# Enumeration

Module 04

# Module Objectives

- 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

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

# What Is Enumeration?

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


- Attackers use extracted information to **identify system attack points** and **perform password attacks** to gain unauthorized access to information system resources
- Enumeration techniques are conducted in an **intranet environment**

# Techniques for Enumeration

Extract user names using email IDs

Extract information using the default passwords

Extract user names using SNMP

Brute force Active Directory

Extract user groups from Windows

Extract information using DNS Zone Transfer

# Services and Ports to Enumerate

**TCP 53**

DNS zone transfer

**TCP 135**

Microsoft RPC Endpoint Mapper

**TCP 137**

NetBIOS Name Service (NBNS)

**TCP 139**

NetBIOS Session Service (SMB over NetBIOS)

**TCP 445**

SMB over TCP (Direct Host)

**UDP 161**

Simple Network Management protocol (SNMP)

**TCP/UDP 389**

Lightweight Directory Access Protocol (LDAP)

**TCP/UDP 3368**

Global Catalog Service

**TCP 25**

Simple Mail Transfer Protocol (SMTP)

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

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 on the network
- Policies and passwords

## NetBIOS Name List

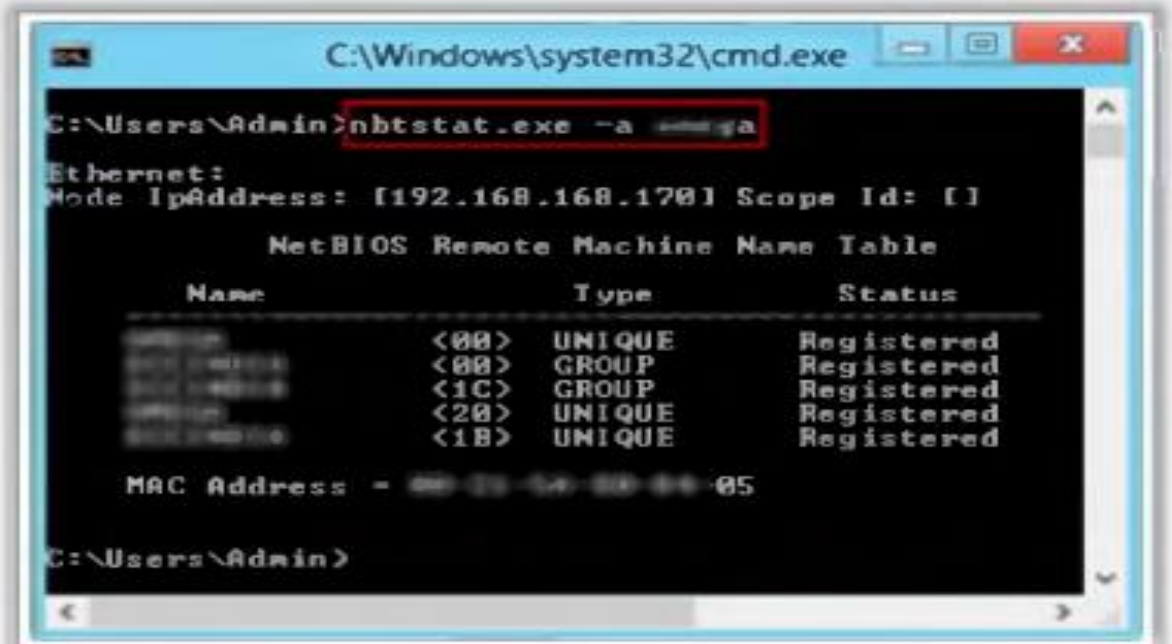
| Name | NetBIOS Code | Type | Information Obtained |
|---|---|---|---|
| <host name> | <00> | UNIQUE | Hostname |
| <domain> | <00> | GROUP | Domain name |
| <host name> | <03> | UNIQUE | Messenger service running for that computer |
| <username> | <03> | UNIQUE | Messenger service running for that 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)

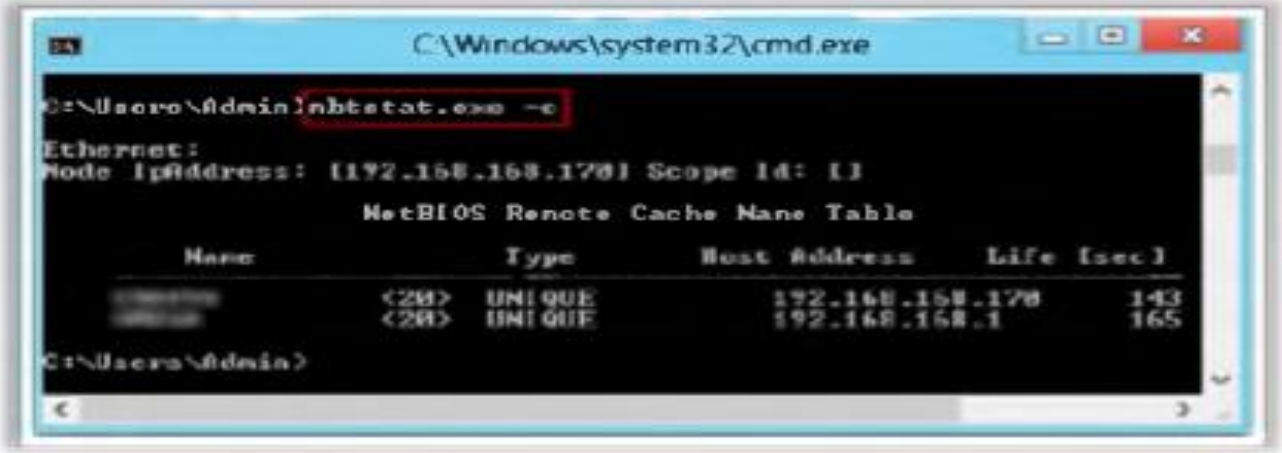
# NetBIOS Enumeration (Cont'd)

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


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




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



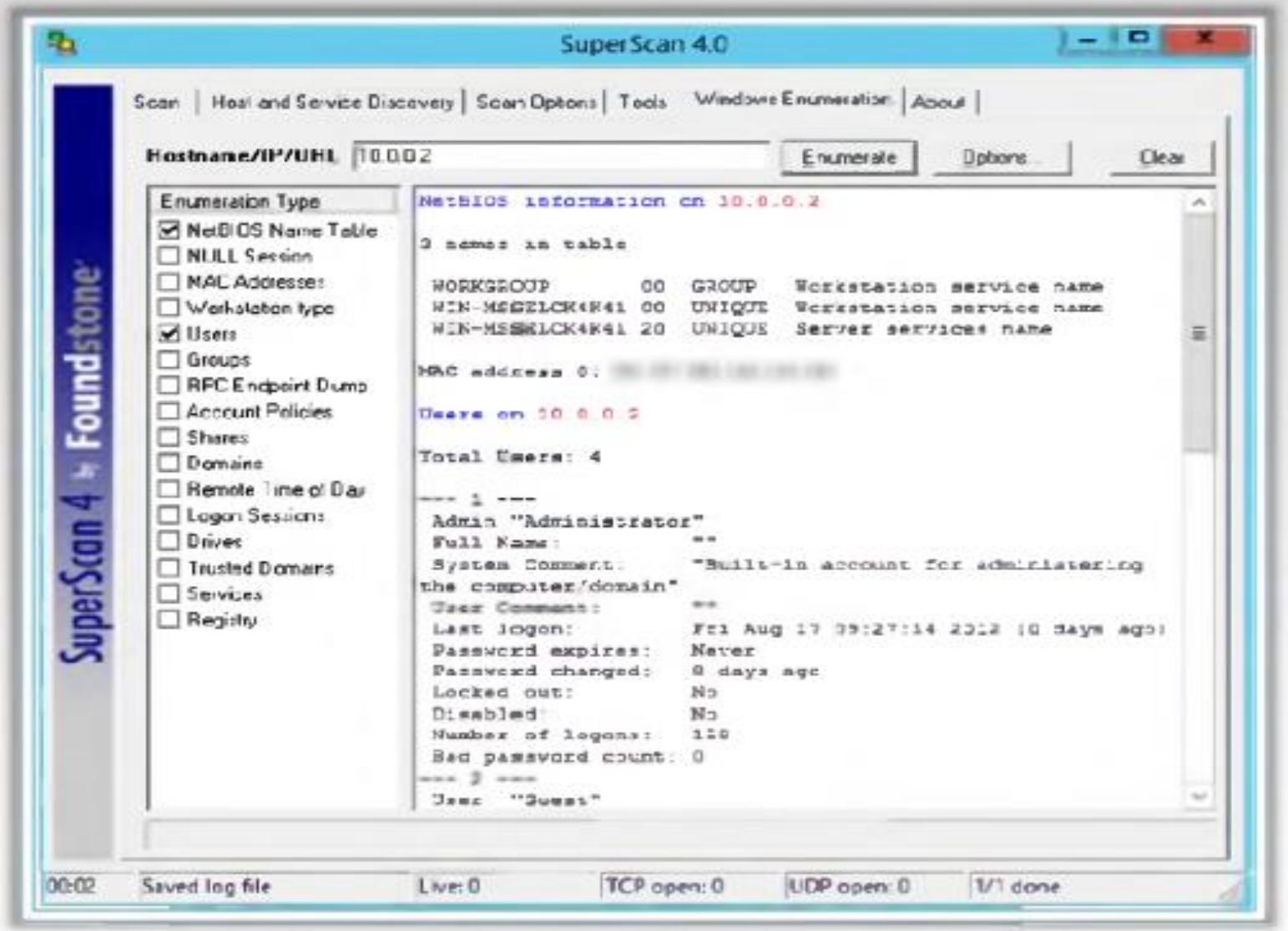

http://technet.microsoft.com

# NetBIOS Enumeration Tool: SuperScan

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

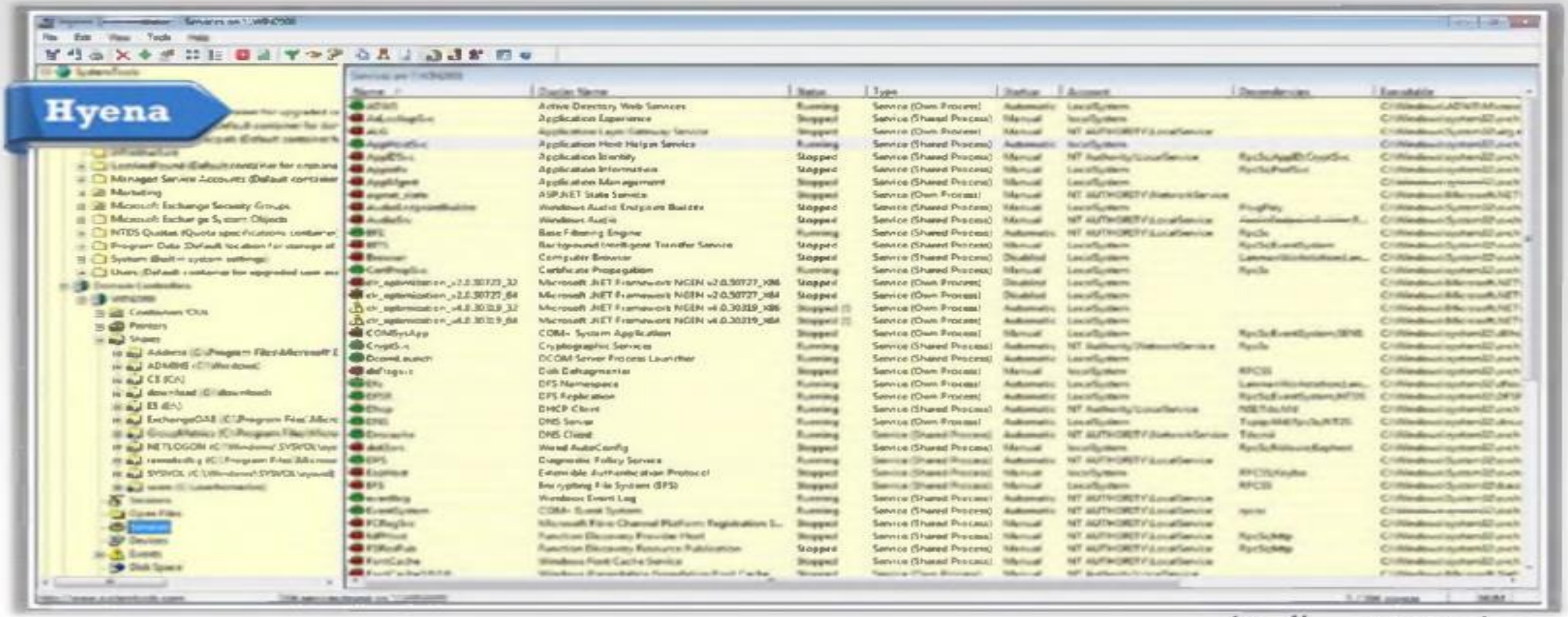
## Features:

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. Fast hostname resolving
7. Extensive banner grabbing
8. Extensive Windows host enumeration



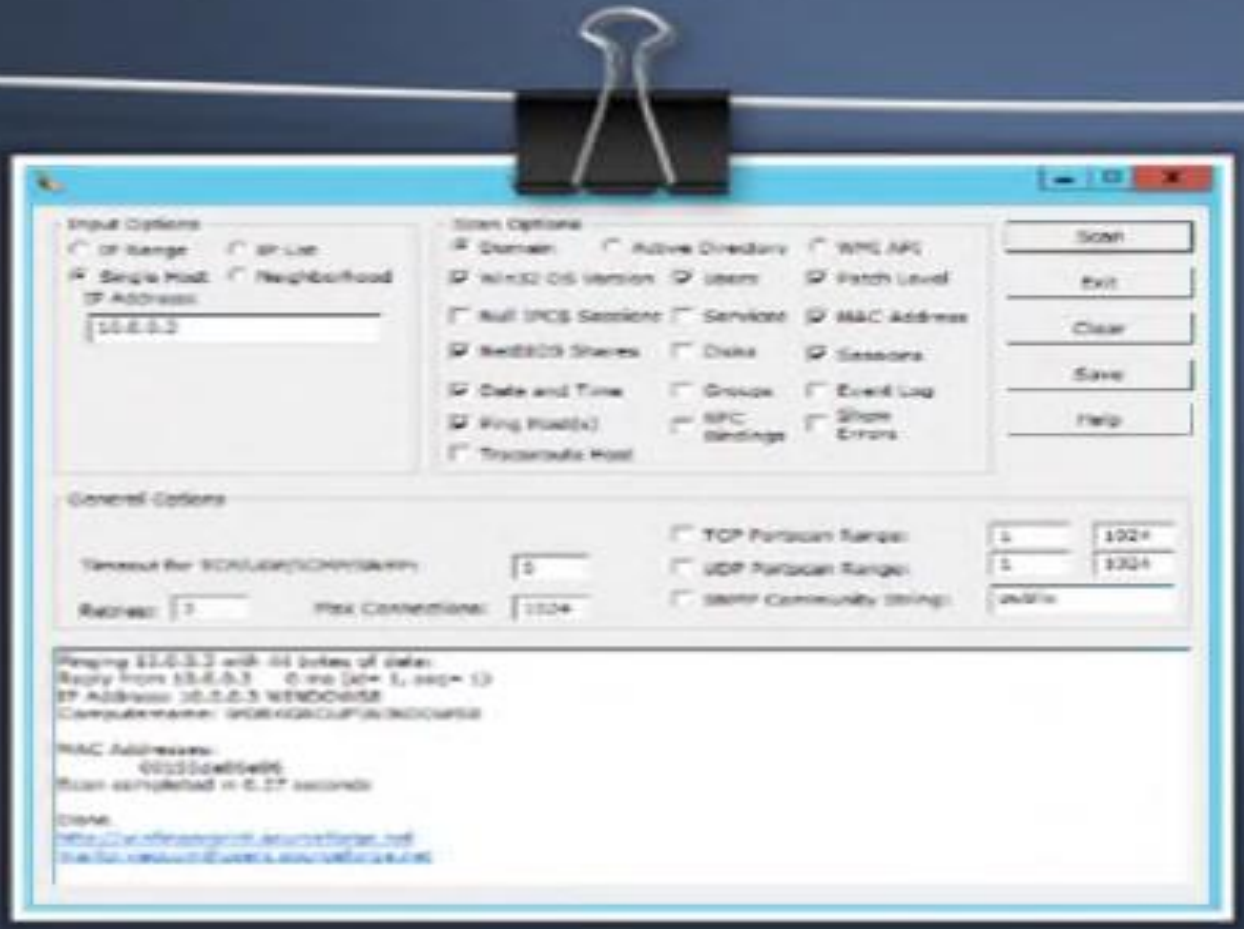
# NetBIOS Enumeration Tool: Hyena

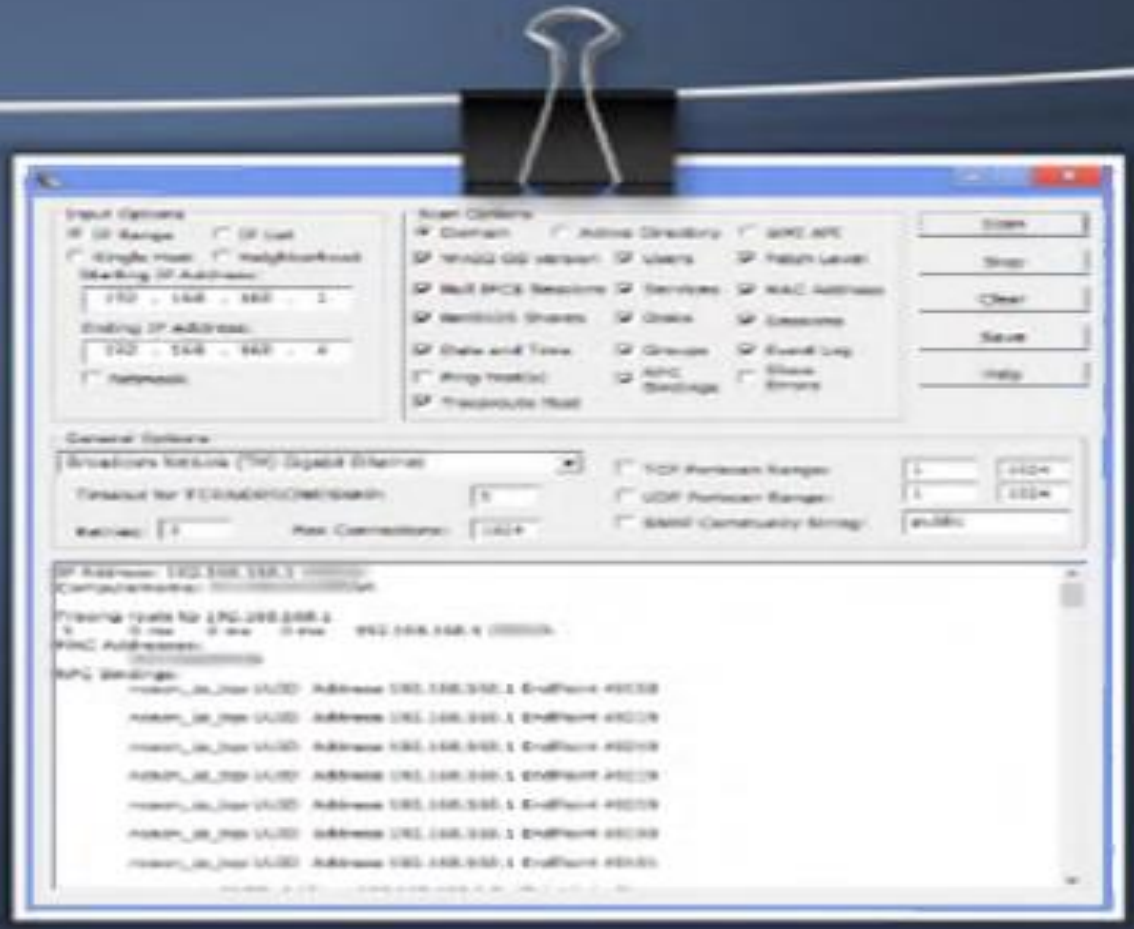
- Hyena is GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Windows servers and domain controllers
- It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.



# NetBIOS Enumeration Tool: Winfingerprint

- Winfingerprint is a Win32 MFC VC++ .NET based security tool that is able to determine OS, **enumerate users**, **groups**, **shares**, **SIDs**, **transports**, **sessions**, **services**, service pack and hotfix level, date and time, disks, and open tcp and udp ports



# 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*

# Enumerate Systems Using Default Passwords


Devices like switches, hubs, routers, access points might still be enabled with a "default password"

Attackers gain unauthorized access to the organization computer network and information resources by using default and common passwords


*http://www.virus.org/default_passwds*

Default Username/Pwd

Ex: admin/synnet

Router

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

# SNMP (Simple Network Management Protocol) Enumeration

**SNMP 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

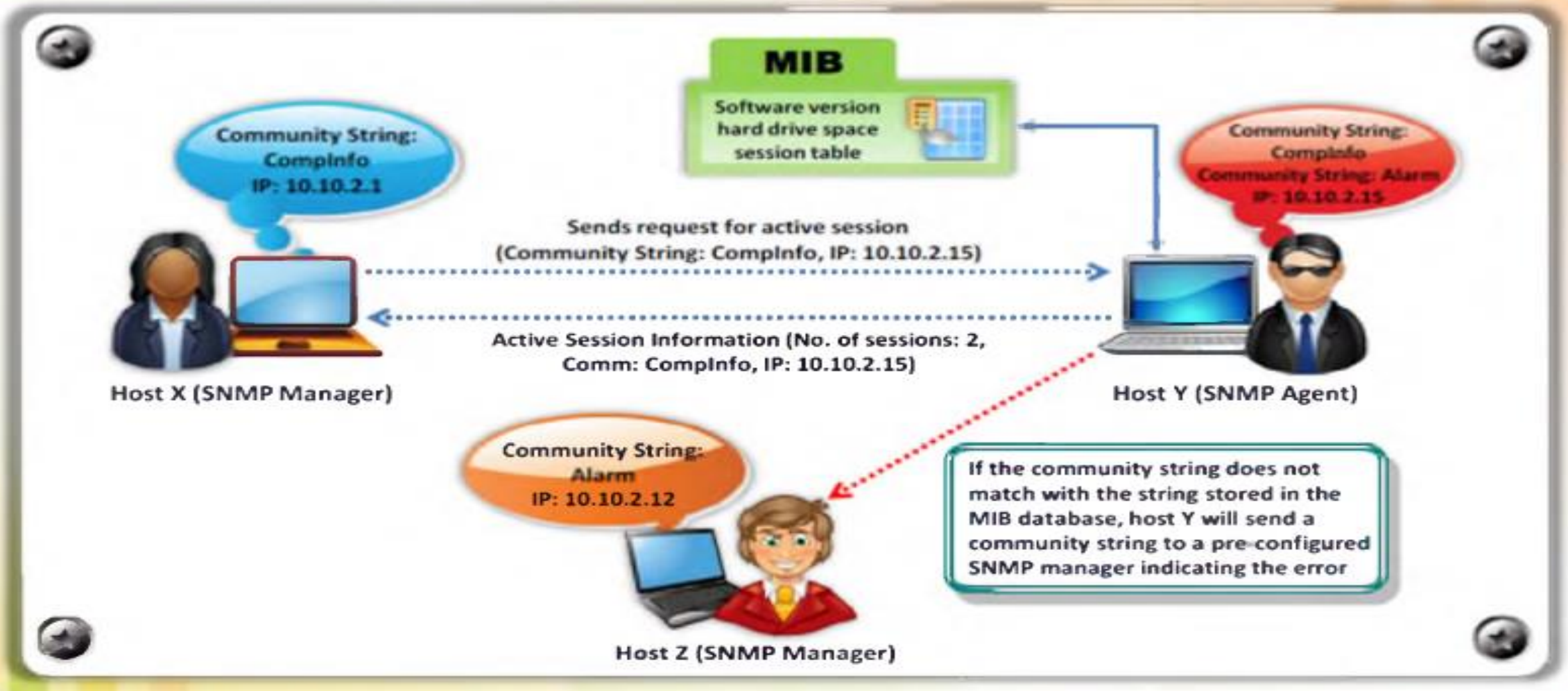
**Passwords**

- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
  - **Read community string**: It is public by default, allows to view the device or system configuration
  - **Read/write community string**: It is private by default, allows to edit or alter configuration on the device

**Attackers**

- 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 statistics, device specific information, 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:

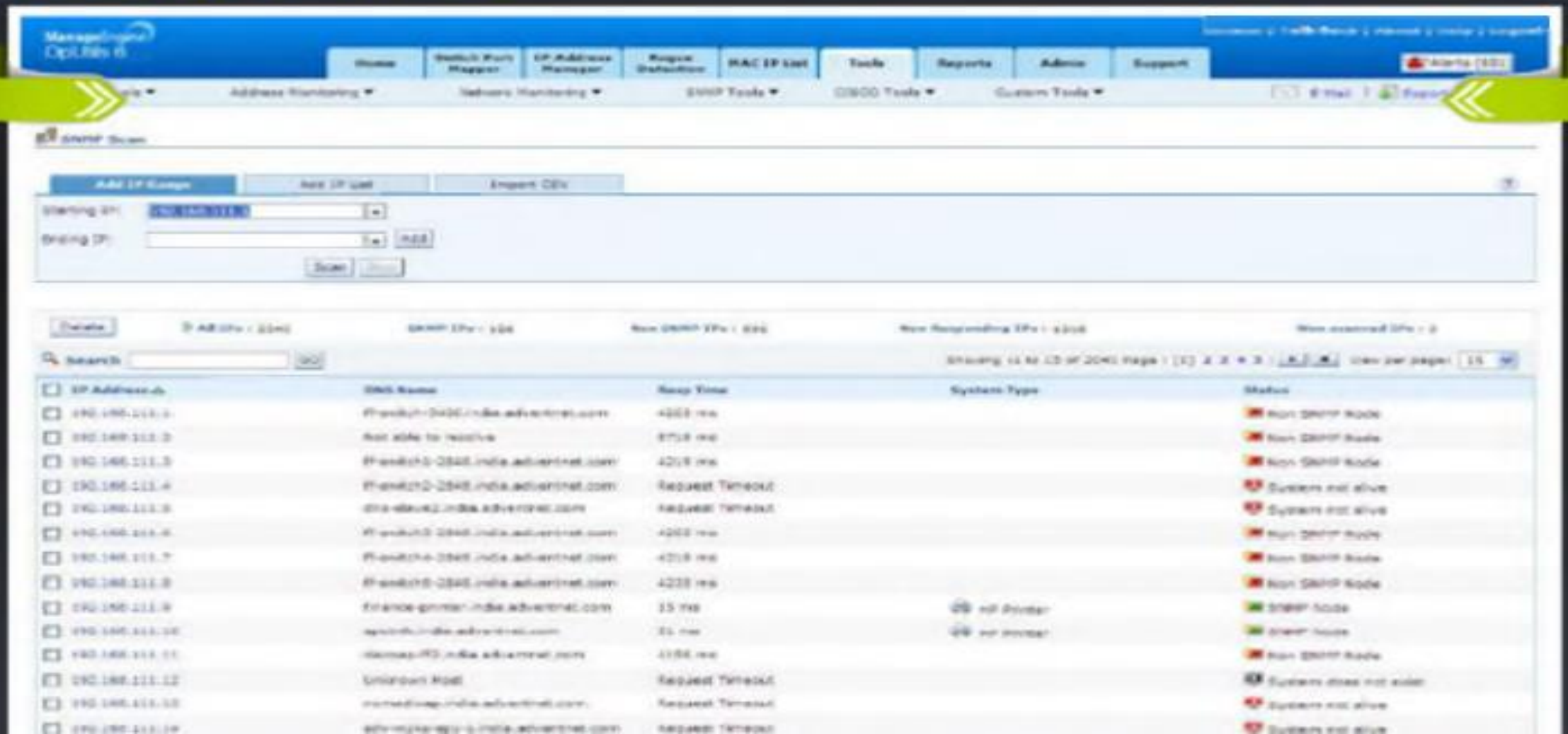
- Scalar objects that define a single object instance
- Tabular objects that define multiple related object instances that are grouped in MIB tables

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

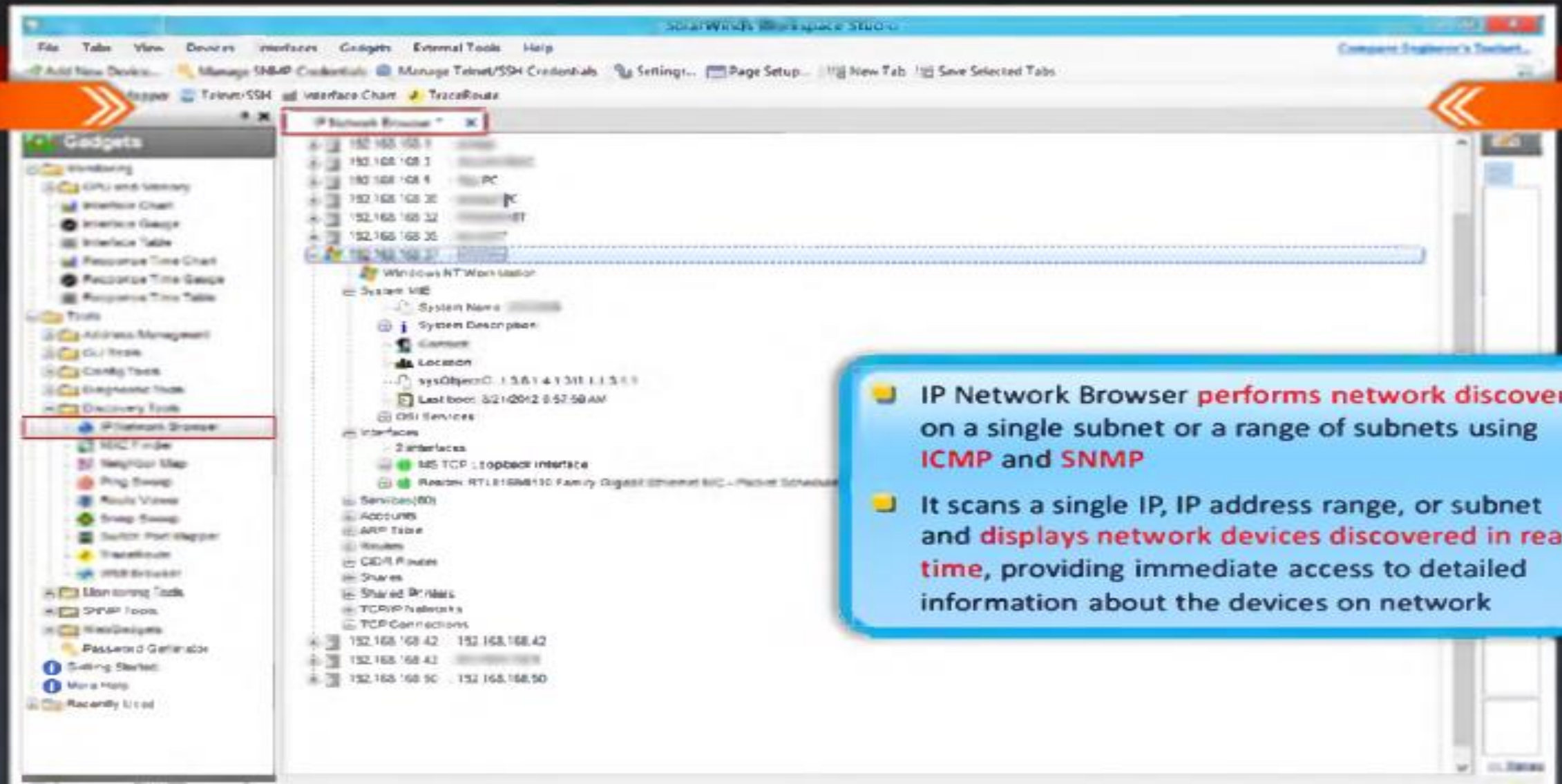
SNMP uses the MIB's hierarchical namespace containing object identifiers (OIDs) to translate the OID numbers into a human-readable display

# SNMP Enumeration Tool: OpUtils

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



# SNMP Enumeration Tool:
# SolarWind's IP Network Browser



# SNMP Enumeration Tools

**Getif**
http://www.wtcs.org

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

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

**SNScan**
http://www.mcafee.com

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

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

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

**Net-SNMP**
http://net-snmp.sourceforge.net

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

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

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

# UNIX/Linux Enumeration Commands

## finger

- Enumerates the user and the host
- 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

```
[root$] finger -l @target.hackme.com
```

## rpcinfo (RPC)

- Helps to enumerate Remote Procedure Call protocol
- RPC protocol allows applications to communicate over the network

```
[root] rpcinfo -p 19x.16x.xxx.xx
```

## rpcclient

- Using rpcclient we can enumerate user names on Linux and OS X

```
[root $] rpcclient $> netshareenum
```

## showmount

- Finds the shared directories on the machine

```
[root $] showmount -e 19x.16x. xxx.xx
```

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

# LDAP Enumeration

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

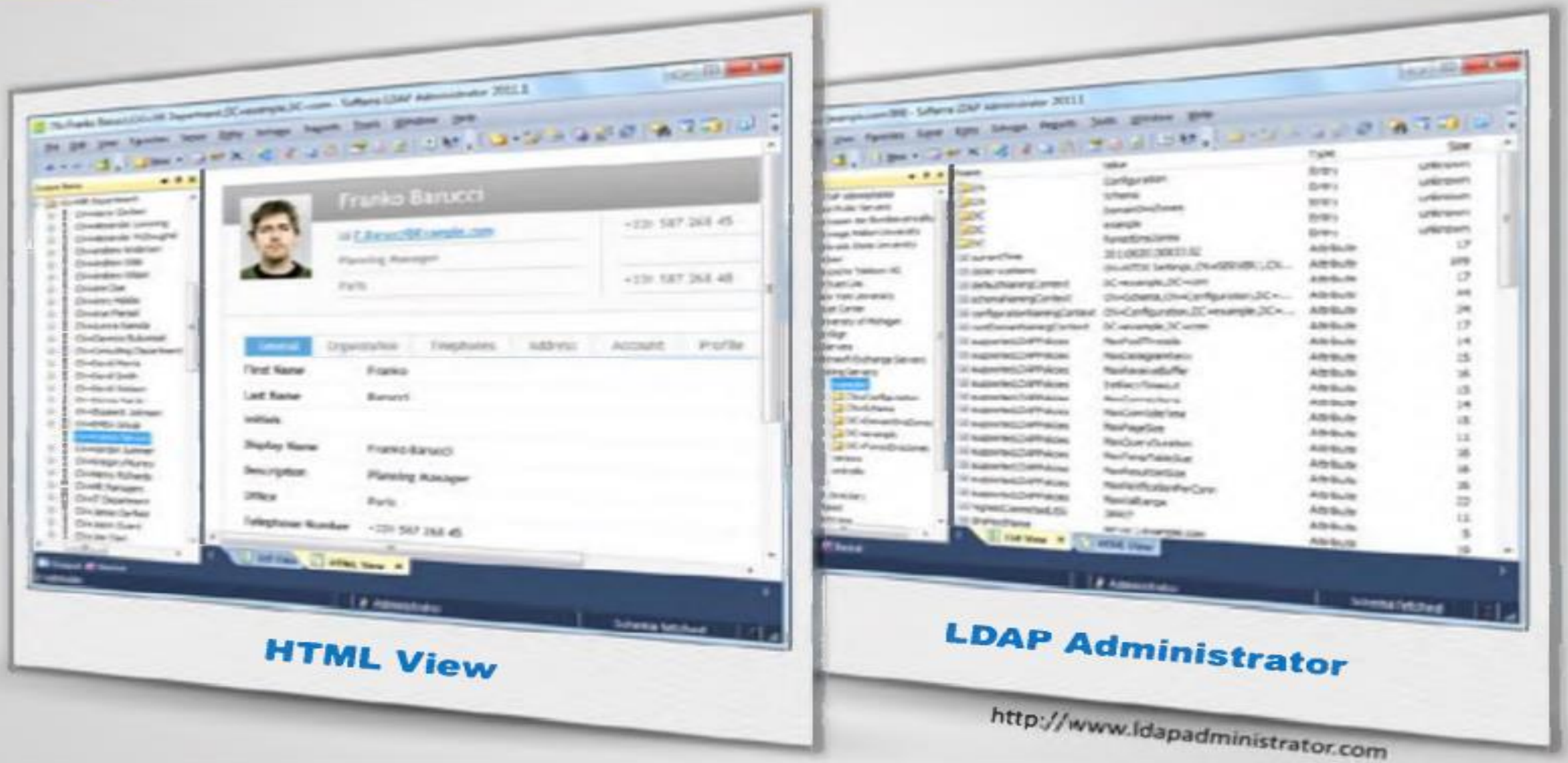
II. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory

III. 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

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

V. 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



# LDAP Enumeration Tools

**JXplorer**
http://www.jxplorer.org

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

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

**LDAP Administration Tool**
http://sourceforge.net

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

**LDAP Search**
http://securityxploded.com

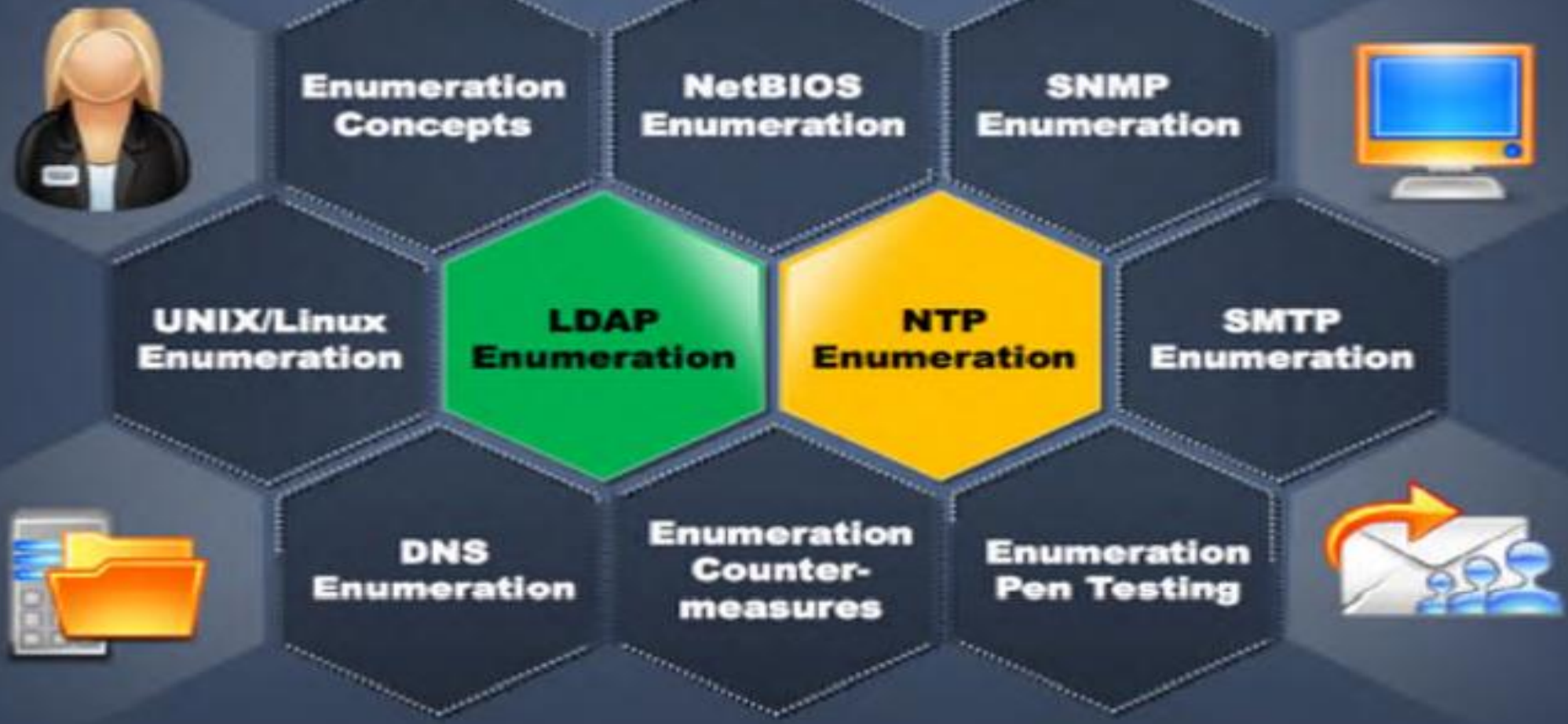
**LEX - The LDAP Explorer**
http://www.ldapexplorer.com

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

**LDAP Admin**
http://www.ldapadmin.org

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

# Module Flow


Enumeration Concepts
NetBIOS Enumeration
SNMP Enumeration
UNIX/Linux Enumeration
LDAP Enumeration
NTP Enumeration
SMTP Enumeration
DNS Enumeration
Enumeration Counter-measures
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

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

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

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

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

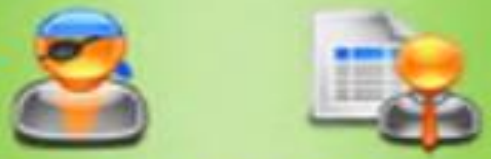
# SMTP Enumeration

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
```

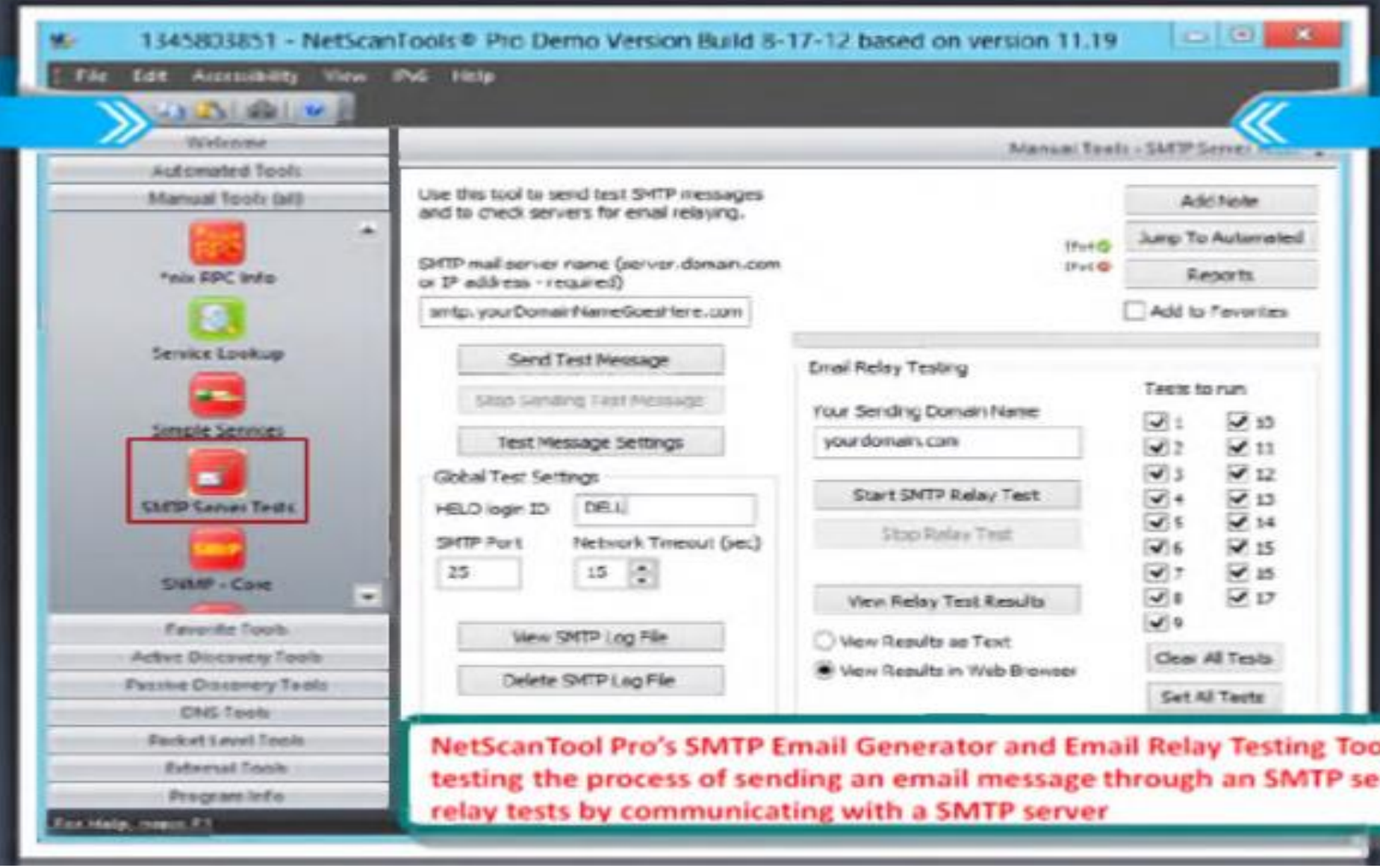
### Using the SMTP EXPN Command

```
$ 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

```
$ 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
```

# 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

# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

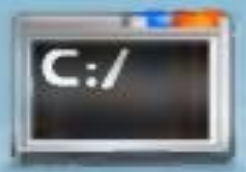
DNS Enumeration

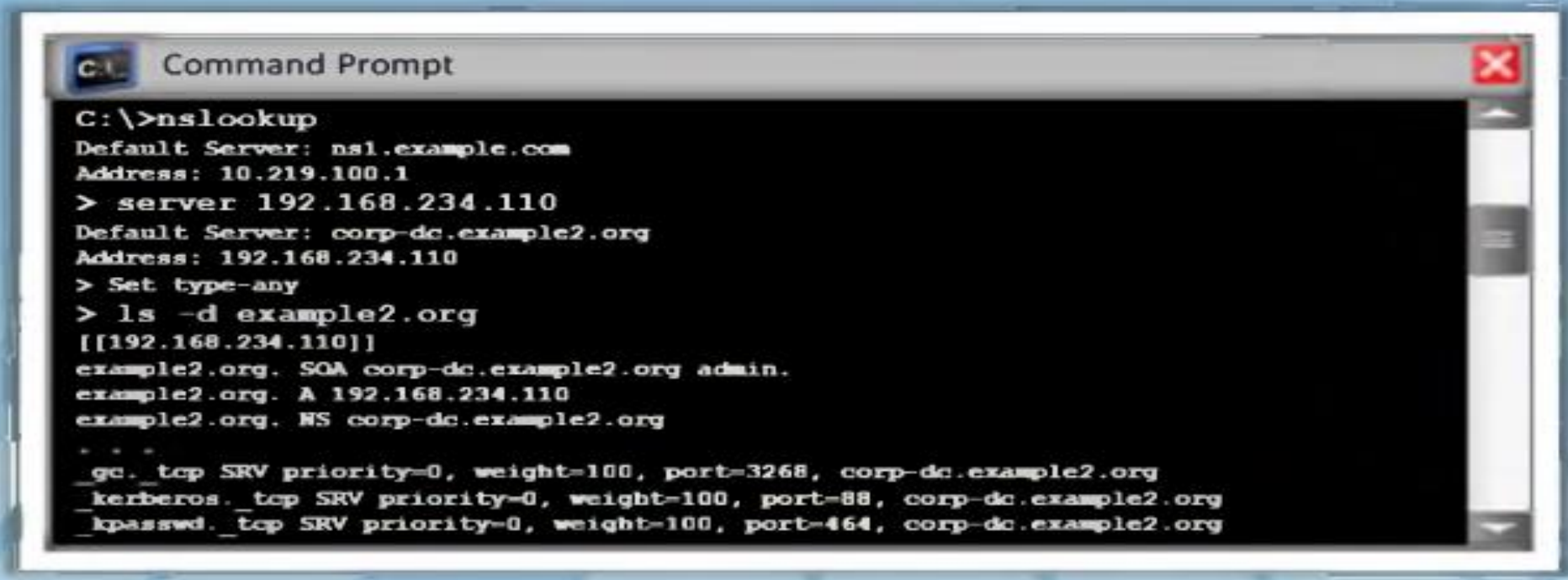
Enumeration Counter-measures

Enumeration Pen Testing

# 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




# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

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 "public" community's name
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Access to null session pipes, null session shares, and IPSec filtering should also be 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)

## 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

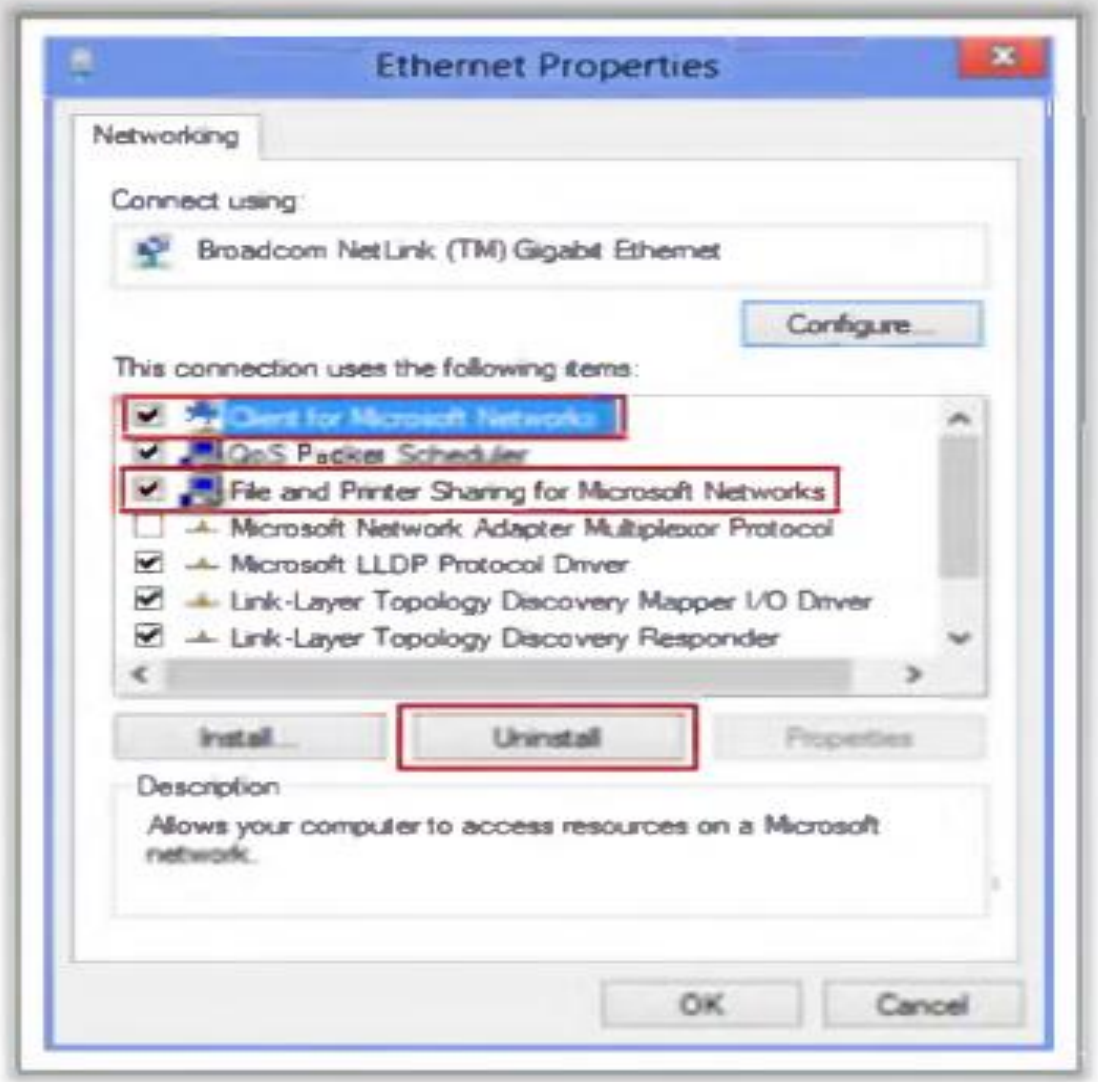
## LDAP

- 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

# SMB Enumeration Countermeasures

## Disabling 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



# Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

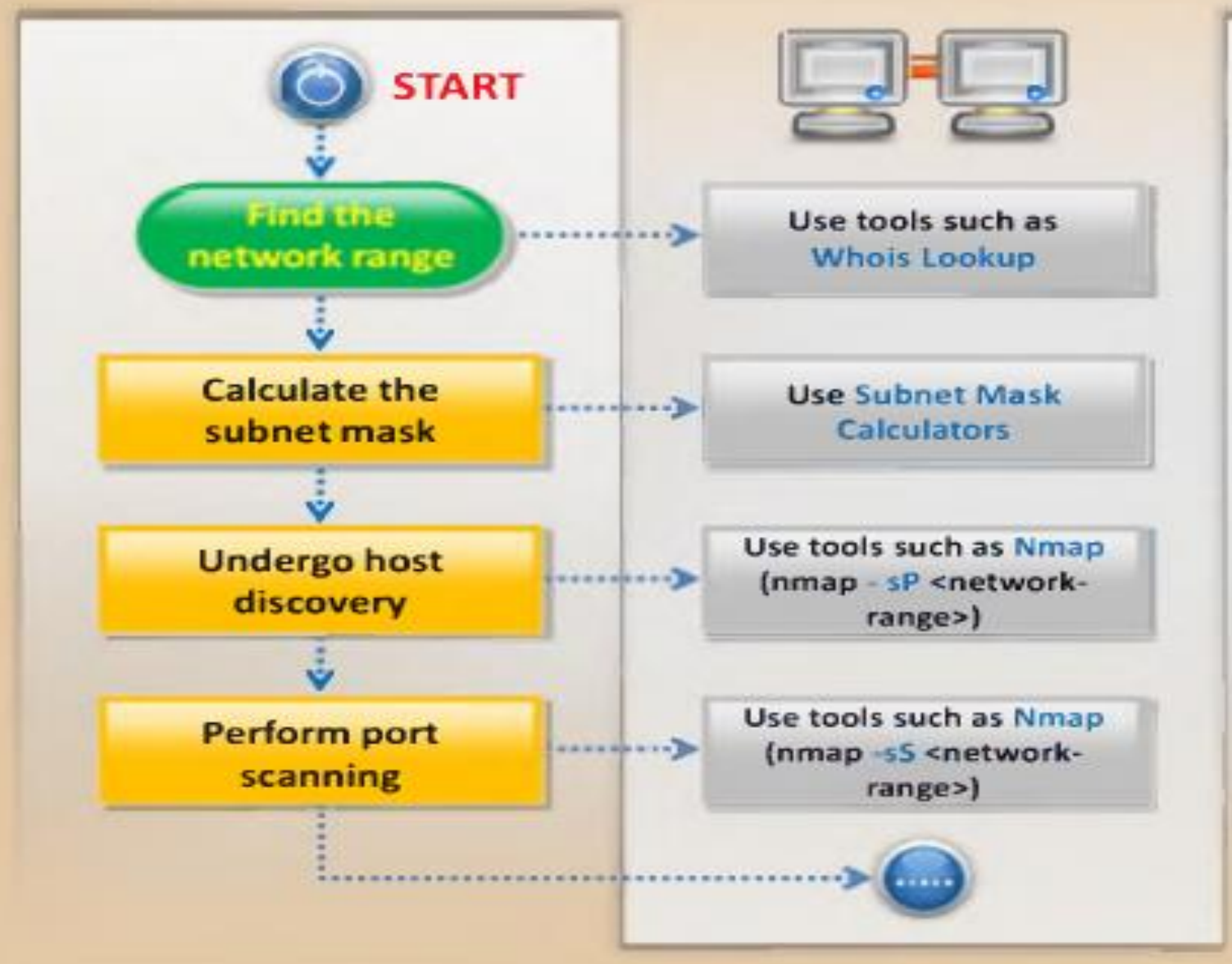
# Enumeration Pen Testing

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**

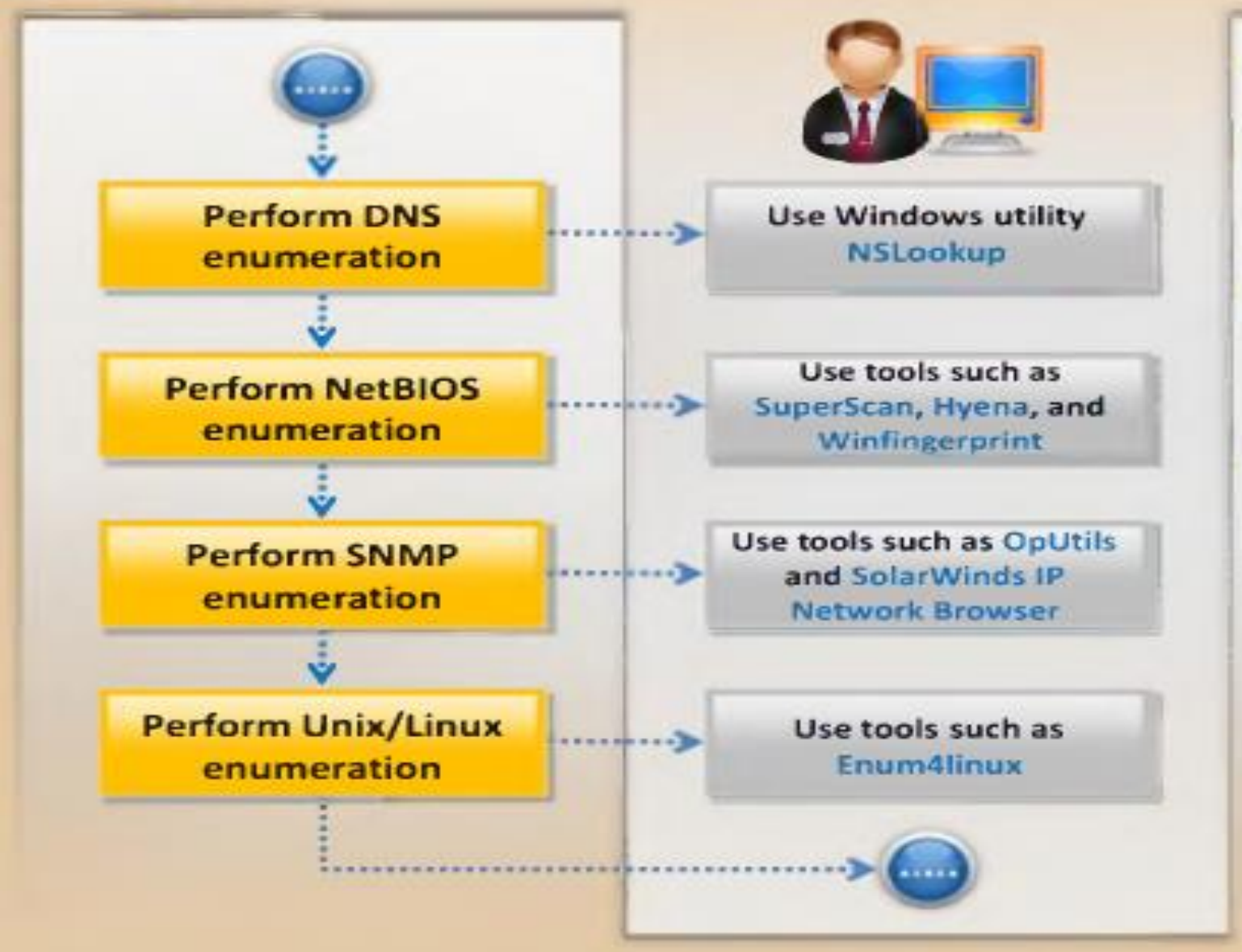
Used in combination with **data collected in the reconnaissance phase**

# 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 as an input to many of the ping sweep and port scanning tools by using Subnet Mask Calculators
- 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 DNS enumeration using Windows utility NSLookup
- Perform NetBIOS enumeration using tools such as SuperScan, Hyena, and Winfingerprint
- Perform SNMP enumeration using tools such as OpUtils Network Monitoring Toolset and SolarWinds IP Network Browser
- Perform Unix/Linux enumeration using tools such as Enum4linux

# Enumeration Pen Testing (Cont'd)

Perform LDAP enumeration → Use tools such as Softerra LDAP Administrator

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

Perform SMTP enumeration → Use tools such as NetScanTools Pro

Document all the findings

- Perform LDAP enumeration using tools such as Softerra LDAP Administrator
- Perform NTP enumeration using commands such as ntptrace, ntpdc, and ntpq
- Perform SMTP enumeration using tools such as NetScanTools Pro


# Module Summary

- Enumeration is defined as the process of extracting user names, 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 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