

# Enumeration

# Enumeration in Ethical Hacking

Enumeration belongs to the first phase of Ethical Hacking, i.e., “Information Gathering”. This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further

# Goals of Enumeration

Ethical hackers use enumeration to gather information on various aspects, including:

1. Network Shares: Identifying shared resources and access permissions on the network.
2. SNMP Data: Examining Simple Network Management Protocol (SNMP) data, particularly if SNMP is not adequately secured.
3. IP Tables: Understanding IP tables and firewall configurations.
4. Usernames: Enumerating usernames associated with different systems.
5. Password Policies: Discovering password policy settings

# Services And Ports to Enumerate

## Enumeration Techniques in Ethical Hacking:

### 1. **Port Scanning:**

- Identify open network ports to understand running services using tools like Nmap or Netcat.

### 2. **Banner Grabbing:**

- Collect service information from open ports, revealing software versions and potential vulnerabilities. Telnet and scripts are common tools.

### 3. **Service Enumeration:**

- Identify services on open ports to discover potential vulnerabilities associated with specific software versions, often using tools like Nmap.

### 4. **User Enumeration:**

- Discover valid usernames through techniques like brute force attacks, user enumeration scripts, or directory harvesting.

### 5. **SNMP Enumeration:**

- Query SNMP-enabled devices for system details and configurations using SNMP enumeration tools.

### 6. **DNS Enumeration:**

- Gather information about the target's domain, subdomains, and IP addresses using tools like nslookup and dig.

### 7. **NetBIOS and SMB Enumeration:**

- Enumerate NetBIOS and SMB services on Windows systems to identify shared resources and user details, using tools like Enum4linux.

### 8. **Web Enumeration:**

- Discover hidden web resources, directories, and parameters manually or using tools like DirBuster in web application testing.

### 9. **FTP Enumeration:**

- Identify accessible directories and files via FTP to uncover potential security issues.

### 10. **Telnet Enumeration:**

- Use Telnet to connect to services like SMTP for user enumeration by checking for valid usernames.

# NetBIOS Enumeration

NetBIOS (Network Basic Input/Output System) is a legacy protocol targeted for enumeration. It reveals information about hosts, shared resources, and user accounts. Key enumeration points include:

- **Unique Names:**
  - **00:** Workstation Service (workstation name)
  - **03:** Windows Messenger service
  - **06:** Remote Access Service
  - **20:** File Service (Host Record)
  - **21:** Remote Access Service client
  - **1B:** Domain Master Browser (Primary Domain Controller)
  - **1D:** Master Browser
- **Group Names:**
  - **00:** Workstation Service (workgroup/domain name)
  - **1C:** Domain Controllers
  - **1E:** Browser Service Elections

## NBTScan

Nbtscan is a command-line tool that scans for NetBIOS name servers open on a local or remote network. It can scan an entire subnet and provide a list of NetBIOS names, IP addresses, and other information.

```
(root@DHEERA) - [/home/dheera]
# nbtscan 192.168.31.14
Doing NBT name scan for addresses from 192.168.31.14

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.31.14    METASPLOITABLE  <server>  METASPLOITABLE 00:00:00:00:00:00

(root@DHEERA) - [/home/dheera]
# nbtscan 192.168.31.215
Doing NBT name scan for addresses from 192.168.31.215

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.31.215  WINDOWS7        <server>  <unknown>      08:00:27:d1:4e:80
```

- **Basic Scan:**
  - `nbtscan 192.168.31.14 -v`
  - Displays services and their types.
- **Human-Readable Format:**
  - `nbtscan 192.168.31.14 -vh`
  - Prints services in a more readable form.
- **Packet Content Dump:**
  - `nbtscan 192.168.31.14 -d`
  - Dumps the contents of the entire packet.
- **Scan from Input File:**
  - `nbtscan -f addresses.txt`
  - Scans multiple IP addresses from a file (`addresses.txt`).

## Nmblookup

Nmblookup is used to query NetBIOS names and map them to IP addresses in a network using NetBIOS over TCP/IP queries. The options allow the name queries to be directed at a particular IP broadcast area or to a particular machine. All queries are done over UDP.

```
(root@DHEERA) - [/home/dheera]
# nmblookup -A 192.168.31.14
Looking up status of 192.168.31.14
METASPLOITABLE <00> - B <ACTIVE>
METASPLOITABLE <03> - B <ACTIVE>
METASPLOITABLE <20> - B <ACTIVE>
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00
```

```
nmblookup -A
```

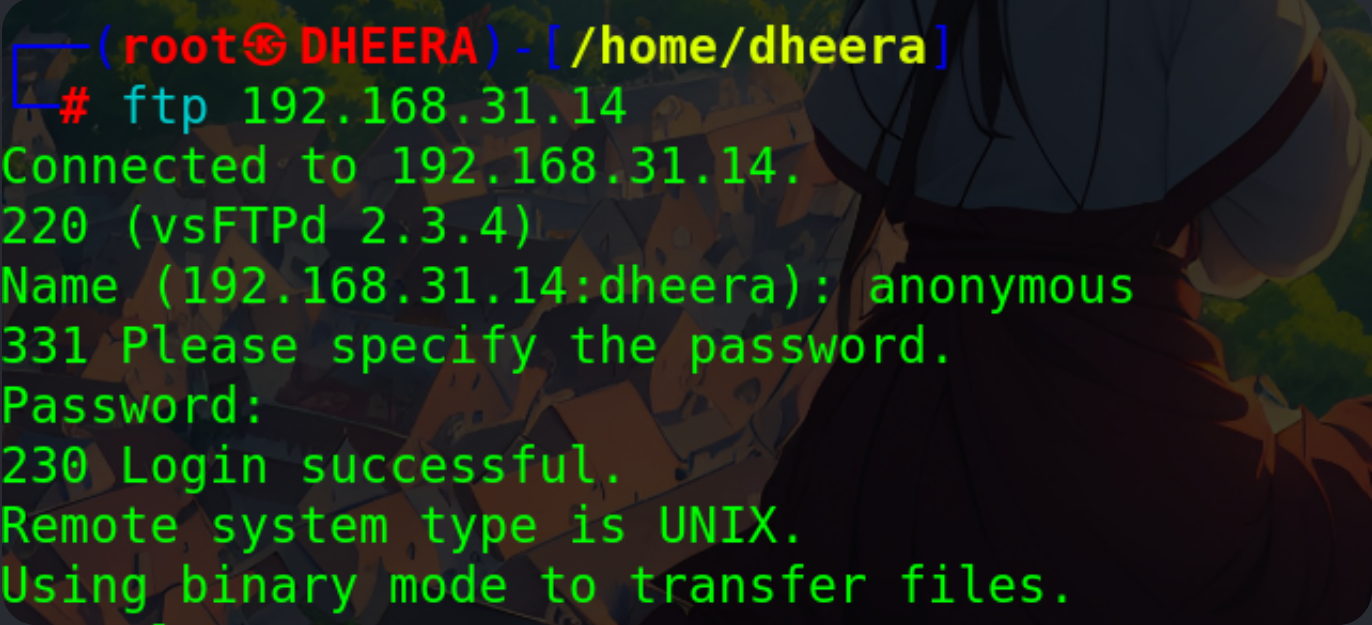
```
nmblookup -A 192.168.31.14
```

```
nmblookup -V 192.168.31.14
```

# FTP (File Transfer Protocol) Enumeration

FTP (File Transfer Protocol) enumeration is the process of gathering information about an FTP server to identify potential vulnerabilities, misconfigurations, and access points. Ethical hackers often perform FTP enumeration as part of penetration testing and security assessments

**Anonymous FTP Login:** - Attempt to log in anonymously. Many FTP servers allow anonymous access with a username of "anonymous" or "ftp" and any email address as the password. Try anonymous login using anonymous:anonymous credentials.

A terminal window with a dark background and green text. The prompt is (root@DHEERA) - [/home/dheera]. The user enters # ftp 192.168.31.14. The output shows a successful connection to 192.168.31.14 using vsFTPD 2.3.4, with the username anonymous and a successful login. The system type is UNIX and it is using binary mode for file transfers.

```
(root@DHEERA) - [/home/dheera]
# ftp 192.168.31.14
Connected to 192.168.31.14.
220 (vsFTPd 2.3.4)
Name (192.168.31.14:dheera): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Hydra Hydra is a popular password-cracking tool that can be used for FTP brute force attacks to guess usernames and passwords. `hydra -l -P ftp://192.168.31.14`

# Enum4linux

Enum4linux is used to enumerate Linux systems. Take a look at the following screenshot and observe how we have found the usernames present in a target host. Enum4linux is a tool for enumerating information from Windows and Samba systems. `#enum4linux -a`

```
#enum4linux -a 192.168.223.130
```

```
#enum4linux -U -o 192.168.1.200
```

# SMBMap

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind and is intended to simplify searching for potentially sensitive data across large networks.

```
#smbmap -H
```

```
#smbmap -H 192.168.223.128
```

```
#smbmap -H -d -u -p
```

```
#smbmap -H 192.168.223.128 -d metasploitable -u msfadmin -p msfadmin
```



# SMTP (Simple Mail Transfer Protocol) Enumeration

SMTP (Simple Mail Transfer Protocol) enumeration is a technique used in ethical hacking to gather information about email services and servers. It can reveal potential vulnerabilities, misconfigurations, and provide insights into the email infrastructure of an organization.

```
(root@DHEERA) - [/home/dheera]
# telnet 192.168.31.14 25
Trying 192.168.31.14...
Connected to 192.168.31.14.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
mail
501 5.5.4 Syntax: MAIL FROM:<address>
```