FSCT 8560 - Network Security 2

Sukh Atwal
Yoshiaki Ryuzaki

Assignment 2

Script

You can run the file, internal.sh for the internal machine and firewall.sh for the machine that's going to use the firewall. You can go to the terminal and run 'sudo bash internal.sh', replacing the internal.sh with firewall.sh for the other machine after setting the permissions using chmod.

The configurable areas are the internal and external interfaces and external IP which should all match your computer. Afterwards, you can allow/block any ports that you may require

****The internal firewall script is as follows:**

```
#!/bin/bash

dns=8.8.8.8
gwaddr=192.168.10.1

sudo ifconfig enp0s8 down
sudo ifconfig enp0s3 192.168.10.2 netmask 255.255.255.0 broadcast 192.168.10.255
sudo route add default gw $gwaddr

echo "nameserver $dns" > /etc/resolv.conf

iptables -F
iptables -X

/sbin/service save
```

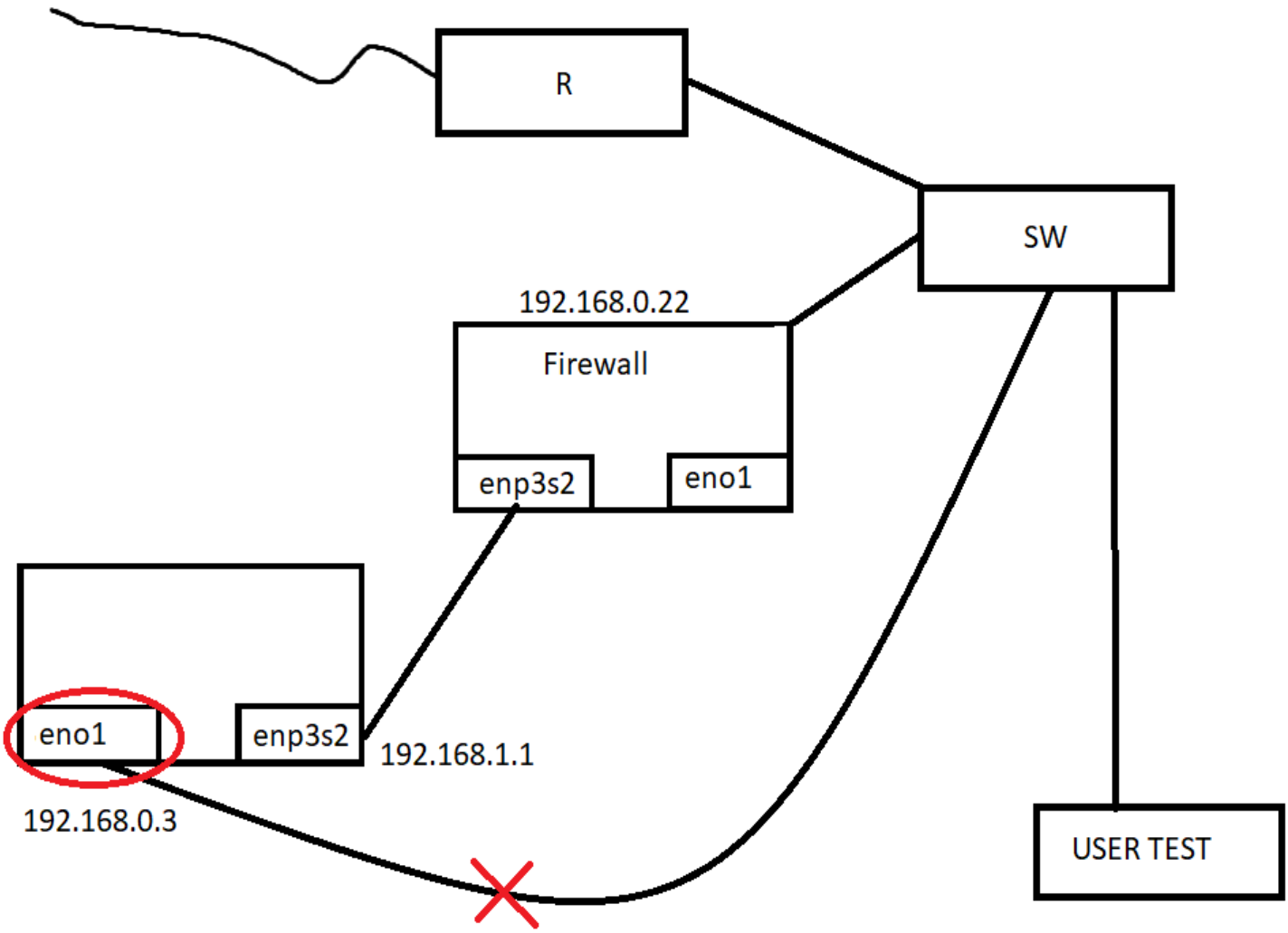
****The host firewall script is as follows:**

```
#!/bin/bash

#####################################################
#############User Configurable Section##############
#####################################################

#Network interface of the internal and external, change depending on your personal network
internalinterface="enp3s2"
externalinterface="eno1"

#ipaddress
externalip="192.168.0.20" ##IP Address of Firewall that you get using IFCONFIG
internalip="192.168.10.1"
internalserverip="192.168.10.2"
internalnet="192.168.10.0/24"

#ports allowed
allowedports="80,22,21,20" #TCPPorts that you allow to go through
highports="1000:65535"
allowedudpports="53,5060" #UDPPorts that you allow to go through

#ICMP types that you allow, change depending on your needs
firsttypeallowed="8"
secondtypeallowed="0"

#####################################################
##########Implementation of iptables rules########
#####################################################

#Utilities
assignip="/usr/sbin/ifconfig"
ipt="/usr/sbin/iptables"

#network configuration
$assignip $internalinterface $internalip up
sudo echo "1" >/proc/sys/net/ipv4/ip_forward

# Default Policies
$ipt -F
$ipt -X
$ipt -t nat -F
$ipt -P INPUT DROP
$ipt -P OUTPUT DROP
$ipt -P FORWARD DROP

#Forward packets

#Option1 Forwarding All Traffic
```

```
#$ipt -A FORWARD -i $internalinterface -o $externalinterface -j ACCEPT
#$ipt -A FORWARD -o $internalinterface -i $externalinterface -j ACCEPT

# POSTROUTING Outbounding Traffic
$ipt -A POSTROUTING -t nat -o $externalinterface -j MASQUERADE

#$ipt -A PREROUTING -t nat -i $externalinterface -j DNAT --to-destination $internalserverip

#option2 Forwarding designed Traffic
#$ipt -A PREROUTING -t nat -i $externalinterface -p tcp -d $externalip --dport 80 -j DNAT --to-destination
$internalserverip

#$ipt -A FORWARD -i $externalinterface -o $internalinterface -p tcp -d $internalserverip --dport 80 -m state --state NEW
-j ACCEPT

#Prerouting and forwarding TCP Traffic
$ipt -A PREROUTING -t nat -i $externalinterface -p tcp --sport $highports -d $externalip -m multiport --dports
$allowedports -j DNAT --to-destination $internalserverip

$ipt -A FORWARD -i $externalinterface -o $internalinterface -p tcp --sport $highports -d $internalserverip -m multiport --
dports $allowedports -m state --state NEW,ESTABLISHED -j ACCEPT

$ipt -A FORWARD -i $internalinterface -o $externalinterface -p tcp -s $internalserverip -m multiport --sports
$allowedports -d 0/0 -m multiport --dports $highports -m state --state ESTABLISHED,RELATED -j ACCEPT


#Prerouting and forwarding UDP Traffic
$ipt -A PREROUTING -t nat -i $externalinterface -p udp --sport $highports -d $externalip -m multiport --dports
$allowedudpports -j DNAT --to-destination $internalserverip

$ipt -A FORWARD -i $externalinterface -o $internalinterface -p udp --sport $highports -d $internalserverip -m multiport -
-dports $allowedudpports -m state --state NEW,ESTABLISHED -j ACCEPT

$ipt -A FORWARD -i $internalinterface -o $externalinterface -p udp -s $internalserverip -m multiport --sports
$allowedudpports -d 0/0 -m multiport --dports $highports -m state --state ESTABLISHED,RELATED -j ACCEPT

# Forwarding ICMP Traffic

$ipt -A PREROUTING -t nat -i $externalinterface -p icmp --icmp-type any -d $externalip -j DNAT --to-destination
$internalserverip

$ipt -A FORWARD -i $externalinterface -o $internalinterface -p icmp --icmp-type $firsttypeallowed -d $internalserverip -j
ACCEPT

$ipt -A FORWARD -i $externalinterface -o $internalinterface -p icmp --icmp-type $secondtypeallowed -d
$internalserverip -j ACCEPT

$ipt -A FORWARD -i $internalinterface -o $externalinterface -p icmp --icmp-type $firsttypeallowed -s $internalserverip -j
ACCEPT
```

```
$ipt -A FORWARD -i $internalinterface -o $externalinterface -p icmp --icmp-type $secondtypeallowed -s $internalserverip -j ACCEPT

#Allow TCP connections initiated from internal client
$ipt -A FORWARD -i $internalinterface -o $externalinterface -p tcp -s $internalserverip --sport $highports -d 0/0 -m multiport --dports $allowedports -m state --state NEW,ESTABLISHED -j ACCEPT

$ipt -A FORWARD -i $externalinterface -o $internalinterface -p tcp -m multiport --sports $allowedports -d $internalserverip -m multiport --dports $highports -m state --state ESTABLISHED,RELATED -j ACCEPT

#Allow UDP connections initiated from internal client
$ipt -A FORWARD -i $internalinterface -o $externalinterface -p udp -s $internalserverip --sport $highports -d 0/0 -m multiport --dports $allowedudpports -m state --state NEW,ESTABLISHED -j ACCEPT
$ipt -A FORWARD -i $externalinterface -o $internalinterface -p udp -m multiport --sports $allowedudpports -d $internalserverip -m multiport --dports $highports -m state --state ESTABLISHED,RELATED -j ACCEPT

#Drop spoofed packets (internal addresses as source coming from outside)
$ipt -A FORWARD -i $externalinterface -o $internalinterface -s $internalnet -j DROP

#Minimum Delay for FTP and SSH, Maximum Throughput for FTP Data
$ipt -t mangle -A PREROUTING -m multiport -p tcp --sports 21,22 -j TOS --set-tos Minimize-Delay
$ipt -t mangle -A PREROUTING -p tcp --sport 20 -j TOS --set-tos Maximize-Throughput
$ipt -t mangle -A PREROUTING -m multiport -p tcp --dports 21,22 -j TOS --set-tos Minimize-Delay
$ipt -t mangle -A PREROUTING -p tcp --sport 20 -j TOS --set-tos Maximize-Throughput

#Save rules
/sbin/service iptables save

#List current iptables rules, current accounting information and reset counters
$ipt -L -n -Z -v
$ipt -t nat -L PREROUTING -v
$ipt -t nat -L POSTROUTING -v
```

Diagram of Firewall



Firewall Test

Rule#	Test Description	Tools Used	Expected Result	Pass/Fail
1	Inbound/Outbound TCP packets on allowed ports	Wireshark, hping, Nmap	See TCP packets going through only on allowed ports	Pass
2	Inbound/Outbound UDP packets on allowed ports	ping	See UDP packets going through only on allowed ports, able to see UDP and use the DNS	Pass
3	Inbound/Outbound ICMP packets based on type	ping	See ICMP reply packets going through only on allowed type	Pass
4	Packets that fall through default rule will be dropped	ping	See packets drop if they fall through default rule	Pass
5	Drop all packets destined for firewall host from outside		Drop the packet if it's from the outside	-
6	Don't accept packets with a source address from the outside matching the internal network	Wireshark, hping	If outside source matches internal, drops the packet	Pass
7	Reject connections coming the wrong way	Wireshark, hping	Denies packets going to higher ports	Pass
8	Don't allow Telnet packets	Wireshark, hping	Drops any telnet packet that comes through	Pass
9	Block all external traffic directed to ports 32768-32775, 137-139, TCP ports 111 and 515	Wireshark, hping	Blocks traffic that's going to the ports specified	Pass
10	For FTP and SSH services, set control connections to 'Minimum Delay' and FTP data to 'Maximum Throughput'	hping		Pass
11	Accept Fragment	Wireshark, hping	See if fragments are received	Pass
12	Drop all TCP with SYN and FIN packets	Wireshark, hping	If the packet has SYN and FIN, it's dropped	Pass

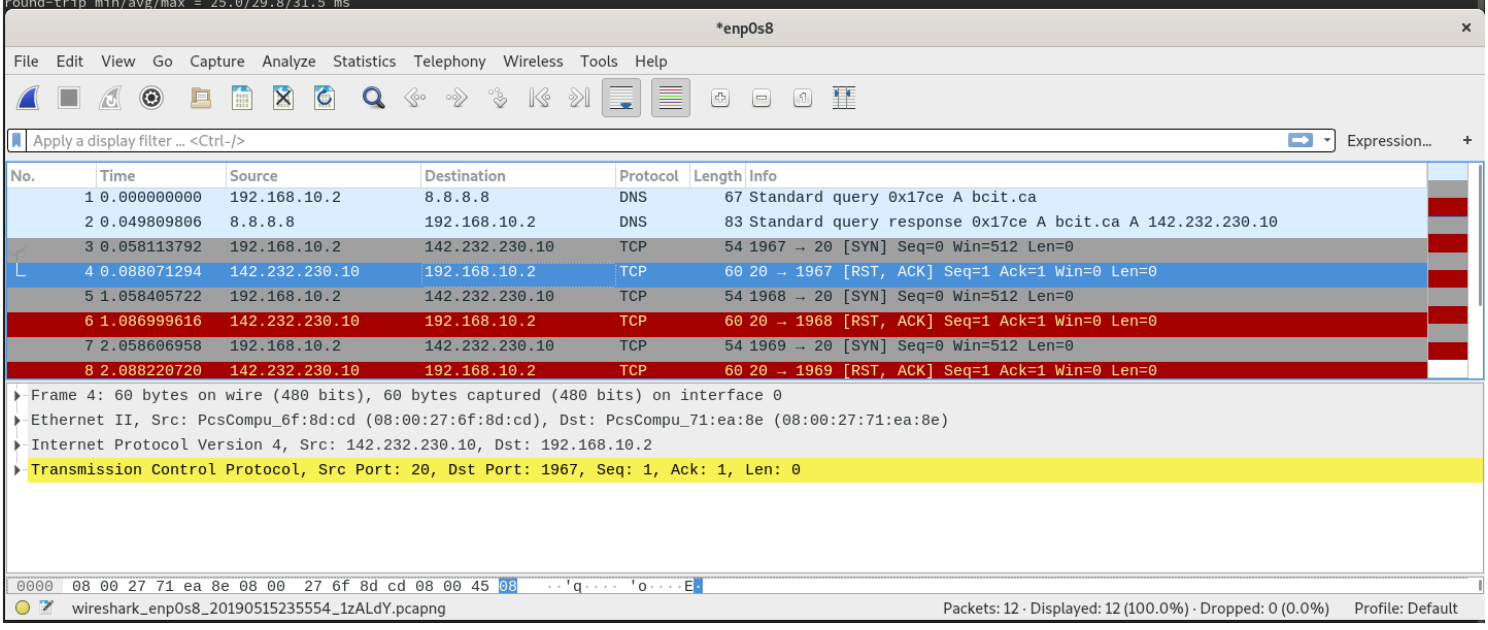
Results

Rule 1

Used Nmap to see which tcp ports are being used, followed by hping to see if the packets interact, which they do for both port 20 and 80. Used Wireshark to verify both.

```
17:01:39(-)root@localhost:~$ nmap 192.168.0.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-15 17:05 PDT
Nmap scan report for 192.168.0.20
Host is up (0.00059s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh
80/tcp  closed http
443/tcp closed https
MAC Address: 98:90:96:DC:E4:A8 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds
17:05:55(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 20
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=20 flags=RA seq=0 win=0 rtt=1.8 ms
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=20 flags=RA seq=1 win=0 rtt=1.8 ms
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 2 packets received, 34% packet loss
round-trip min/avg/max = 1.8/1.8/1.8 ms
17:10:44(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 80
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.9 ms
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=1.8 ms
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=1.7 ms
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.8/1.9 ms
```

```
[root@localhost ~]# hping3 bcit.ca -S -p 20
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes
len=46 ip=142.232.230.10 ttl=246 DF id=38813 sport=20 flags=RA seq=0 win=0 rtt=30.9 ms
len=46 ip=142.232.230.10 ttl=246 DF id=39028 sport=20 flags=RA seq=1 win=0 rtt=30.7 ms
len=46 ip=142.232.230.10 ttl=246 DF id=41260 sport=20 flags=RA seq=2 win=0 rtt=29.9 ms
len=46 ip=142.232.230.10 ttl=246 DF id=39616 sport=20 flags=RA seq=3 win=0 rtt=31.5 ms
len=46 ip=142.232.230.10 ttl=246 DF id=46131 sport=20 flags=RA seq=4 win=0 rtt=31.0 ms
len=46 ip=142.232.230.10 ttl=246 DF id=40977 sport=20 flags=RA seq=5 win=0 rtt=25.0 ms
^C
--- bcit.ca hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 25.0/29.8/31.5 ms
```



Rule 2 + 3

Pinged www.google.ca to check if the UDP ports were open as well as if the ICMP protocols were working correctly, which they were. Used Wireshark to verify.

```
17:35:29(~)root@localhost:Assignment2$ ping www.google.ca
PING www.google.ca (172.217.3.195) 56(84) bytes of data.
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=1 ttl=51 time=5
.48 ms
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=2 ttl=51 time=5
.20 ms
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=3 ttl=51 time=5
.47 ms
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=4 ttl=51 time=5
.27 ms
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=5 ttl=51 time=5
.29 ms
64 bytes from sea15s12-in-f3.1e100.net (172.217.3.195): icmp_seq=6 ttl=51 time=5
.28 ms
^C
--- www.google.ca ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 5.209/5.336/5.485/0.119 ms
```

```
[root@localhost ~]# ping www.google.com
PING www.google.com (216.58.217.36) 56(84) bytes of data.
64 bytes from den03s10-in-f36.1e100.net (216.58.217.36): icmp_seq=1 ttl=54 time=20.10 ms
64 bytes from den03s10-in-f36.1e100.net (216.58.217.36): icmp_seq=2 ttl=54 time=38.2 ms
64 bytes from den03s10-in-f36.1e100.net (216.58.217.36): icmp_seq=3 ttl=54 time=30.7 ms
64 bytes from den03s10-in-f36.1e100.net (216.58.217.36): icmp_seq=4 ttl=54 time=22.7 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 20.952/28.135/38.192/6.869 ms
[root@localhost ~]#
```

*enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
8	0.142080293	8.8.8.8	192.168.10.2	DNS	182	Standard query response 0xb3f7 PTR 36.217.58.216.in-addr.arpa PTR den03…
9	1.091435549	192.168.10.2	216.58.217.36	ICMP	98	Echo (ping) request id=0x1471, seq=2/512, ttl=64 (reply in 10)
10	1.129606076	216.58.217.36	192.168.10.2	ICMP	98	Echo (ping) reply id=0x1471, seq=2/512, ttl=54 (request in 9)
11	2.092272121	192.168.10.2	216.58.217.36	ICMP	98	Echo (ping) request id=0x1471, seq=3/768, ttl=64 (reply in 12)
12	2.122930187	216.58.217.36	192.168.10.2	ICMP	98	Echo (ping) reply id=0x1471, seq=3/768, ttl=54 (request in 11)
13	3.095417197	192.168.10.2	216.58.217.36	ICMP	98	Echo (ping) request id=0x1471, seq=4/1024, ttl=64 (reply in 14)
14	3.118084368	216.58.217.36	192.168.10.2	ICMP	98	Echo (ping) reply id=0x1471, seq=4/1024, ttl=54 (request in 13)

```
▸ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
▸ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 216.58.217.36
▸ Internet Control Message Protocol
```

```
0000  08 00 27 6f 8d cd 08 00  27 71 ea 8e 08 00 45 00   ··'o···· 'q····E·
```

wireshark_enp0s8_20190515235811_IRBYDU.pcapng Packets: 14 · Displayed: 14 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Rule 4

Shows the packet getting dropped if it falls from the default rules.

```
[root@localhost ~]# ping 8.8.8.8 -c 5
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 126ms
```

Rule 5

Rule 6

Used the same internal IP, it gets sent but never received.

```
[root@localhost ~]# hping3 192.168.10.2 -S -p 80
HPING 192.168.10.2 (enp0s8 192.168.10.2): S set, 40 headers + 0 data bytes
^C
--- 192.168.10.2 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
```

Rule 7

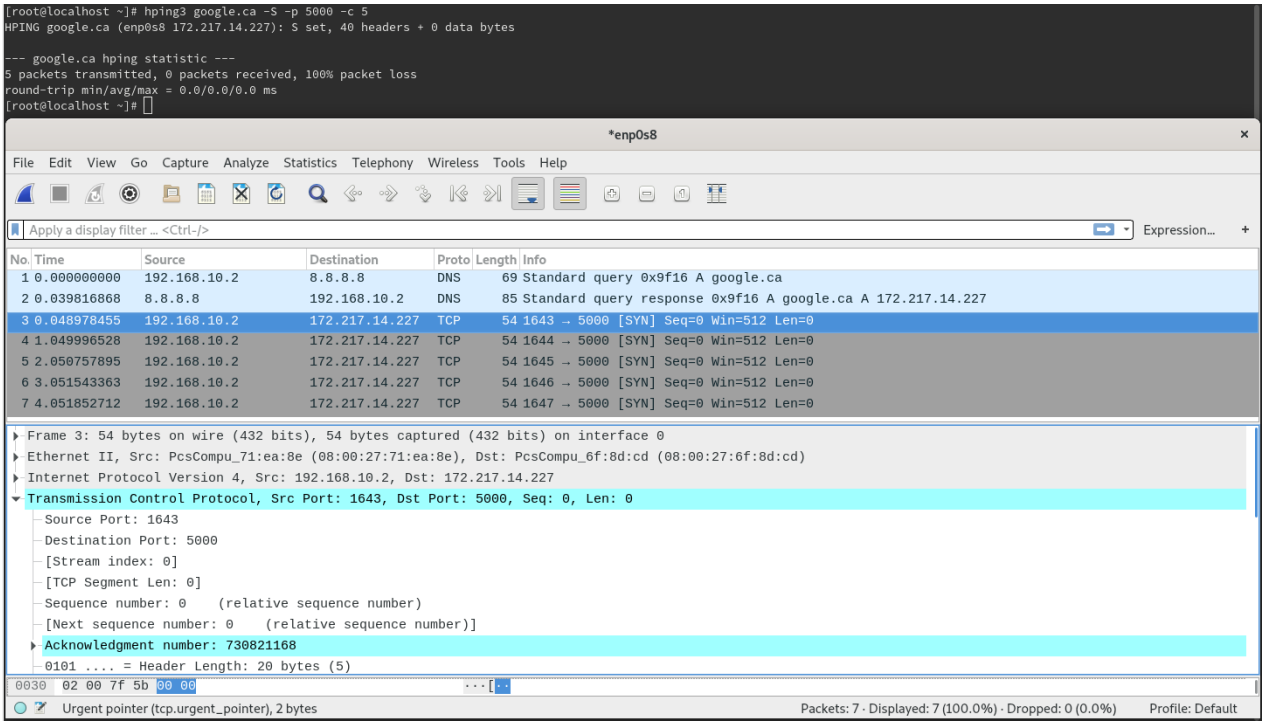
Opened ports 5000 and 8000 to see if either would go through, neither did. Used Wireshark to verify, no response from either of the ports.

```
[root@localhost ~]# hping3 google.ca -S -p 8000 -c 5
HPING google.ca (enp0s8 172.217.14.227): S set, 40 headers + 0 data bytes

--- google.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]# hping3 google.ca -S -p 5000 -c 5
HPING google.ca (enp0s8 172.217.14.227): S set, 40 headers + 0 data bytes

--- google.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
```

```
[root@localhost ~]# '/home/zz/Desktop/firewall.sh'
[root@localhost ~]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.10.2         tcp spts:cadlock
2:65535 multiport dports http,ssh,ftp,ftp-data,https,irdmi,commplex-main state
 NEW,ESTABLISHED
ACCEPT     tcp  --  192.168.10.2         anywhere             multiport sports
 http,ssh,ftp,ftp-data,https,irdmi,commplex-main multiport dports cadlock2:655
35 state RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             192.168.10.2         udp spts:cadlock
2:65535 multiport dports domain,sip state NEW,ESTABLISHED
ACCEPT     udp  --  192.168.10.2         anywhere             multiport sports
 domain,sip multiport dports cadlock2:65535 state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             192.168.10.2         icmp echo-reques
t
ACCEPT     icmp --  anywhere             192.168.10.2         icmp echo-reply
ACCEPT     icmp --  192.168.10.2         anywhere             icmp echo-reques
t
ACCEPT     icmp --  192.168.10.2         anywhere             icmp echo-reply
ACCEPT     tcp  --  192.168.10.2         anywhere             tcp spts:cadlock
2:65535 multiport dports http,ssh,ftp,ftp-data,https,irdmi,commplex-main state
 NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.10.2         multiport sports
 http,ssh,ftp,ftp-data,https,irdmi,commplex-main multiport dports cadlock2:655
35 state RELATED,ESTABLISHED
ACCEPT     udp  --  192.168.10.2         anywhere             udp spts:cadlock
2:65535 multiport dports domain,sip state NEW,ESTABLISHED
ACCEPT     udp  --  anywhere             192.168.10.2         multiport sports
 domain,sip multiport dports cadlock2:65535 state RELATED,ESTABLISHED
DROP       all  --  192.168.10.0/24      anywhere

Chain OUTPUT (policy DROP)
target     prot opt source               destination
[root@localhost ~]#
```

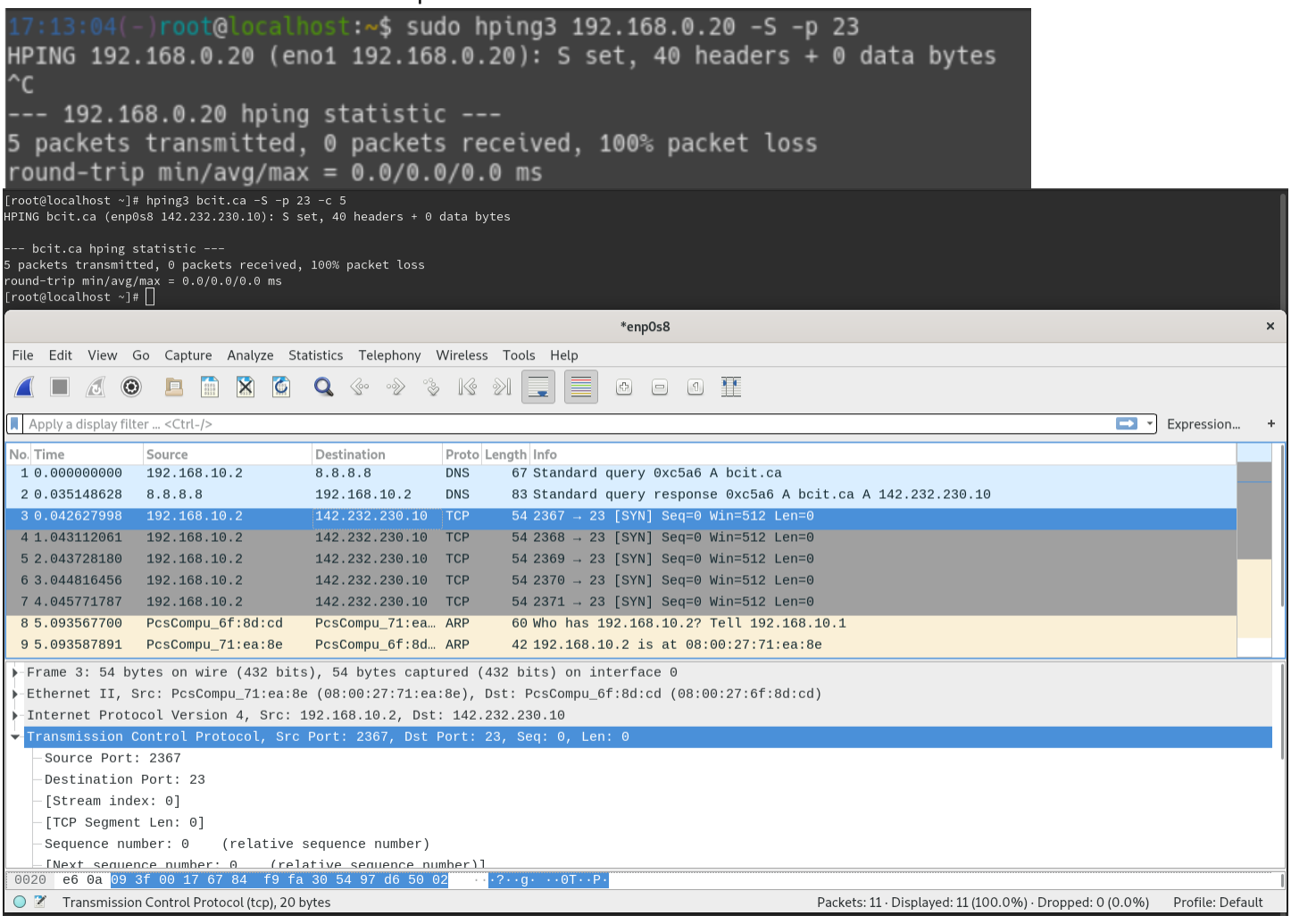
```
#!/bin/bash


#####################################################
############User Configurable Section##############
#####################################################

#interfaces
internalinterface="enp0s8"
externalinterface="enp0s3"


#ipaddress
externalip="172.16.0.44"
internalip="192.168.10.1"
internalserverip="192.168.10.2"
internalnet="192.168.10.0/24"

#ports allowed
allowedports="80,22,21,20,443,8000,5000" #TCPPorts
highports="1000:65535"
allowedudpports="53,5060"

#ICMP types
firsttypeallowed="8"
secondtypeallowed="0"

#####################################################
#########Implementation of iptablesables rules########
#####################################################


#network configuration
ifconfig $internalinterface $internalip up
sudo echo "1" >/proc/sys/net/ipv4/ip_forward
```

sh Tab Width: 8 Ln 20, Col 40 INS



Rule 8

Used hping to test if Telnet packets (Port 23) are all blocked. Packets are transmitted but not received, showcasing that it works. Wireshark verifies with no response shown as well.



Rule 9

Used hping to test if all the external traffic directed to the ports are blocked, which they are. Packets are sent but no response is received. All of them are verified with Wireshark.

```
17:13:24(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 32770
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
17:13:55(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 23770
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
17:14:02(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 139
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
17:14:08(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 111
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.20 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
17:14:16(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 515
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.20 hping statistic ---
6 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
[root@localhost ~]# hping3 bcit.ca -S -p 32770 -c 5
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes

--- bcit.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
```

*enp0s8

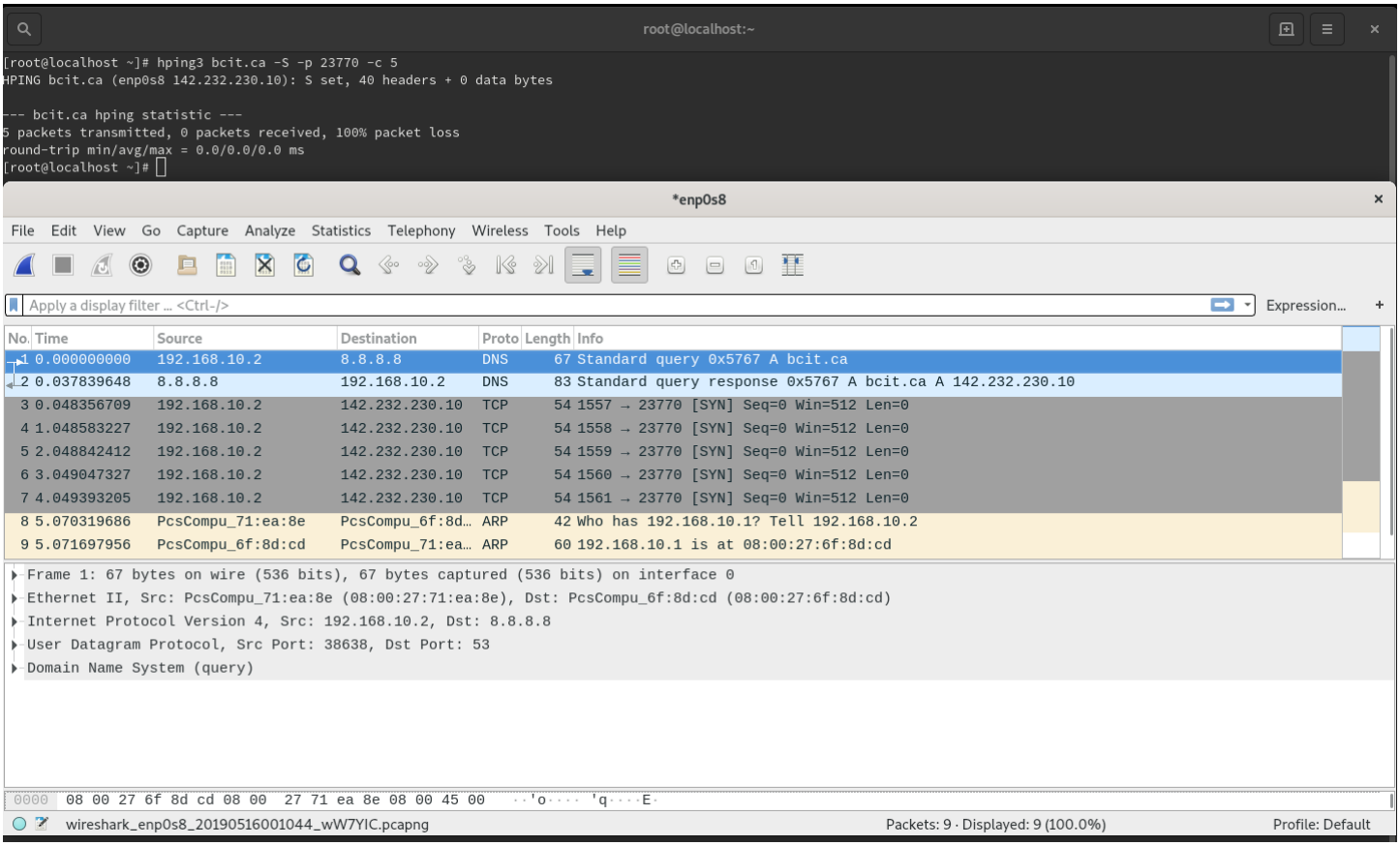
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

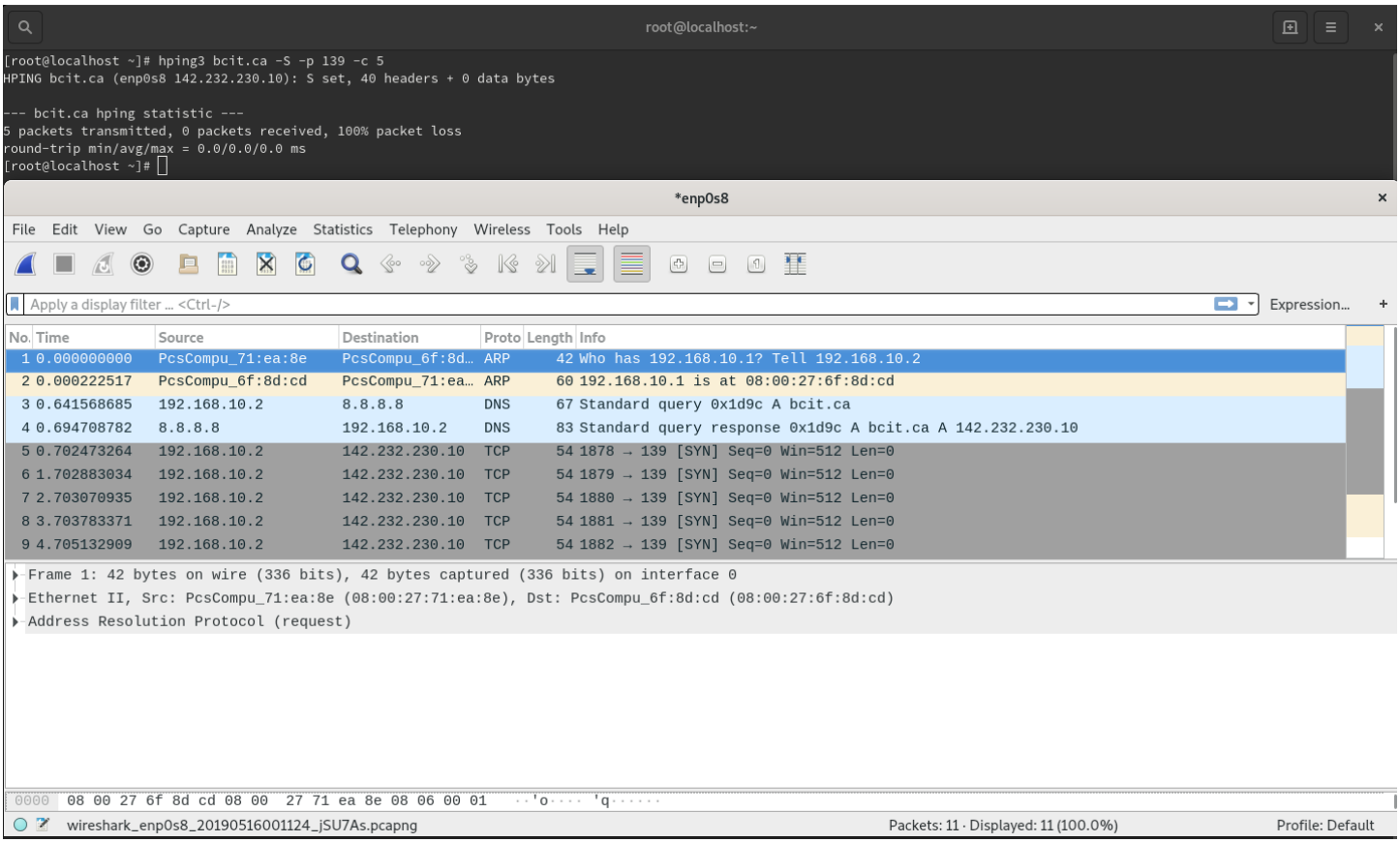
Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000000	192.168.10.2	8.8.8.8	DNS	67	Standard query 0x432d A bcit.ca
2	0.031406021	8.8.8.8	192.168.10.2	DNS	83	Standard query response 0x432d A bcit.ca A 142.232.230.10
3	0.038849586	192.168.10.2	142.232.230.10	TCP	54	2048 → 32770 [SYN] Seq=0 Win=512 Len=0
4	1.039117099	192.168.10.2	142.232.230.10	TCP	54	2049 → 32770 [SYN] Seq=0 Win=512 Len=0
5	2.039482632	192.168.10.2	142.232.230.10	TCP	54	2050 → 32770 [SYN] Seq=0 Win=512 Len=0
6	3.040356786	192.168.10.2	142.232.230.10	TCP	54	2051 → 32770 [SYN] Seq=0 Win=512 Len=0
7	4.040879909	192.168.10.2	142.232.230.10	TCP	54	2052 → 32770 [SYN] Seq=0 Win=512 Len=0
8	5.348937936	PcsCompu_71:ea:8e	PcsCompu_6f:8d…	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
9	5.349652135	PcsCompu_6f:8d:cd	PcsCompu_71:ea…	ARP	60	192.168.10.1 is at 08:00:27:6f:8d:cd

```
▸ Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
▸ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 142.232.230.10
▾ Transmission Control Protocol, Src Port: 2048, Dst Port: 32770, Seq: 0, Len: 0
    Source Port: 2048
    Destination Port: 32770
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
0020  e6 0a 08 00 80 02 48 91  17 fe 2e 88 fe ef 50 02   ······H· ··.···P·
```

Transmission Control Protocol (tcp), 20 bytes Packets: 9 · Displayed: 9 (100.0%) · Dropped: 0 (0.0%) Profile: Default


root@localhost:~
[root@localhost ~]# hping3 bcit.ca -S -p 23770 -c 5
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes
--- bcit.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Proto Length Info
1 0.000000000 192.168.10.2 8.8.8.8 DNS 67 Standard query 0x5767 A bcit.ca
2 0.037839648 8.8.8.8 192.168.10.2 DNS 83 Standard query response 0x5767 A bcit.ca A 142.232.230.10
3 0.048356709 192.168.10.2 142.232.230.10 TCP 54 1557 → 23770 [SYN] Seq=0 Win=512 Len=0
4 1.048583227 192.168.10.2 142.232.230.10 TCP 54 1558 → 23770 [SYN] Seq=0 Win=512 Len=0
5 2.048842412 192.168.10.2 142.232.230.10 TCP 54 1559 → 23770 [SYN] Seq=0 Win=512 Len=0
6 3.049047327 192.168.10.2 142.232.230.10 TCP 54 1560 → 23770 [SYN] Seq=0 Win=512 Len=0
7 4.049393205 192.168.10.2 142.232.230.10 TCP 54 1561 → 23770 [SYN] Seq=0 Win=512 Len=0
8 5.070319686 PcsCompu_71:ea:8e PcsCompu_6f:8d… ARP 42 Who has 192.168.10.1? Tell 192.168.10.2
9 5.071697956 PcsCompu_6f:8d:cd PcsCompu_71:ea… ARP 60 192.168.10.1 is at 08:00:27:6f:8d:cd
Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
Internet Protocol Version 4, Src: 192.168.10.2, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 38638, Dst Port: 53
Domain Name System (query)
0000 08 00 27 6f 8d cd 08 00 27 71 ea 8e 08 00 45 00
wireshark_enp0s8_20190516001044_wW7YIC.pcapng
Packets: 9 · Displayed: 9 (100.0%)
Profile: Default


root@localhost:~
[root@localhost ~]# hping3 bcit.ca -S -p 139 -c 5
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes
--- bcit.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Proto Length Info
1 0.000000000 PcsCompu_71:ea:8e PcsCompu_6f:8d… ARP 42 Who has 192.168.10.1? Tell 192.168.10.2
2 0.000222517 PcsCompu_6f:8d:cd PcsCompu_71:ea… ARP 60 192.168.10.1 is at 08:00:27:6f:8d:cd
3 0.641568685 192.168.10.2 8.8.8.8 DNS 67 Standard query 0x1d9c A bcit.ca
4 0.694708782 8.8.8.8 192.168.10.2 DNS 83 Standard query response 0x1d9c A bcit.ca A 142.232.230.10
5 0.702473264 192.168.10.2 142.232.230.10 TCP 54 1878 → 139 [SYN] Seq=0 Win=512 Len=0
6 1.702883034 192.168.10.2 142.232.230.10 TCP 54 1879 → 139 [SYN] Seq=0 Win=512 Len=0
7 2.703070935 192.168.10.2 142.232.230.10 TCP 54 1880 → 139 [SYN] Seq=0 Win=512 Len=0
8 3.703783371 192.168.10.2 142.232.230.10 TCP 54 1881 → 139 [SYN] Seq=0 Win=512 Len=0
9 4.705132909 192.168.10.2 142.232.230.10 TCP 54 1882 → 139 [SYN] Seq=0 Win=512 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
Address Resolution Protocol (request)
0000 08 00 27 6f 8d cd 08 00 27 71 ea 8e 08 06 00 01
wireshark_enp0s8_20190516001124_jSU7As.pcapng
Packets: 11 · Displayed: 11 (100.0%)
Profile: Default

```
[root@localhost ~]# hping3 bcit.ca -S -p 111 -c 5
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes

--- bcit.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
```

*enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000000	192.168.10.2	8.8.8.8	DNS	67	Standard query 0x33b5 A bcit.ca
2	0.040519567	8.8.8.8	192.168.10.2	DNS	83	Standard query response 0x33b5 A bcit.ca A 142.232.230.10
3	0.051044866	192.168.10.2	142.232.230.10	TCP	54	3010 → 111 [SYN] Seq=0 Win=512 Len=0
4	1.051545738	192.168.10.2	142.232.230.10	TCP	54	3011 → 111 [SYN] Seq=0 Win=512 Len=0
5	2.051713145	192.168.10.2	142.232.230.10	TCP	54	3012 → 111 [SYN] Seq=0 Win=512 Len=0
6	3.052314322	192.168.10.2	142.232.230.10	TCP	54	3013 → 111 [SYN] Seq=0 Win=512 Len=0
7	4.052837701	192.168.10.2	142.232.230.10	TCP	54	3014 → 111 [SYN] Seq=0 Win=512 Len=0
8	5.332894650	PcsCompu_6f:8d:cd	PcsCompu_71:ea…	ARP	60	Who has 192.168.10.2? Tell 192.168.10.1
9	5.332917734	PcsCompu_71:ea:8e	PcsCompu_6f:8d…	ARP	42	192.168.10.2 is at 08:00:27:71:ea:8e

```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
▸ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 57111, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  08 00 27 6f 8d cd 08 00  27 71 ea 8e 08 00 45 00   ··'o···· 'q····E·
```

wireshark_enp0s8_20190516001209_NqTSuS.pcapng Packets: 9 · Displayed: 9 (100.0%) Profile: Default

```
[root@localhost ~]# hping3 bcit.ca -S -p 515 -c 5
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 0 data bytes

--- bcit.ca hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost ~]#
```

*enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000000	192.168.10.2	8.8.8.8	DNS	67	Standard query 0x4dda A bcit.ca
2	0.027536999	8.8.8.8	192.168.10.2	DNS	83	Standard query response 0x4dda A bcit.ca A 142.232.230.10
3	0.036452308	192.168.10.2	142.232.230.10	TCP	54	2210 → 515 [SYN] Seq=0 Win=512 Len=0
4	1.036824937	192.168.10.2	142.232.230.10	TCP	54	2211 → 515 [SYN] Seq=0 Win=512 Len=0
5	2.037670397	192.168.10.2	142.232.230.10	TCP	54	2212 → 515 [SYN] Seq=0 Win=512 Len=0
6	3.038064494	192.168.10.2	142.232.230.10	TCP	54	2213 → 515 [SYN] Seq=0 Win=512 Len=0
7	4.038353256	192.168.10.2	142.232.230.10	TCP	54	2214 → 515 [SYN] Seq=0 Win=512 Len=0
8	5.390293259	PcsCompu_6f:8d:cd	PcsCompu_71:ea…	ARP	60	Who has 192.168.10.2? Tell 192.168.10.1
9	5.390314211	PcsCompu_71:ea:8e	PcsCompu_6f:8d…	ARP	42	192.168.10.2 is at 08:00:27:71:ea:8e

```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
▸ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 54894, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  08 00 27 6f 8d cd 08 00  27 71 ea 8e 08 00 45 00   ··'o···· 'q····E·
```

wireshark_enp0s8_20190516001246_lSeVvo.pcapng Packets: 11 · Displayed: 11 (100.0%) Profile: Default

Rule 10

Testing the ssh to localhost and GitHub

```
[root@localhost ~]# ssh git@github.com
The authenticity of host 'github.com (192.30.253.112)' can't be established.
RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.
Are you sure you want to continue connecting (yes/no)? no
Host key verification failed.
[root@localhost ~]# ssh localhost
ssh: connect to host localhost port 22: Connection refused
[root@localhost ~]# ssh git@github.com
The authenticity of host 'github.com (192.30.253.112)' can't be established.
RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,192.30.253.112' (RSA) to the list of known hosts.
git@github.com: Permission denied (publickey).
[root@localhost ~]#
```

Rule 11

Testing if fragments can be received using hping and frags (f) and data size of 1024 which they can as we see a response to our reply. Verified using Wireshark.

```
17:14:25(-)root@localhost:~$ sudo hping3 192.168.0.20 -S -p 80 -f -d 1024
HPING 192.168.0.20 (eno1 192.168.0.20): S set, 40 headers + 1024 data bytes
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.9 ms
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=1.6 ms
len=46 ip=192.168.0.20 ttl=63 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=3.2 ms
^C
--- 192.168.0.20 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.6/2.2/3.2 ms
```

```
[root@localhost ~]# hping3 bcit.ca -S -p 80 -f -d 1024
HPING bcit.ca (enp0s8 142.232.230.10): S set, 40 headers + 1024 data bytes
len=46 ip=142.232.230.10 ttl=246 DF id=38897 sport=80 flags=SA seq=0 win=1608 rtt=30.0 ms
len=46 ip=142.232.230.10 ttl=246 DF id=55835 sport=80 flags=SA seq=1 win=1608 rtt=31.0 ms
len=46 ip=142.232.230.10 ttl=246 DF id=39699 sport=80 flags=SA seq=2 win=1608 rtt=170.9 ms
len=46 ip=142.232.230.10 ttl=246 DF id=56985 sport=80 flags=SA seq=3 win=1608 rtt=29.4 ms
^C
--- bcit.ca hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 29.4/65.3/170.9 ms
```

*enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Proto	Length	Info
3	0.041911039	192.168.10.2	142.232.230.10	TCP	1078	1060 → 80 [SYN] Seq=0 Win=512 Len=1024 [TCP segment of a reassembled PDU]
4	0.070611326	142.232.230.10	192.168.10.2	TCP	60	80 → 1060 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0
5	0.070652426	192.168.10.2	142.232.230.10	TCP	54	1060 → 80 [RST] Seq=1 Win=0 Len=0
6	1.042324287	192.168.10.2	142.232.230.10	TCP	1078	1061 → 80 [SYN] Seq=0 Win=512 Len=1024 [TCP segment of a reassembled PDU]
7	1.071899019	142.232.230.10	192.168.10.2	TCP	60	80 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0
8	1.071950412	192.168.10.2	142.232.230.10	TCP	54	1061 → 80 [RST] Seq=1 Win=0 Len=0
9	2.042670370	192.168.10.2	142.232.230.10	TCP	1078	1062 → 80 [SYN] Seq=0 Win=512 Len=1024 [TCP segment of a reassembled PDU]
	2.211587146	142.232.230.10	192.168.10.2	TCP	60	80 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0
	2.211616644	192.168.10.2	142.232.230.10	TCP	54	1062 → 80 [RST] Seq=1 Win=0 Len=0
	3.043324555	192.168.10.2	142.232.230.10	TCP	1078	1063 → 80 [SYN] Seq=0 Win=512 Len=1024 [TCP segment of a reassembled PDU]

```
▸ Frame 6: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_71:ea:8e (08:00:27:71:ea:8e), Dst: PcsCompu_6f:8d:cd (08:00:27:6f:8d:cd)
▸ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 142.232.230.10
▾ Transmission Control Protocol, Src Port: 1061, Dst Port: 80, Seq: 0, Len: 1024
    Source Port: 1061
    Destination Port: 80
    [Stream index: 1]
0020  e6 0a 04 25 00 50 56 a7  18 99 58 d6 b4 fa 50 02   ···%·PV· ··X···P·
```

Transmission Control Protocol (tcp), 20 bytes Packets: 16 · Displayed: 16 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Rule 12

If it has SYN and FIN in the packet, it's blocked which shows as the 4 packets are never received. Verified by Wireshark as well.