

# 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



Extract user names  
using email IDs

01

02

Extract information using  
the **default passwords**



Extract user names  
using **SNMP**

03

04

Brute force **Active Directory**



Extract **user groups**  
from Windows

05

06

Extract information using  
**DNS Zone Transfer**





# Services and Ports to Enumerate



## TCP/UDP 53

DNS Zone Transfer



## UDP 161

Simple Network Management protocol (SNMP)



## TCP/UDP 135

Microsoft RPC Endpoint Mapper



## TCP/UDP 389

Lightweight Directory Access Protocol (LDAP)



## UDP 137

NetBIOS Name Service (NBNS)



## TCP/UDP 3268

Global Catalog Service



## TCP 139

NetBIOS Session Service (SMB over NetBIOS)



## TCP 25

Simple Mail Transfer Protocol (SMTP)



## TCP/UDP 445

SMB over TCP (Direct Host)



## 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 16<sup>th</sup> 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 "**nbtstat.exe -c**" to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses

```
C:\Windows\system32\cmd.exe
C:\Users>nbtstat -c
Ethernet:
Node IpAddress: {10.0.2.15} Scope Id: {}

NetBIOS Remote Cache Name Table

Name                Type                Host Address        Life [sec]
-----
<20>                UNIQUE              10.0.2.15            572
C:\Users>
```



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

```
C:\Windows\system32\cmd.exe
C:\Users>nbtstat.exe -a 192.168.1.1
Ethernet:
Node IpAddress: {10.0.2.15} Scope Id: {}

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
<00>                UNIQUE              Registered
<00>                GROUP              Registered
<1C>                GROUP              Registered
<20>                UNIQUE              Registered
<1B>                UNIQUE              Registered
MAC Address = 08 00 2B 01 01 05
```

<http://technet.microsoft.com>



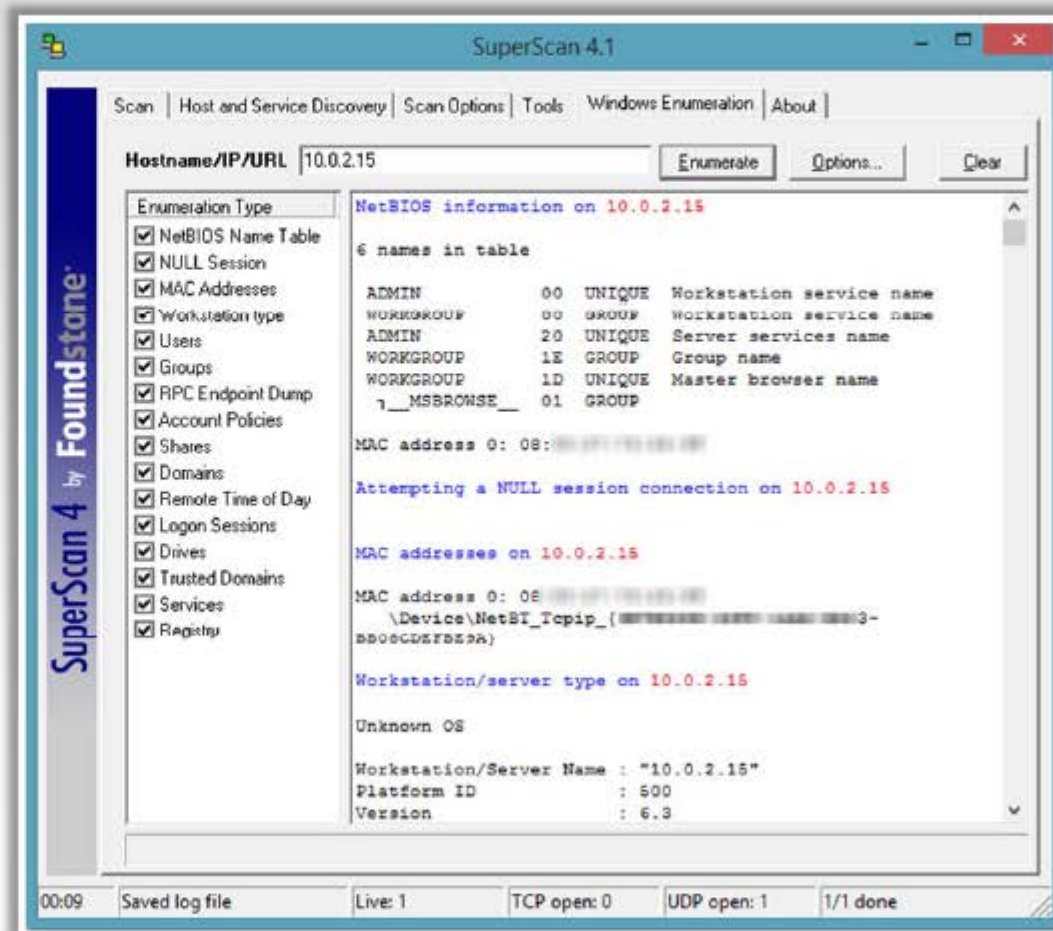
# NetBIOS Enumeration Tool: SuperScan

**CEH**  
Certified Ethical Hacker

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

**CEH**  
Certified Ethical Hacker

- 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.



**Hyena**

Services on \\ADMIN

Name	Display Name	Status	Type	Startup	Account	Dependencies	Executable
AelLookupSvc	Application Experience	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\sys...
ALG	Application Layer Gateway Ser...	Stopped	Service (Own Process)	Manual	NT AUTHORITY\LocalS...		C:\Windows\Sys...
AllUserInstallAgent	Windows All-User Install Agent	Stopped	Service (Shared Process)	Disabled	LocalSystem		C:\Windows\Sys...
AppIDSvc	Application Identity	Stopped	Service (Shared Process)	Manual	NT Authority\LocalServ...	RPCSS	C:\Windows\Sys...
AppInfo	Application Information	Running	Service (Shared Process)	Manual	LocalSystem	RpcSs;ProfSvc	C:\Windows\sys...
AppMgmt	Application Management	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\sys...
AppReadiness	App Readiness	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\Sys...
AppXSvc	AppX Deployment Service (Ap...	Stopped	Service (Shared Process)	Manual	LocalSystem	rpcss	C:\Windows\Sys...
aspnet_state	ASP.NET State Service	Stopped	Service (Own Process)	Manual	NT AUTHORITY\Netwo...		C:\Windows\Mi...
AudioEndpointB...	Windows Audio Endpoint Buil...	Running	Service (Shared Process)	Automatic	LocalSystem		C:\Windows\Sys...
AudioSrv	Windows Audio	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LocalS...	AudioEndpointBuilder;R...	C:\Windows\Sys...
AxinstSV	ActiveX Installer (AxinstSV)	Stopped	Service (Shared Process)	Manual	LocalSystem	rpcss	C:\Windows\sys...
BDESVC	BitLocker Drive Encryption Ser...	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\Sys...
BFE	Base Filtering Engine	Running	Service (Shared Process)	Automatic	NT AUTHORITY\LocalS...	RpcSs;WfpLwf	C:\Windows\sys...
BITS	Background Intelligent Transfe...	Running	Service (Shared Process)	Automatic (D...	LocalSystem	RpcSs;EventSystem	C:\Windows\Sys...
BrokerInfrastruct...	Background Tasks Infrastructu...	Running	Service (Shared Process)	Automatic	LocalSystem	RpcEptMapper;DcomLa...	C:\Windows\sys...
Browser	Computer Browser	Running	Service (Shared Process)	Manual	LocalSystem	LanmanWorkstation;La...	C:\Windows\Sys...
bluetooth	Bluetooth Support Service	Stopped	Service (Shared Process)	Manual	NT AUTHORITY\LocalS...		C:\Windows\sys...
CertPropSvc	Certificate Propagation	Stopped	Service (Shared Process)	Manual	LocalSystem	RPCSS	C:\Windows\sys...
COMSysApp	COM+ System Application	Stopped	Service (Own Process)	Manual	LocalSystem	RpcSs;EventSystem;SENS	C:\Windows\sys...
CryptSvc	Cryptographic Services	Running	Service (Shared Process)	Automatic	NT Authority\Network...	RpcSs	C:\Windows\Sys...
CscService	Offline Files	Stopped	Service (Shared Process)	Manual	LocalSystem	RpcSs	C:\Windows\Sys...
DcomLaunch	DCOM Server Process Launcher	Running	Service (Shared Process)	Automatic	LocalSystem		C:\Windows\sys...
DealplyLive	DealPly Live Service (dealplylive)	Stopped	Service (Own Process)	Automatic (D...	LocalSystem	RPCSS	C:\Program File...
DealplyLive	DealPly Live Service (dealplyliv...	Stopped	Service (Own Process)	Manual	LocalSystem	RPCSS	C:\Program File...
defragvsc	Optimize drives	Stopped	Service (Own Process)	Manual	LocalSystem	RPCSS	C:\Windows\sys...
DeviceAssociation...	Device Association Service	Running	Service (Shared Process)	Manual	LocalSystem		C:\Windows\sys...
DeviceInstall	Device Install Service	Stopped	Service (Shared Process)	Manual	LocalSystem		C:\Windows\sys...
Dhcp	DHCP Client	Running	Service (Shared Process)	Automatic	NT Authority\LocalServ...	NSI;TdxAfd	C:\Windows\sys...

http://www.systemtools.com Last object clicked: 'AppInfo' - [1] selected object(s) 1 / 176 objects NUM

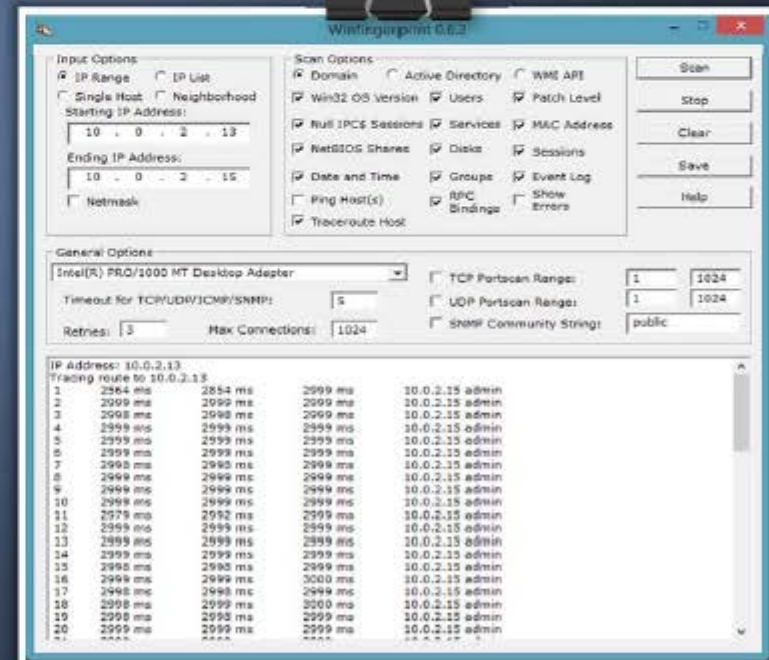
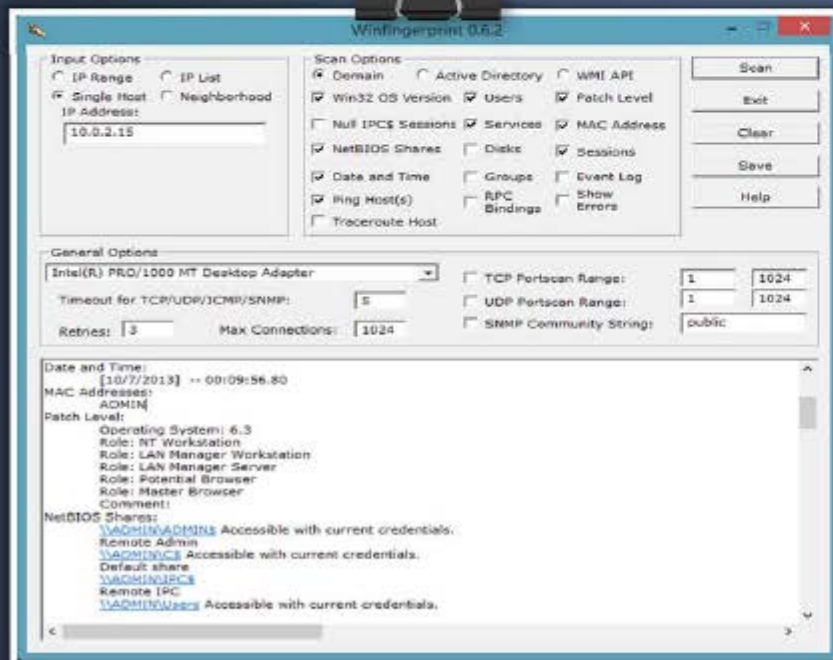
<http://www.systemtools.com>



# 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



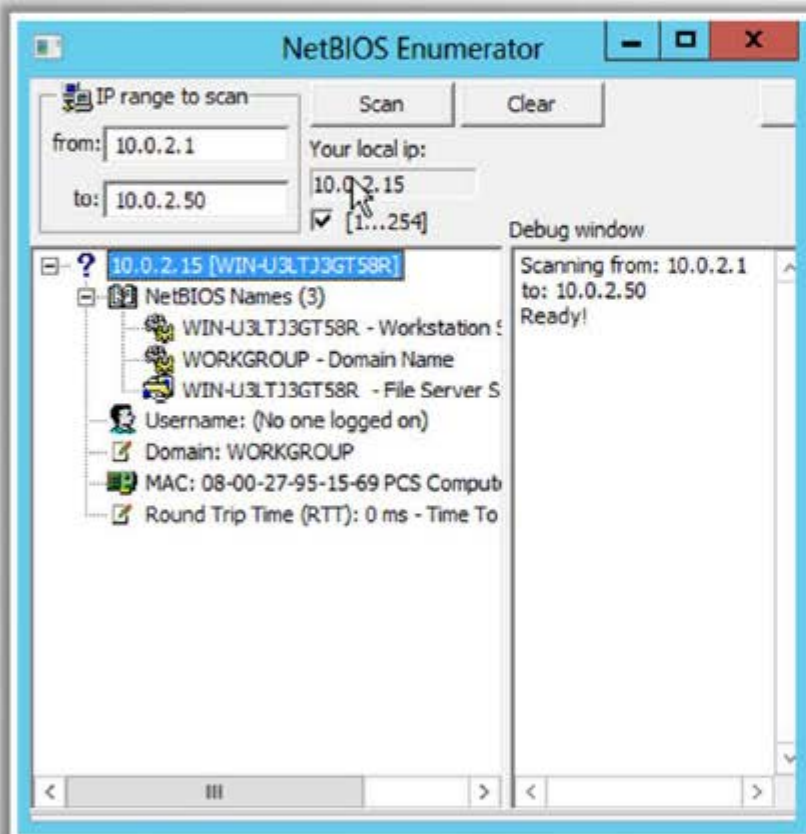
<http://www.winfingerprint.com>



# NetBIOS Enumeration Tools: NetBIOS Enumerator and Nsauditor Network Security Auditor

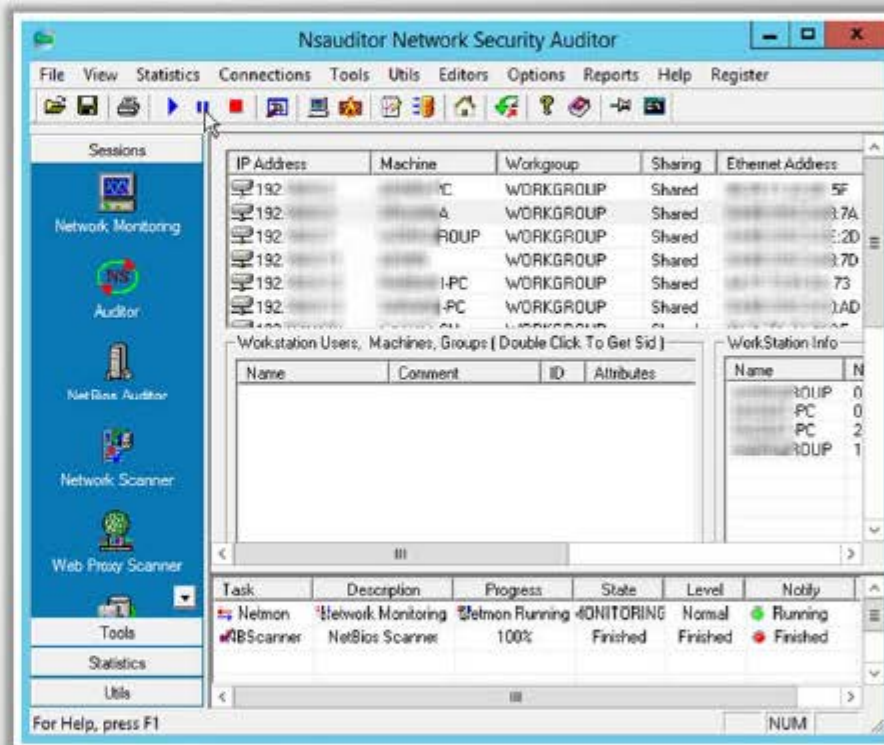


## NetBIOS Enumerator



<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>`



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\...>net view \\10.0.2.15
Shared resources at \\10.0.2.15

Share name  Type  Used as  Comment
-----
Users       Disk
The command completed successfully.

C:\Users\...>
```



# 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

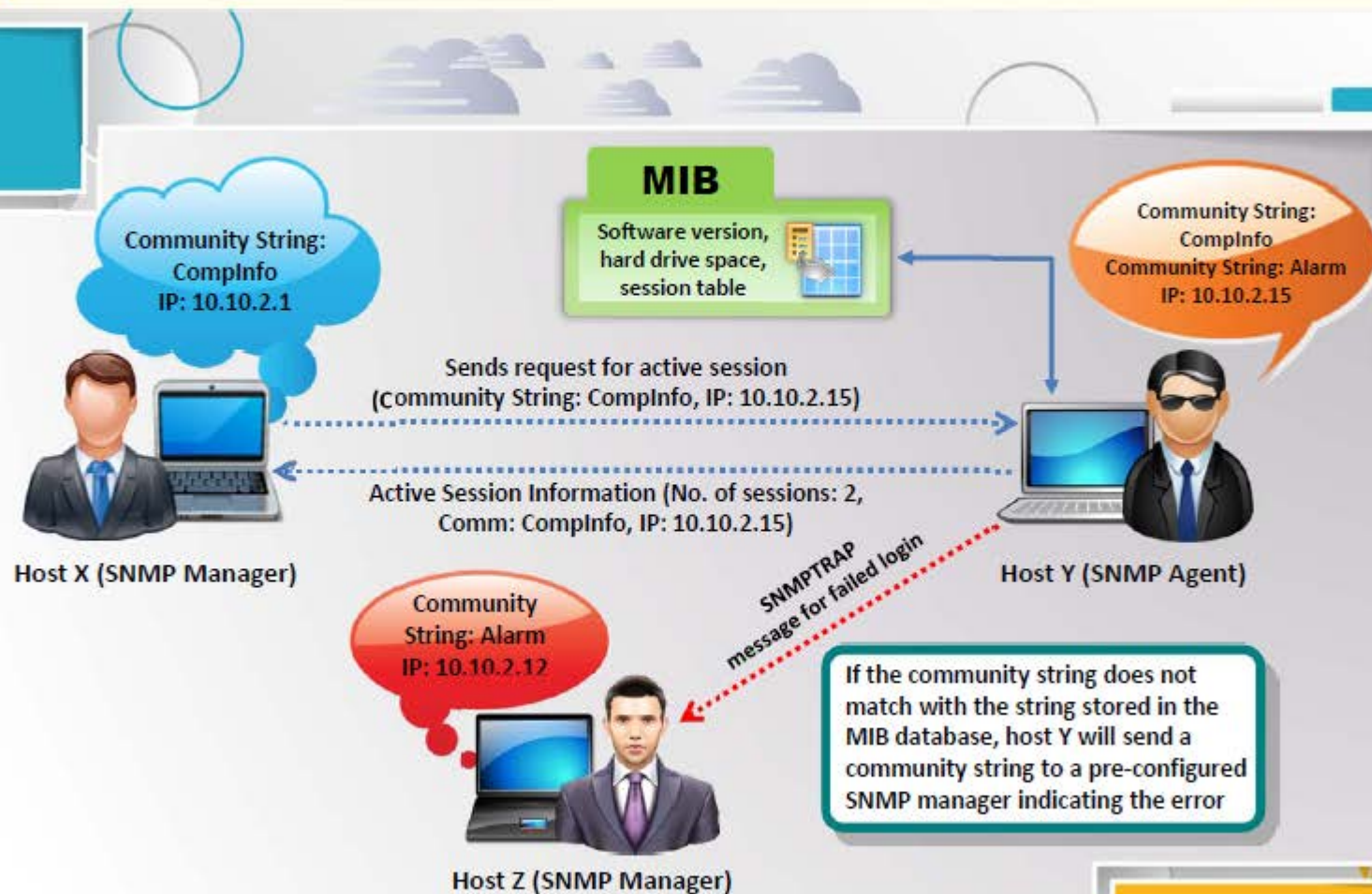


- Attacker uses these **default community strings** to extract information about a device
- Attackers enumerate SNMP to extract information about **network resources** such as hosts, routers, devices, shares, etc. and **network information** such as ARP tables, routing tables, traffic, etc.





# 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



The screenshot displays the ManageEngine OpUtils 6 web interface. The top navigation bar includes links for Home, Switch Port Mapper, IP Address Manager, Request Detection, MAC IP List, Tools, Reports, Admin, and Support. Below this, a secondary navigation bar shows Diagnostic Tools, Address Monitoring, Network Monitoring, SNMP Tools, CISCO Tools, and Custom Tools. The main content area is titled 'SNMP Scan' and features a form for adding IP ranges or lists. Below the form, a table displays the results of a scan, showing IP addresses, DNS names, response times, system types, and their status.

IP Address	DNS Name	Resp Time	System Type	Status
192.168.111.1	ff-switch-3400.india.adventnet.com	4203 ms		Non SNMP Node
192.168.111.2	Not able to resolve	8719 ms		Non SNMP Node
192.168.111.3	ff-switch1-2848.india.adventnet.com	4219 ms		Non SNMP Node
192.168.111.4	ff-switch3-2848.india.adventnet.com	Request Timeout		System not alive
192.168.111.8	dns-slave2.india.adventnet.com	Request Timeout		System not alive
192.168.111.6	ff-switch3-2848.india.adventnet.com	4203 ms		Non SNMP Node
192.168.111.7	ff-switch4-2848.india.adventnet.com	4219 ms		Non SNMP Node
192.168.111.8	ff-switch5-2848.india.adventnet.com	4235 ms		Non SNMP Node
192.168.111.9	finance-printer.india.adventnet.com	15 ms	HP Printer	SNMP Node
192.168.111.10	sputnik.india.adventnet.com	31 ms	HP Printer	SNMP Node
192.168.111.11	discoep-f12.india.adventnet.com	4156 ms		Non SNMP Node
192.168.111.12	Unknown Host	Request Timeout		System does not exist
192.168.111.13	nomadixep.india.adventnet.com	Request Timeout		System not alive
192.168.111.14	edy-a2pc-spl-1.india.adventnet.com	Request Timeout		System not alive

<http://www.manageengine.com>



# SNMP Enumeration Tool: Engineer's Toolset

**CEH**  
Certified Ethical Hacker

The screenshot displays the 'Engineer's Toolset' application window. The title bar reads 'Engineer's Toolset'. The menu bar includes: Start, Export, Print, Copy, Copy, Stop, Zoom, Ping, Telnet, Trace, Config, Surf, Settings, and Help. The main window shows a tree view on the left with categories like System MIB, Interfaces, Cards, and IOS. The right pane displays the output of a scan for '199.1.1 : Tex-2821.tex'. The output includes details about the Cisco 2821 router, its IOS version (12.4(9)T3), and a list of discovered IP addresses under the 'Routes' section.

**199.1.1 : Tex-2821.tex**  
Cisco 2821 : Cisco 2800 series router with one Network Module slot, one EVH,  
Community String: public  
System MIB  
Interfaces  
Cards  
IOS  
Bootstrap Rom: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1) Technical Support: <http://www.cisco.com/techsup>  
ROM IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3) Technical  
Running IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3) Techn  
Current config register: 0x2102  
Config register on next reload: 0x2102  
Reason for last reload: power-on  
Last Boot: 11/19/2011 8:35:17 AM  
Processor RAM: 244 MB  
Free Processor RAM: 125 MB  
Non-volatile memory: 240 K bytes  
Non-volatile memory used: 18.5 K bytes  
Flash Memory  
Hub ports  
TCP/IP Networks  
IPX Network  
Routes  
0.0.0.0 : 0.0.0.0  
1.1.250.201 : 255.255.255.255  
10.199.1.0 : 255.255.255.0  
10.199.2.0 : 255.255.255.0  
10.199.2.0 : 255.255.255.0  
10.199.2.0 : 255.255.255.0

Perform network discovery on a single subnet or a range of subnets using ICMP and SNMP.

Display discovered devices in real time.

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

It scans a single IP, IP address range, or subnet and **displays network devices discovered in real time**

<http://www.solarwinds.com>



# SNMP Enumeration Tools

**CEH**  
Certified Ethical Hacker



## 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

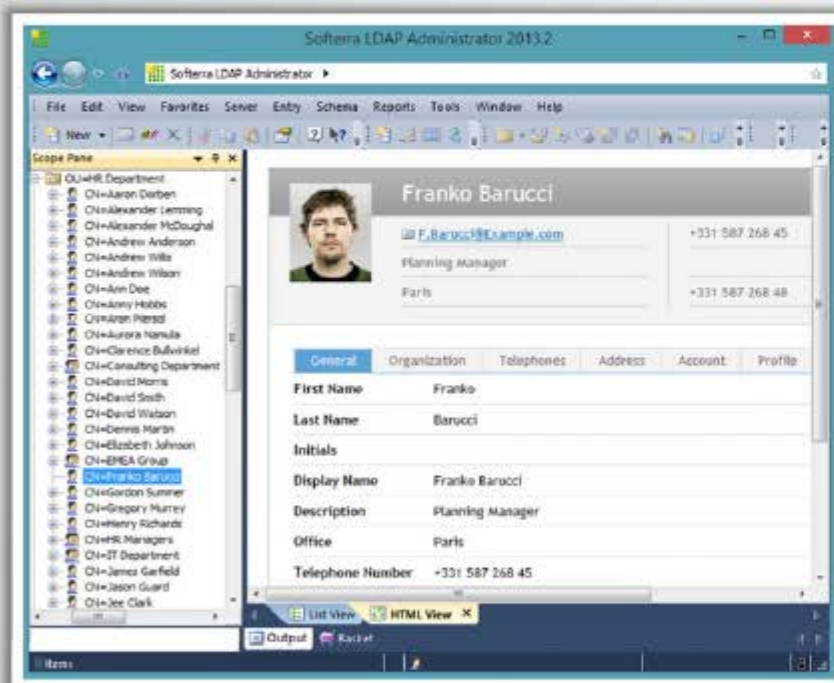




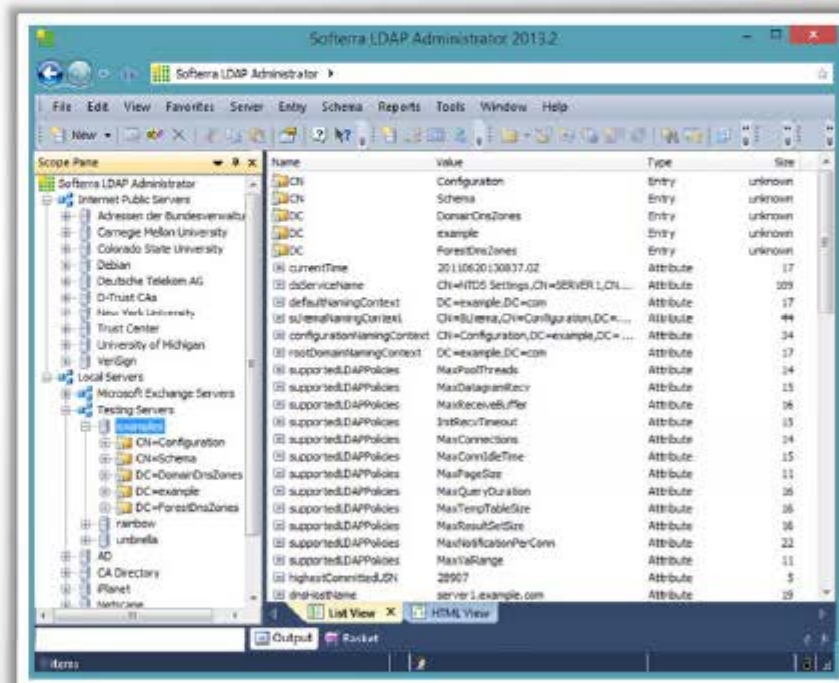
# LDAP Enumeration Tool: Softerra LDAP Administrator



## 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



**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 [ -vdm ] [ -r retries ] [ -t timeout ] [ server ]`

## ntpd

- Monitors operation of the NTP daemon, ntpd
- `/usr/bin/ntpd [-n] [-v] host1 [ IPAddress1...`

## ntpq

- Monitors NTP daemon ntpd operations and determines performance
- `ntpq [-inp] [-c command] [host] [...]`

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ntptrace  
localhost: stratum 3, offset 0.000000, synch distance 0.127189  
120.88.46.10: timed out, nothing received  
***Request timed out  
root@kali:~#
```

ntptrace

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ntpdc  
ntpdc> ?  
ntpdc commands:  
addpeer      controlkey  fudge      keytype     quit        timeout  
addrefclock  cllstate    help       listpeers   readkeys    tierstate  
addserver    debug       host       loopinfo    requestkey  traps  
addrtrap     delay       hostnames  monstats    reset       trustedkey  
authinfo     delrestrict ifreload   monlist     restrict    unconfig  
broadcast    disable     ifstats    passwd      restrict    unrestrict  
clkbug       dpeers      iostats    peers       showpeer    untrustedkey  
clockstat    enable      kerninfo   preset      sysinfo     version  
clitrap      exit        keyid      pstats      sysstats  
ntpdc> monlist  
remote address      port local address      count m ver rstr avgint  lstat  
-----  
web10.hnshosting.com 123 10.0.0.13             15 4 4 1d0 35 19  
113.38.137.34         123 10.0.0.13             16 4 4 1d0 33 28  
120-88-47-10.infra.hns 123 10.0.0.13             15 4 4 1d0 35 59  
123.180.200.163       123 10.0.0.13             15 4 4 1d0 35 64  
ntpdc>
```

ntpdc: monlist query

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ntpq  
ntpq> ?  
ntpq commands:  
lconfig      delay      nreadvar   readlist  
addvars      exit       nrl         readvar  
associations help       arv         rl  
authenticate host       ntpversion  rvars  
cl            hostnames opeers      rvc  
clearvars    keyid      passassociations saveconfig  
clockvar     keytype    passwd      showvars  
config-from-file lpeers     peers       timeout  
cooked       lpassociations poll         version  
cv            lpeers     pstatus     writelist  
debug        nreadlist  raw         writevar  
ntpq> readlist  
associd=0 status=0615 leap=none, sync_ntp, 1 event, clock sync,  
version="ntpd 4.2.6p501.2349-o Sat May 12 09:07:10 UTC 2012 (1)",  
processor="i686", system="Linux/3.7-trunk-686-pae", leap=00, stratum=3,  
precision=10, rootdelay=100.200, rootdisp=146.761, rofid=120.88.46.10,  
refid=05c2e57c.09f048e7 Thu Mar 16 2014 17:45:56.370,  
clock=05c2e57f.c4a29452 Thu Mar 16 2014 17:45:59.760, peer=23300, tc=7,  
mintc=3, offset=-21.582, frequency=2.766, sys_jitter=4.451,  
clk_jitter=11.664, clk_wander=4.352  
ntpq>
```

ntpq: readlist query



# NTP Enumeration Tools



**NTP Server Scanner**

<http://www.bytefusion.com>



**PresenTense NTP Auditor**

<http://www.bytefusion.com>



**Nmap**

<http://nmap.org>



**PresenTense Time Server**

<http://www.bytefusion.com>



**Wireshark**

<http://www.wireshark.org>



**PresenTense Time Client**

<http://www.bytefusion.com>



**AtomSync**

<http://www.atomsync.com>



**NTP Time Server Monitor**

<http://www.meinbergglobal.com>



**NTPQuery**

<http://www.bytefusion.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

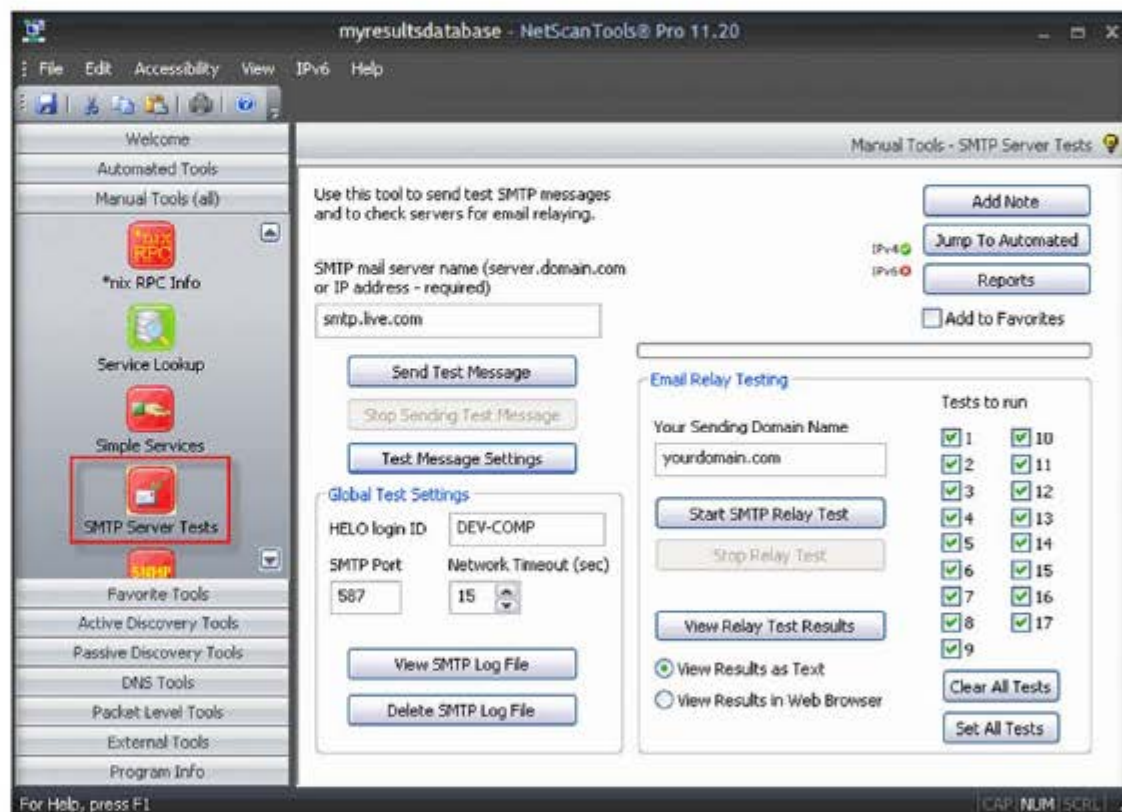
```
$ telnet1 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder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



# SMTP 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>

## Telnet

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

## 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

```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>telnet 10.10.0.3 25
Trying 10.10.0.3...
Connected to 10.10.0.3.
Escape character is '^]'.
220 myhost ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 myhost Hello [10.10.0.99] pleased to meet you
VRFY root
250 Super-User <root@myhost>
VRFY blah
550 blah... User unknown
```



# 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)

## 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**

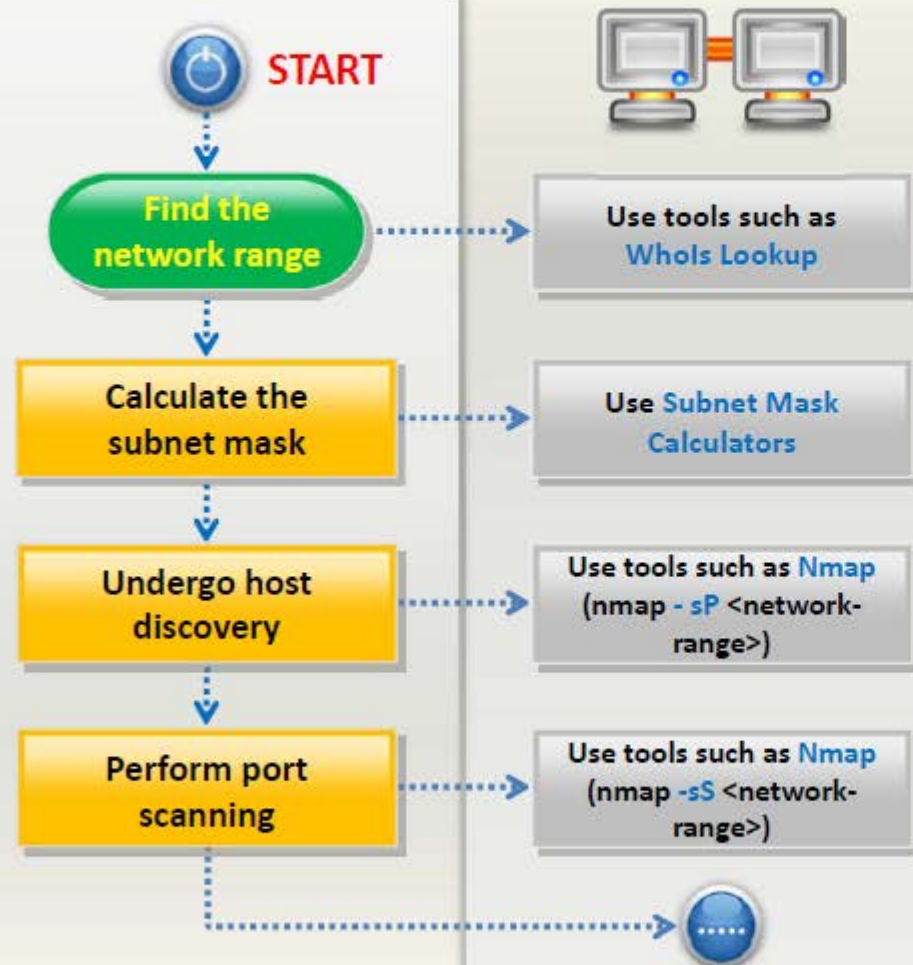


Used in combination with **data collected in the reconnaissance phase**



# Enumeration Pen Testing

(Cont'd)

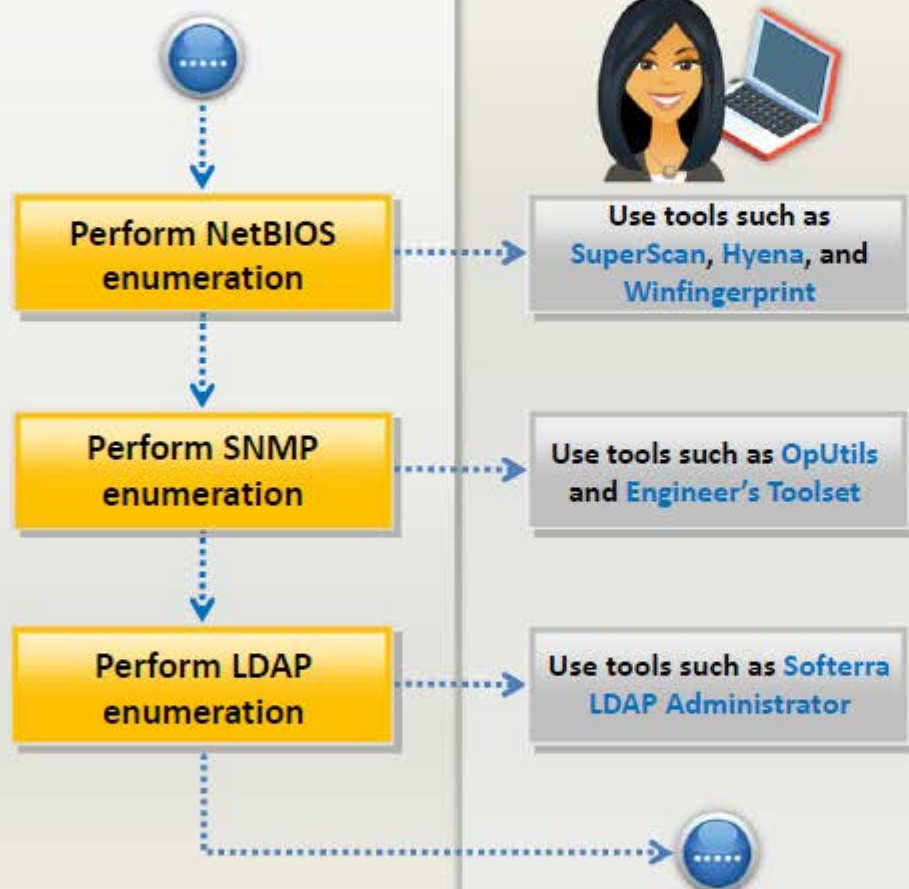


- In order to enumerate important servers, find the network range using tools such as **Whois Lookup**
- Calculate the subnet mask required for the IP range using **Subnet Mask Calculators**, that can be given as an input to many of the ping sweep and port scanning tools
- Find the servers connected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



Perform NTP enumeration

Use commands such as **ntptrace**, **ntpd**, 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**, **ntpd**, 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