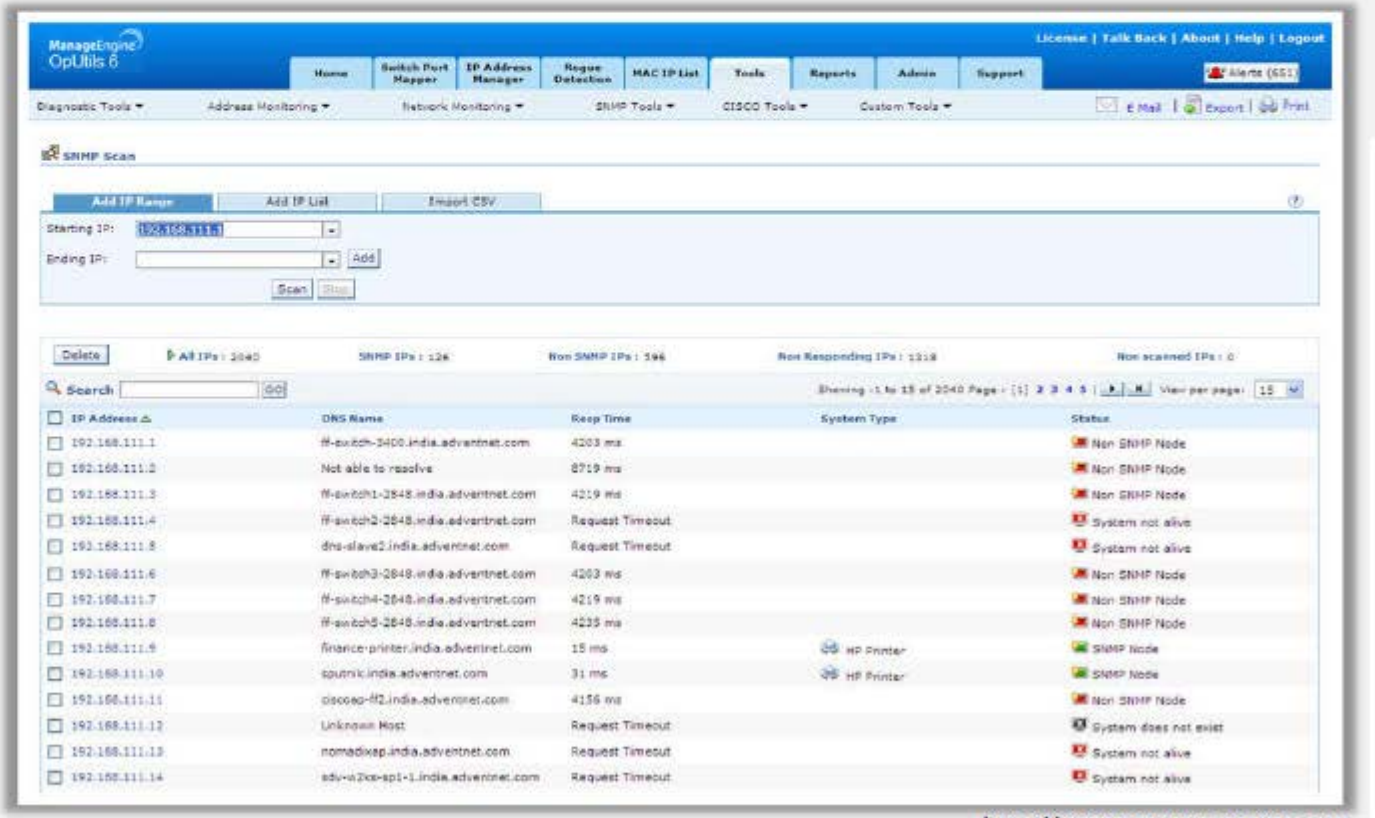
- Two types of **managed objects** exist:
  - **Scalar objects** that define a single object instance
  - **Tabular objects** that define multiple related object instances are grouped in **MIB tables**

- The OID includes the type of **MIB object** such as counter, string, or address, access level such as not-accessible, accessible-for-notify, read-only or read-write, size restrictions, and range information

- SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the **OID numbers** into a **human-readable** display

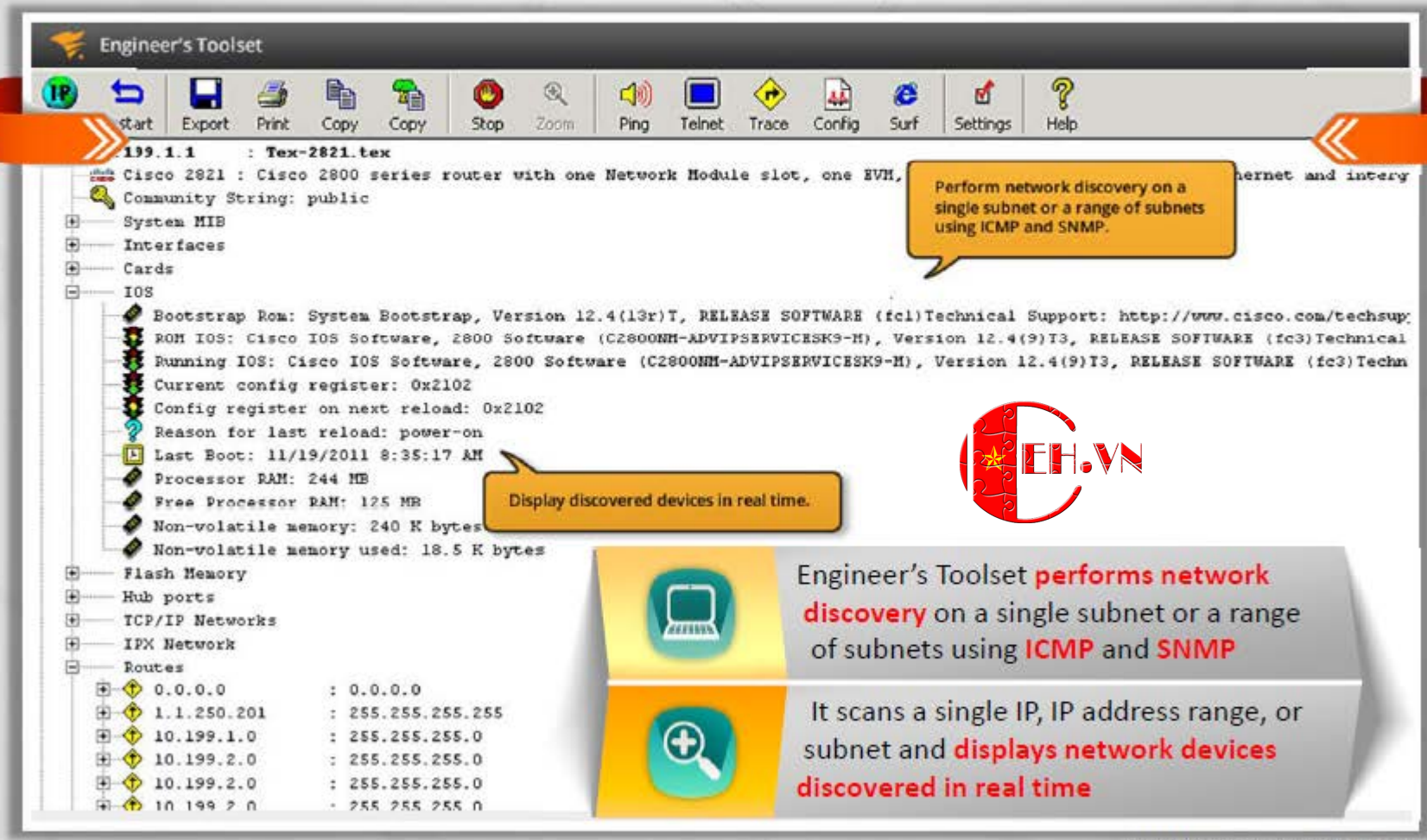
SNMP Enumeration Tool: OpUtils

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



http://www.manageengine.com

SNMP Enumeration Tool: Engineer's Toolset



http://www.solarwinds.com

SNMP Enumeration Tools

SNMP Scanner
http://www.secure-bytes.com

SoftPerfect Network Scanner
http://www.softperfect.com

Getif
http://www.wtcs.org

SNMP Informant
http://www.snmp-informant.com

OiDViEW SNMP MIB Browser
http://www.oidview.com

Net-SNMP
http://www.net-snmp.org

iReasoning MIB Browser
http://tl1.ireasoning.com

Nsauditor Network Security Auditor
http://www.nsauditor.com

SNScan
http://www.mcafee.com

Spiceworks
http://www.spiceworks.com

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

LDAP Enumeration

01 Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services

02 Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory

03 A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA

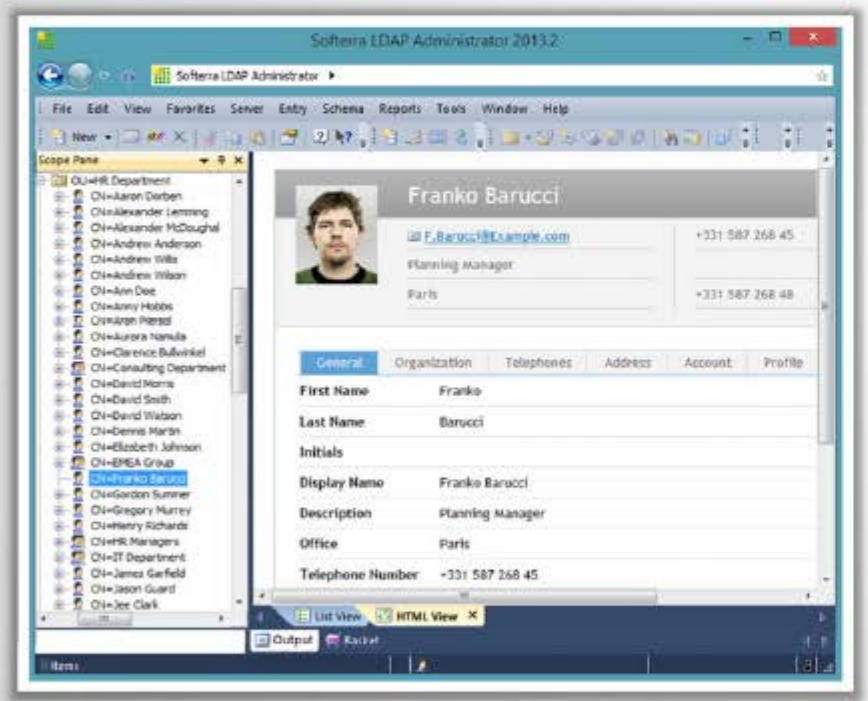
04 Information is transmitted between the client and the server using Basic Encoding Rules (BER)

05 Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks

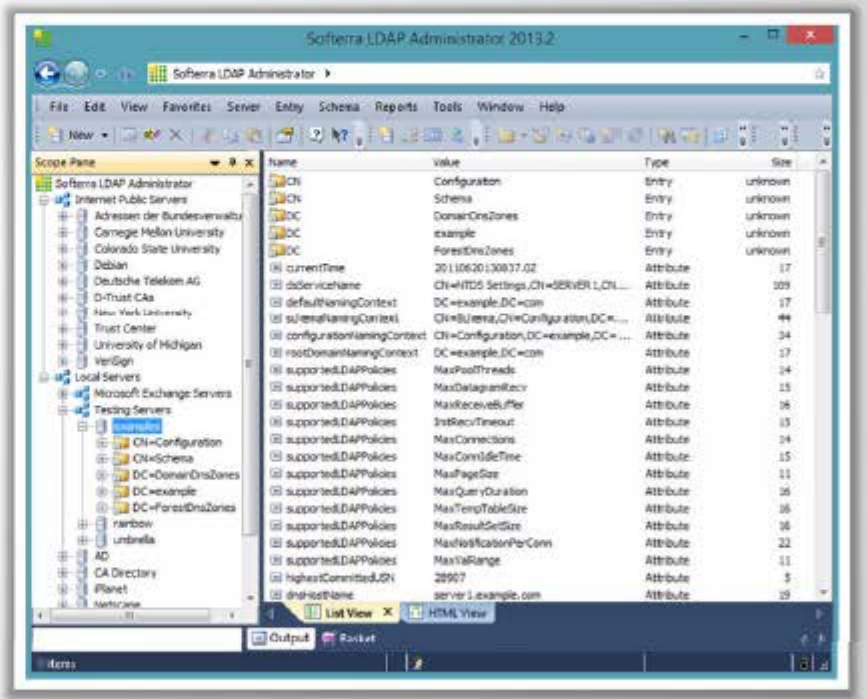
LDAP Enumeration Tool: Softerra LDAP Administrator

C|EH Certified Ethical Hacker

HTML View



LDAP Administrator



http://www.ldapadministrator.com

LDAP Enumeration Tools

JXplorer
http://www.jxplorer.org

LDAP Admin Tool
http://www.ldapsoft.com

LDAP Account Manager
http://www.ldap-account-manager.org

LEX - The LDAP Explorer
http://www.ldapexplorer.com

LDAP Admin
http://www.ldapadmin.org

Active Directory Explorer
http://technet.microsoft.com

LDAP Administration Tool
http://sourceforge.net

LDAP Search
http://securityxploded.com

Active Directory Domain Services Management Pack
http://www.microsoft.com

LDAP Browser/Editor
http://www.novell.com

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

NTP Enumeration

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

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

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

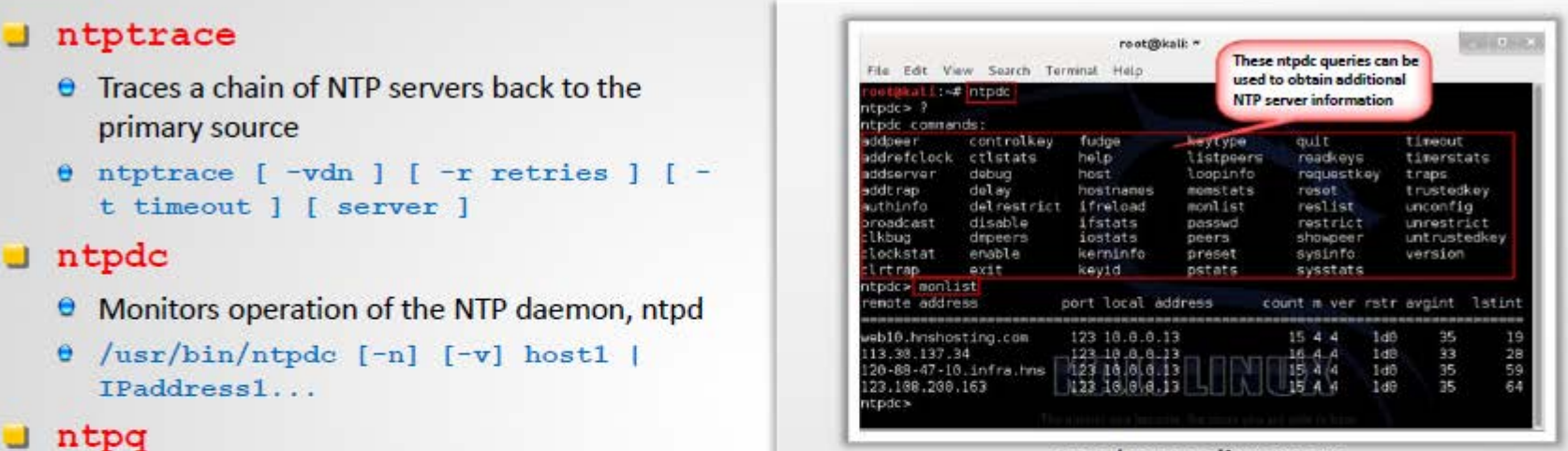
It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions

Attacker queries NTP server to gather valuable information such as:

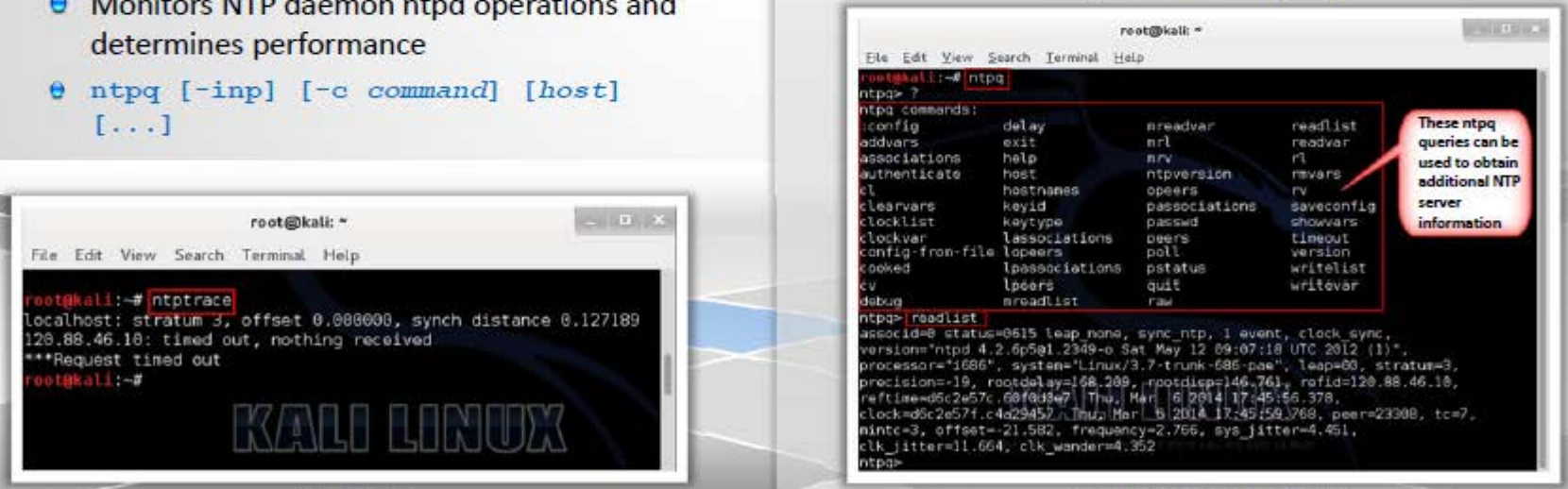
- List of **hosts connected to NTP server**
- **Clients IP addresses** in a network, their system names and OSs
- **Internal IPs** can also be obtained if NTP server is in the DMZ

NTP Enumeration Commands

- **ntptrace**
  - Traces a chain of NTP servers back to the primary source
  - `ntptrace [ -vdn ] [ -r retries ] [ -t timeout ] [ server ]`
- **ntpdc**
  - Monitors operation of the NTP daemon, ntpd
  - `/usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...`
- **ntpq**
  - Monitors NTP daemon ntpd operations and determines performance
  - `ntpq [-inp] [-c command] [host] [...]`



ntpdc: monlist query



ntpq: readlist query

ntptrace

NTP Enumeration Tools

NTP Server Scanner
http://www.bytefusion.com

Nmap
http://nmap.org

Wireshark
http://www.wireshark.org

AtomSync
http://www.atomsync.com

NTPQuery
http://www.bytefusion.com

PresenTense NTP Auditor
http://www.bytefusion.com

PresenTense Time Server
http://www.bytefusion.com

PresenTense Time Client
http://www.bytefusion.com

NTP Time Server Monitor
http://www.meinbergglobal.com

LAN Time Analyser
http://www.bytefusion.com

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - VRFY - Validates users
  - EXPN - Tells the actual delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of the message

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

Using the SMTP VRFY Command

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

Using the SMTP EXPN Command

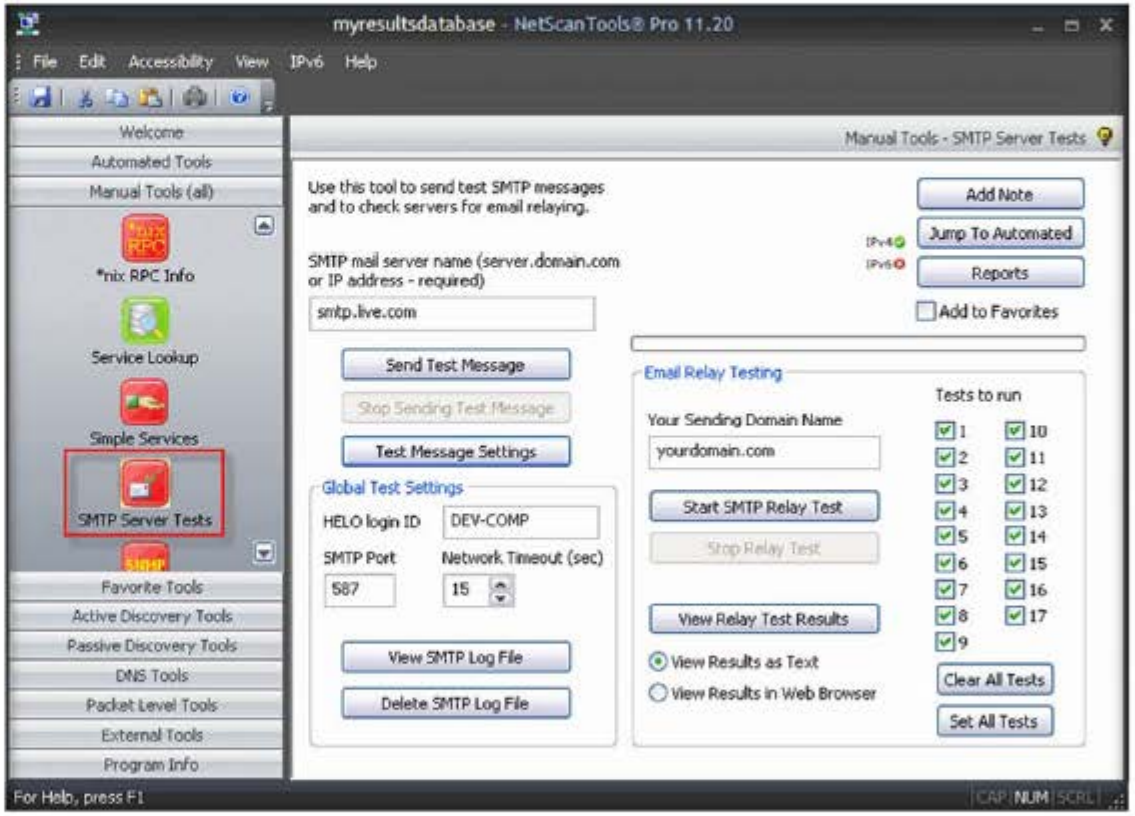
```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN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

Using the SMTP RCPT TO Command

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

SMTP Enumeration Tool: NetScanTools Pro

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



http://www.netscantools.com

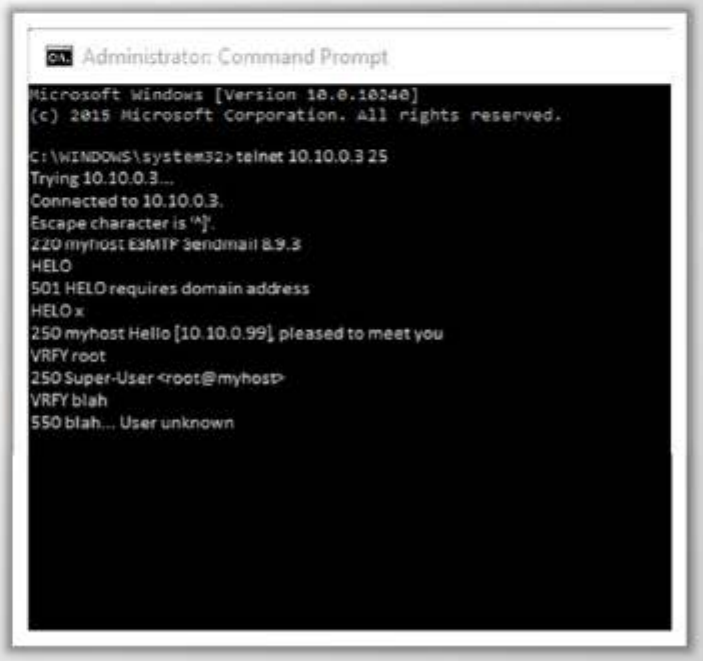
SMTP Enumeration Tools

```
root@pentestlab:/pentest/enumeration/smtp/smtp-user-enum# perl smtp-user-enum.pl -M VRFY -U
users.txt -t 172.16.212.133
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

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

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 12
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ...........

######## Scan started at Fri Nov 16 10:50:58 2012 #########
172.16.212.133: lp exists
172.16.212.133: daemon exists
172.16.212.133: bin exists
172.16.212.133: sync exists
172.16.212.133: root exists
172.16.212.133: mail exists
172.16.212.133: backup exists
172.16.212.133: news  exists
######## Scan completed at Fri Nov 16 10:50:58 2012 #########
8 results.

12 queries in 1 seconds (12.0 queries / sec)
```

http://pentestmonkey.net
https://pentestlab.wordpress.com

smtp-user-enum

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



Telnet

- Telnet can be used to **probe an SMTP** server using VRFY, EXPN and RCPT TO parameters and enumerate users

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

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
```

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

Enumeration Countermeasures

SNMP

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

DNS

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

Enumeration Countermeasures (Cont'd)

C|EH Certified Ethical Hacker

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

LDAP

- 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**

SMB Enumeration Countermeasures

Disable SMB protocol on Web and DNS Servers

Disable SMB protocol on Internet facing servers

Disable ports TCP 139 and TCP 445 used by the SMB protocol

Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

LDAP Enumeration

NTP Enumeration

SMTP and DNS Enumeration

Enumeration Countermeasures

Enumeration Pen Testing

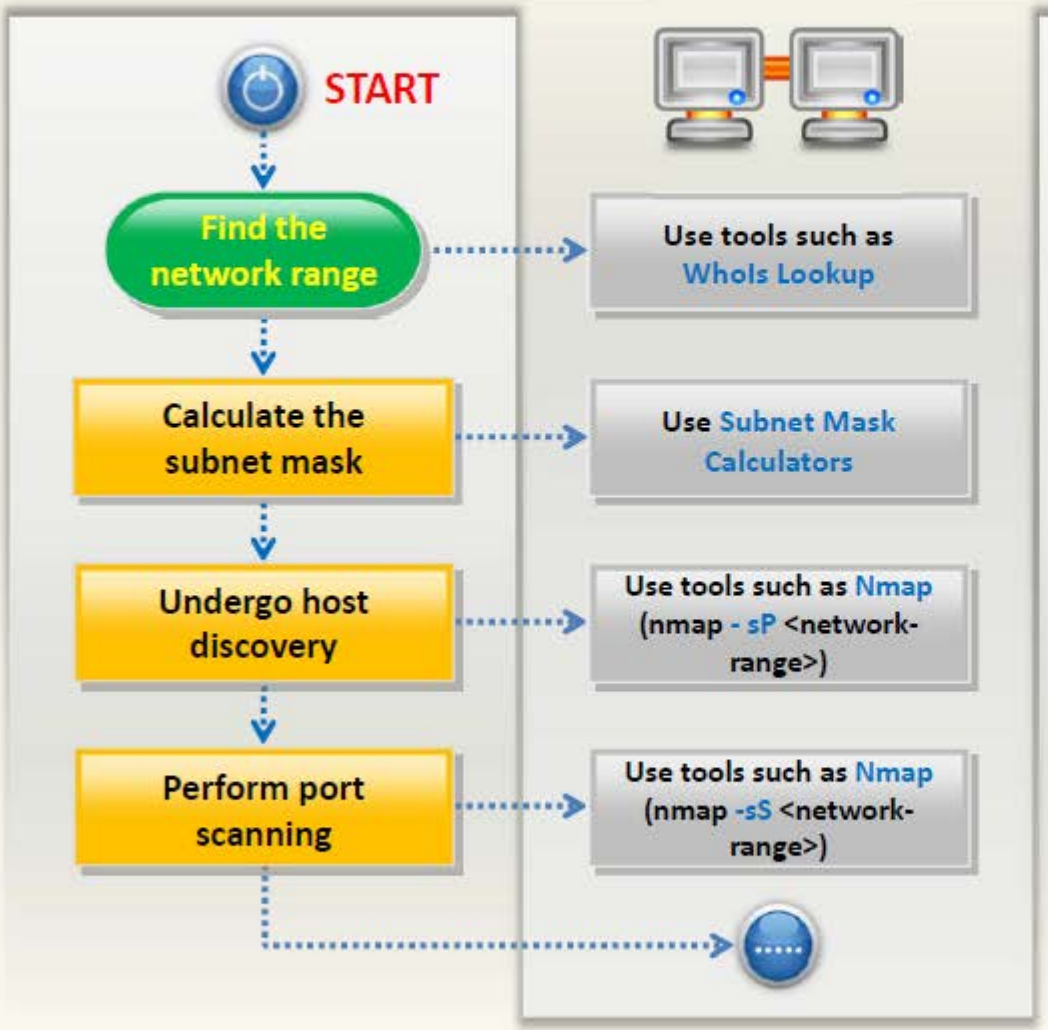
Enumeration Pen Testing

Used to identify **valid user accounts** or **poorly protected resource shares** using active connections to systems and directed queries

The information can be **users and groups, network resources and shares,** and **applications**

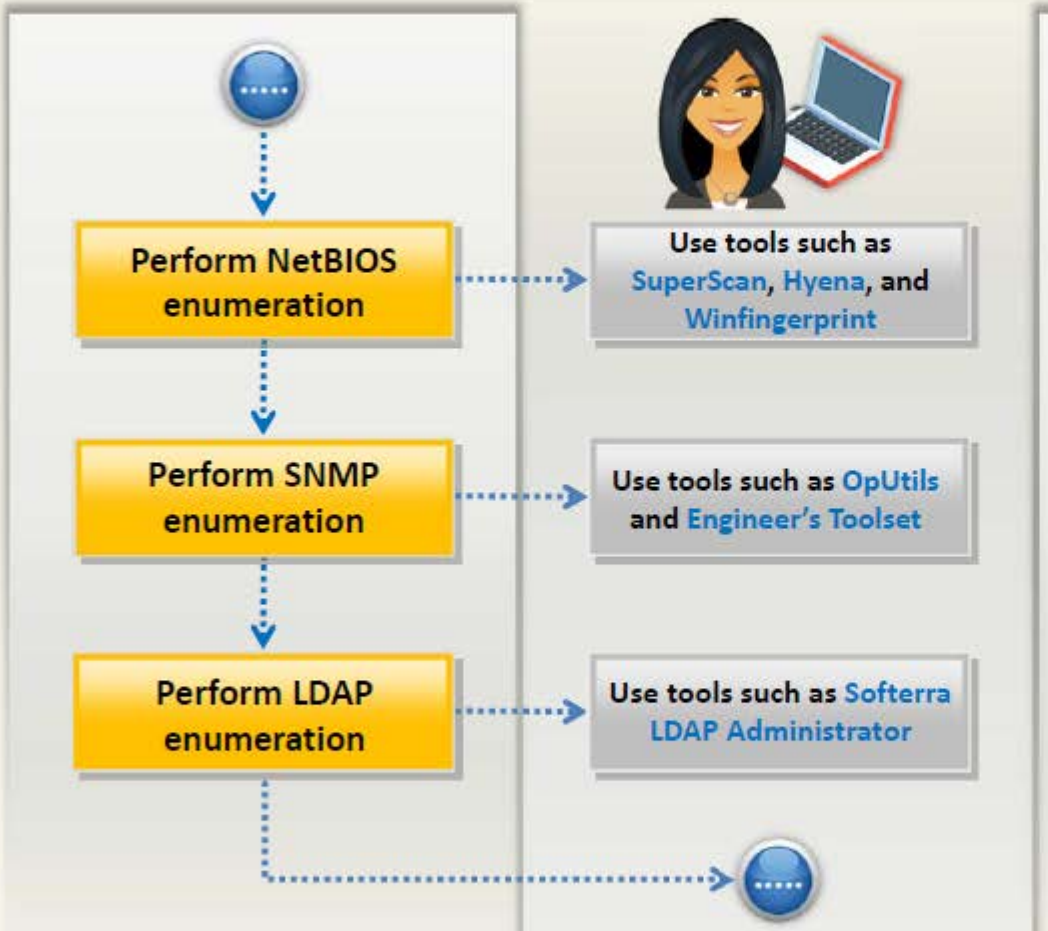
Used in combination with **data collected in the reconnaissance phase**

Enumeration Pen Testing (Cont'd)



- In order to enumerate important servers, find the network range using tools such as **Whois Lookup**
- Calculate the subnet mask required for the IP range using **Subnet Mask Calculators**, that can be given as an input to many of the ping sweep and port scanning tools
- Find the servers connected to the Internet using tools such as **Nmap**
- Perform port scanning to check for the open ports on the nodes using tools such as **Nmap**

Enumeration Pen Testing (Cont'd)



- Perform NetBIOS enumeration using tools such as **SuperScan**, **Hyena**, and **Winfingerprint**
- Perform SNMP enumeration using tools such as **OpUtils Network Monitoring Toolset** and **Engineer's Toolset**
- Perform LDAP enumeration using tools such as **Softerra LDAP Administrator**

Enumeration Pen Testing (Cont'd)

C|EH Certified Ethical Hacker

Perform NTP enumeration → Use commands such as ntptrace, ntpdc, and ntpq

Perform SMTP enumeration → Use tools such as NetScanTools Pro

Perform DNS enumeration → Use Windows utility NSLookup

Document all the findings

- Perform NTP enumeration using commands such as **ntptrace**, **ntpdc**, and **ntpq**
- Perform SMTP enumeration using tools such as **NetScanTools Pro**
- Perform DNS enumeration using Windows utility **NSLookup**

Module Summary

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