



Certified | Ethical Hacker

Module 04

# Enumeration

# Module Objectives



- Understanding Enumeration Concepts
- Understanding Different Techniques for NetBIOS Enumeration
- Understanding Different Techniques for SNMP Enumeration
- Understanding Different Techniques for LDAP and NTP Enumeration
- Understanding Different Techniques for SMTP and DNS Enumeration
- Understanding Other Enumerations such as IPsec, VoIP, RPC, and Linux/Unix enumeration
- Understanding Different Enumeration Countermeasures
- Overview of Enumeration Pen Testing

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

Enumeration  
Pen Testing

# What is Enumeration?

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

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

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

## Information Enumerated by Intruders



Network resources



Network shares



Routing tables



Audit and service settings



SNMP and FQDN details



Machine names



Users and groups



Applications and banners

# Techniques for Enumeration



Extract user names using  
email IDs

01



Extract information using  
default passwords

02



Brute force Active Directory

03



Extract information using  
DNS Zone Transfer

04



Extract user groups from  
Windows

05



06

Extract user names using  
SNMP

# Services and Ports to Enumerate

**TCP/UDP 53**

Domain Name System (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

**UDP 500**

ISAKMP/Internet Key Exchange (IKE)

**TCP/UDP 5060, 5061**

Session Initiation Protocol (SIP)

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

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 the 16<sup>th</sup> 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 in 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 Primary domain controller (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



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

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator\ nbtstat -c
Ethernet0:
Node IpAddress: (10.10.10.12) Scope Id: []
NetBIOS Remote Cache Name Table
Name          Type      Host Address   Life [sec]
WIN-H3DMM9IIRR?C<20>  UNIQUE    10.10.10.12  538
```

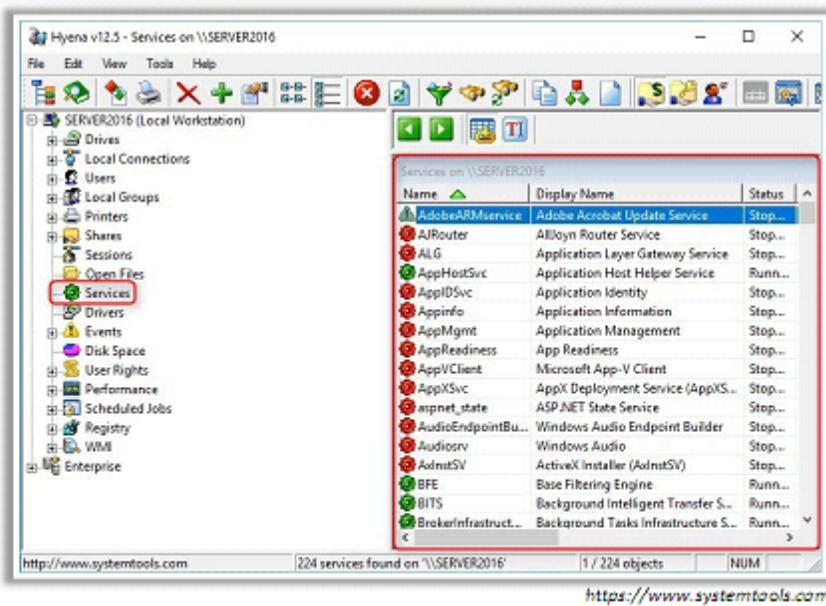
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator\ nbtstat -a 10.10.10.12
Ethernet0:
Node IpAddress: (10.10.10.12) Scope Id: []
NetBIOS Remote Machine Name Table
Name          Type      Status
WIN-      R2C<00>  UNIQUE  Registered
CEH      <00>    GROUP   Registered
CEH      <1C>    GROUP   Registered
WIN-      R2C<20>  UNIQUE  Registered
CEH      <1B>    UNIQUE  Registered
MAC Address =  -50
```

<https://technet.microsoft.com>

# NetBIOS Enumeration Tools

## 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.



**Nsauditor Network Security Auditor**  
<https://www.nsauditor.com>



**NetScanTools Pro**  
<https://www.netscan.tools.com>



**SoftPerfect Network Scanner**  
<https://www.softperfect.com>



**SuperScan**  
<https://www.mcafee.com>



**NetBIOS Enumerator**  
<http://nbtenum.sourceforge.net>

# Enumerating User Accounts

- Enumerating user accounts using **PsTools** suite helps to control and manage remote systems from the command line

**PsExec** - execute processes remotely

**PsFile** - shows files opened remotely

**PsGetSid** - display the SID of a computer or a user

**PsKill** - kill processes by name or process ID

**PsInfo** - list information about a system

**PsList** - list detailed information about processes

**PsLoggedOn** - see who's logged on locally and via resource sharing

**PsLogList** - dump event log records

**PsPasswd** - changes account passwords

**PsShutdown** - shuts down and optionally reboots a computer

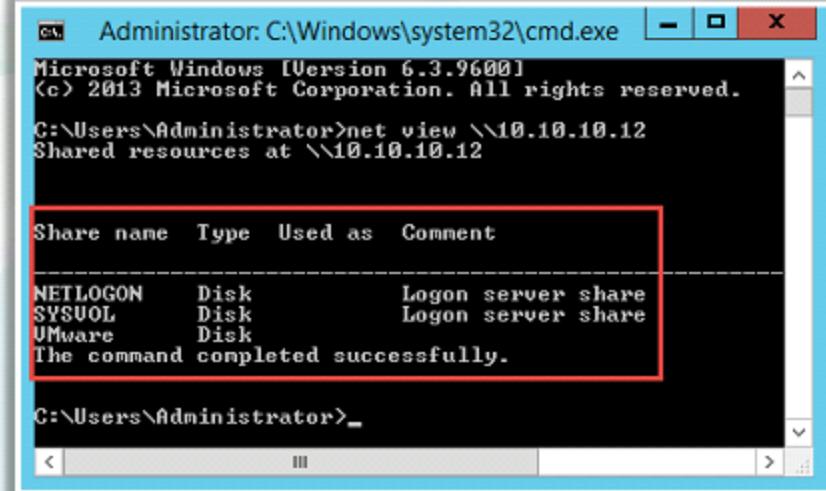
<https://docs.microsoft.com>

# 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>



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net view \\10.10.10.12
Shared resources at \\10.10.10.12

Share name Type Used as Comment
NETLOGON Disk Logon server share
SYSVOL Disk Logon server share
UWare Disk
The command completed successfully.

C:\Users\Administrator>
```

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

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



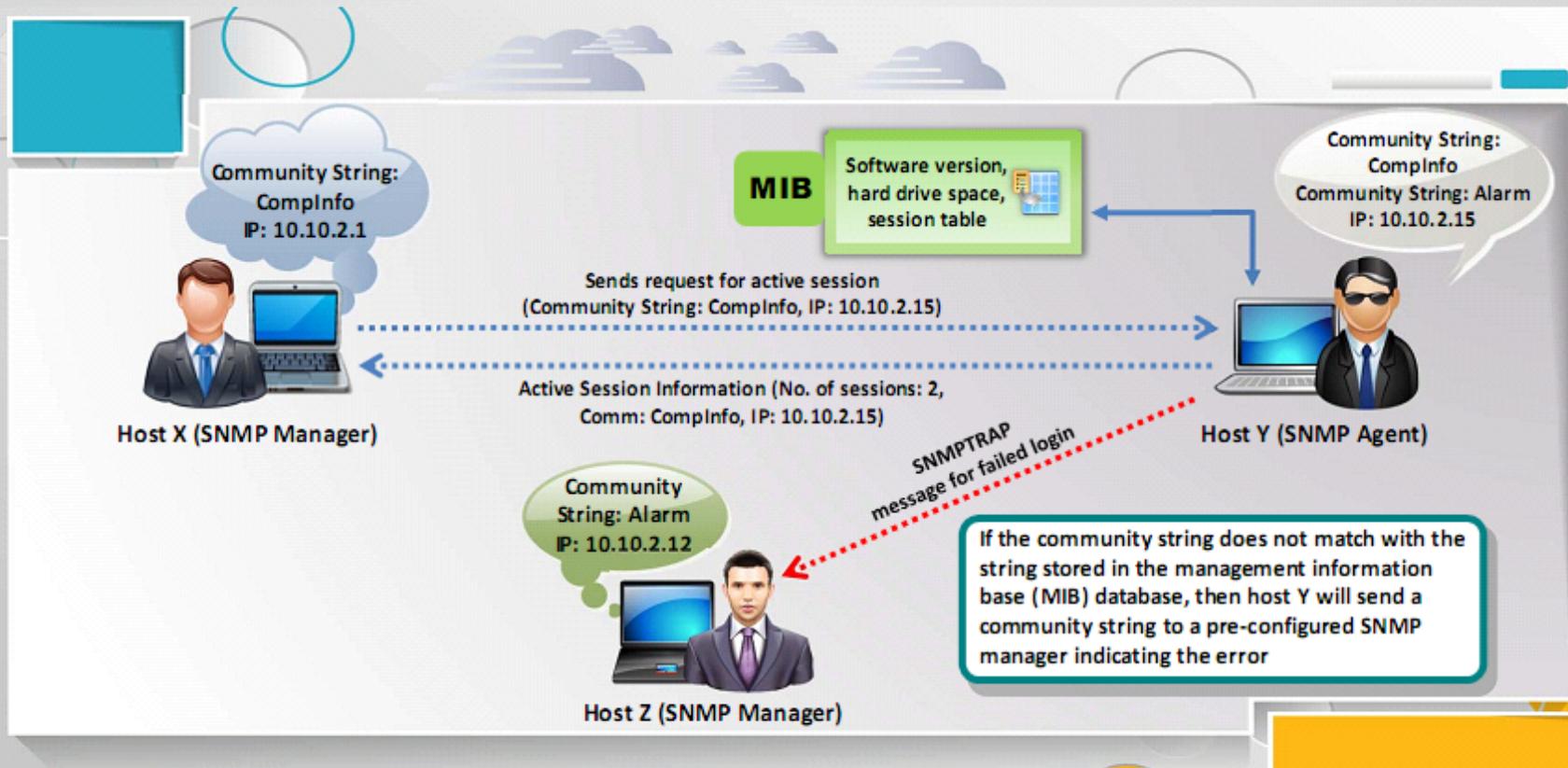
- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
  - **Read community string:** It is public by default; allows viewing of device/system configuration
  - **Read/write community string:** It is private by default; allows remote editing of configuration



- 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)

- O MIB is a virtual database containing **formal description of all the network objects** that can be managed using SNMP 
- O The MIB database is hierarchical and each managed object in a MIB is addressed through **Object Identifiers (OIDs)** 
- O 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**
- O 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 
- O SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the **OID numbers** into a **human-readable** display 

# SNMP Enumeration Tools

## OpUtils

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

The screenshot shows the OpUtils interface with the following details:

- Header:** Home, Switch Port Mapper, IP Address Manager, Rogue Detection, MAC IP Link, Tools, Reports, Advice, Support, Alerts [612].
- Sub-Header:** Diagnostic Tools, Address Monitoring, Network Monitoring, Show Tools, CISCO Tools, Custom Tools, E-Mail, Export, Print.
- Section:** SNMP Scan.
- Form:** Add IP Range, Add IP List, Direct CSV. Starting IP: 192.168.31.0, Ending IP: \_\_\_\_\_, Scan, Stop.
- Table:** Shows a list of discovered devices:
 

IP Address	DNS Name	Keep Time	System Type	Status
192.168.111.1	ffwrd-3149.india.advenet.com	4203 ms	■ Non-SNMP Node	
192.168.111.2	Not able to resolve	8779 ms	■ Non-SNMP Node	
192.168.111.3	ffwrd-0-2848.india.advenet.com	4219 ms	■ Non-SNMP Node	
192.168.111.4	ffwrd-0-2849.india.advenet.com	Request Timeout	■ System not alive	
192.168.111.5	drivesrv2.india.advenet.net	Request Timeout	■ System not alive	
192.168.111.6	ffwrd-0-2848.india.advenet.com	4203 ms	■ Non-SNMP Node	
192.168.111.7	ffwrd-4-2848.india.advenet.com	4219 ms	■ Non-SNMP Node	
192.168.111.8	ffwrd-0-2848.india.advenet.com	4235 ms	■ Non-SNMP Node	
192.168.111.9	finance-printer.india.advenet.com	19 ms	HP Printer	■ SNMP Node
192.168.111.10	spurnl.india.advenet.com	31 ms	HP Printer	■ SNMP Node
192.168.111.11	cisco-pf2.india.advenet.com	4156 ms	■ Non-SNMP Node	
192.168.111.12	Unknown host	Request Timeout	■ System does not exist	
192.168.111.13	monmedip.india.advenet.com	Request Timeout	■ System not alive	
192.168.111.14	svr02.india-advenet.com	Request Timeout	■ System not alive	

<https://www.manageengine.com>

## Engineer's Toolset

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

The screenshot shows the Engineer's Toolset interface with the following details:

- Header:** New, Restart, Export, Print, Copy, Stop, Zoom, Ping, Telnet, Trace, Config, Surf, Settings, Help.
- Section:** 10.159.2.1 : Tex-2811.vmx Cisco 2811 : Cisco 2800 series router with one Network Module slot, one ISDN, one VTY port.
- Tree View:**
  - Community String: public
  - Interfaces
  - Cards
  - ICG
  - Bootstrap Rom: System Bootstrap, Version 12.4(18r1T), RELEASE SOFTWARE [fc1] Technical Support: <http://www.cisco.com/techsup>
  - ROM IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICES3-M), Version 12.4(3)T3, RELEASE SOFTWARE [fc2] Technical Support: <http://www.cisco.com/techsup>
  - Running IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICES3-M), Version 12.4(3)T3, RELEASE SOFTWARE [fc3] Technical Support: <http://www.cisco.com/techsup>
  - Current config register: 0x2102
  - Config register on next reload: 0x2102
  - Reason for last reload: powered-on
  - Last Boot: 11/19/2011 0:25:17 AM
  - Processor RAM: 244 MB
  - Free Processor RAM: 126 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
 

Network	Mask	Gateway
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	
10.199.7.0	255.255.255.0	
- Callout:** Perform network discovery on a single subnet or a range of subnets using ICMP and SNMP.
- Callout:** Display discovered devices in real time.

<http://www.solarwinds.com>

# SNMP Enumeration Tools (Cont'd)



**Nsauditor Network Security Auditor**  
<https://www.nsauditor.com>



**Spiceworks Network Monitor**  
<https://www.spiceworks.com>



**NetScanTools Pro**  
<https://www.netscantools.com>



**SoftPerfect Network Scanner**  
<https://www.softperfect.com>



**Network Performance Monitor**  
<http://www.solarwinds.com>



**SNMP Informant**  
<https://www.snmp-informant.com>



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



**iReasoning MIB Browser**  
<http://ireasoning.com>



**SNScan**  
<https://www.mcafee.com>



**SNMPCHECK**  
<http://www.no think.org>

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

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 a LDAP session by connecting to a **Directory System Agent** (DSA) on TCP port 389 and then sends an operation request to the DSA



04

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



05

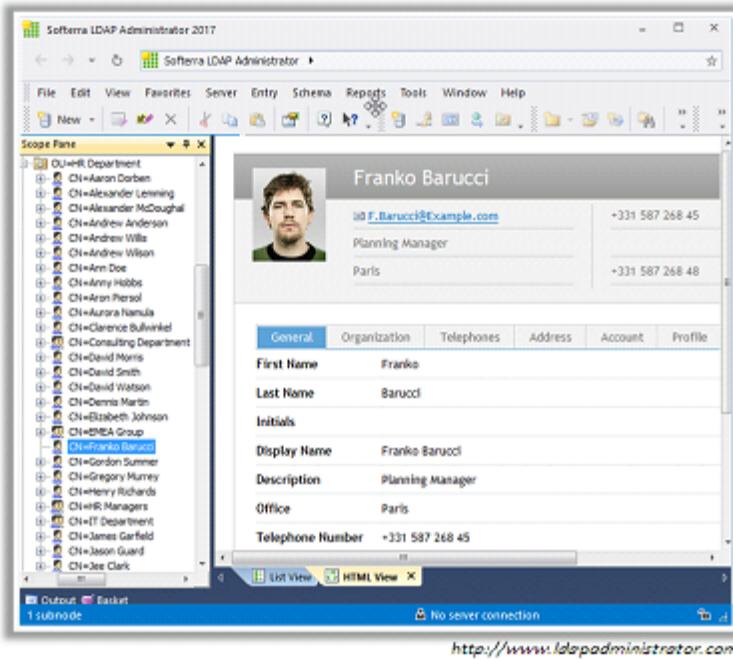
Attacker queries LDAP service to gather information such as **valid user names, addresses, departmental details**, etc. that can be further used to perform attacks



# LDAP Enumeration Tools

## Softerra LDAP Administrator

- Softerra LDAP Administrator provides a wide variety of features essential for **LDAP development, deployment, and administration of directories**



### LDAP Admin Tool

<https://wwwldapsoft.com>



### LDAP Account Manager

<https://wwwldap-account-manager.org>



### LDAP Search

<http://securityxploded.com>



### JXplorer

<http://wwwjxplorer.org>



### Active Directory Explorer

<https://docs.microsoft.com>

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

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 demilitarized zone (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
- `ntpdc [-ilnps] [-c command] [host] [...]`

## ntpq

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

```
root@kali:~#
root@kali:~# ntptrace
localhost: stratum 3, offset -0.003180, synch distance 0.286704
13.126.27.131: timed out, nothing received
***Request timed out
root@kali:~#
```

ntptrace

```
root@kali:~# ntpdc
ntpdc> ?
ntpdc commands:
addpeer    controlkey   fudge      keytype    quit      timeout
addrclock  ctlsstats   help       listpeers  requestkey traps
addserver  debug       host       loopinfo   requestkey timerstats
addtrap   delay        hostnames  monstats  reset     trustedkey
authinfo   delrestrict  ifreload  monlist   reslist   unconfig
broadcast  disable     ifstats   peers     restrict  unrestrict
clkbug    dmpeers     iostats   preset    showpeer untrustedkey
clockstat enable     kerninfo  pstats   sysinfo  version
clrtrap   exit        keyid    pstats   sysstats
ntpdc>
```

These ntpdc queries can be used to obtain additional NTP server information

ntpdc queries

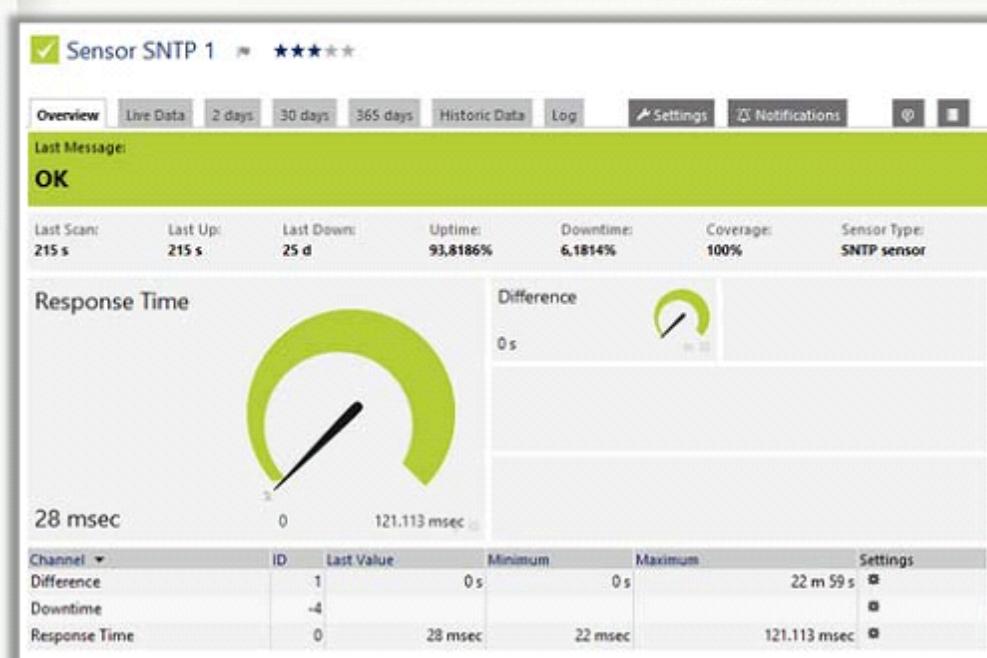
```
root@kali:~# ntpq
ntpq> ?
ntpq commands:
:config   drefid    breadlist   readvar
:odvvars  exit      rreadvar   reslist
:peers   help      mrl        rl
:associations host      mrulist   revars
:authenticat hostnames  mrv      rv
:authinfo   ifstats   ntpversion saveconfig
:cl      iostats   peers     showvars
:clearvars  kerninfo  passociations sysinfo
:clocklist keyid    passwd    sysstats
:clockvar  keytype   peers     timeout
:config-from-file lassociations poll     timerstats
:cooked   lpeers    pstats   version
:cv      lpassociations quit    writelist
:debug   lpeers    raw      writevar
:delay   monstats  readlist
ntpq> readlist
associd=0 status=b64 leap:none, sync_ntp, 1 event, freq_mode,
version="ntp4 4.2.8pl001.3728-o (1)", processor="x86_64",
system="Linux/4.13.0-kali1-amd64", leap=00, stratum=3, precision=-23,
rootdelay=69.138, rootdisp=104.945, refid=13.126.27.131,
reftime=de04523b.0851418 Sat, Jan 13 2018 4:39:07.032,
clock=d045264.fb595c2a Sat, Jan 13 2018 4:39:08.981, peer=29093, tc=6,
mintc=3, offset=-3.180400, frequency=0.000, sys_jitter=8.452883,
clk_jitter=44.262, clk_wander=0.000, tai=37, leapsec=201701010000,
expire=2018062800000
ntpq>
```

These ntpq queries can be used to obtain additional NTP server information

ntpq: readlist query

# NTP Enumeration Tools

- PRTG Network Monitor includes **SNTP Sensor monitors**, a Simple Network Time Protocol (SNTP) server that shows response time of the server and time difference in comparison to the local system time



## NTP Enumeration Tools

- Nmap (<https://nmap.org>)
- Wireshark (<https://www.wireshark.org>)
- udp-proto-scanner (<https://labs.portcullis.co.uk>)
- NTP Time Server Monitor (<https://www.meinbergglobal.com>)

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

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
```

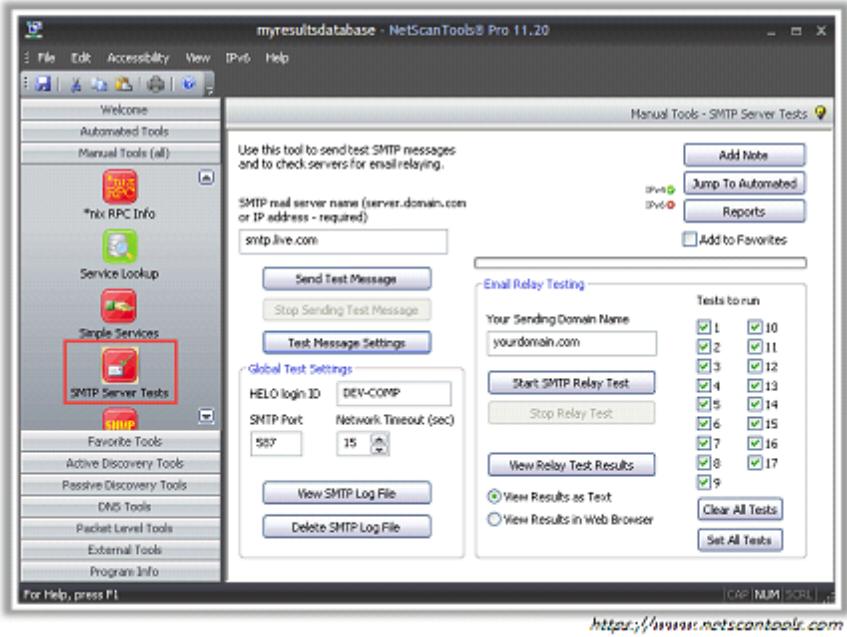
## Using the SMTP RCPT TO Command

```
$ 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 Tools

## NetScanTools Pro

- NetScanTools 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



## 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

The screenshot shows a terminal window on a Kali Linux system with the root prompt. The command "root@kali:~# smtp-user-enum -M VRFY -u root -t 10.10.10.12" is run. The output shows the tool starting and performing a scan. It lists the mode as VRFY, worker processes as 5, target count as 1, and username count as 1. It also shows the target TCP port as 25, query timeout as 5 secs, and the target domain as 10.10.10.12. The log indicates a scan started at Sat Jan 13 05:07:18 2018 and completed at the same time. It shows 0 results and 1 query in 1 second. The URL "http://pentestmonkey.net, https://pentestlab.blog" is visible at the bottom.

```

root@kali:~# smtp-user-enum -M VRFY -u root -t 10.10.10.12
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

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

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain ..... 10.10.10.12

#####
Scan started at Sat Jan 13 05:07:18 2018 #####
#####
Scan completed at Sat Jan 13 05:07:18 2018 #####
0 results.

1 queries in 1 seconds (1.0 queries / sec)
root@kali:~#

```

# DNS Enumeration Using Zone Transfer

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



```
C:\ 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

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

Enumeration  
Pen Testing

# IPsec Enumeration

- IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange) to secure **communication between virtual private network (VPN) end points**
- Most IPsec based **VPNs use Internet Security Association and Key Management Protocol (ISAKMP)**, a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment
- A simple **scanning for ISAKMP at UDP port 500** can indicate the presence of a VPN gateway
- Attackers can probe further using a tool such as **ike-scan** to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA LifeDuration, etc.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sU -p 500 193.248.1.1
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 07:49 EST
Nmap scan report for 193.248.1.1
Host is up (0.020s latency).

PORT      STATE SERVICE
500/udp    open  isakmp

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ike-scan -M 104.36.1.1
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
104.36.1.1 Main Mode Handshake returned
HDR=(CKY-R=9c61b827d522e1a2)
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.300 seconds (3.33 hosts/sec). 1 returned handshake; 0 returned notify
root@kali:~#
```

# VoIP Enumeration

- VoIP uses **SIP (Session Initiation Protocol) protocol** to enable voice and video calls over an IP network
  
- SIP service generally uses **UDP/TCP ports 2000, 2001, 5050, 5061**
  
- VoIP enumeration provide sensitive information such as **VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones User-agent IP addresses and user extensions**
  
- This information can be used to launch various VoIP attacks such as **Denial-of-Service (DoS), Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony (SPIT), VoIP phishing (Vishing), etc.**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# svmap 192.168.0.1/24
| SIP Device | User Agent | Fingerprint |
| 192.168.0.167:5060 | Grandstream GXP1620 1.0.4.33 | disabled |
| 192.168.0.87:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.109:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.54:5060 | Grandstream GXP1620 1.0.2.27 | disabled |
| 192.168.0.113:5060 | Grandstream GXP1620 1.0.2.27 | disabled |

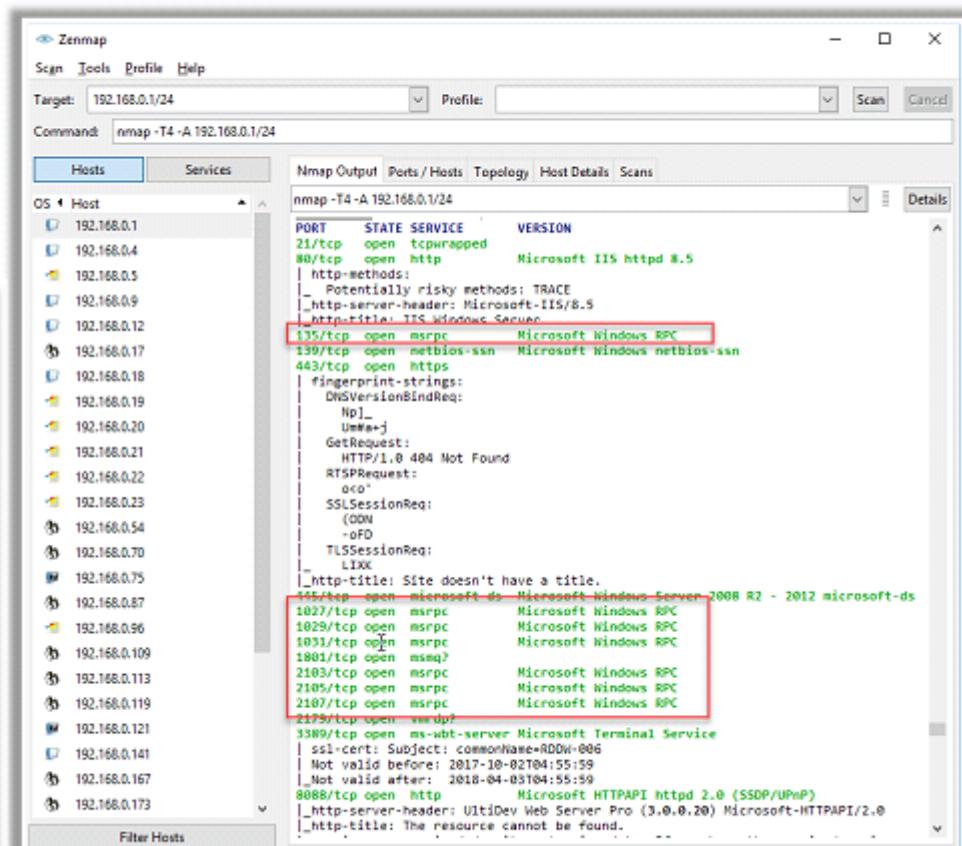
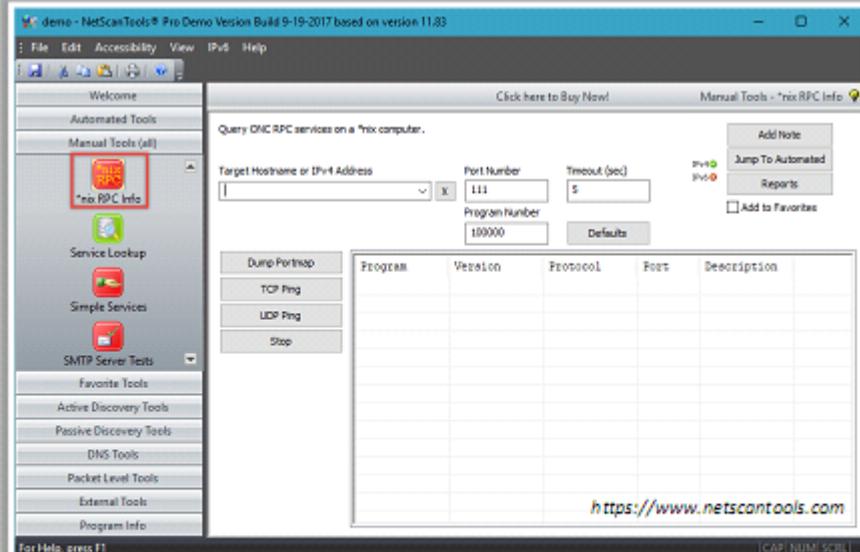
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/sip/enumerator
msf auxiliary(enumarator) > use auxiliary/scanner/sip/options
msf auxiliary(options) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf auxiliary(options) > run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK {"User-Agent"=>"Grandstream GXP1620 1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK {"User-Agent"=>"Grandstream GXP1620 1.0.4.33", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(options) >

```

# RPC Enumeration

- Remote Procedure Call (RPC) allows client and server to communicate in **distributed client/server programs**
  - Enumerating RPC endpoints enable attackers to **identify any vulnerable services** on these service ports



# Unix/Linux User Enumeration

**rusers**

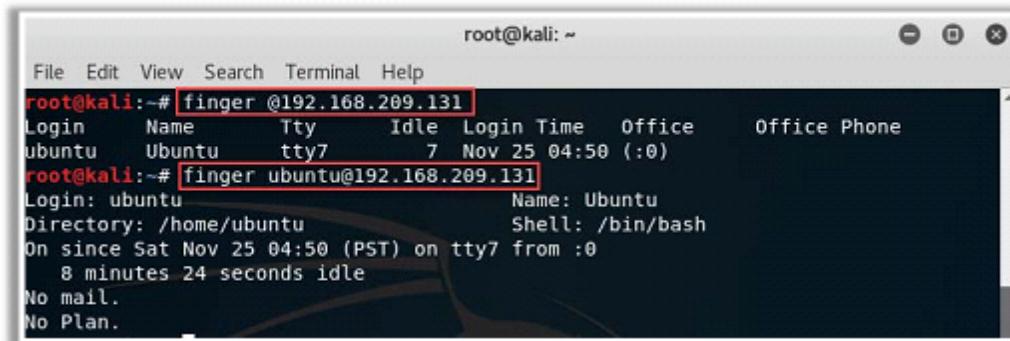
- Displays a list of users who are logged on to remote machines or machines on local network
- Syntax: `/usr/bin/rusers [-a] [-l] [-u] -h| -i] [Host ...]`

**rwho**

- Displays a list of users who are logged in to hosts on the local network
- Syntax: `rwho [-a]`

**finger**

- Displays information about system users such as user's login name, real name, terminal name, idle time, login time, office location and office phone numbers
- Syntax: `finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]`



A terminal window titled "root@kali:~" showing the output of the finger command. The first command, "finger @192.168.209.131", lists all users on the host 192.168.209.131. The second command, "finger ubuntu@192.168.209.131", provides detailed information for the user "ubuntu".

```
root@kali:~# finger @192.168.209.131
Login      Name      Tty      Idle   Login Time   Office      Office Phone
ubuntu    Ubuntu      tty7          7 Nov 25 04:50 (:0)
root@kali:~# finger ubuntu@192.168.209.131
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Sat Nov 25 04:50 (PST) on tty7 from :0
  8 minutes 24 seconds idle
No mail.
No Plan.
```

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

Enumeration  
Pen Testing

# Enumeration Countermeasures

## SNMP



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

## DNS



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

# Enumeration Countermeasures (Cont'd)

## SMTP

Configure SMTP servers to:

- ➊ Ignore **email messages** to unknown recipients
- ➋ Not to include sensitive **mail server** and **local host information** in mail responses
- ➌ Disable **open relay** feature
- ➍ **Limit the number of accepted connections** from a source in order to prevent brute force attacks



## LDAP

- ➊ By default, LDAP traffic is transmitted unsecured; **use SSL or STARTTLS technology** to encrypt the traffic
- ➋ Select a **user name different** from your email address and enable **account lockout**



## SMB

- ➊ Disable SMB protocol on **Web and DNS Servers**
- ➋ Disable SMB protocol on **Internet facing servers**
- ➌ Disable ports **TCP 139** and **TCP 445** used by the SMB protocol
- ➍ Restrict anonymous access through **RestrictNullSessAccess** parameter from the **Windows Registry**

# Module Flow

1

Enumeration Concepts

2

NetBIOS Enumeration

3

SNMP Enumeration

4

LDAP Enumeration

5

NTP Enumeration

6

SMTP and DNS  
Enumeration

7

Other Enumeration  
Techniques

8

Enumeration  
Countermeasures

9

Enumeration  
Pen Testing

# Enumeration Pen Testing

Enumeration pen testing is used to identify **valid user accounts** or **poorly protected resource shares** using active connections to systems and directed queries



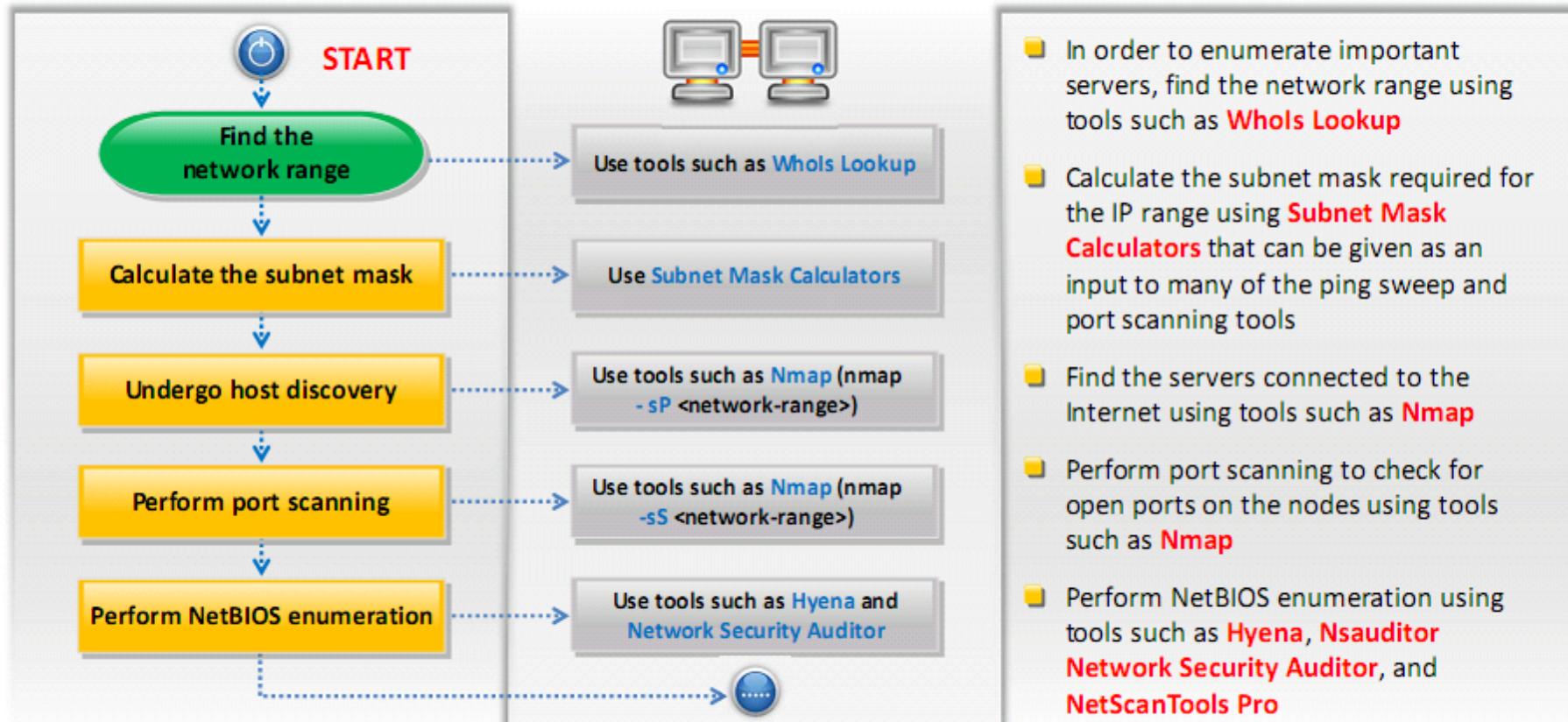
The information can be **users and groups**, **network resources and shares**, and **applications**



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



# Enumeration Pen Testing (Cont'd)



# 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 specific port with telnet to enumerate the server version running on the remote host
- ❑ Attacker queries RPC service to identify any vulnerable services
- ❑ Attacker performs Unix/Linux user enumeration to extract information about system users