

Enumeration

Module 04



Module Objectives

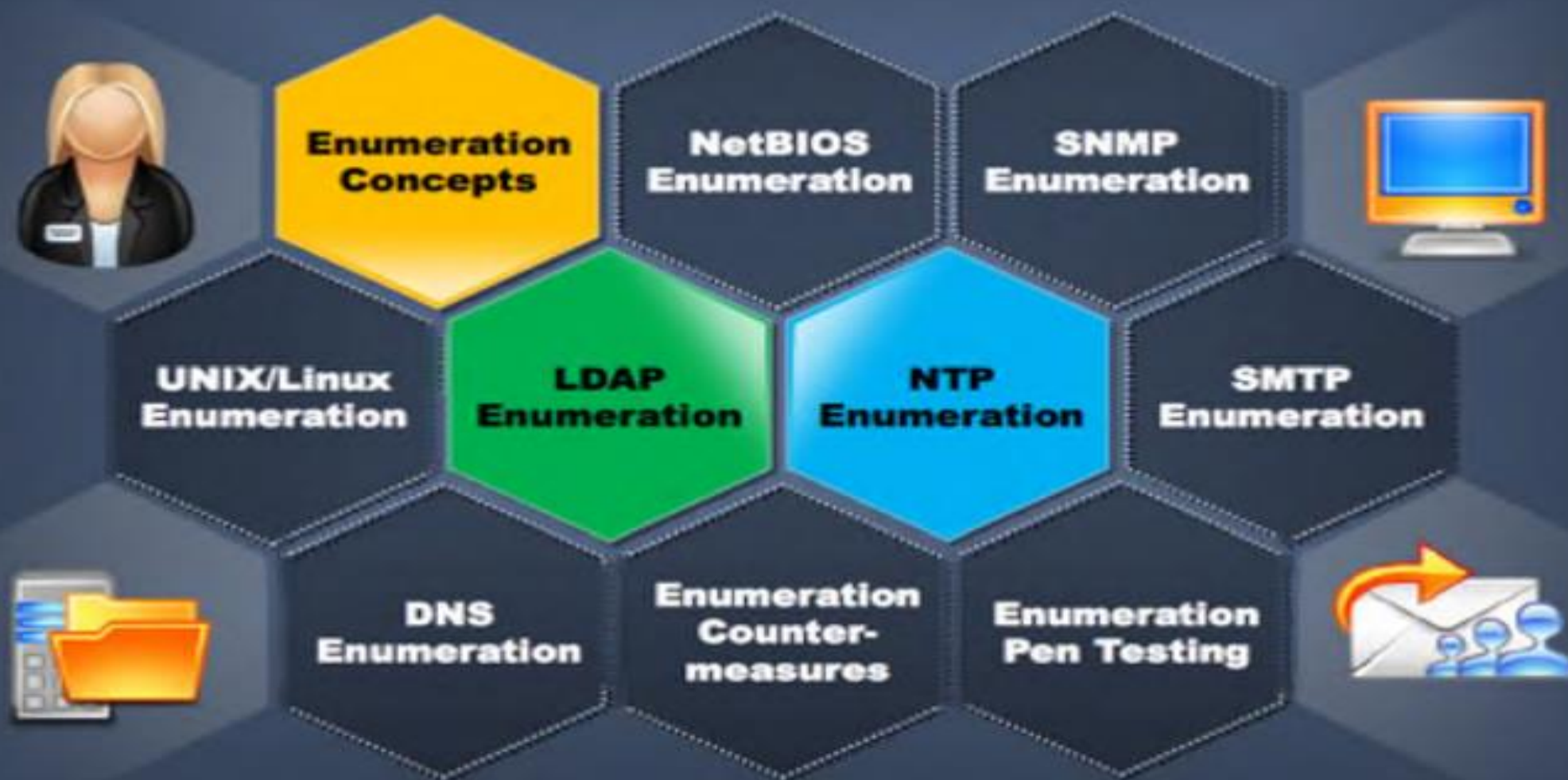
- What Is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- Enumerate Systems Using Default Passwords
- SNMP Enumeration



- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

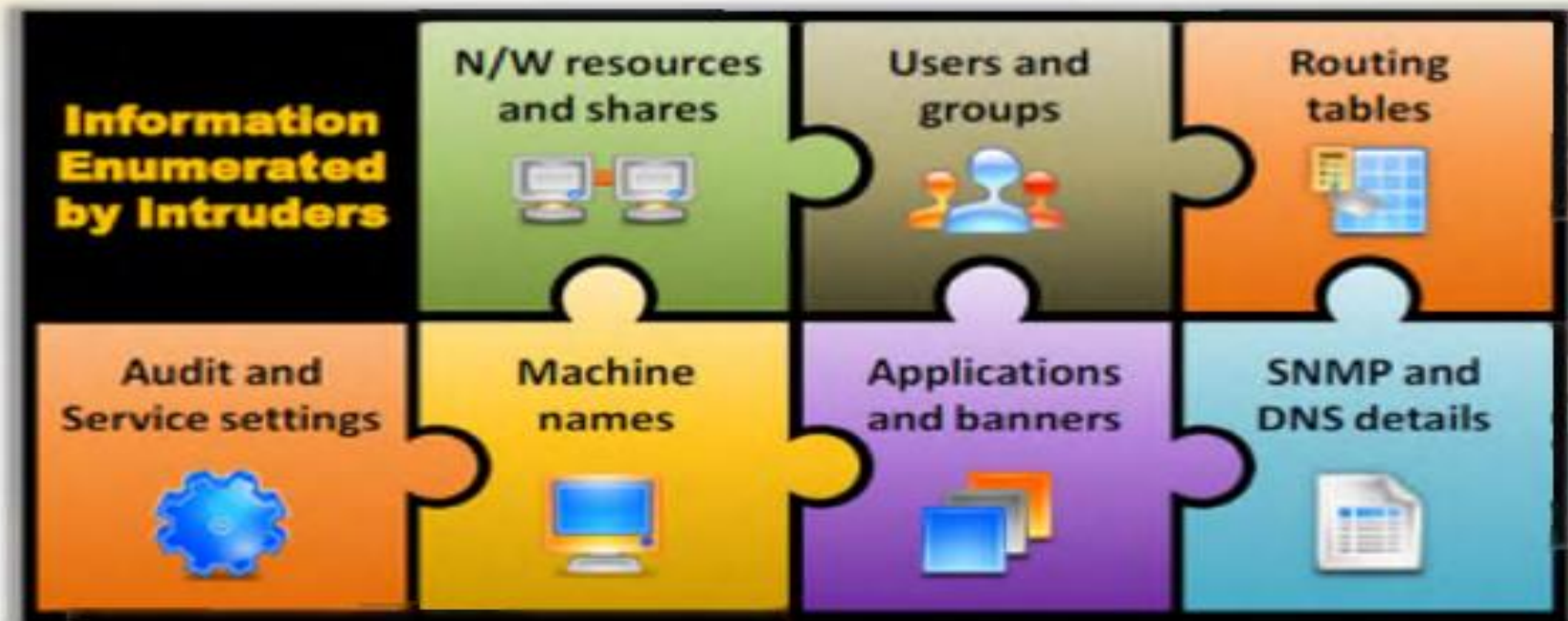


Module **Flow**



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



UDP 161

Simple Network Management protocol (SNMP)



TCP 135

Microsoft RPC Endpoint Mapper



TCP/UDP 389

Lightweight Directory Access Protocol (LDAP)



TCP 137

NetBIOS Name Service (NBNS)



TCP/UDP 3368

Global Catalog Service



TCP 139

NetBIOS Session Service (SMB over NetBIOS)



TCP 25

Simple Mail Transfer Protocol (SMTP)

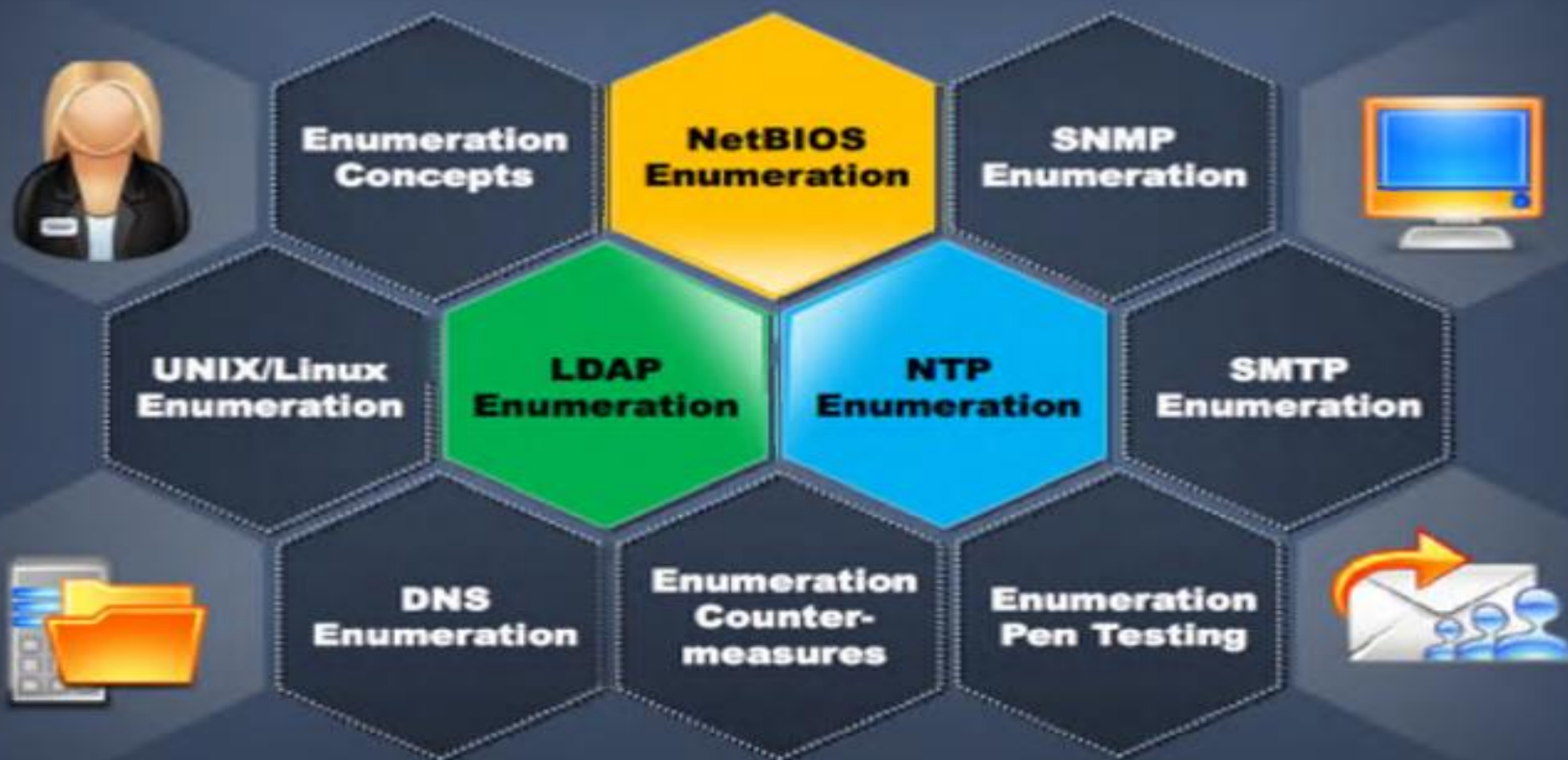


TCP 445

SMB over TCP (Direct Host)



Module **Flow**



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**



NetBIOS Name List

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



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

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>nbtstat.exe -a <remote>

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
<00>                <00>                UNIQUE             Registered
<00>                <00>                GROUP              Registered
<1C>                <1C>                GROUP              Registered
<20>                <20>                UNIQUE             Registered
<1B>                <1B>                UNIQUE             Registered

MAC Address = 00-00-00-00-00-05

C:\Users\Admin>
```

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>nbtstat.exe -c

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

NetBIOS Remote Cache Name Table

Name                Type                Host Address        Life [sec]
-----
<20>                UNIQUE             192.168.168.170     143
<20>                UNIQUE             192.168.168.1       165

C:\Users\Admin>
```

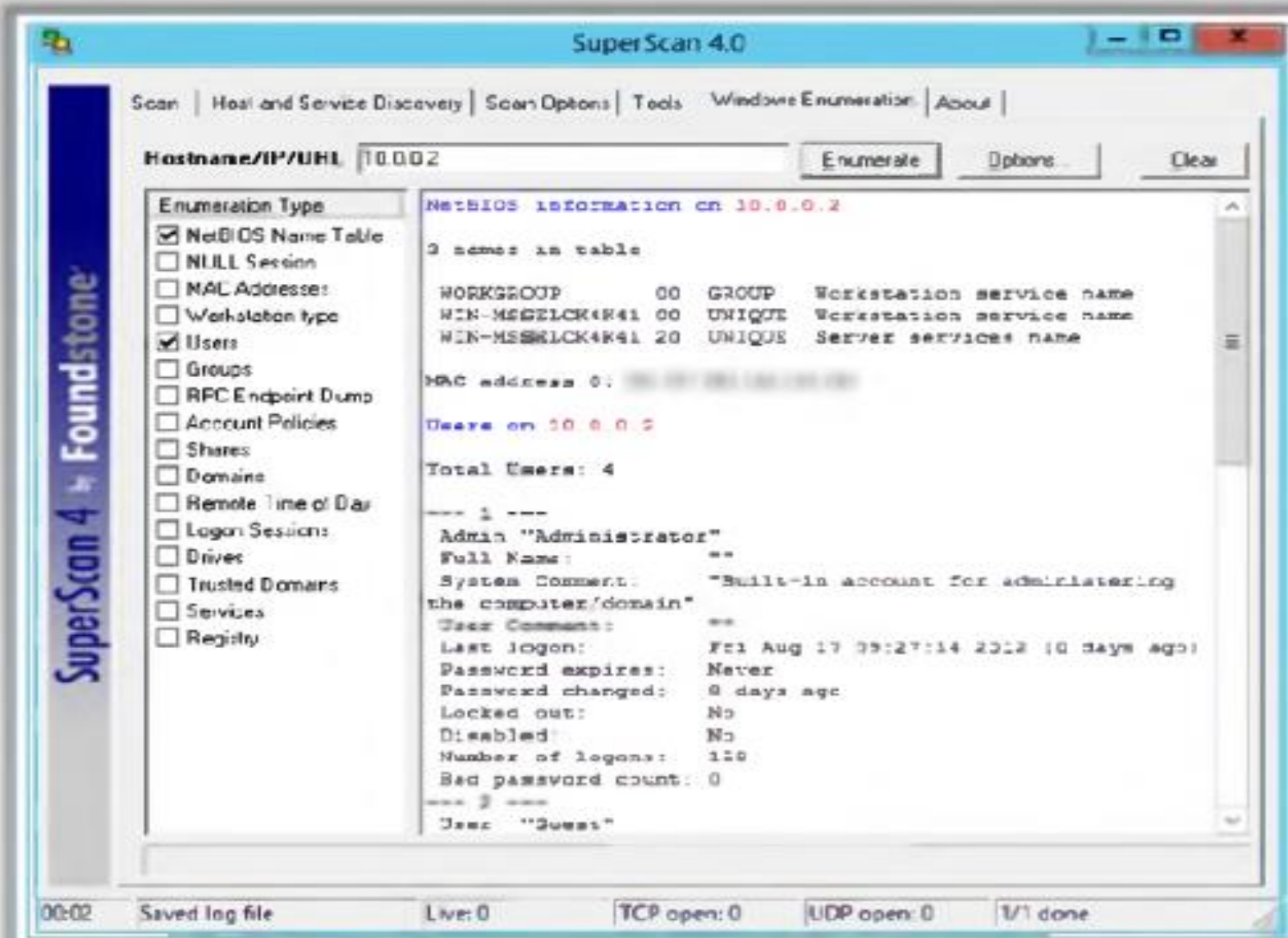
<http://technet.microsoft.com>

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
- 5 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 login names for Windows servers and domain controllers
- It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.

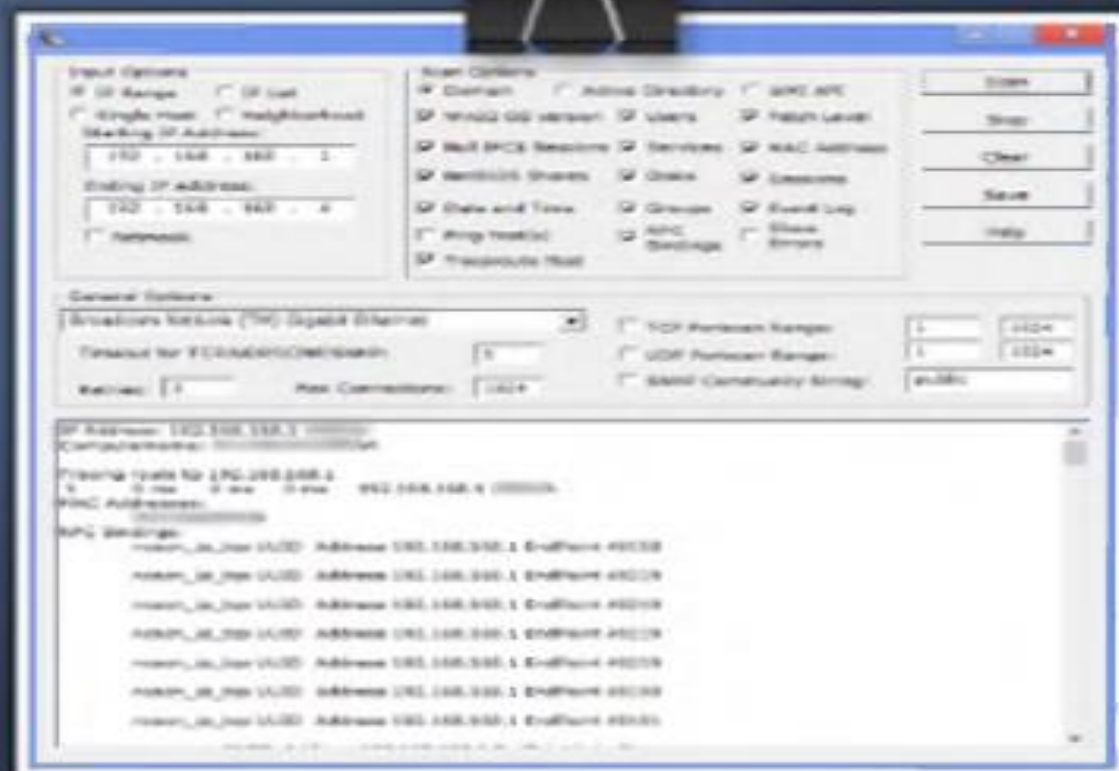
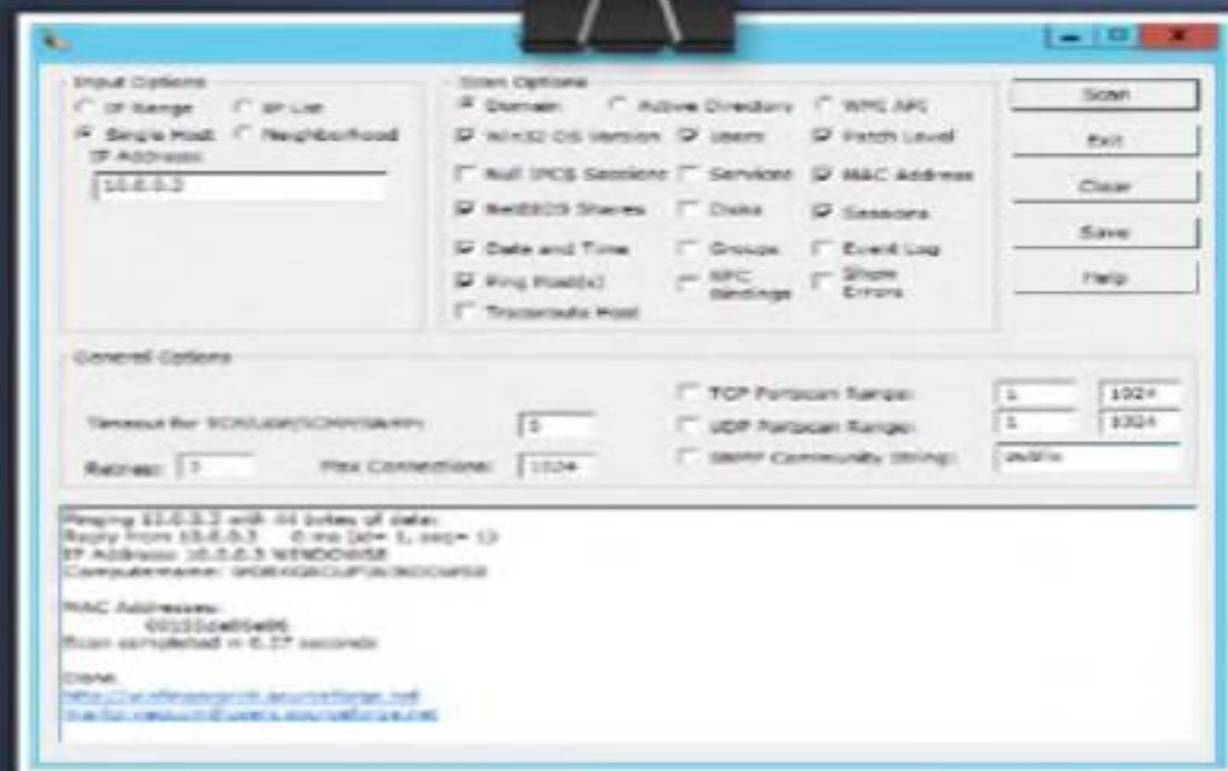


The screenshot displays the Hyena application window. On the left, there is a tree view showing the system's structure, including folders like 'System', 'Users', and 'Groups'. The main area shows a list of services with columns for Name, Display Name, Status, Type, Path, Account, Description, and Remarks. The services listed include Active Directory Web Services, Application Experience, Application Gateway Service, Application Host Helper Service, Application Identity, Application Information, Application Management, ASP.NET State Service, Windows Audio Endpoint Builder, Windows Audio, Base Filtering Engine, Background Intelligent Transfer Service, Certificate Browser, Certificate Propagation, Microsoft .NET Framework NGIN v2.0.50727_x86, Microsoft .NET Framework NGIN v2.0.50727_x64, Microsoft .NET Framework NGIN v4.0.30319_x86, Microsoft .NET Framework NGIN v4.0.30319_x64, COM+ System Application, Cryptographic Services, DCOM Server Process Launcher, Disk Defragmenter, DFS Namespaces, DFS Replication, DHCP Client, DNS Server, DNS Client, Wired AutoConfig, Diagnostic Policy Service, Extensible Authentication Protocol, File System (DFS), Windows Event Log, COM+ Event System, Microsoft File Channel Platform Registration S..., Function Discovery Provider Host, Function Discovery Resource Publication, Windows Host Cache Service, and Windows Management Framework Host Process.

Name	Display Name	Status	Type	Path	Account	Description	Remarks
ADWS	Active Directory Web Services	Running	Service (Own Process)	Automatic	LocalSystem		C:\Windows\ADWS\Microsoft...
AppExperience	Application Experience	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
AppGateway	Application Gateway Service	Stopped	Service (Own Process)	Manual	NT AUTHORITY\SYSTEM		C:\Windows\System32\apph...
AppHostHelper	Application Host Helper Service	Running	Service (Shared Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
AppIdentity	Application Identity	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE	AppIdentityControlService	C:\Windows\System32\apph...
AppInfo	Application Information	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
AppMgmt	Application Management	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
ASPNETState	ASP.NET State Service	Stopped	Service (Own Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
AudioEndpointBuilder	Windows Audio Endpoint Builder	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
Audio	Windows Audio	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE	AudioEndpointBuilder...	C:\Windows\System32\apph...
BFE	Base Filtering Engine	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
BITS	Background Intelligent Transfer Service	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
CertBrowser	Certificate Browser	Stopped	Service (Shared Process)	Disabled	LocalSystem	Common-System-Applicat...	C:\Windows\System32\apph...
CertPropSvc	Certificate Propagation	Running	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
clr_apimscorshim_v2.0.50727_x86	Microsoft .NET Framework NGIN v2.0.50727_x86	Stopped	Service (Own Process)	Disabled	LocalSystem		C:\Windows\System32\apph...
clr_apimscorshim_v2.0.50727_x64	Microsoft .NET Framework NGIN v2.0.50727_x64	Stopped	Service (Own Process)	Disabled	LocalSystem		C:\Windows\System32\apph...
clr_apimscorshim_v4.0.30319_x86	Microsoft .NET Framework NGIN v4.0.30319_x86	Stopped	Service (Own Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
clr_apimscorshim_v4.0.30319_x64	Microsoft .NET Framework NGIN v4.0.30319_x64	Stopped	Service (Own Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
COMSysApp	COM+ System Application	Running	Service (Own Process)	Manual	LocalSystem		C:\Windows\System32\apph...
CryptSrv	Cryptographic Services	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
DCOMLaunch	DCOM Server Process Launcher	Running	Service (Shared Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
defrag	Disk Defragmenter	Stopped	Service (Own Process)	Manual	LocalSystem		C:\Windows\System32\apph...
DFS	DFS Namespaces	Running	Service (Own Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
DFSRepl	DFS Replication	Running	Service (Own Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
DHCP	DHCP Client	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
DNS	DNS Server	Running	Service (Own Process)	Automatic	LocalSystem		C:\Windows\System32\apph...
DNSClient	DNS Client	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
WiredAutoConfig	Wired AutoConfig	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
DiagnosticPolicyService	Diagnostic Policy Service	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
ExtAuthProtocol	Extensible Authentication Protocol	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
FileSystem	File System (DFS)	Running	Service (Shared Process)	Manual	LocalSystem		C:\Windows\System32\apph...
EventLog	Windows Event Log	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
COM+EventSystem	COM+ Event System	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
MicrosoftFileChannelPlatformRegistrationS...	Microsoft File Channel Platform Registration S...	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
FunctionDiscoveryProviderHost	Function Discovery Provider Host	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
FunctionDiscoveryResourcePublication	Function Discovery Resource Publication	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
HostCache	Windows Host Cache Service	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...
WindowsManagementFrameworkHostProcess	Windows Management Framework Host Process	Running	Service (Own Process)	Manual	NT AUTHORITY\LOCALSERVICE		C:\Windows\System32\apph...

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

1

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

2

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



The screenshot shows a web interface for a default password database. It includes a search bar at the top with a 'Search' button. Below the search bar are radio buttons for 'Vendor', 'Product', and 'Model'. A list of characters is provided for selection. The main content is a table with columns: Vendor, Product, Model/Revision, Login, Password, and Access Level.

Vendor	Product	Model/Revision	Login	Password	Access Level
Ziire	WiFi Routers		(none)	Wireless	Admin
3COM	CardPlex	7000	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	tech	tech	
3COM	HiFlex/SEC	vs. 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			LSB	snmp-read
3COM	Office Connect ISON Routers	5x0	iva	PASSWORD	Admin

http://www.virus.org/default_passwds



Default **Username/Pwd**

Ex: **admin/synnet**

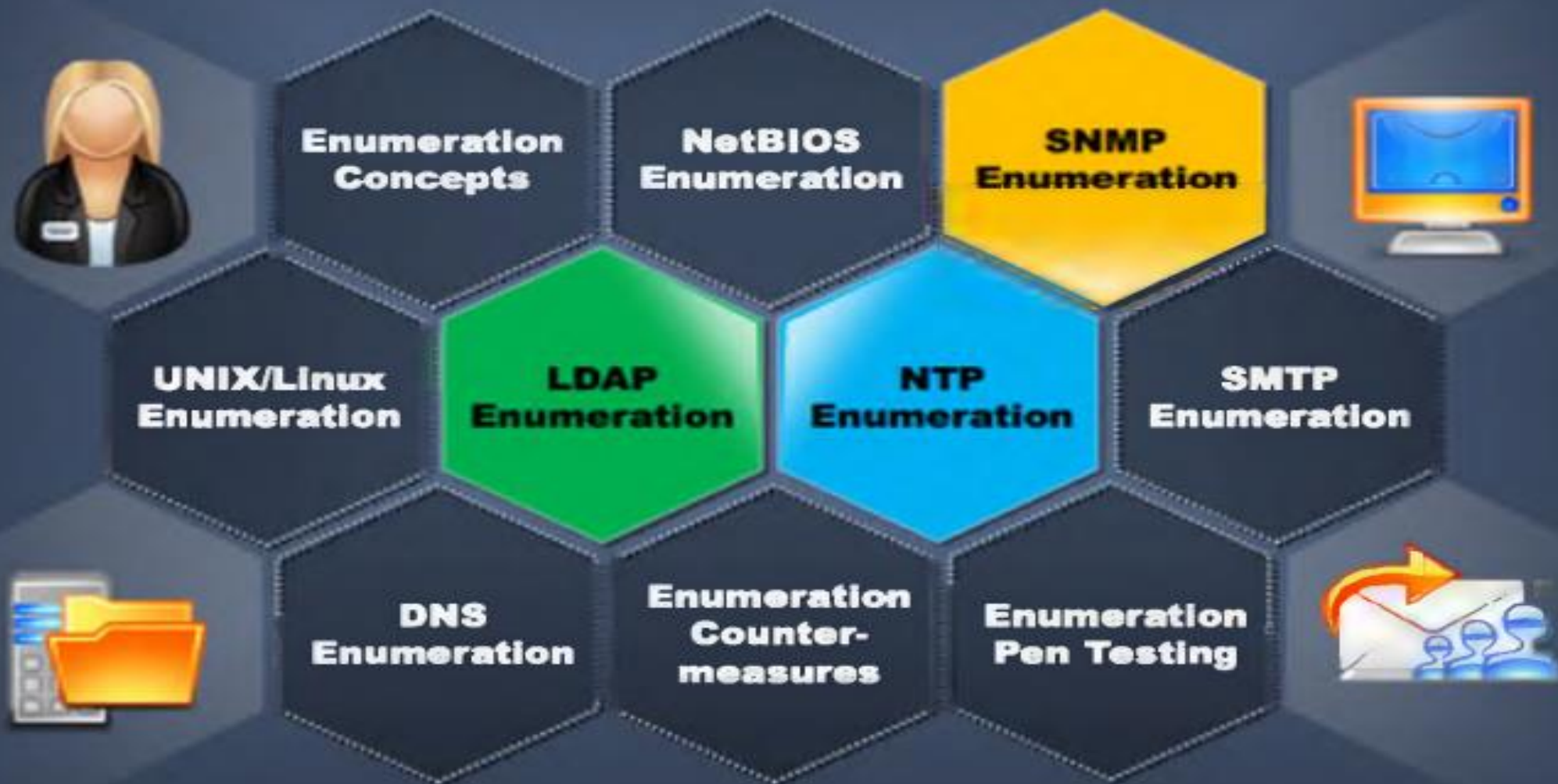


Router



Enterprise Network

Module **Flow**



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



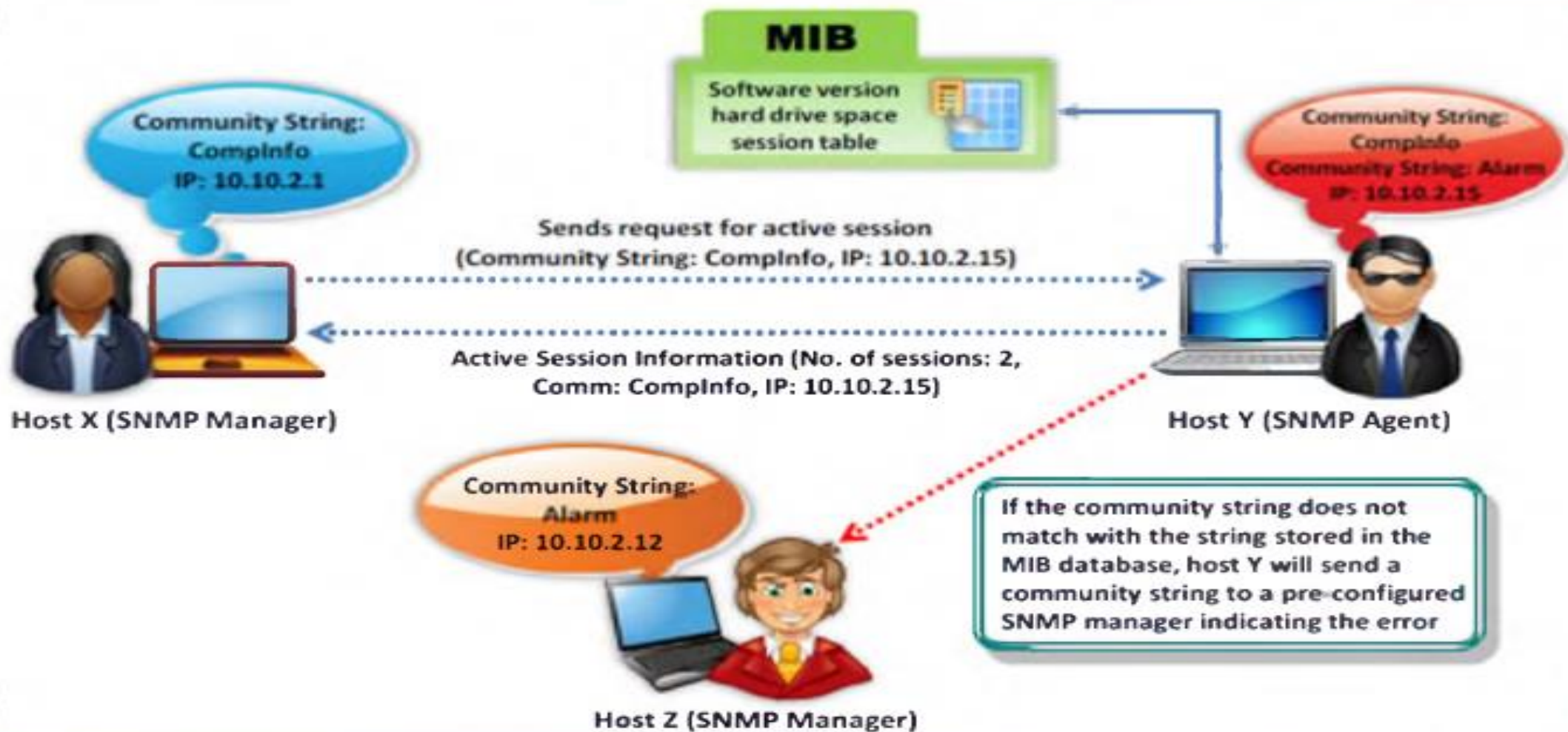
- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
 - ⊖ **Read community string**: It is public by default, allows to view the device or system configuration
 - ⊖ **Read/write community string**: It is private by default, allows to edit or alter configuration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

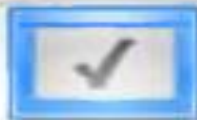


The MIB database is hierarchical and each managed object in a MIB is addressed through **object identifiers (OIDs)**



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

Management
OpUtils 6

Home Health Check Manager IP Address Manager Ping Traceroute MAC IP List Tools Reports Admin Support

Address Monitoring Network Monitoring SNMP Tools OS/DB Tools Custom Tools

Alerts (10)

SNMP Scan

Add IP Group Add IP List Export CSV

Starting IP: 190.188.111.1

Ending IP: 190.188.111.14

Scan

IP Address: 190.188.111.1

Host Name: 190.188.111.1

Response Time: 190.188.111.1

System Type: 190.188.111.1

Status: 190.188.111.1

IP Address	Host Name	Response Time	System Type	Status
190.188.111.1	190.188.111.1	190.188.111.1	190.188.111.1	190.188.111.1
190.188.111.2	190.188.111.2	190.188.111.2	190.188.111.2	190.188.111.2
190.188.111.3	190.188.111.3	190.188.111.3	190.188.111.3	190.188.111.3
190.188.111.4	190.188.111.4	190.188.111.4	190.188.111.4	190.188.111.4
190.188.111.5	190.188.111.5	190.188.111.5	190.188.111.5	190.188.111.5
190.188.111.6	190.188.111.6	190.188.111.6	190.188.111.6	190.188.111.6
190.188.111.7	190.188.111.7	190.188.111.7	190.188.111.7	190.188.111.7
190.188.111.8	190.188.111.8	190.188.111.8	190.188.111.8	190.188.111.8
190.188.111.9	190.188.111.9	190.188.111.9	190.188.111.9	190.188.111.9
190.188.111.10	190.188.111.10	190.188.111.10	190.188.111.10	190.188.111.10
190.188.111.11	190.188.111.11	190.188.111.11	190.188.111.11	190.188.111.11
190.188.111.12	190.188.111.12	190.188.111.12	190.188.111.12	190.188.111.12
190.188.111.13	190.188.111.13	190.188.111.13	190.188.111.13	190.188.111.13
190.188.111.14	190.188.111.14	190.188.111.14	190.188.111.14	190.188.111.14

SNMP Enumeration Tool: SolarWind's IP Network Browser

The screenshot displays the SolarWind's IP Network Browser application. The interface includes a menu bar (File, Tools, View, Devices, Interfaces, Gadgets, External Tools, Help), a toolbar with options like 'Add New Device...', 'Manage SNMP Credentials', and 'Manage Telnet/SSH Credentials', and a 'Gadgets' sidebar on the left. The 'Gadgets' sidebar has categories like 'Monitoring', 'Tools', and 'Discovery Tools', with 'IP Network Browser' highlighted. The main window shows a tree view of a discovered network device, identified as a 'Windows NT Workstation'. The tree structure includes 'System MIB', 'Interfaces', 'Services', 'Accounts', 'ARP Table', 'Routers', 'CDR Routers', 'Shares', 'Shared Drives', 'TCP/IP Networks', and 'TCP Connections'. A table at the bottom lists discovered IP addresses and their corresponding hostnames.

IP Address	Host Name
192.168.168.1	192.168.168.1
192.168.168.2	192.168.168.2
192.168.168.3	192.168.168.3
192.168.168.4	192.168.168.4
192.168.168.5	192.168.168.5
192.168.168.6	192.168.168.6
192.168.168.7	192.168.168.7
192.168.168.8	192.168.168.8
192.168.168.9	192.168.168.9
192.168.168.10	192.168.168.10
192.168.168.11	192.168.168.11
192.168.168.12	192.168.168.12
192.168.168.13	192.168.168.13
192.168.168.14	192.168.168.14
192.168.168.15	192.168.168.15
192.168.168.16	192.168.168.16
192.168.168.17	192.168.168.17
192.168.168.18	192.168.168.18
192.168.168.19	192.168.168.19
192.168.168.20	192.168.168.20
192.168.168.21	192.168.168.21
192.168.168.22	192.168.168.22
192.168.168.23	192.168.168.23
192.168.168.24	192.168.168.24
192.168.168.25	192.168.168.25
192.168.168.26	192.168.168.26
192.168.168.27	192.168.168.27
192.168.168.28	192.168.168.28
192.168.168.29	192.168.168.29
192.168.168.30	192.168.168.30
192.168.168.31	192.168.168.31
192.168.168.32	192.168.168.32
192.168.168.33	192.168.168.33
192.168.168.34	192.168.168.34
192.168.168.35	192.168.168.35
192.168.168.36	192.168.168.36
192.168.168.37	192.168.168.37
192.168.168.38	192.168.168.38
192.168.168.39	192.168.168.39
192.168.168.40	192.168.168.40
192.168.168.41	192.168.168.41
192.168.168.42	192.168.168.42
192.168.168.43	192.168.168.43
192.168.168.44	192.168.168.44
192.168.168.45	192.168.168.45
192.168.168.46	192.168.168.46
192.168.168.47	192.168.168.47
192.168.168.48	192.168.168.48
192.168.168.49	192.168.168.49
192.168.168.50	192.168.168.50

IP Network Browser performs network discovery on a single subnet or a range of subnets using ICMP and SNMP

It scans a single IP, IP address range, or subnet and displays network devices discovered in real time, providing immediate access to detailed information about the devices on network

SNMP Enumeration Tools



Getif

<http://www.wtcs.org>



SoftPerfect Network Scanner

<http://www.softperfect.com>



OidVIEW SNMP MIB Browser

<http://www.oidview.com>



SNMP Informant

<http://www.snmp-informant.com>



iReasoning MIB Browser

<http://tl1.ireasoning.com>



Net-SNMP

<http://net-snmp.sourceforge.net>



SNScan

<http://www.mcafee.com>



Nsauditor Network Security Auditor

<http://www.nsauditor.com>



SNMP Scanner

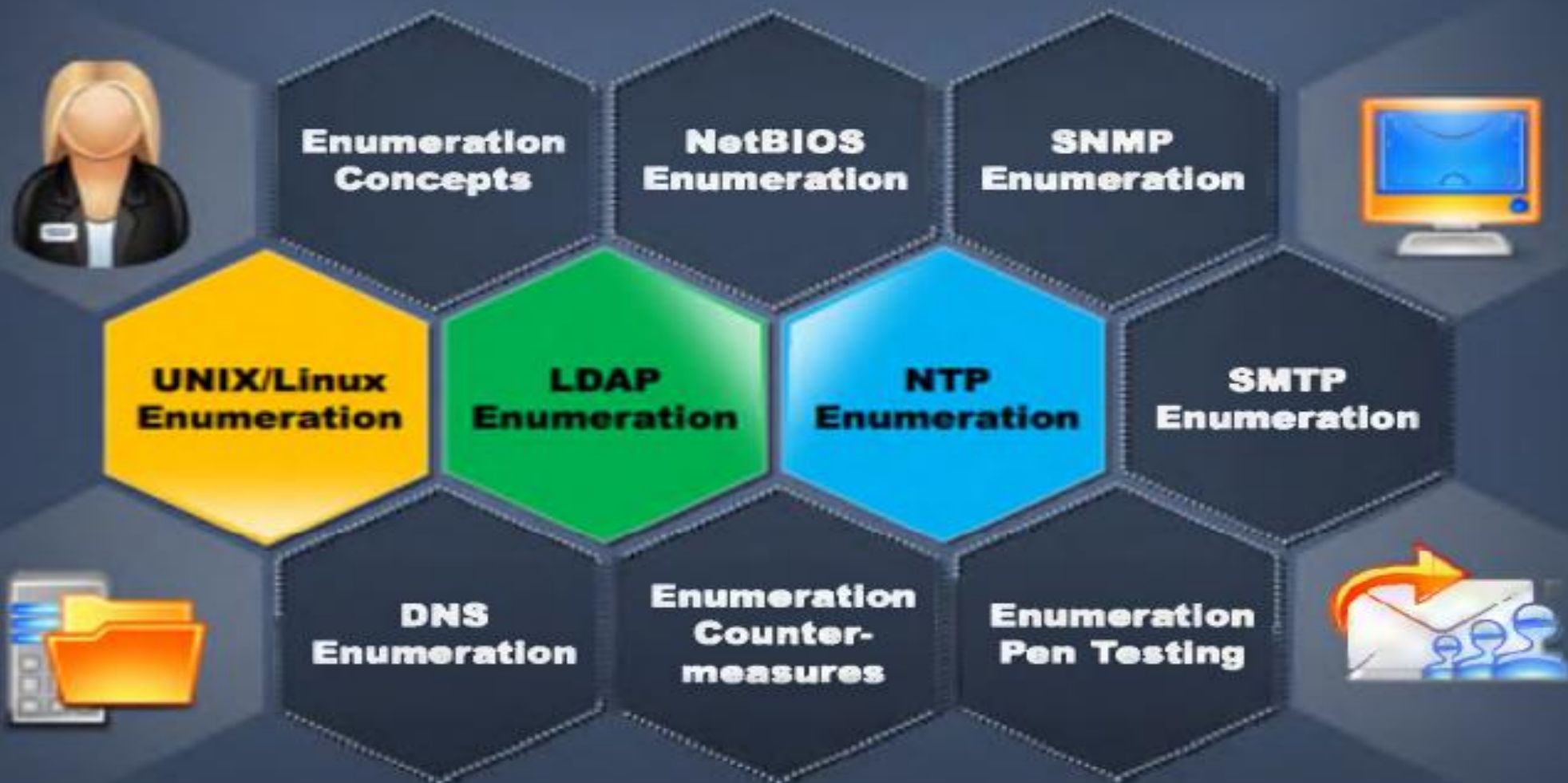
<http://www.secure-bytes.com>



Spiceworks

<http://www.spiceworks.com>

Module Flow



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
```

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

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

rpcinfo (RPC)

rpcclient

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

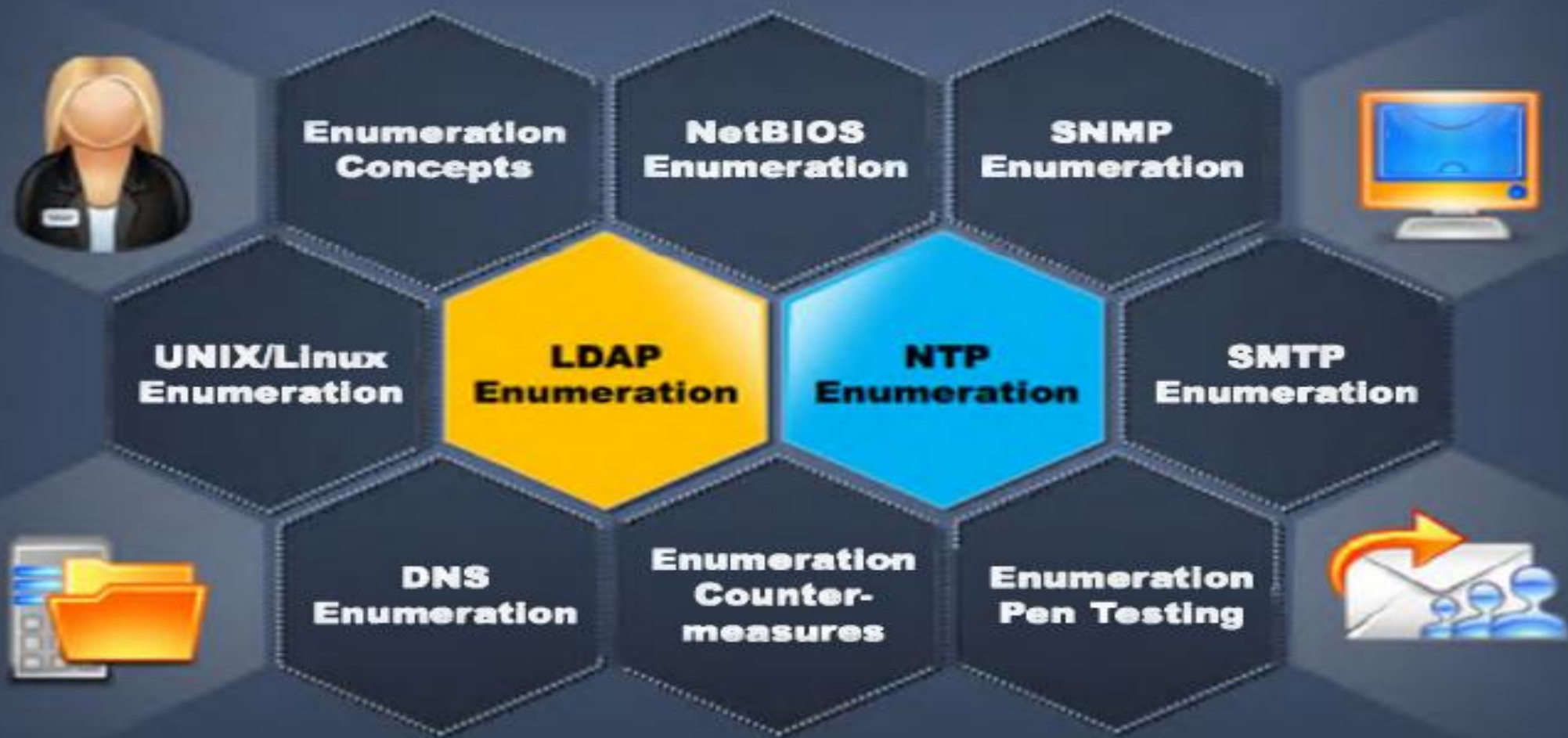
```
[root $] rpcclient $> netshareenum
```

- Finds the shared directories on the machine

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

showmount

Module **Flow**



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)

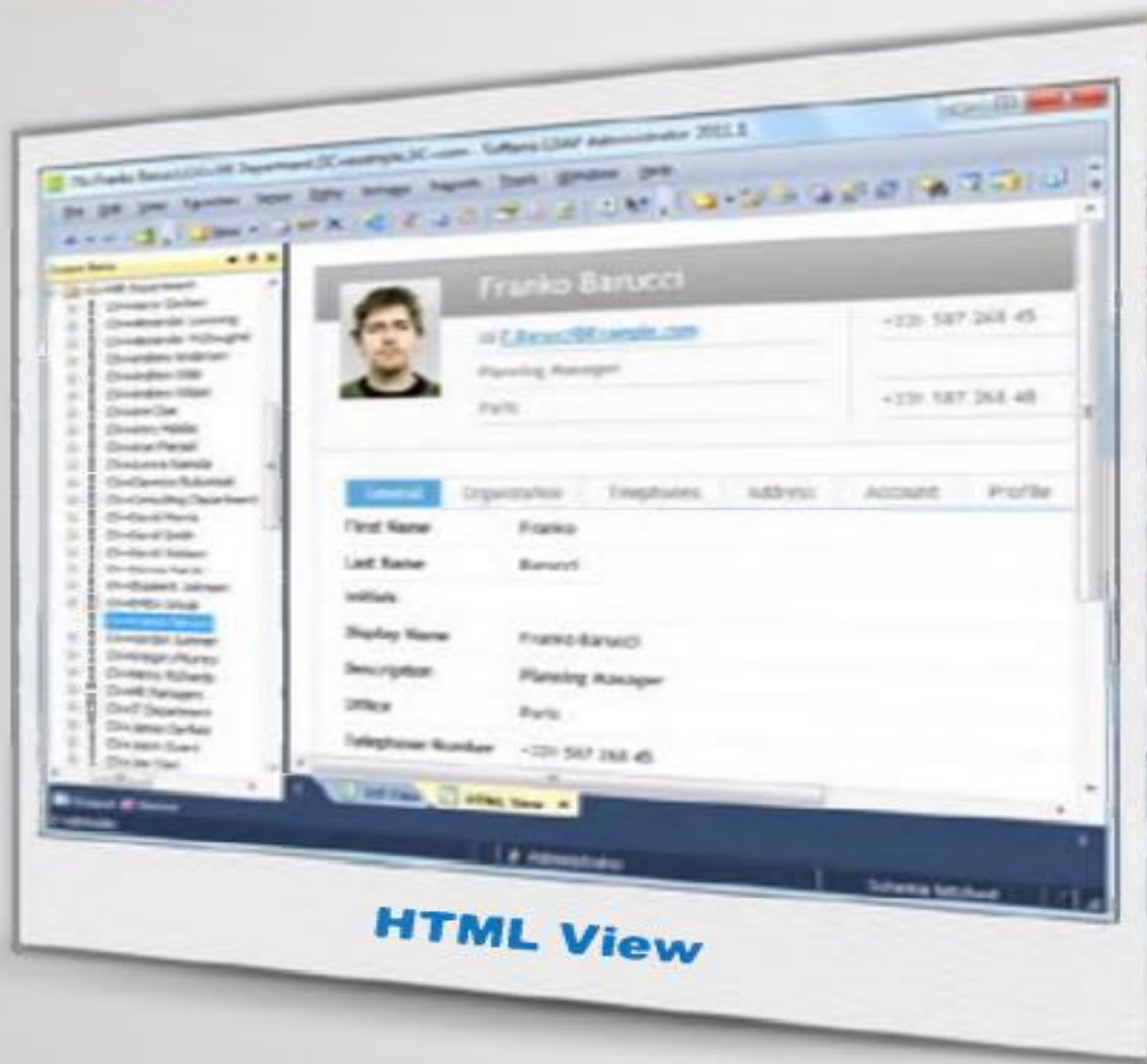
V

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



HTML View



LDAP Administrator

<http://www.ldapadministrator.com>

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**



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**

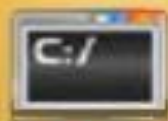


SMTP Enumeration

SMTP provides 3 built-in-commands:

- **VERFY** - Validates users
- **EXPN** - Tells the actual delivery addresses of aliases and mailing lists
- **RCPT TO** - Defines the recipients of the message

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can **determine valid users on SMTP server**



Attackers can directly interact with SMTP via the telnet prompt and collect **list of valid users** on the SMTP server



Using the SMTP VRFY Command

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

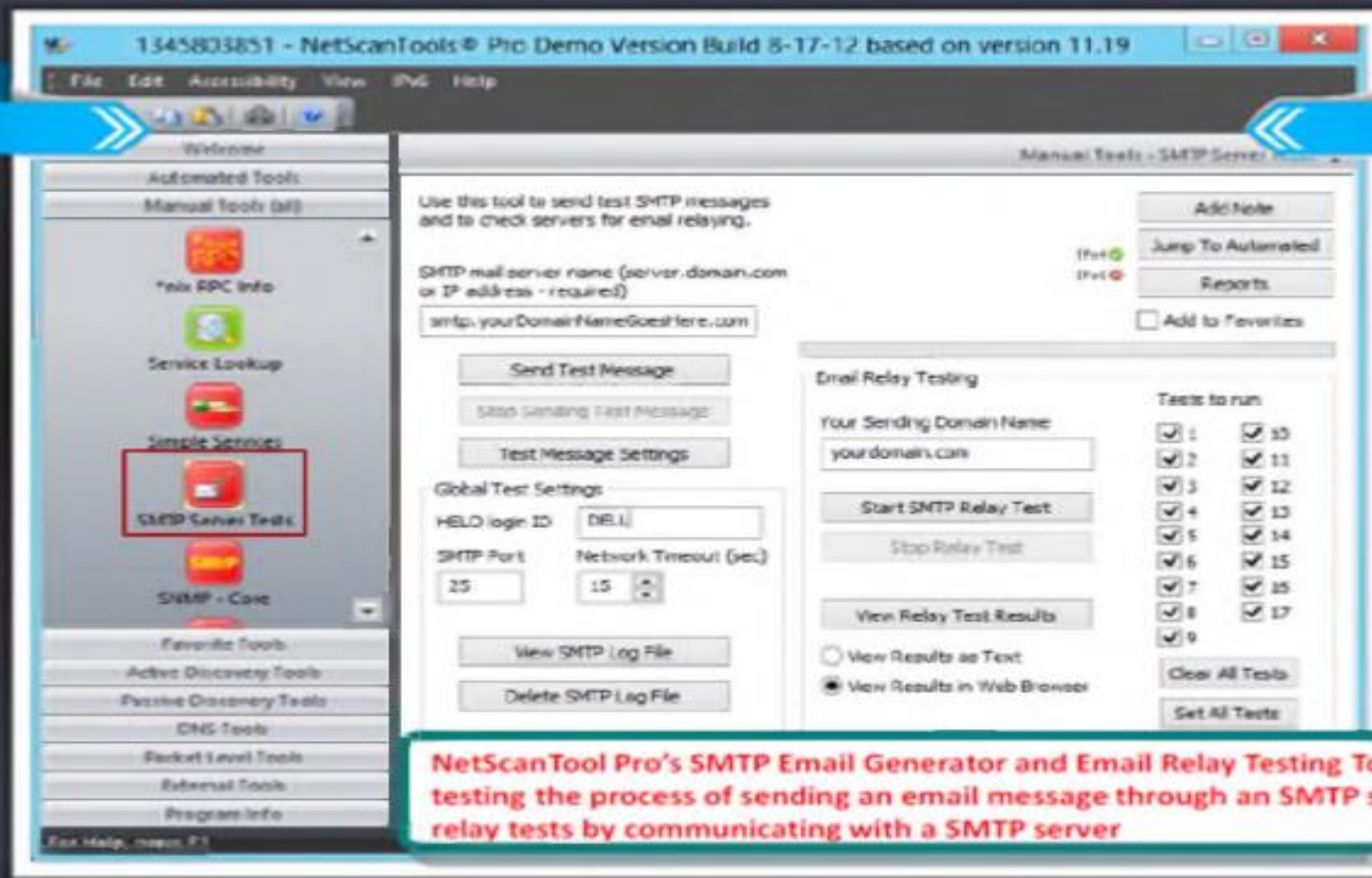
Using the SMTP EXPN Command

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

Using the SMTP RCPT TO Command

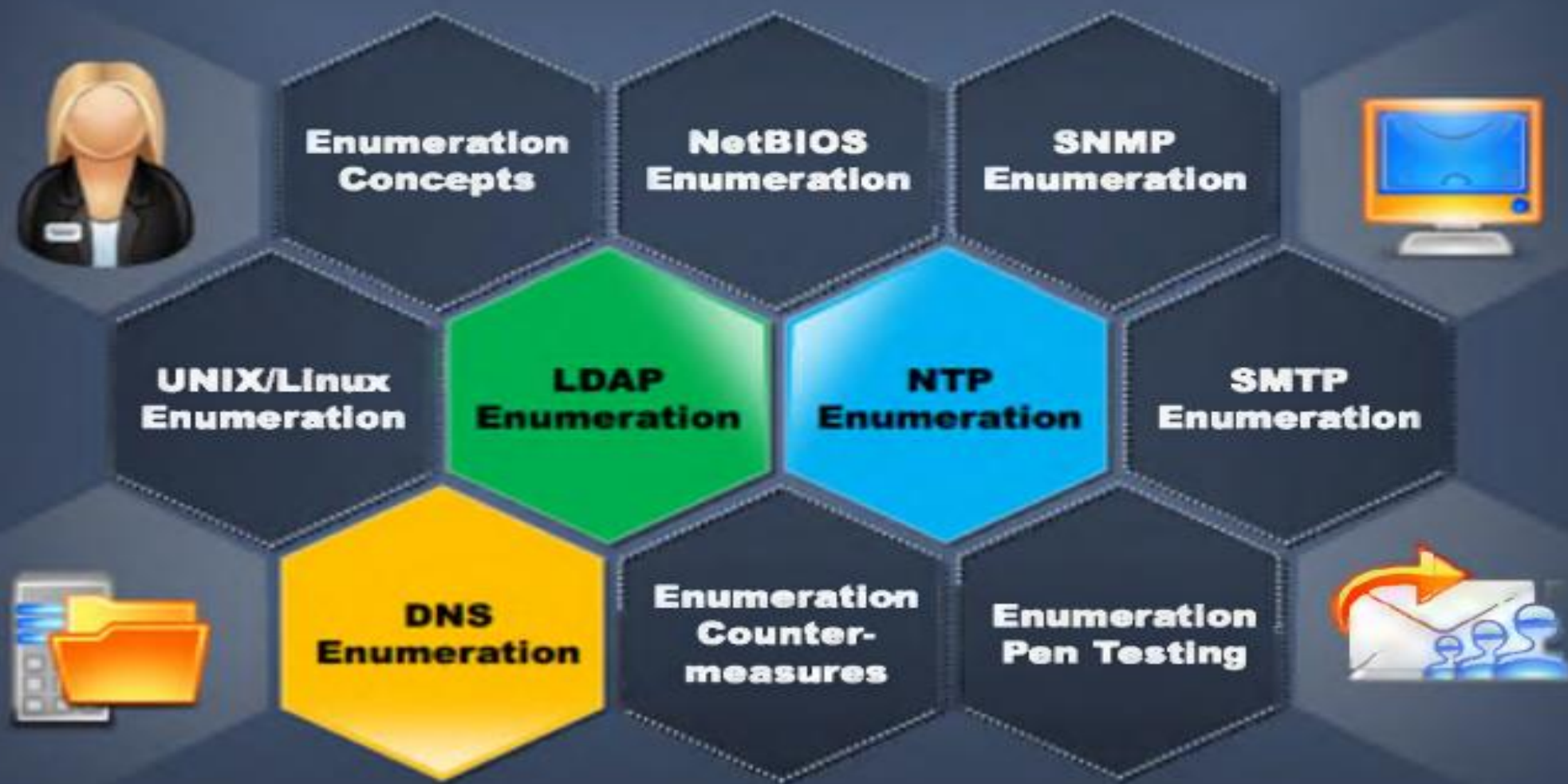
```
$ telnet 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder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

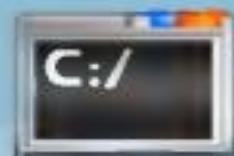
Module Flow



DNS Zone Transfer Enumeration

Using NSLookup

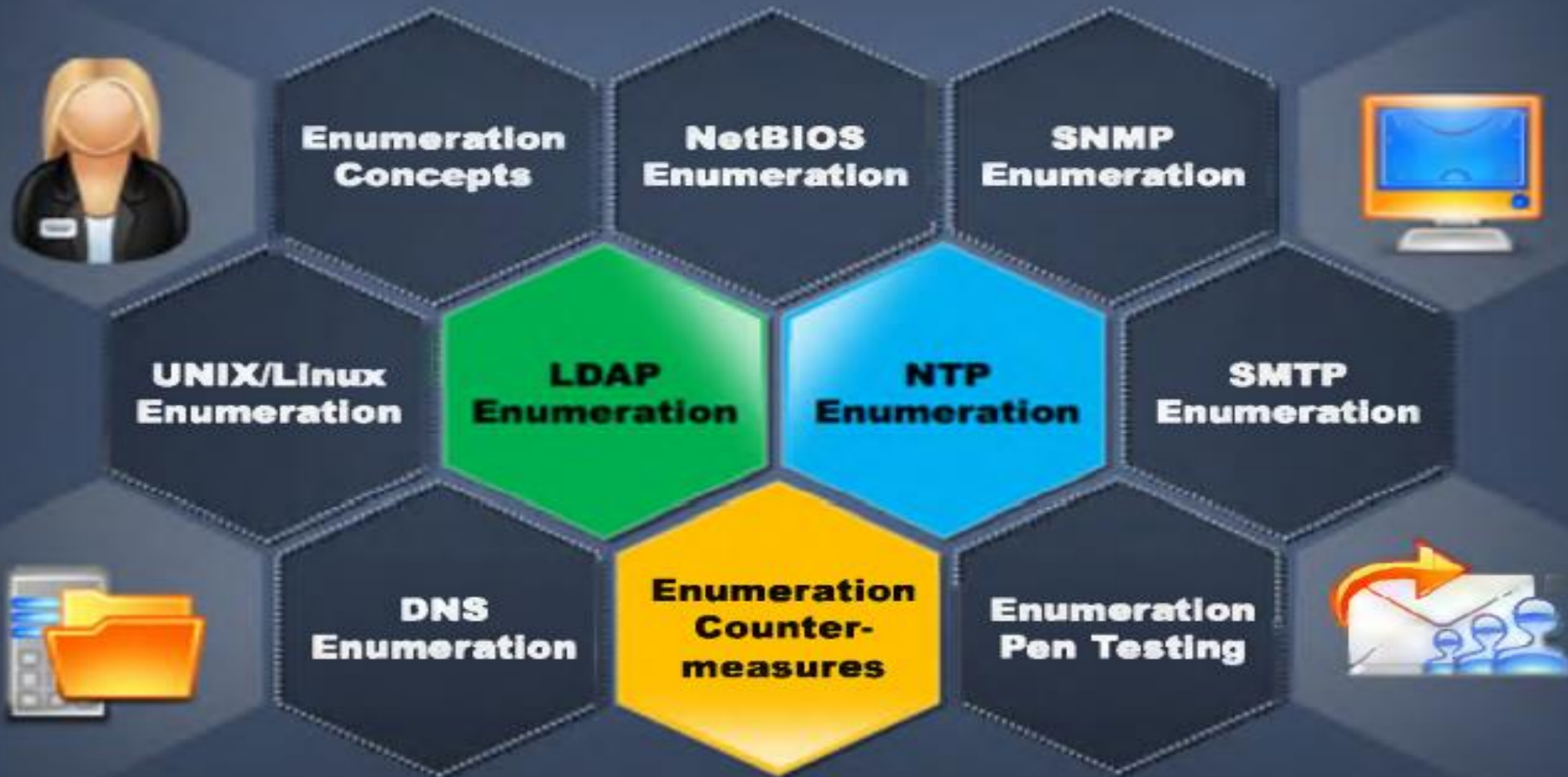
- It is a process of **locating the DNS server** and the **records of a target network**
- An attacker can gather valuable **network information** such as DNS server names, hostnames, machine names, user names, IP addresses of the potential targets, etc.
- In a DNS zone transfer enumeration, an attacker 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
```



Module **Flow**



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



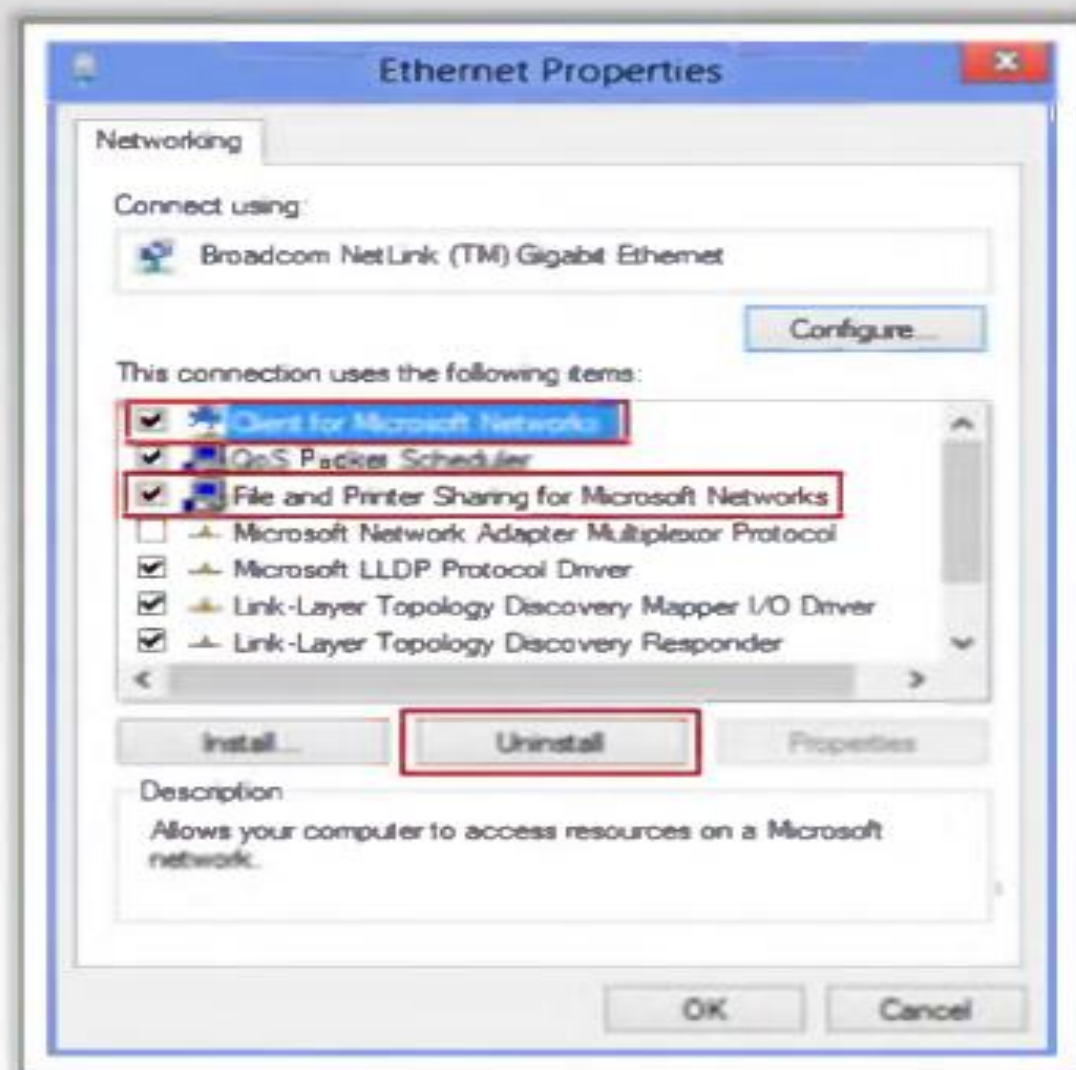
LDAP

- 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**

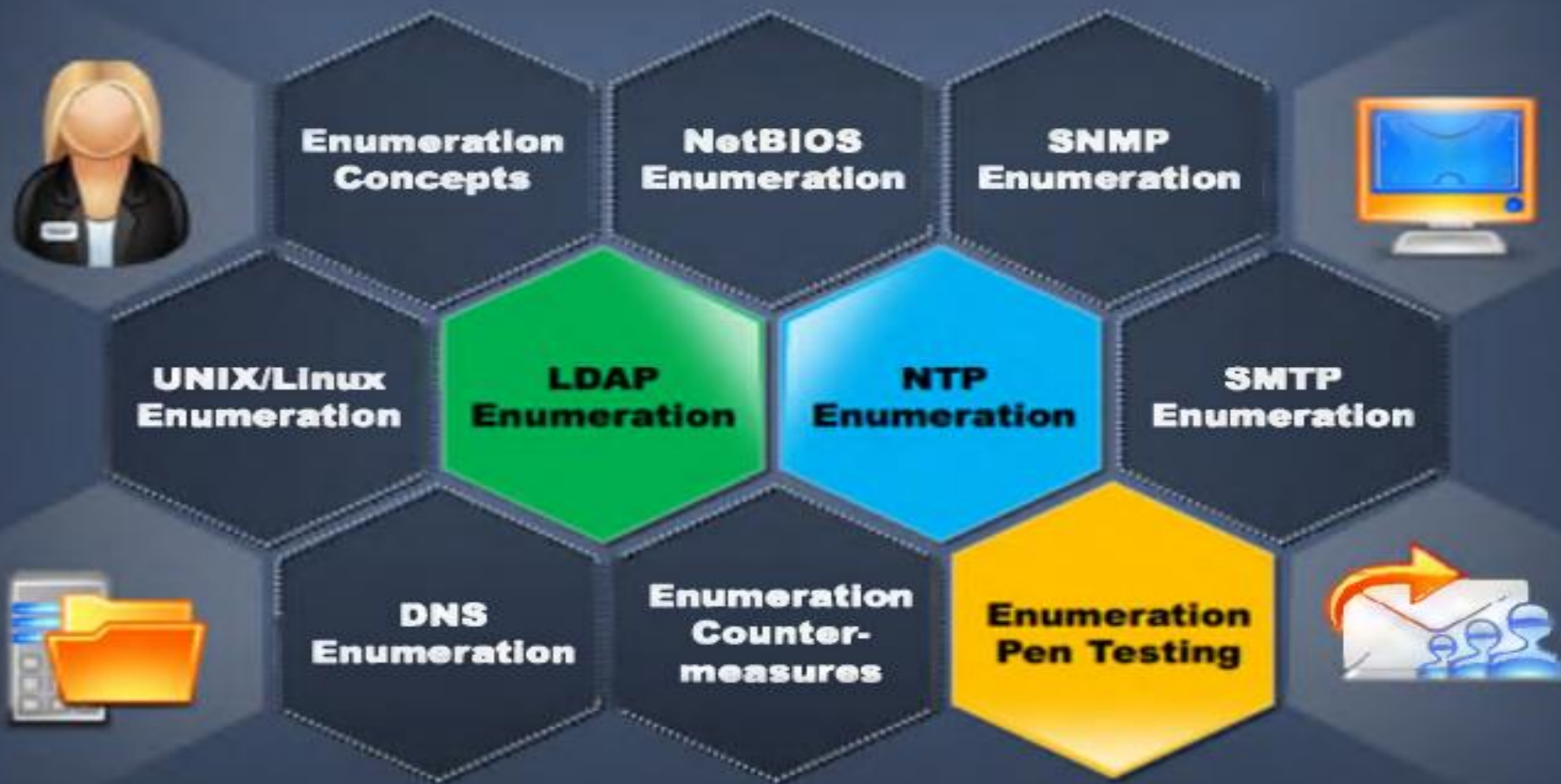


SMB Enumeration Countermeasures

Disabling SMB



Module **Flow**



Enumeration **Pen Testing**



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



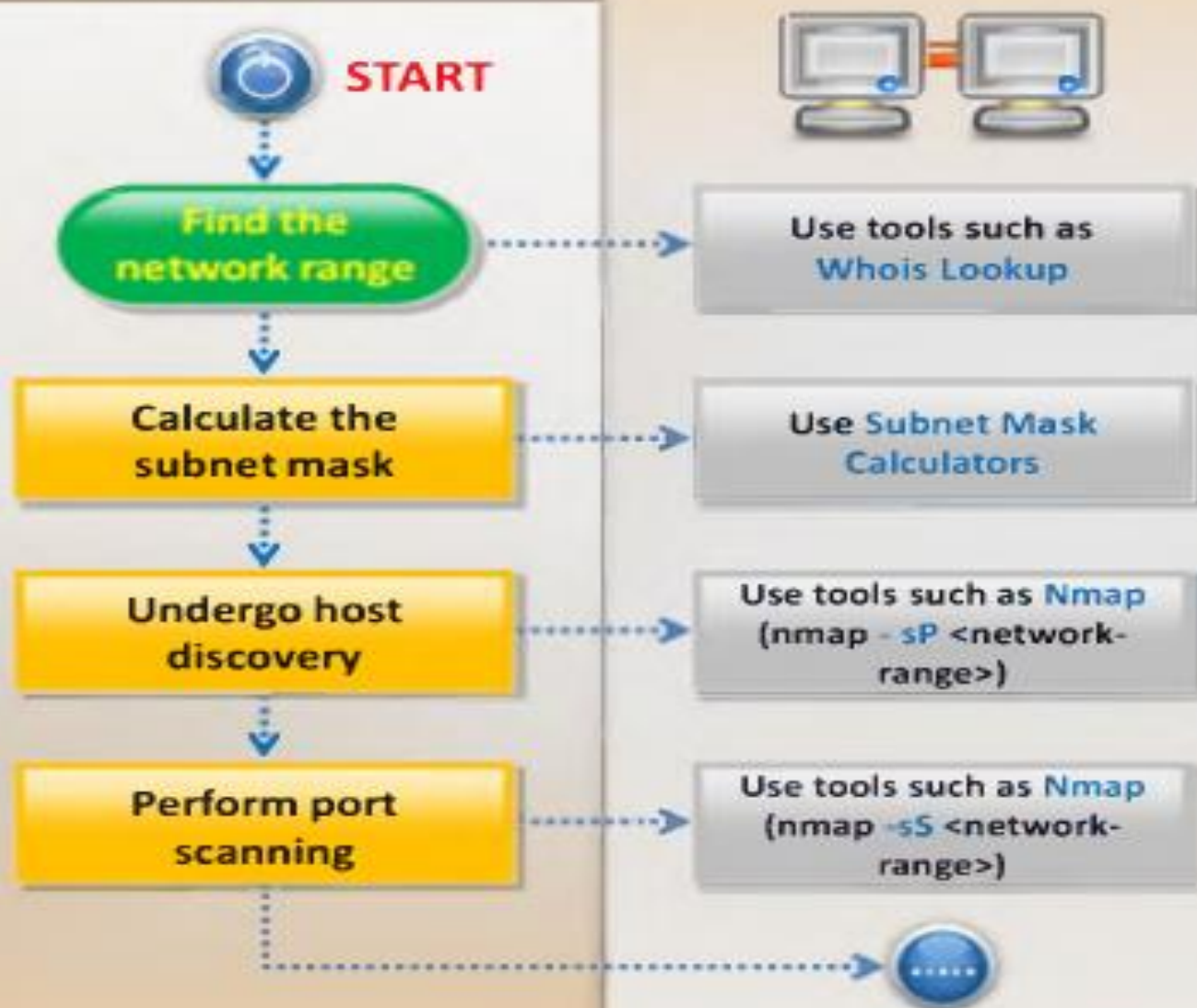
The information can be **users and groups**, **network resources and shares**, and **applications**



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

Enumeration Pen Testing

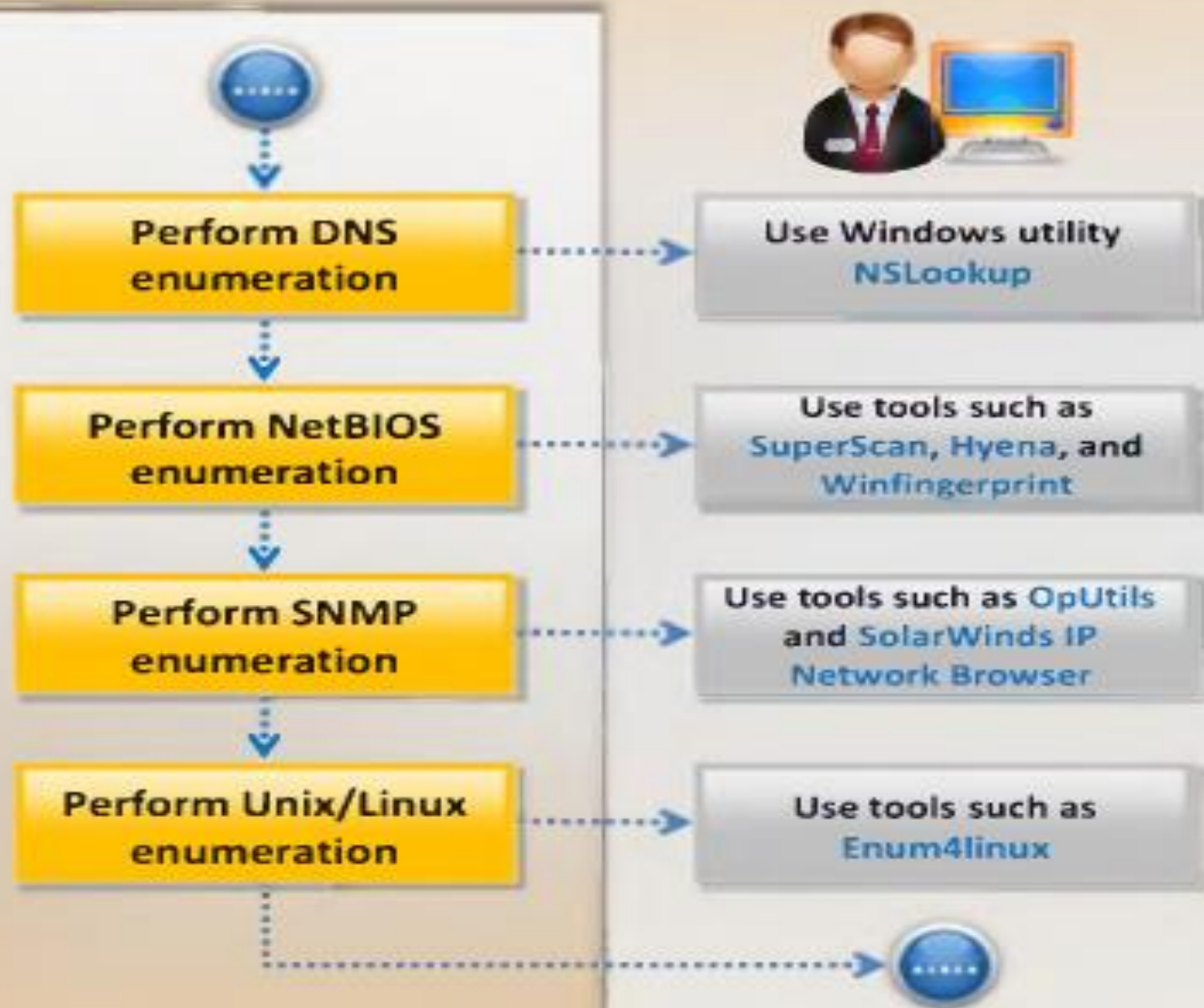
(Cont'd)



- 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)



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