Module Objectives

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

02

Extract information using default passwords

Brute force Active Directory

03

04

Extract information using DNS Zone Transfer

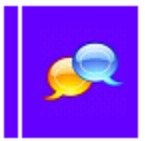
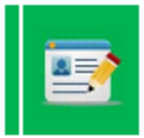
Extract user groups from Windows

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 16th character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts in the network
- Policies and passwords

NetBIOS Name List

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

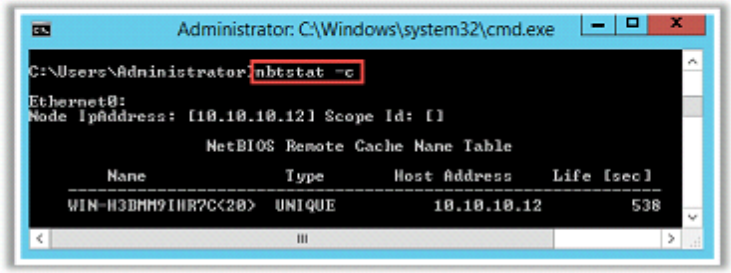
Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

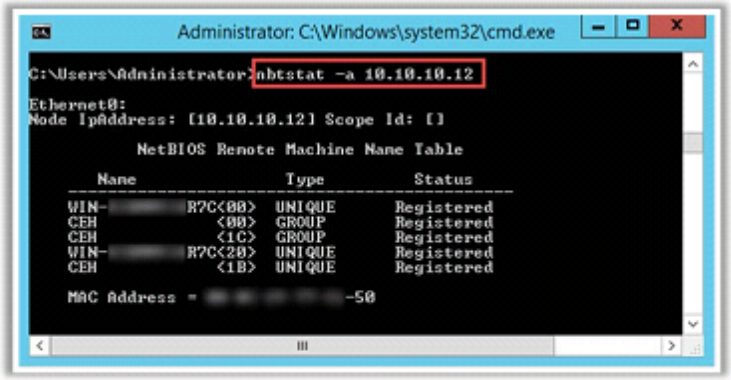
NetBIOS Enumeration (Cont'd)

- 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



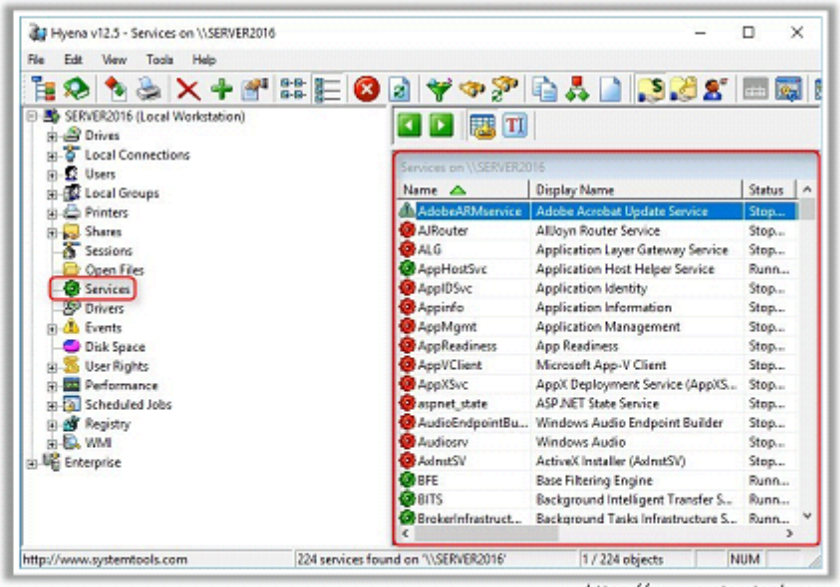


https://technet.microsoft.com

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.



https://www.systemtools.com

- **Nsauditor Network Security Auditor**
  https://www.nsauditor.com
- **NetScanTools Pro**
  https://www.netscantools.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

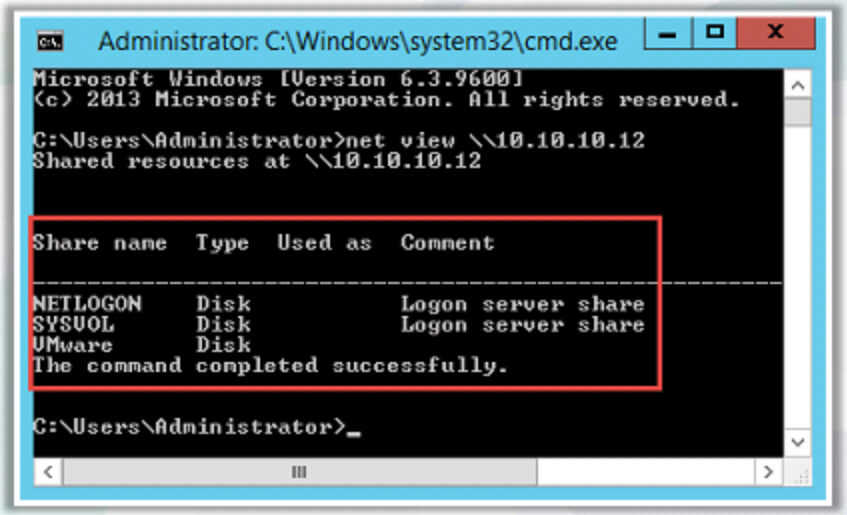
https://docs.microsoft.com

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>



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

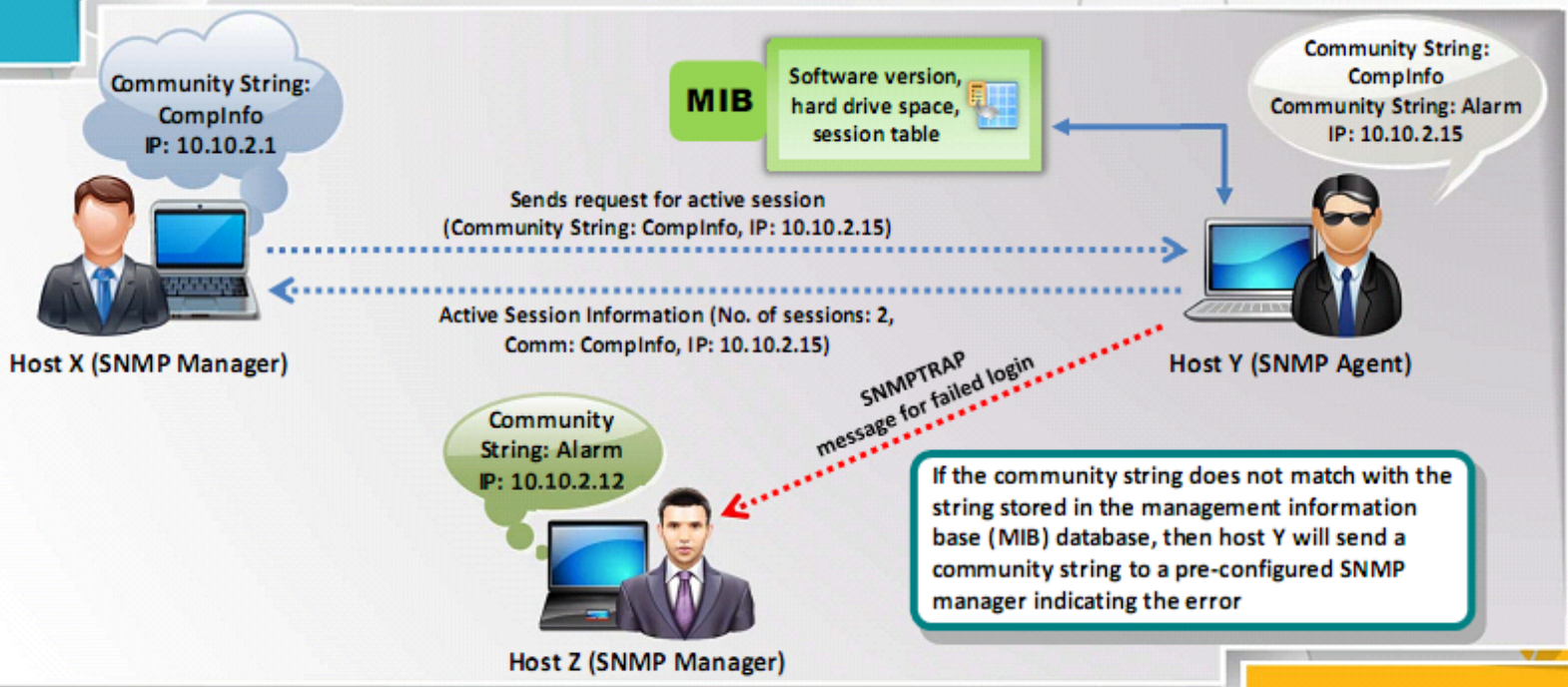
SNMP (Simple Network Management Protocol) Enumeration

- 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

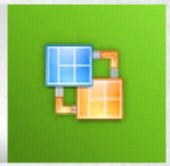


Management Information Base (MIB)

- 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**



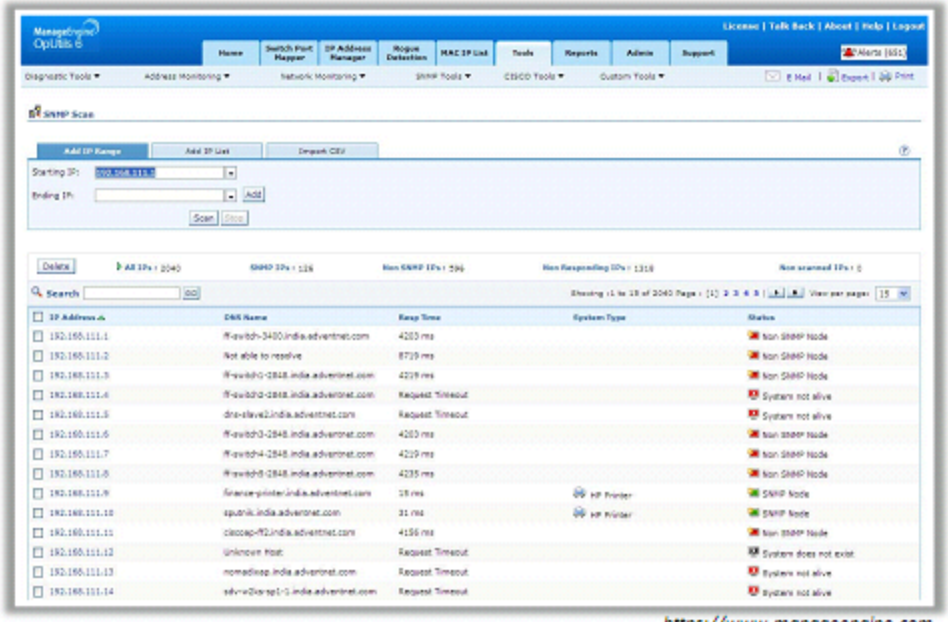
- OID includes the type of **MIB object** such as counter, string, or address; access level such as not-accessible, accessible-for-notify, read-only, or read-write; size restrictions; and range information

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

SNMP Enumeration Tools

OpUtils

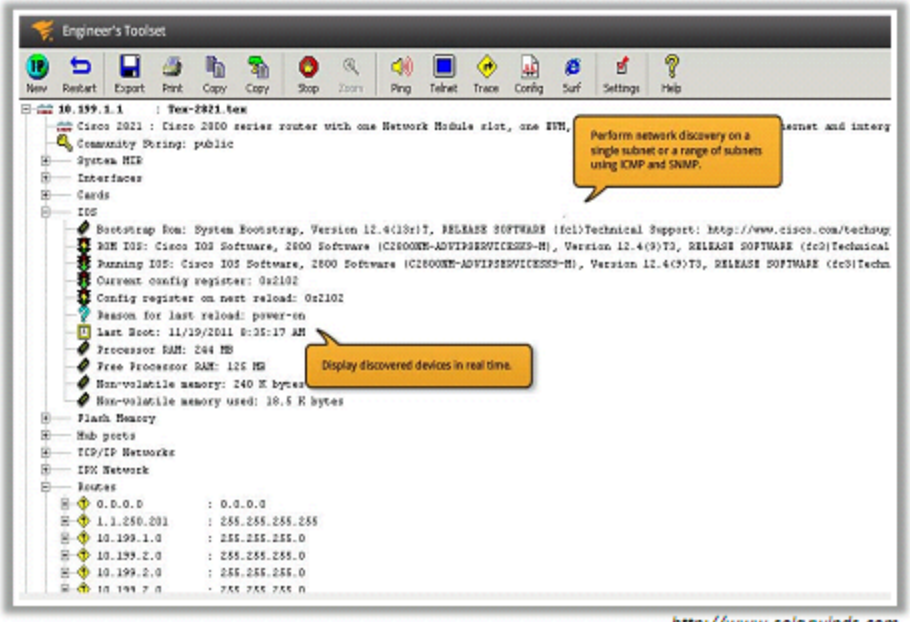
OpUtils with its integrated set of tools helps network engineers to **monitor**, **diagnose**, and **troubleshoot** their IT resources



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**



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.nothink.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

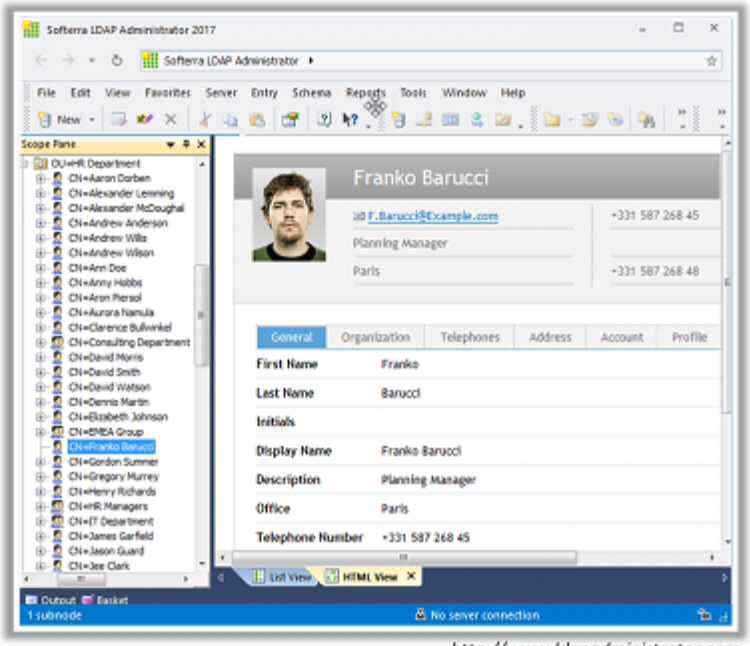
04 Information is transmitted between the client and the server using **Basic Encoding Rules** (BER)

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



http://www.ldapadministrator.com

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

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

LDAP Search
http://securityxploded.com

JXplorer
http://www.jxplorer.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

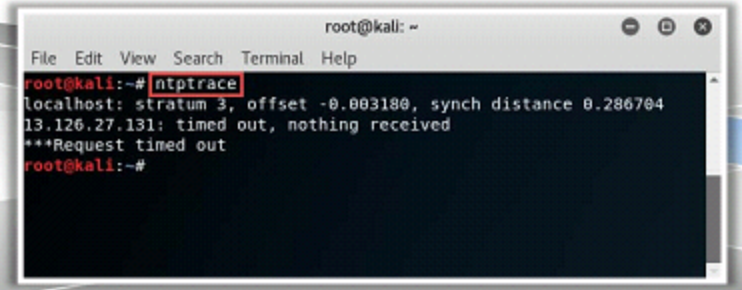
It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions

Attacker queries NTP server to gather valuable information such as:

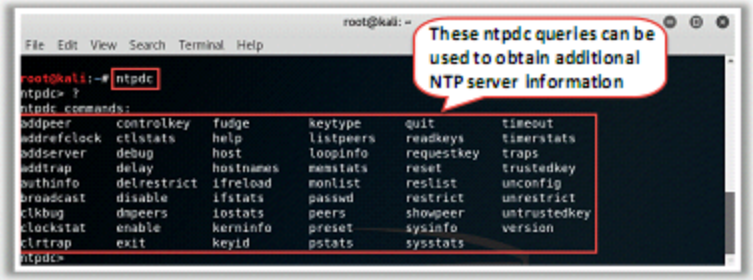
- List of **hosts connected to NTP server**
- **Clients IP addresses** in a network, their system names and Oss
- **Internal IPs** can also be obtained if NTP server is in the demilitarized zone (DMZ)

NTP Enumeration Commands

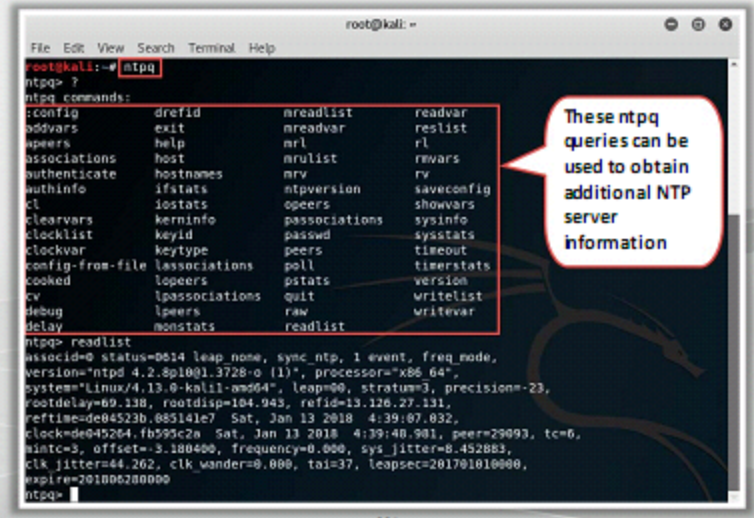
- **ntptrace**
  - Traces a chain of NTP servers back to the primary source
  - `ntptrace [ -vdn ] [ -r retries ] [ -t timeout ] [ server ]`
- **ntpdc**
  - Monitors operation of the NTP daemon, ntpd
  - `ntpdc [-ilnps] [-c command] [host] [...]`
- **ntpq**
  - Monitors NTP daemon ntpd operations and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



ntptrace



ntpdc queries



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

https://www.paessler.com

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
```

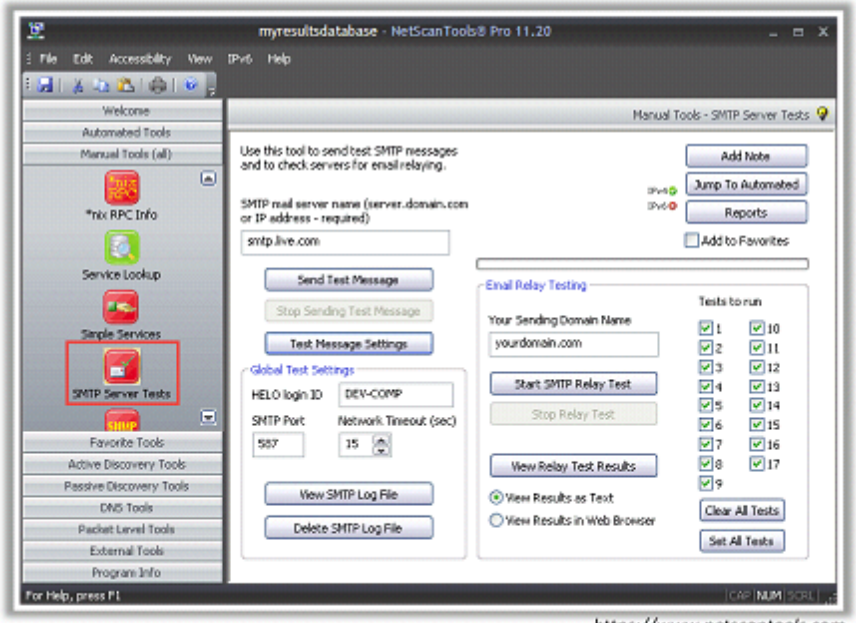
Using the SMTP RCPT TO Command

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

SMTP Enumeration Tools

NetScanTools Pro

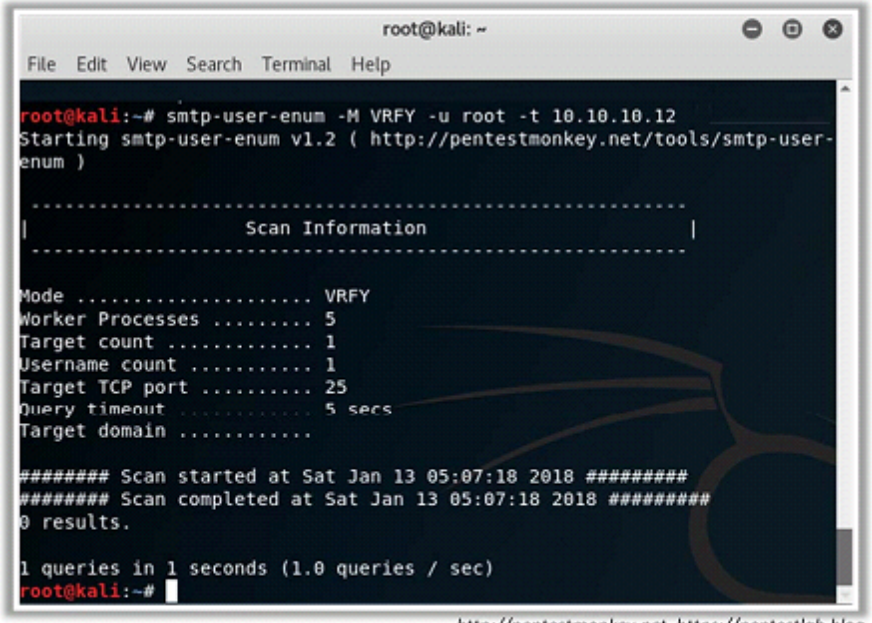
- NetScanTools Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and performing relay tests by communicating with a SMTP server



https://www.netscantools.com

smtp-user-enum

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



http://pentestmonkey.net, https://pentestlab.blog

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

Command Prompt

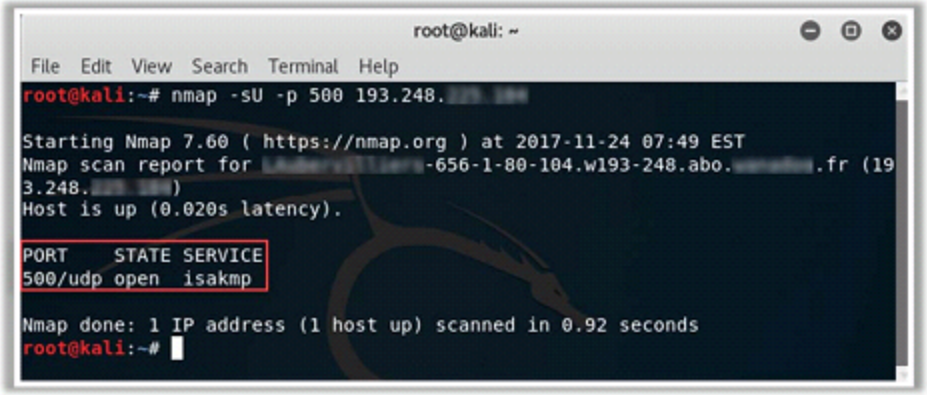
```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> Set type=any
> ls -d example2.org
[[192.168.234.110]]
example2.org. SOA corp-dc.example2.org admin.
example2.org. A 192.168.234.110
example2.org. 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
```

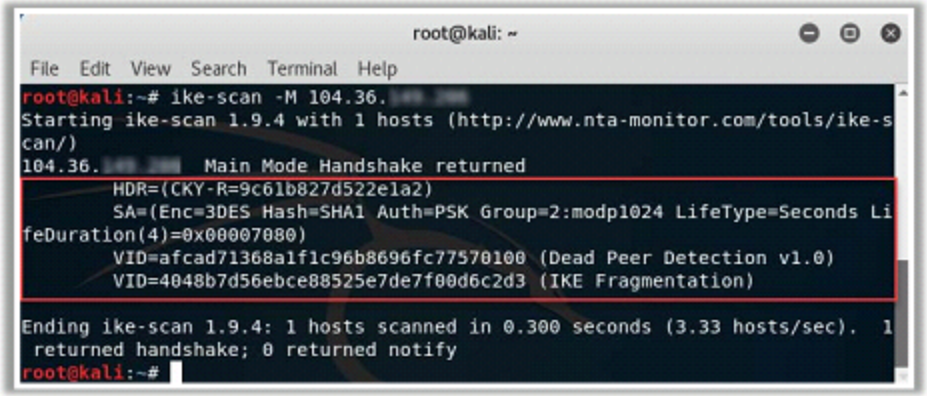
Module Flow

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

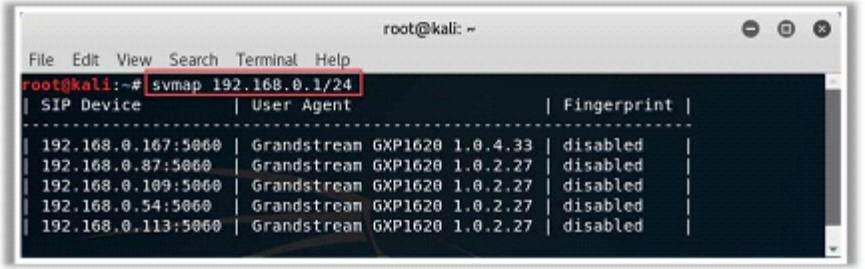
- IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange) to secure **communication between virtual private network (VPN) end points**
- Most IPsec based **VPNs use Internet Security Association and Key Management Protocol (ISAKMP)**, a part of IKE, 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.

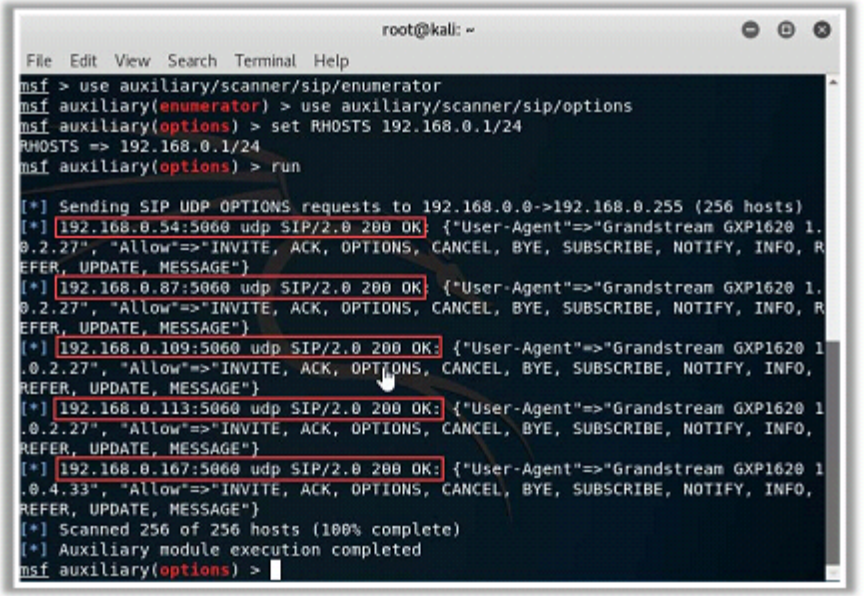




VoIP Enumeration

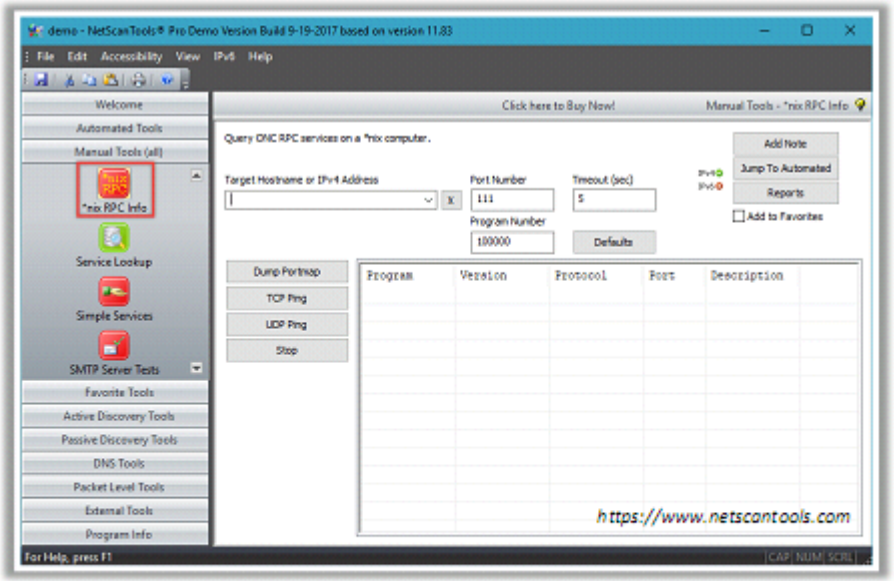
- VoIP uses **SIP (Session Initiation Protocol) protocol** to enable voice and video calls over an IP network
- SIP service generally uses **UDP/TCP ports 2000**, 2001, 5050, 5061
- VoIP enumeration provide sensitive information such as **VoIP gateway/servers**, **IP-PBX systems**, **client software** (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.

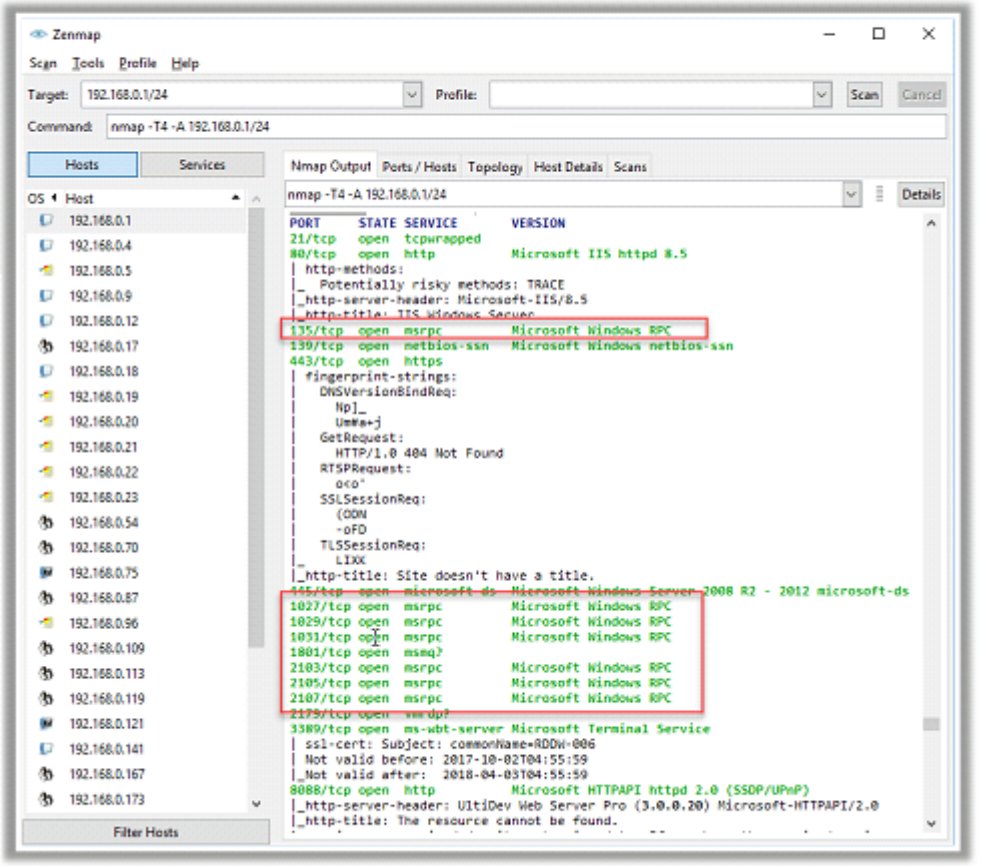




RPC Enumeration

- 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

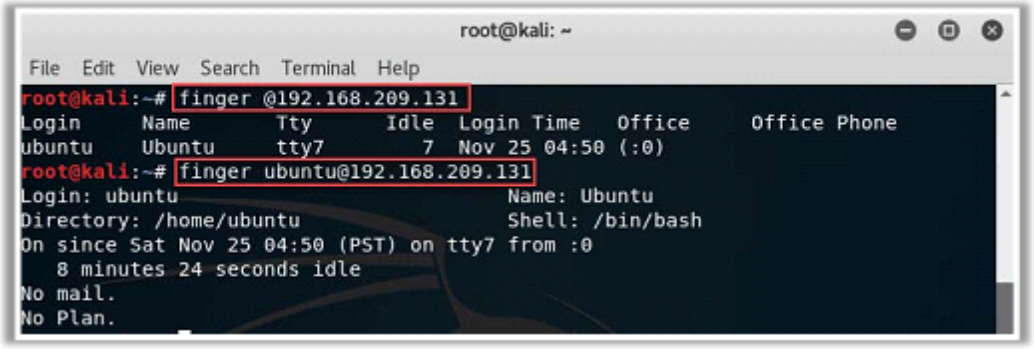
- Displays a list of users who are logged in to hosts on the local network

  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 ... ]`



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

- **Remove the SNMP agent** or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default **community string names**
- **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 in **DNS zone files** of public DNS server
- Use **premium DNS registration services** that hide sensitive information such as host information (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 to include sensitive **mail server** and **local host information** in mail responses
- Disable **open relay** feature
- **Limit the number of accepted connections** from a source in order to prevent brute force attacks

LDAP

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

SMB

- 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

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

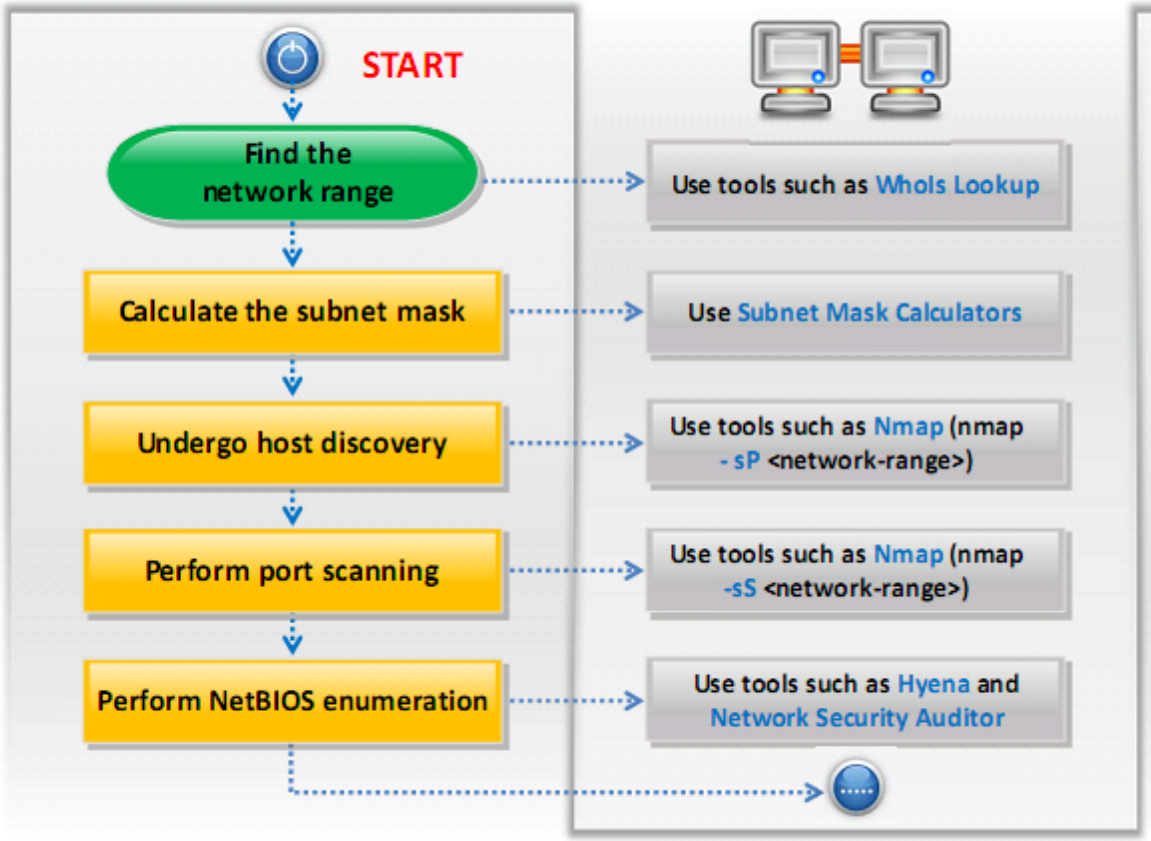
Enumeration Pen Testing

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)



- 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 open ports on the nodes using tools such as **Nmap**
- Perform NetBIOS enumeration using tools such as **Hyena**, **Nsauditor Network Security Auditor**, and **NetScanTools Pro**

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