Enumeration Module - 4

by Durgesh Thakare

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.

Techniques For Enumeration

Enumeration in ethical hacking involves various techniques to gather information about a target system or network. Here are some common techniques used during the enumeration phase:

1. **Port Scanning**: Port scanning involves probing a target system to identify which network ports are open. It helps to understand which services are running on the target system. Tools like Nmap and Netcat are commonly used for port scanning.
2. **Banner Grabbing**: Banner grabbing is the process of collecting information about the services running on open ports. This information often includes software versions, service details, and sometimes even operating system information. Banner grabbing helps identify potential vulnerabilities. Telnet and banner grabbing scripts are often used.
3. **Service Enumeration**: Ethical hackers enumerate the services running on open ports to identify known vulnerabilities associated with specific software versions. They aim to discover potential entry points for exploitation. Tools like Nmap can assist in service enumeration.
4. **User Enumeration**: In some cases, ethical hackers may attempt to enumerate user accounts on the target system. The goal is to identify valid usernames, which can be valuable for further attacks. Techniques can include brute force attacks, user enumeration scripts, or directory harvesting.
5. **SNMP Enumeration**: SNMP (Simple Network Management Protocol) enumeration involves querying network devices for information about system details and configurations. SNMP enumeration tools are used to extract information from SNMP-enabled devices.
6. **DNS Enumeration**: Ethical hackers perform DNS enumeration to gather information about the target's domain, subdomains, and associated IP addresses. DNS enumeration tools and commands like nslookup and dig are used for this purpose.
7. **NTP Enumeration**: This technique involves identifying Network Time Protocol (NTP) servers in the network and their configurations. It can provide insights into time synchronization within the network.
8. **NetBIOS and SMB Enumeration**: On Windows-based systems, enumerating NetBIOS and SMB services can help identify shared resources, users, and system details. Tools like Enum4linux are used for SMB enumeration.
9. **Web Enumeration**: In web application testing, ethical hackers may enumerate web resources to find hidden directories, files, or parameters. This process can be manual or automated using tools like DirBuster..
10. **FTP Enumeration**: If the target system uses FTP (File Transfer Protocol), ethical hackers may enumerate directories and files accessible via FTP. This helps identify potential security issues.
11. **Telnet Enumeration**: Telnet can be used to connect to various services, including SMTP (Simple Mail Transfer Protocol), to perform user enumeration by checking for valid usernames.
12. **Database Enumeration**: When targeting databases, ethical hackers may enumerate database services and attempt to discover database users, tables, and configurations.

Services And Ports to Enumerate

When conducting enumeration in ethical hacking, it's essential to be aware of common services and their associated ports that are typically targeted for information gathering and potential vulnerabilities. Here is a list of services and the corresponding ports that are often enumerated during an ethical hacking engagement:

1. **FTP (File Transfer Protocol)**
   - Port: 21
   - Enumeration may involve checking for anonymous access, listing directories, and identifying files.
2. **SSH (Secure Shell)**
   - Port: 22
   - Enumeration might include checking for default credentials and authorized users.
3. **Telnet**
   - Port: 23
   - Enumeration can involve trying to log in with default or common passwords.
4. **SMTP (Simple Mail Transfer Protocol)**
   - Port: 25
   - Enumeration may include verifying valid email addresses and users using commands like VRFY and EXPN.
5. **DNS (Domain Name System)**
   - Port: 53 (both UDP and TCP)
   - Enumeration includes querying DNS servers for domain information, subdomains, and IP addresses.
6. **HTTP (Hypertext Transfer Protocol)**
   - Port: 80
   - Enumeration can involve web scraping, directory/file enumeration, and finding hidden resources.
7. **HTTPS (Secure HTTP)**
   - Port: 443
   - Enumeration includes web application scanning, SSL certificate analysis, and testing for vulnerabilities.
8. **SNMP (Simple Network Management Protocol)**
   - Port: 161 (SNMP) and 162 (SNMP Trap)
   - Enumeration involves querying SNMP-enabled devices for system details and configurations.
9. **SMB (Server Message Block)**
   - Port: 139 (NetBIOS Session Service) and 445 (Microsoft-DS)
   - Enumeration may include identifying shares, users, and system information.
10. **NetBIOS**
    - Port: 137 (NetBIOS Name Service)
    - Enumeration can involve querying NetBIOS names to find information about hosts.
11. **RDP (Remote Desktop Protocol)**
    - Port: 3389
    - Enumeration might include checking for valid usernames and accounts.
12. **MySQL**
    - Port: 3306
    - Enumeration may involve checking for valid database users and configurations.
13. **PostgreSQL**
    - Port: 5432
    - Enumeration can include verifying the presence of databases and accessing information.
14. **Oracle Database**
    - Port: 1521
    - Enumeration involves checking for Oracle databases, users, and configurations.
15. **NTP (Network Time Protocol)**
    - Port: 123
    - Enumeration can involve identifying NTP servers and their configurations.
16. **VNC (Virtual Network Computing)**
    - Port: 5900 and others
    - Enumeration includes checking for open VNC servers and attempting to access them.
17. **LDAP (Lightweight Directory Access Protocol)**
    - Port: 389 (LDAP) and 636 (LDAPS)
    - Enumeration may involve querying the LDAP directory for user and system information.
18. **SQL Server**
    - Port: 1433 (default for Microsoft SQL Server)
    - Enumeration includes checking for SQL Server instances and user accounts.
19. **POP3 (Post Office Protocol 3)**
    - Port: 110
    - Enumeration may involve checking for valid email accounts.
20. **IMAP (Internet Message Access Protocol)**
    - Port: 143
    - Enumeration includes checking for valid email accounts and messages.

NetBIOS Enumeration

NetBIOS (Network Basic Input/Output System) is a legacy networking protocol that is often targeted for enumeration in ethical hacking engagements. NetBIOS enumeration can provide information about hosts, shared resources, and user accounts on a network. Here are some common techniques and tools used for NetBIOS enumeration:

For unique names:_

00: Workstation Service (workstation name)
03: Windows Messenger service
06: Remote Access Service
20: File Service (also called Host Record)
21: Remote Access Service client
1B: Domain Master Browser – Primary Domain Controller for a domain
1D: Master Browser

For group names:-

00: Workstation Service (workgroup/domain name)
1C: Domain Controllers for a domain
1E: Browser Service Elections

Netstat

Netstat is a utility for obtaining protocol statistics, NetBIOS name table, name cache information and current TCP/IP connections over NBT (NetBIOS over TCP/IP), assisting in the resolution of NetBIOS name resolution issues. Name resolution is normally performed when NetBIOS over TCP/IP is operational

Netstat Parameters and their respective functions

Examples

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:36543         0.0.0.0:*               LISTEN
tcp       78      0 DHEERA:40800            ec2-3-12-156-111.:https CLOSE_WAIT
tcp        0      0 DHEERA:46350            ec2-3-137-12-160.:https ESTABLISHED
tcp        0      0 DHEERA:40786            ec2-3-12-156-111.:https ESTABLISHED
tcp        0      0 DHEERA:36362            ec2-3-23-161-31.u:https ESTABLISHED
tcp       64      0 DHEERA:33916            ec2-3-231-130-62.:https CLOSE_WAIT
tcp        0      0 DHEERA:33900            ec2-3-231-130-62.:https ESTABLISHED
tcp        0      0 DHEERA:49306            172.67.74.135:https     ESTABLISHED
tcp       25      0 DHEERA:55716            185.104.208.93:https    CLOSE_WAIT
tcp        0      0 DHEERA:34032            ec2-3-17-227-38.u:https ESTABLISHED
tcp        0      0 DHEERA:45394            ec2-3-17-227-38.u:https ESTABLISHED
tcp        0      0 DHEERA:48752            ec2-3-132-11-126.:https ESTABLISHED
tcp        0      0 DHEERA:33414            181.214.120.34.bc:https ESTABLISHED
tcp        0      0 DHEERA:59970            a1370dc23e25e46ce:https ESTABLISHED
tcp        0      0 DHEERA:53514            ec2-34-237-73-95.:https ESTABLISHED
```

1. To display the NetBIOS name table of a remote computer

Netstat -a

2. To see IPv4/IPv6 Group Memberships

Netstat -g

3. To display kernel interface

Netstat -i

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
```

The most basic way to run this tool is to give it a range of IP addresses. In this case, there is only one machine on the network so I will give its IP address as an example.

nbtscan 192.168.31.14

We can get a little more information by setting verbose output with the **-v** flag.

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# nbtscan 192.168.31.215 -v
Doing NBT name scan for addresses from 192.168.31.215


NetBIOS Name Table for Host 192.168.31.215:

Incomplete packet, 173 bytes long.
Name             Service          Type
---------------------------------------
WINDOWS7         <00>           UNIQUE
WORKGROUP        <00>            GROUP
WINDOWS7         <20>           UNIQUE
WORKGROUP        <1e>            GROUP

Adapter address: 08:00:27:d1:4e:80
---------------------------------------
```

nbtscan 192.168.31.14 -v

We can see some services and their types. This is sort of jumbled, which brings us to the next option, which will print the services in human-readable form. Use the **-h** flag along with the **-v** option.

nbtscan 192.168.31.14 -vh

Now we can see a bit more information that might prove to be useful. We can also set the **-d** flag to dump the contents of the entire packet.

nbtscan 192.168.31.14 -d

If you have a list of IP addresses you wish to scan stored in a file, the **-f** flag can be used to specify the input file to read from. Again, in this case, there is only one machine on the network so only that one shows up during our scan.

nbtscan -f 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 <host ip>
nmblookup -A 192.168.31.14
nmblookup -V 192.168.31.14

nmblookup is a helpful command for enumerating domain/workstation and MAC address. NetBIOS work with the help of NetBIOS suffixes as a state following information

SNMP Enumeraion

SNMP (Simple Network Management Protocol) enumeration is a common technique used in ethical hacking to gather information about network devices and systems that support SNMP. SNMP is a protocol used for managing and monitoring network devices, and enumeration can provide valuable insights into the configuration, status, and potential vulnerabilities of these devices.

During SNMP enumeration, ethical hackers can gather information about system details, network devices, interface configurations, hardware, and more. This information can be valuable for identifying potential vulnerabilities and weaknesses in the network.

NMAP

NMAP gives you the ability to use scripts to enumerate and exploit remote host with the use of the NMAP Scripting Engine. Today we will be using NMAP scripts against a remote host running the SNMP service.

```
nmap -sU -p 161 --script=snmp-info 192.168.31.14
```

snmp-interfaces

To return Network Information about the remote host run the 'snmp-interfaces'

```
nmap -sU -p 161 --script=snmp-interfaces 192.168.31.14
```

snmp-netstat

You can also gather active netstat output from a remote host running SNMP with the 'snmp-netstat' script.

```
nmap -sU -p 161 --script=snmp-netstat 192.168.31.14
```

snmp-sysdescr

Reterive the SNMP Server type and Operating system with the 'snmp-sysdescr' script.

```
nmap -sU -p 161 --script=snmp-sysdescr 192.168.31.14
```

snmp-processes

List all processes on the target machine with the 'snmp-processes' script. Be careful this will generate quit a lot of output on the screen so it is better to log it to a file.

```
nmap -sU -p 161 --script=snmp-processes 192.168.31.14
```

snmp-w32-software

List all software on the remote machine with the 'snmp-win32-software'. This will also generate a lot of output.

```
nmap -sU -p 161 --script=snmp-win32-software 192.168.31.14
```

Run All Scripts Against a Host

Finally, to run all SNMP enumeration nmap scripts against a host use the '-sC' option.

```
nmap -sU -p 161 -sV -sC 192.168.31.14
```

Enumerating SNMP Servers Community Strings

NMAP give you the ability to brute force SNMP community strings to look for valid users on the remote machine. We can do this by using the NMAP Scripting Engine and the 'snmp-brute' script.

```
nmap -sU -p 161 --script snmp-brute 127.0.0.1 --script-args snmp-brute.communitiesdb=/home/sam/comstring.txt
```

SNMPwalk

- SNMP Walk is a command that allows you to retrieve information from SNMP-enabled devices by traversing the Management Information Base (MIB) tree. It can provide a wide range of data, including system information, device interfaces, and more.

`snmpwalk -v <SNMP_version> -c <community_string> <target_IP>`

- `<SNMP_version>`: The SNMP version to use (e.g., 1, 2c, or 3).
- `<community_string>`: The community string, which acts as a password for SNMP access (usually "public" or "private" for read-only access).
- `<target_IP>`: The IP address of the SNMP-enabled device.

SNMP Get

- The SNMP Get command is used to retrieve specific information from an SNMP-enabled device, typically a single variable from the MIB tree.

`snmpget -v <SNMP_version> -c <community_string> <target_IP> <OID>`

- `<SNMP_version>`, `<community_string>`, and `<target_IP>` are the same as in SNMP Walk.
- `<OID>`: The Object Identifier that specifies the data you want to retrieve.

SNMPcheck

Same as `snmpwalk` but give nice output

`snmpcheck -t 192.168.1.X -c public`

LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) enumeration is a technique used in ethical hacking to gather information about directory services, such as Active Directory, LDAP-based databases, and network user accounts. It can provide insights into the structure of the directory, user accounts, groups, and potentially sensitive information

Several tools and scripts are available for automating LDAP enumeration. These tools can streamline the process and provide organized results. Some common LDAP enumeration tools include:

ldapsearch

This is a command-line utility included with most LDAP client installations. It allows you to perform LDAP searches and retrieve information from LDAP directories. The usage typically involves specifying the LDAP server, port, search base, and query filters.

```
ldapsearch -x -h <LDAP_server> -p <port> -b <search_base> -D <bind_DN> -W <query_filter>
```

- `-x`: Use simple authentication.
- `-h`: Specifies the LDAP server.
- `-p`: Specifies the LDAP server's port (usually 389).
- `-b`: Specifies the search base, which is the starting point for the LDAP search.
- `-D`: Specifies the distinguished name (DN) to bind to the LDAP server.
- `-W`: Prompts for the password associated with the bind DN.
- `<query_filter>`: Defines the search filter to retrieve specific information.
- **LDAP Enumeration Scripts:** Various Python and Perl scripts are available for LDAP enumeration, such as "ldapenum," which can perform tasks like user enumeration and group enumeration.

Enumeration Queries

Enumeration typically involves crafting LDAP search queries to retrieve information about user accounts, groups, and organizational units (OUs). Examples of enumeration queries might include:

- Listing all user accounts in the directory:

```
ldapsearch -x -h <LDAP_server> -p <port> -b <search_base> -D <bind_DN> -W "(objectClass=user)"
```

Enumerating group memberships for a specific user:

```
ldapsearch -x -h <LDAP_server> -p <port> -b <search_base> -D <bind_DN> -W "(&(objectClass=user)(sAMAccountName=<username>))"
```

NTP Enumeration & NFS Enumeration

Enumeration of NTP (Network Time Protocol) and NFS (Network File System) services is an important part of ethical hacking and penetration testing, as it can reveal vulnerabilities, misconfigurations, and potential attack vectors. Here's an overview of how to perform enumeration for NTP and NFS services:

NTP EnumerationNTP Query (ntpq): The `ntpq` command-line utility allows you to query NTP servers for various information, including system status, peer associations, and time synchronization details.

```
ntpq -c peers <target_IP>
```

- `-c peers` specifies the command to retrieve peer information.
- `<target_IP>` is the IP address of the NTP server.

NTP Monlist Attack: NTP servers that have not been properly configured can be used for Distributed Denial of Service (DDoS) attacks due to their "monlist" command. Ethical hackers can use tools like "NTPdc" to perform this type of enumeration:

```
ntpdc -n -c monlist <target_IP>
```

- -n specifies not to perform a DNS resolution.
- -c monlist requests the monlist information.

NFS Enumeration

Showmount:

- The `showmount` command is used to display the NFS exports on a remote server. It can reveal information about shared directories and their configurations.

```
showmount -e <target_IP>
```

NFSstat:

- The `nfsstat` command can provide information about NFS statistics, client/server counts, and performance-related data.

```
nfsstat -s <target_IP>
```

NFS Enumeration Tools:

- Various enumeration tools and scripts exist for NFS enumeration, such as "enum4linux." Enum4linux is primarily used for enumerating information from Windows and Samba systems but can also be applied to NFS shares.

```
enum4linux -a <target_IP>
```

FTP (File Transfer Protocol) Enumeration

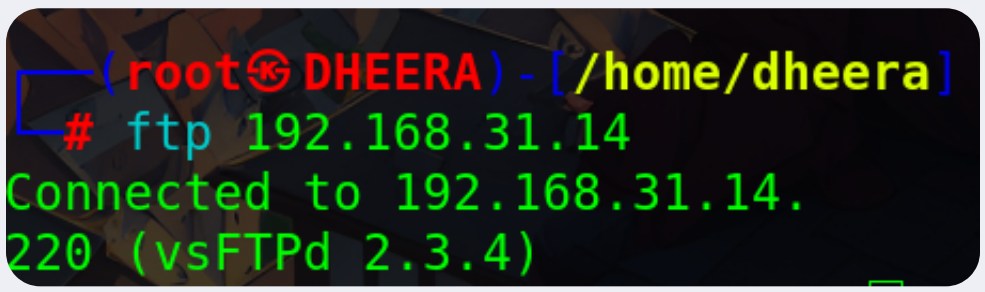
FTP (File Transfer Protocol) enumeration is the process of gathering information about an FTP server to identify potential vulnerabilities, misconfigurations, and access points. Ethical hackers often perform FTP enumeration as part of penetration testing and security assessments

Ethical hackers may use techniques to enumerate valid usernames on the FTP server, which can be helpful in subsequent attacks. This may involve trying different usernames and observing the server's responses.

Connect to the FTP Server

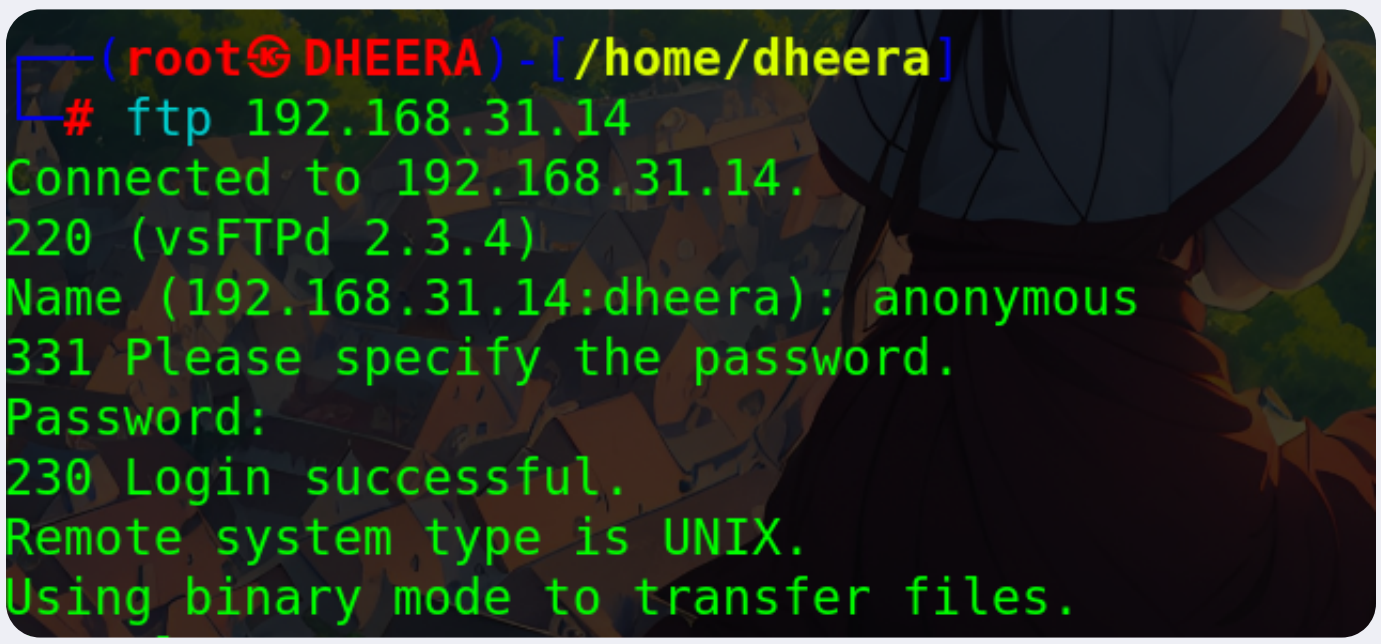
Use an FTP client or command-line tool to connect to the FTP server. Common command-line FTP clients include `ftp` and `ncftp`. For example:

```
ftp 192.168.31.14
```



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.



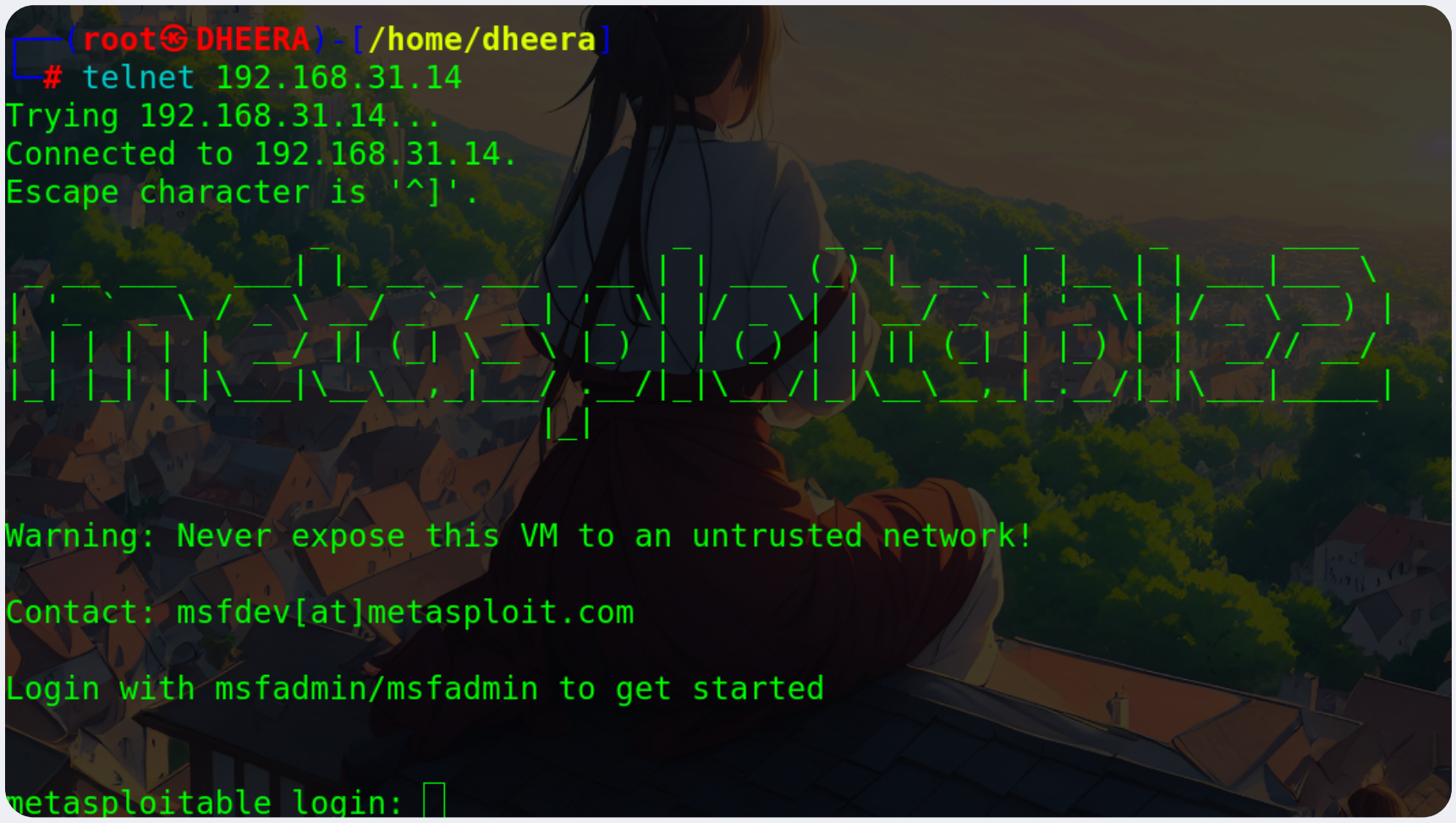
Hydra

Hydra is a popular password-cracking tool that can be used for FTP brute force attacks to guess usernames and passwords.

```
hydra -l <username> -P <password_list> ftp://192.168.31.14
```

Telnet Enumeration

Enumeration of Telnet services involves gathering information about Telnet servers to identify potential vulnerabilities, weaknesses, and unauthorized access points. Ethical hackers often perform Telnet enumeration as part of penetration testing and security assessments. Here's how to enumerate Telnet services:



Connect to the Telnet Server

```
telnet 192.168.31.14
```

nmap

Use nmap with the Telnet enumeration script to identify Telnet services and retrieve additional information.

```
nmap -p 23 --script=telnet-ntlm-info,telnet-encryption,telnet-ntlm-v2,msrpc-enum 192.168.31.14
```

SSH Enumeration

Enumeration of SSH (Secure Shell) services involves gathering information about SSH servers to identify potential vulnerabilities, misconfigurations, and access points. Ethical hackers often perform SSH enumeration as part of penetration testing and security assessments

Connect to the SSH Server:

Use an SSH client, such as OpenSSH or PuTTY, to connect to the SSH server. For example:

```
ssh <username>@<target_IP>
```

nmap

Use nmap with the SSH enumeration script to identify SSH services and retrieve additional information.

```
nmap -p 22 --script=ssh-auth-methods,ssh-hostkey,ssh-run <target_IP>
```

Hydra

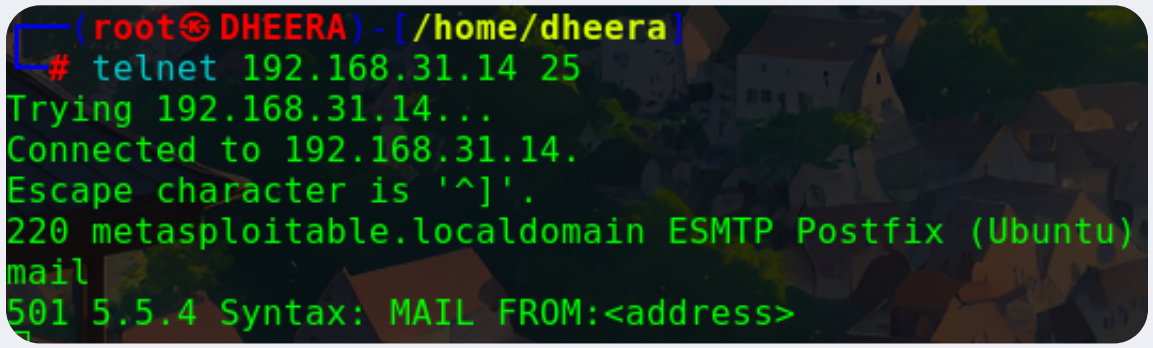
Hydra is a popular password-cracking tool that can be used for SSH brute force attacks to guess usernames and passwords.

```
hydra -l <username> -P <password_list> ssh://<target_IP>
```

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.

Connect to the SMTP Server: - Use a Telnet client or command-line tool to connect to the SMTP server. You can typically connect on port 25, which is the default SMTP port. For example:




```
telnet <target_IP> 25
```

SMTP Commands

After connecting to the SMTP server, use SMTP commands to interact with the server, send email, and retrieve information. Common SMTP commands include `HELO`, `EHLO`, `MAIL FROM`, `RCPT TO`, and `QUIT`.

nmap

Use nmap with the SMTP enumeration script to identify SMTP services and retrieve additional information.

```
nmap -p 25 --script=smtp-commands,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720 <target_IP>
```

DNS (Domain Name System) Enumeration

DNS (Domain Name System) enumeration is the process of gathering information about DNS servers, domains, and subdomains. It's a crucial step in ethical hacking and penetration testing as it can reveal information about an organization's network infrastructure and potential attack vectors.

a. Query DNS Servers:

- You can use various command-line tools to manually query DNS servers for information. The most common tool for this purpose is nslookup:

```
nslookup <target_domain>
```

b. **Zone Transfer:** - If the DNS server is misconfigured and allows zone transfers, you can use `nslookup` or other tools to attempt a zone transfer. Zone transfers can reveal all the DNS records for a domain.

```
nslookup
> set type=any

> ls -d <target_domain>
```

nmap

- Use nmap with the DNS enumeration script to identify DNS servers and retrieve additional information.

```
nmap -p 53 --script=dns-zone-transfer,dns-recursion <target_IP>
```

dnsenum

- The `dnsenum` tool is a DNS enumeration script that automates the process of gathering information about DNS servers, domains, and subdomains.

```
dnsenum <target_domain>
```

DNS Zone Transfer:

- Attempt to perform a zone transfer using tools like `dig`. Zone transfers can provide a list of DNS records for a domain, including subdomains, mail servers, and more.

```
dig axfr <target_domain> @<target_IP>
```

4. Subdomain Enumeration:

- Use subdomain enumeration tools like `Sublist3r`, `Amass`, or `OWASP Amass` to discover subdomains associated with a target domain.

```
sublist3r -d <target_domain>
```

5. Google Dorks:

- Use Google Dorks to search for DNS-related information. You can use Google to search for specific DNS records, subdomains, or other DNS-related data.

```
site:<target_domain> -inurl:www
```

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
```

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 <host ip>
#enum4linux -a 192.168.223.130
#enum4linux -U -o 192.168.1.200
```

smtp-user-enum

smtp-user-enum 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. It could be adapted to work against other vulnerable SMTP daemons, but this hasn't been done as of v1.0.

```
#smtp-user-enum -M VREY -u -t
#smtp-user-enum -M VREY -u root -t
```

-u: set the user name -t: host Server host running SMTP service

```
#smtp-user-enum -M VRFY -U -t
#smtp-user-enum -M VRFY -U /root/Desktop/user.txt -t
```

-M: mode Method to use for username guessing EXPN, VRFY or RCPT -U: file File of usernames to check via SMTP service -t: host Server host running SMTP service

```
#smtp-user-enum -M VRFY -D -u -t
#smtp-user-enum -M VRFY -D mail.ignite.lab -u raj -t 192.168.1.107
```

-D: dom Domain to append to supplied user list to make email addresses; Use this option when you want to guess valid email addresses instead of just usernames.