

Ethical Hacking

Session 4 Enumeration



Learning Objective



1

- Understand enumeration

2

- List the different enumeration techniques

3

- Explain Web enumeration

4

- Understand enumeration countermeasures

Introduction 1-3

Enumeration is:

- ❑ A detailed study of computers.
- ❑ A process that is carried out by connecting all the system and enables in identifying:
 - System details
 - User accounts
 - Service accounts
 - System accounts
- ❑ The process involves active connections to systems and directed queries that identify system account resources or user accounts that are less protected for hacking.

Introduction 2-3

❑ Hackers:

- Use hacking tools to gather secured information.
- Can easily find exploitable servers on Google by simply searching for default servers.

❑ Following items are extracted during the process of enumeration:

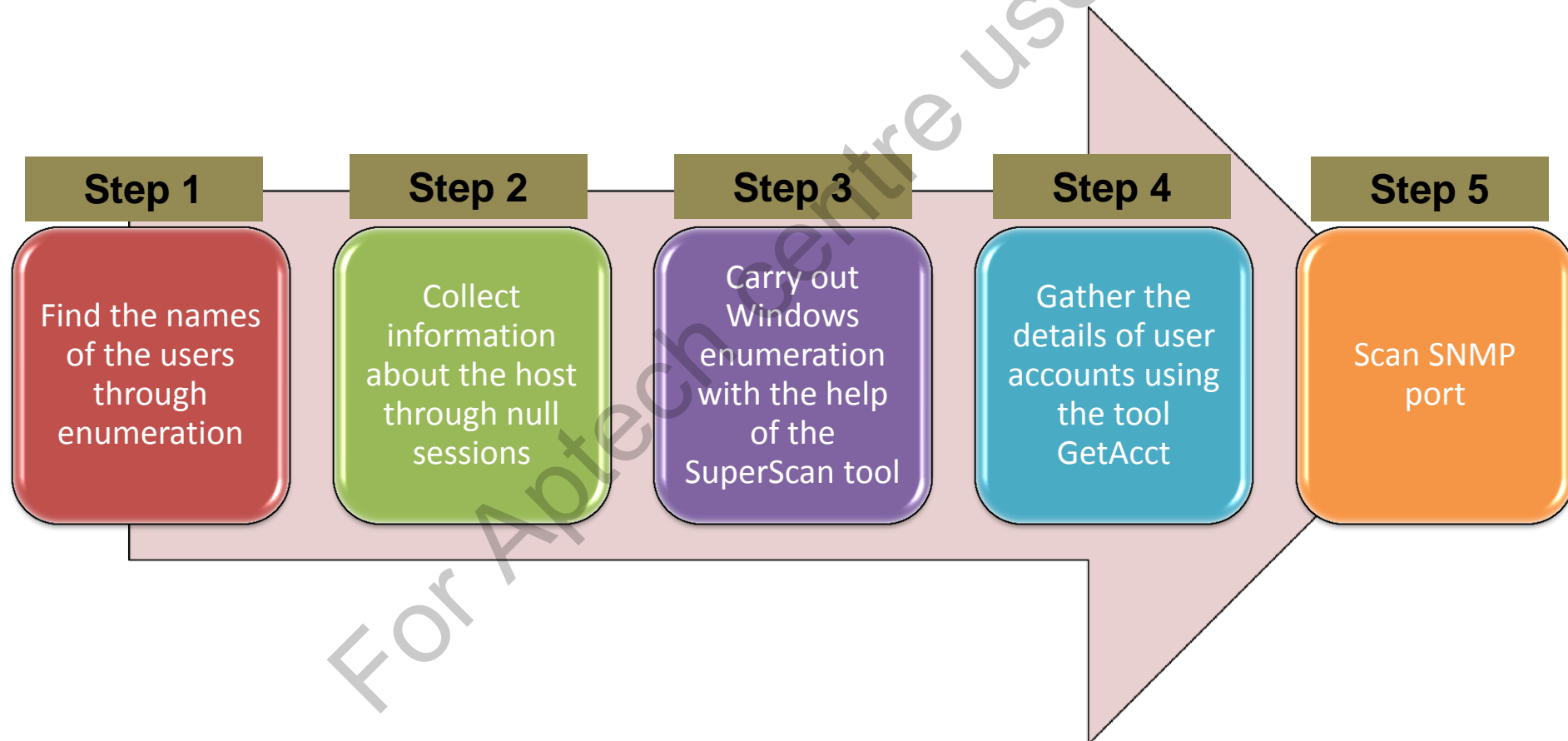
- Machine names
- User names
- Shares
- Services from a system
- Network resources

Introduction 3-3

- ❑ Enumeration techniques are conducted all the time in an intranet atmosphere, in which active connections to systems and directed queries are involved.

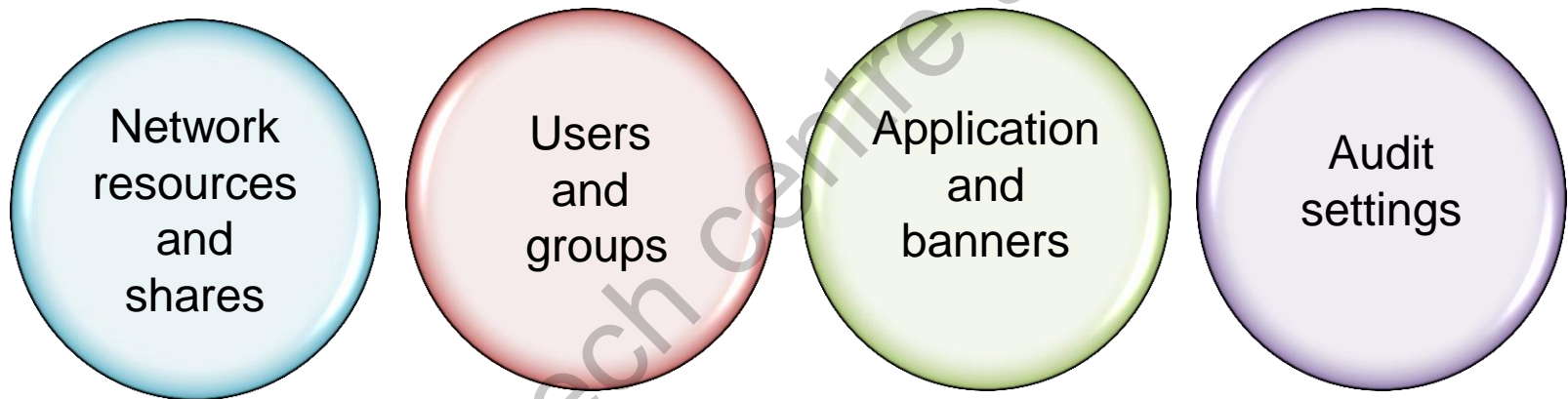
Enumeration Steps

- ❑ The process of enumeration involves the following steps:



Types of Information that Hacker's Enumerate

- ❑ The types of information that is enumerated by intruders are grouped as follows:



Enumeration Techniques 1-6

- An attacker collects data from sources such as:
 - Routing tables
 - Group names
 - Simple Network Management Protocol (SNMP) information
 - Network users

Enumeration Techniques 2-6

- ❑ Some enumeration techniques are as follows:

By using Windows

- User names can be extracted from groups and sessions account can be verified to check if they are in a group or not.

By using SNMP

- User names can be extracted and the attackers can identify the strings.

By using email addresses

- User names can be extracted.

Enumeration Techniques 3-6

❑ Some enumeration techniques are as follows:

By using default passwords

- More information can be extracted.
- If a user forgets to change the default password, then the data can be enumerated by attackers.

By using Brute Force Active Directory

- Information can be extracted. When the 'logon hours' feature is enabled, attackers can enumerate user names by conducting a brute force attack.

By using DNS Zone Transfer

- An attacker succeeds in collecting valuable information about the zone that has been requested.

Enumeration Techniques 4-6

❑ Following are the services and ports to enumerate:

DNS Zone Transfer uses TCP 53 as this protocol helps to provide DNS database between servers.

Microsoft RPC Endpoint Mapper uses TCP 135 as this protocol helps to locate the message service that is using the mapper.

NetBIOS Name Service (NBNS) uses TCP 137, as this protocol helps to provide resolution service to computers that run NetBIOS. NBNS matches the IP address with the names and queries of NetBIOS which is also the first service that is attacked.

Enumeration Techniques 5-6

■ Following are the services and ports to enumerate:

NetBIOS Session Service (SMB over NetBIOS) uses TCP 139, as this protocol helps to set up or destroy sessions between NetBIOS computers.

SMB over TCP uses TCP port 445.

SNMP uses UDP 161 because this protocol helps to log and manage information to remote monitoring appliances.

Enumeration Techniques 6-6

❑ Following are the services and ports to enumerate:

Lightweight Directory Access Protocol (LDAP) uses port TCP/UDP 389, as this protocol helps to look up contact information from a server.

Global Catalog Service uses port TCP/UDP 3368 that sets up communication.

Simple Mail Transfer Protocol (SMTP) uses port TCP 25 so that emails across the local network as well as the Internet can be moved.

NetBIOS Enumeration 1-12

❑ Network Basic Input Output System (NetBIOS):

- Is used as an Application Programming Interface (API) to enumerate a Windows machine.
- Was developed by IBM in collaboration with Sytek which has a 16 ASCII character string that identifies network devices over TCP/IP.
- Is available on Local-Area Networks (LANs) that use a 15 character username.
- The 16th character is reserved for the type of name record.
- Is non-routable and runs on Transmission Control Protocol/Internet Protocol (TCP/IP).

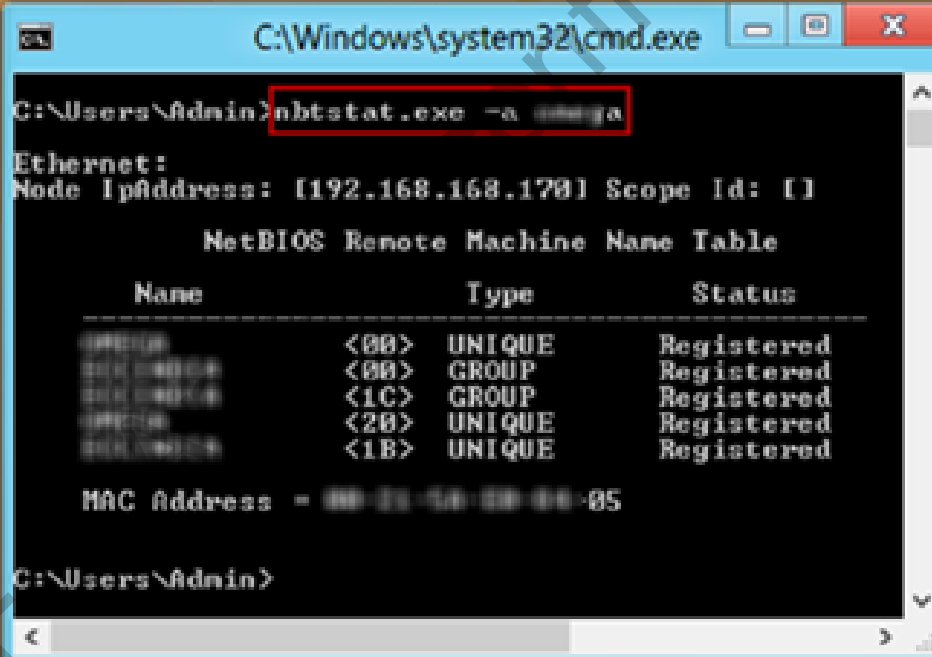
NetBIOS Enumeration 2-12

■ Following table displays NetBIOS name list:

Name	Code of NetBIOS	Type of NetBIOS	Information Collected
<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 the user that has logged in
<host name>	<20>	UNIQUE	Server service running
<domain>	<ID>	GROUP	Master browser name for the subnet
<domain>	<IB>	UNIQUE	Domain master browser name identifies the PDC for that domain

NetBIOS Enumeration 3-12

- NetBIOS combines with Server Message Blocks (SMBs) that allow accessing shared directories and files remotely, as shown in the following figure.



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

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

    NetBIOS Remote Machine Name Table

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

    MAC Address = 00-23-54-00-00-05

C:\Users\Admin>
```


NetBIOS Enumeration 4-12

- ❑ NetBIOS helps attackers to collect passwords, policies and list of computers of a domain and the shares of the hosts on the network.
- ❑ Before starting with hacking of the system, a null session using the net command, `net use \\ computer name\ipc$ "" /u:""` needs to be set up.

NetBIOS Enumeration 5-12

❑ A null session:

- Can be established with a Windows (NT/2000/XP) host, a user name and a password.
- Is also called the Holy Grail of Windows Hacking. It occurs when Common Internet File System (CIFS) or Server Messaging Block (SMB) is weak.
- Helps in gathering information of users and groups, machines, shares, users and Host Security Identifiers (SIDS) from the host.
- Helps users to access information such as user names, shares, groups, policies, permissions with the help of a null user.

NetBIOS Enumeration 6-12

□ Tools that are used to enumerate a Windows system are:

DumpSec

GetAcct

SuperScan

GetUserInfo

Ldp

User2sid

NBTStat

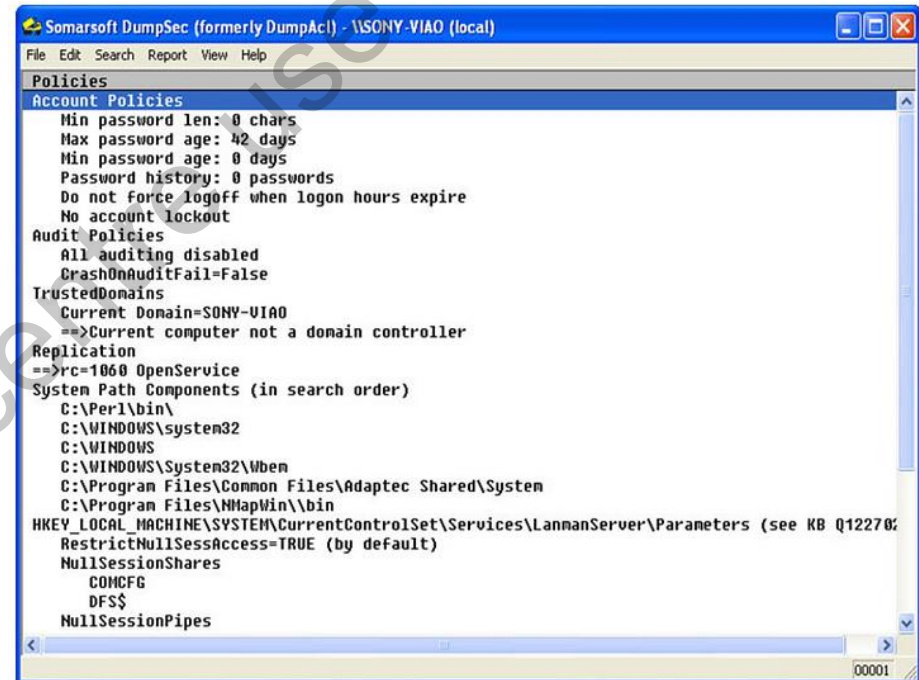
Hyena

**NetBIOS
Enumerator**

NetBIOS Enumeration 7-12

❑ DumpSec tool:

- Remotely connects to Windows machines and dumps all the information.
- Is a Graphical User Interface (GUI) based on Windows as shown in figure.



NetBIOS Enumeration 8-12

❑ GetAcct:

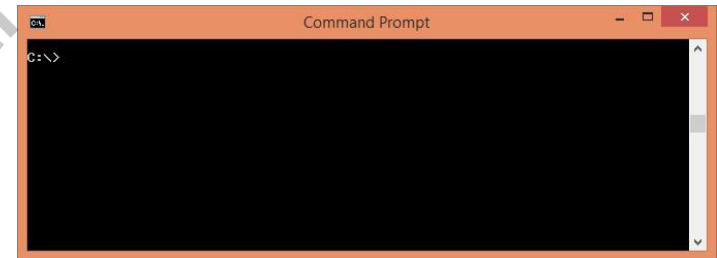
- Helps to extract name of the computer and account information by entering the IP address or NetBIOS.

NetBIOS Enumeration 9-12

NBTstat Tool:

- ❑ The steps to start NBTstat tool are as follows:

- The **Command Prompt** is opened as shown in figure.



- To get the name table of remote computer, a user needs to run nbtstat command, nbtstat -a <NetBIOS name of the remote machine>, as shown in figure.




NetBIOS Enumeration 10-12

NBTstat Tool:

- ❑ The steps to start NBTstat tool are as follows:

- To display the NetBIOS name cache, the table of NetBIOS names and the resolved IP address, a user needs to run the command, `nbtstat.exe -c`, as shown in the figure.



```
C:\>nbtstat.exe -a compl
VirtualBox Host-Only Network:
Node IpAddress: [192.168.150.5] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    ----                -
    COMPI                <00>             UNIQUE         Registered
    JOINWORKGROUP        <00>             GROUP          Registered
    COMPI                <20>             UNIQUE         Registered
    JOINWORKGROUP        <1E>             GROUP          Registered

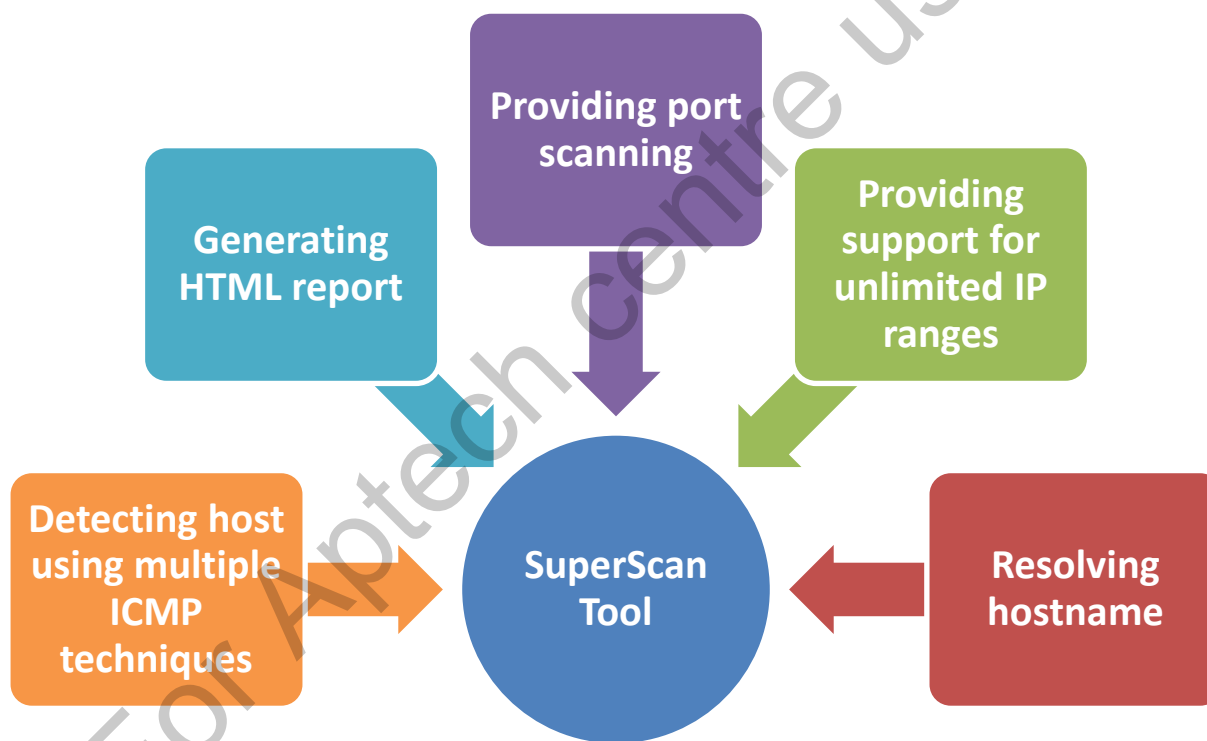
    MAC Address = 08-00-27-67-C7-9D
```

NetBIOS Enumeration 11-12

- ❑ The SuperScan tool is a TCP pinger, port scanner and resolves hostnames.
- ❑ Ping sweeps can be carried out using this tool.
- ❑ It can also be used for scanning IP range with multithreading and asynchronous techniques.

NetBIOS Enumeration 12-12

- ❑ The following functionalities can be restored by running this tool:



Simple Network Management Protocol (SNMP) Enumeration 1-6

❑ Simple Network Management Protocol (SNMP):

- Is a Transmission Control Protocol (TCP)/Internet Protocol (IP) standard that monitors and manages hosts, routers, nodes, agents and devices on a network.
- Is an application-layer protocol that monitors strength and safety of network and computer devices such as routers and Uninterruptible Power Supply (UPS).
- Assigns the SNMP agent and the SNMP management station for communication.
- Is used to manage and monitor hardware devices connected to a network.

Simple Network Management Protocol (SNMP) Enumeration 2-6

- ❑ Three distinct components are required to use SNMP and they are as follows:

Network Management System (NMS)

SNMP Agents

Managed Devices (SNMP agent deployed)

Simple Network Management Protocol (SNMP) Enumeration 3-6

- ❑ Three distinct components are required to use SNMP and they are as follows:

Network Management System (NMS)

- Managed devices record the information with the help of the deployed agent and communicate with the overarching Network Management System.
- The information is stored in a Management Information Base (MIB).
- **Note:** An MIB is a virtual database that manages the entities in a communications network.

Simple Network Management Protocol (SNMP) Enumeration 4-6

SNMP Agents

- SNMP is a clear text protocol that provides valuable information to an attacker.

Managed Devices (SNMP agent deployed)

- Network equipments such as routers, computer equipment and UPS are included.

Simple Network Management Protocol (SNMP) Enumeration 5-6

- ❑ Hackers use SNMP enumeration to collect information of network resources.
- ❑ It consists of a manager that is installed on a computer and an agent that is embedded on each network device.
- ❑ Requests and replies are sent by the agents that refer to configuration variables, which are accessible by the agent software.
- ❑ MIB is the database of configuration variables available on the networking device.
- ❑ Events such as interface failure or reboot are identified using traps.

Simple Network Management Protocol (SNMP) Enumeration 6-6

- Following are some SNMP enumeration tools available on Windows and Linux:

OpUtils

SNMP
Scanner

snmpwalk

IP Network
Browser

SNScan

Simple Mail Transfer Protocol (SMTP)

Enumeration 1-2

❑ Simple Mail Transfer Protocol (SMTP):

- Transmits email messages.
- Helps hackers to enumerate username using the EXPN, RCPT and VRFY commands.
- Is performed by tools like Netcat by typing the following command:

```
nc -v -z -w 2 IP Address 1-1024
```
- Is a tool that enumerates user accounts on Solaris via the SMTP send mail service.

❑ Solaris:

- ❑ Is a UNIX operating system originally developed by Sun Microsystems.
- ❑ Inspects the responses to commands such as Verify (VRFY), Expand (EXPN) and Recipient (RCPT).

Simple Mail Transfer Protocol (SMTP)

Enumeration 2-2

- ❑ Some SMTP enumeration tools are listed as follows:



NetScanTools
Pro

Nmap

Telnet

UNIX/Linux Enumeration 1-2

- ❑ Linux may not provide techniques that Windows offer.
- ❑ Following are some tools that enumerate usernames on systems which include:

Rpcclient

- A hacker uses the `rpcclient` command to enumerate usernames. For example, `rpcclient $> netshareenum.`

Showmount

- The `showmount` command enumerates a list of clients that have remotely mounted a file system from a computer.

Finger

- The host and the user is enumerated using the `finger` command, enabling a hacker to access information of the user's location of office, the time the user logged in, the time the user was idle, home directory and the last mail that was viewed by the user.

UNIX/Linux Enumeration 2-2

Rpinfo

- Remote Procedure Call (RPC) protocol is enumerated using the `rpinfo` command by calling an RPC server and reporting the details of the findings.

Showmount

- Information from Windows and Samba systems are enumerated using the `enum4linux` command and it acts as a covering around the Samba commands `smbclient`, `rpcclient`, `net` and `nmblookup`.

LDAP Enumeration 1-2

❑ The Lightweight Directory Access Protocol (LDAP):

- Accesses the Active Directory and also other directory services. The directory follows a logical format similar to the organisational hierarchy system.
- Helps in quick lookups and query resolutions since it is tied into the Domain Name System. It runs on Port 389.

LDAP Enumeration 2-2

Following are the steps to start LDAP Explorer:

Step 1 : IP address and user credentials of the domain controller are entered as shown in the following figure.

Connect to Active Directory

☒ Enter a name for an Active Directory database to which you want to connect. If you previously saved a connection, you do not need to enter a database name.

Connect to: 192.168.150.1

User: administrator

Password:

☐ Enter the path of a previous snapshot to load.

Path:

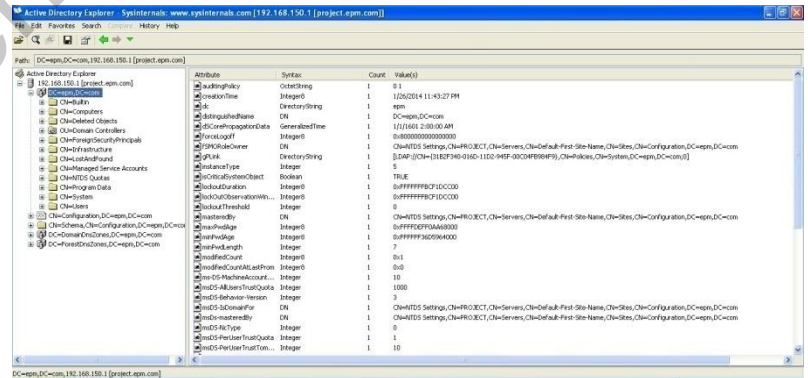
If you want to save this connection for future use, select Save this connection, and then enter a name for the saved connection.

☐ Save this connection

Name:

OK Cancel

Step 2 : The hacker then explores the various details of the Active Directory as shown in the figure.



NTP Enumeration 1-3

❑ Network Time Protocol (NTP):

- Synchronises clocks of computers that have been networked. UDP port 123 is used as a means of communication.
- Allows maintaining time to an accuracy level of 10 milliseconds (1/100 per second) on the Internet.
- Helps in achieving 200 microseconds or even less on local area networks.

NTP Enumeration 2-3

❑ The commands are as follows:

Ntpdate	<ul style="list-style-type: none">• Time samples are collected using this command
Ntptrace	<ul style="list-style-type: none">• Time servers back up are preferred to primary time server
Ntpdc	<ul style="list-style-type: none">• The state of the time server is monitored
Ntpq	<ul style="list-style-type: none">• Performance is monitored using this command

NTP Enumeration 3-3

- ❑ Following are the various enumeration tools:

**NTP Server
Scanner**

**LAN Time
Analyser**

**PresenTense
Time Server**

Web Enumeration

- ❑ Hackers search for default server pages to attack exploitable servers.
- ❑ If applications are left in default mode, hackers are able to find such error pages and locate servers that are connected to the Internet.
- ❑ Web enumeration involves DNS and HTTP enumeration.

DNS Enumeration 1-3

❑ The process of Domain Name System (DNS) enumeration:

- Helps find DNS servers internally and externally.
- Performs lookups of DNS records.
- Helps hacker to gather valuable network information that include computer names, usernames, IP addresses of weak systems and performing zone transfers.
- Helps hacker to attempt to retrieve a file from a DNS server.

DNS Enumeration 2-3

- Following are the tools used for DNS enumeration:

NSLookup

DigDug

WhereIsIP

NetInspector

DNS Enumeration 3-3

NSLookup Tool:

- ❑ To start NSLookup tool, a hacker enters `nslookup` on Command Prompt as shown in the figure.



```
C:\>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
>
```

HTTP Enumeration 1-11

- ❑ In an enumeration attack, an attacker can make the target host list of the various resources that are available on the said host or network.

- ❑ For example,
 - User names and privileges

 - Services

 - Shares policies

HTTP Enumeration 2-11

- ❑ HTTP enumeration helps in enumerating directories and files to return an enumerable collection of strings.
- ❑ While working with large collections of files and directories, enumerable collections offer quality performance.
- ❑ The Web application security has many tools that are available for different operating systems and are also used to locate a bug in a Web application.
- ❑ HTTP uses Port 80 and 443 to communicate.

HTTP Enumeration 3-11

- ❑ In a Web-based Directory Enumeration posted by Pentestmonkey, a hacker sends a request for each directory name from a dictionary file.
- ❑ The HTTP response code for each request is as follows:
 - **http://host/admin (401)**
 - **http://host/cgi-bin (403)**
 - **http://host/test (404)**
 - **http://host/logs (200)**
 - **http://host/awstats (404)**
 - **http://host/scripts (404)**

HTTP Enumeration 4-11

- ❑ The hacker ignores HTTP 404 and the directories that fail to return a 404 are considered to exist.
- ❑ Following two enumeration tools help list the directories that are not available on a Web site:
 - http-dir-enum
 - DirBuster

HTTP Enumeration 5-11

❑ Wikto:

- Is a Web server assessment tool.
- Works by locating directories and files on the Web site.
- Tries to look for vulnerable scripts or Web servers.

HTTP Enumeration 6-11

❑ The key features of Wikto are as follows:

- Fully supports HTTP proxy
- Uses enumeration of Apache user name
- Logs on to metasploit
- Supports Secure Socket Layer (SSL)
- Supports a subdomain brute forcing
- Easy to update
- Saves report on multiple format

HTTP Enumeration 7-11

❑ The requirements of Wikto are as follows:

- A operating system (with PERL installed)
- OpenSSL: <http://www.openssl.org/>
- ActiveState Perl: <http://www.activestate.com/>

HTTP Enumeration 8-11

❑ WebEnum Tool:

- Is used to carry out penetration testing on Web servers.
- Helps to Brute force Web accounts and passwords. HTTP responses use dynamically generated queries to enumerate.
- Helps to discover files, users and directories with Apache method.
- Helps in locating table names and columns size in SQL injection.

HTTP Enumeration 9-11

❑ WebEnum generates URL, POST data or headers using special dynamic strings such as:

- %%WORD%%
- %%WORD[0-9]%%
- %%INT%%
- %%CHAR%%
- %%TABLE%%)

HTTP Enumeration 10-11

- ❑ Following are the dynamic strings that are allowed in URL, headers and POST data:
 - **%%WORD%%**: This generates strings from an internal wordlist of ~900 common words.
 - **%%WORD[0-9]%%**: This generates strings from wordlist files that are specified in -w options.
 - **%%INT%%**: This generates integer ranges that range from 0 to 50, by default.
 - **%%CHAR%%**: This generates character and string ranges. Default range is from 'a' to 'z'.
 - **%%TABLE%%**: This generates 1, 1, ... 1 string that is useful in SQL injection to enumerate columns. The range is from 0 to 50, by default.

HTTP Enumeration 11-11

- ❑ The INT, CHAR and TABLE default options can be customised by using [end] or [start]:[end].
- ❑ For example, %%INT100:110%%, %%INT1%%, %%CHARaaa:zzz%% and %%TABLE100%%.
- ❑ The dynamic strings are allowed in POST data (-d) and headers (-h) as in URL.

User Enumeration 1-10

❑ User Enumeration:

- ❑ Is a test to verify if it is possible to collect a set of valid usernames by interacting with the authentication mechanism of the application.
- ❑ Will be useful for testing the brute force, in which, we verify if given a valid username, it is possible to find the corresponding password.

User Enumeration 2-10

□ HTTP Response Message:

Testing for Valid user/right password:

- The server answer is recorded when a valid user ID and password is submitted.

Result Expected:

Using WebScarab, the information retrieved from this successful authentication (HTTP 200 Response, length of the response) is noted.

User Enumeration 3-10

Testing for Valid user/wrong password:

- Now, the tester should try to insert a valid user ID and a wrong password and record the error message generated by the application.

Result Expected:

From the browser, expect any one of the messages as displayed in figure.

Authentication failed.
Return to Login page

- The following figure displays another message that shows 'No configuration found':

No configuration found.
Contact your system Administrator.
Return to Login page

User Enumeration 4-10

- ❑ Against any message that reveals the existence of user, for instance, message similar to:

Login for User foo: invalid password

- Using WebScarab, the information retrieved from this unsuccessful authentication attempt (HTTP 200 Response, length of the response) is noted.

User Enumeration 5-10

Testing for a nonexistent username:

- The tester should try to insert an invalid user ID and a wrong password and record the server answer (the tester should be confident that the username is not valid in the application). The error message and the server answer must be recorded.
- **Result Expected:**
If a nonexistent user ID is entered, the following message is received as displayed in figure.

This user is not active.

Contact your system administrator.
Return to Login page

User Enumeration 6-10

Testing for a nonexistent username:

- Or message like the following one is displayed:

Login failed for User foo: invalid Account

User Enumeration 7-10

- ❑ Generally, the application should respond with the same error message and length to different wrong requests.
- ❑ If it is seen that the responses are not the same, a tester should investigate and find out the key that creates a difference between the two responses.
- ❑ For example,
 - **Client request:** Valid user/wrong password --> Server answer: 'The password is not correct'
 - **Client request:** Wrong user/wrong password --> Server answer: 'User not recognised'

User Enumeration 8-10

- ❑ These responses let the client understand that for the first request we have a valid user name.
- ❑ It is possible to interact with the application requesting a set of possible user IDs and observing the answer.
- ❑ Looking at the second server response, it can be understood in the same way that the tester does not hold a valid username.
- ❑ The user can interact in the same manner and create a list of valid user ID looking at the server answers.

User Enumeration 9-10

❑ WebScarab:

- Is a framework for analysing applications that communicate using the HTTP and HTTPS protocols.
- Is written in Java and thus, portable to many platforms.
- Has several modes of operation, implemented by a number of plugins.

User Enumeration 10-10

❑ In its most common usage, WebScarab:

- Operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser, before they are sent to the server and to review and modify responses returned from the server, before they are received by the browser.
- Is able to intercept both HTTP and HTTPS communication. The operator can also review the conversations (requests and responses) that have passed through WebScarab.

Enumeration Countermeasures 1-5

❑ Effective enumeration countermeasures to secure sensitive information are as follows:

To safeguard
SNMP
enumeration:

- The SNMP service should be switched off or the SNMP agent should be plugged off.
- If the SNMP cannot be turned off, the default name of the public community should be changed.
- By upgrading to SNMP3, messages and passwords can be encrypted.
- For unknown connections, 'Additional restrictions from the Group Policy security' option can be used.
- Access to IPSec filtering, null session shares and null session pipes should be limited.

Enumeration Countermeasures 2-5

To safeguard
DNS
enumeration:

- DNS zone transfer to unknown hosts should be restricted by configuring name servers.
- Non-public hostnames should not be referenced to IP that are found in the publicly accessible DNS servers or in the DNS zone files.
- Host Information (HINFO) and other important records should not appear in DNS zone files.
- To prevent social engineering and war dialing attacks, it should be ensured that standard network admin contact details in Network Information Center databases are provided.

Enumeration Countermeasures 3-5

To safeguard
SMTP
enumeration:

- SMTP server should be configured in such a way that the messages to anonymous recipients are ignored or do not reveal any details of mail relay systems such as MS Exchange or Sendmail.
- Internal IP address or host information should not be revealed.
- By configuring SMTP servers, emails to anonymous recipients can be ignored.

Enumeration Countermeasures 4-5

To safeguard
LDAP
enumeration:

- To restrict access to only known users, it needs to be ensured that NTLM or basic authentication is used.
- It should be ensured that SSL technology is used to encrypt the traffic as LDAP traffic is transmitted unsecured.
- It should also be ensured that the username is completely different from the email id. It is recommended to enable account lockout.

Enumeration Countermeasures 5-5

To safeguard
SMB
enumeration:

- To disable SMB, the following steps are used:
 - Navigate to **Local Area Connection** properties.
 - Select the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** check box.
 - Click **Uninstall** and follow the steps for installing.

Summary 1-3



- ❑ Enumeration process involves active connections to systems and directed queries that identify system account resources or user accounts that are less protected for hacking.
- ❑ Hackers use hacking tools to gather secured information.
- ❑ Enumeration techniques are conducted all the time in an intranet atmosphere in which the active connections to systems and directed queries are involved.
- ❑ Those who have a NetBIOS connection to computers are able to access information such as user names, shares, groups, policies, permissions with the help of null user.

Summary 2-3



- ❑ Simple Network Management Protocol (SNMP) is a Transmission Control Protocol (TCP)/Internet protocol (IP) standard that monitors and manages hosts, routers, nodes, agents and devices on a network.
- ❑ Hackers use SNMP enumeration to collect information of network resources.
- ❑ SMTP transmits email messages.
- ❑ LDAP accesses the Active Directory and also other directory services.
- ❑ NTP synchronises clocks of computers that have been networked. UDP port 123 is used as a means of communication.

Summary 3-3



- ❑ If applications are left in default mode, hackers are able to find such error pages and locate servers that are connected to the Internet.
- ❑ DNS enumeration helps to find DNS servers internally and externally. It also performs lookups of DNS records.
- ❑ HTTP enumeration helps in enumerating directories and files to return an enumerable collection of strings.