TU765
Digital Forensics &
Cyber Security

DFCS H3015 -
Network Security
[1114.VLE-BN]

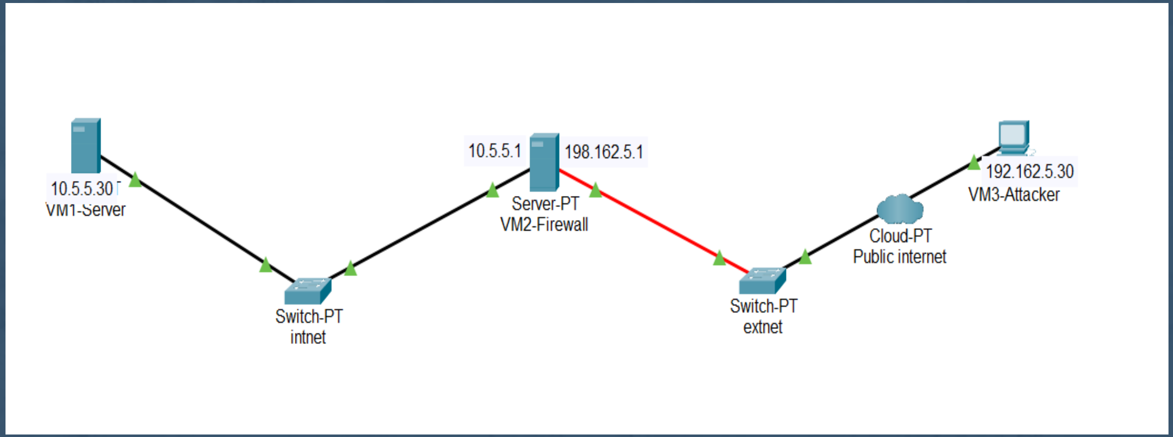
Nftable

Student Name: Sebastian Konefal

Student Number: b00168561

Email address: b00168561@mytudublin.ie

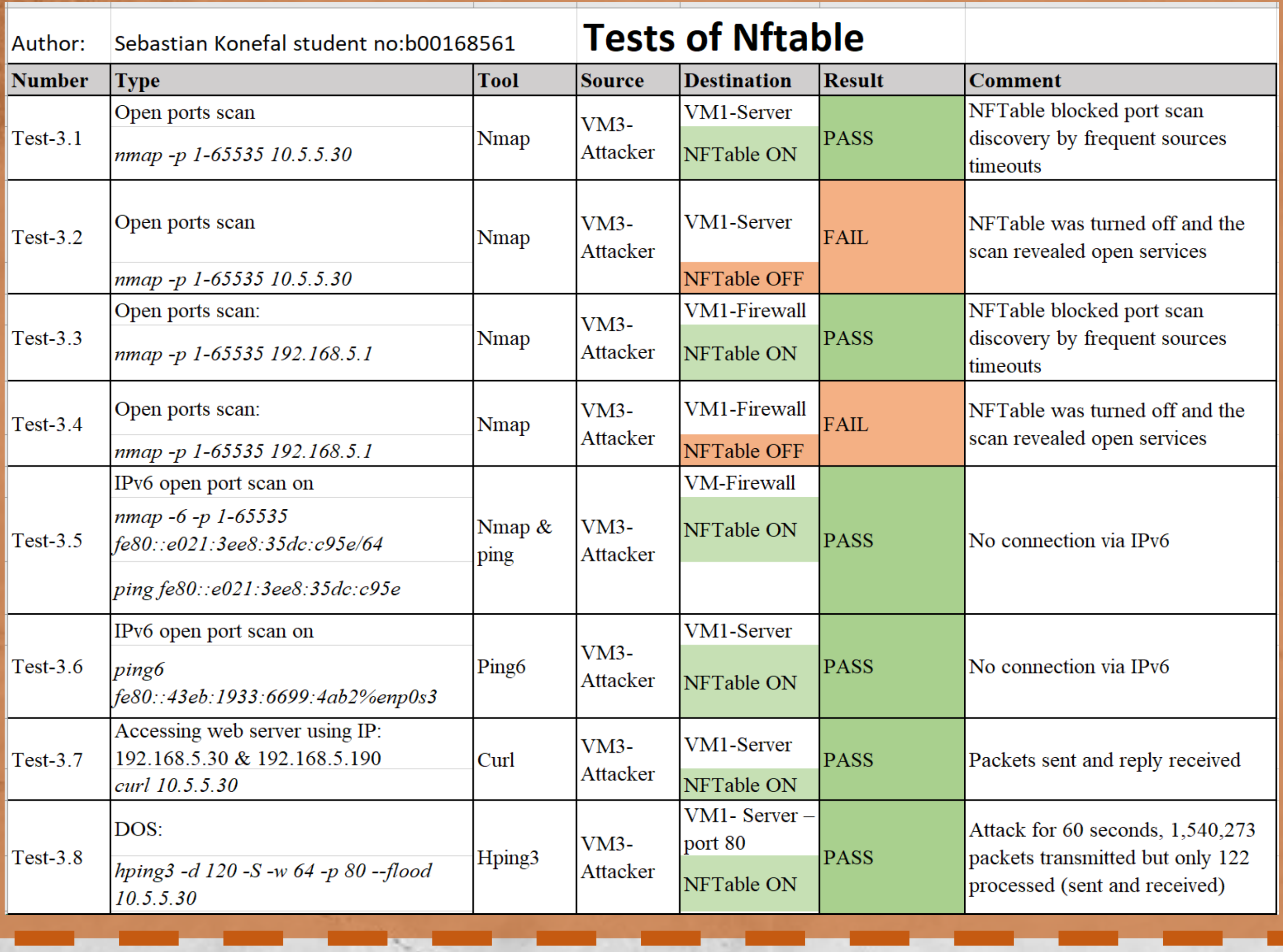
Topology and main features:



Main features:

- Modular Structure organised into chains
- Flood Attack Prevention
- Security Timeouts for SSH
- Dedicated IP range for privileged SSH access
- Connection Tracking
- Port Filtering

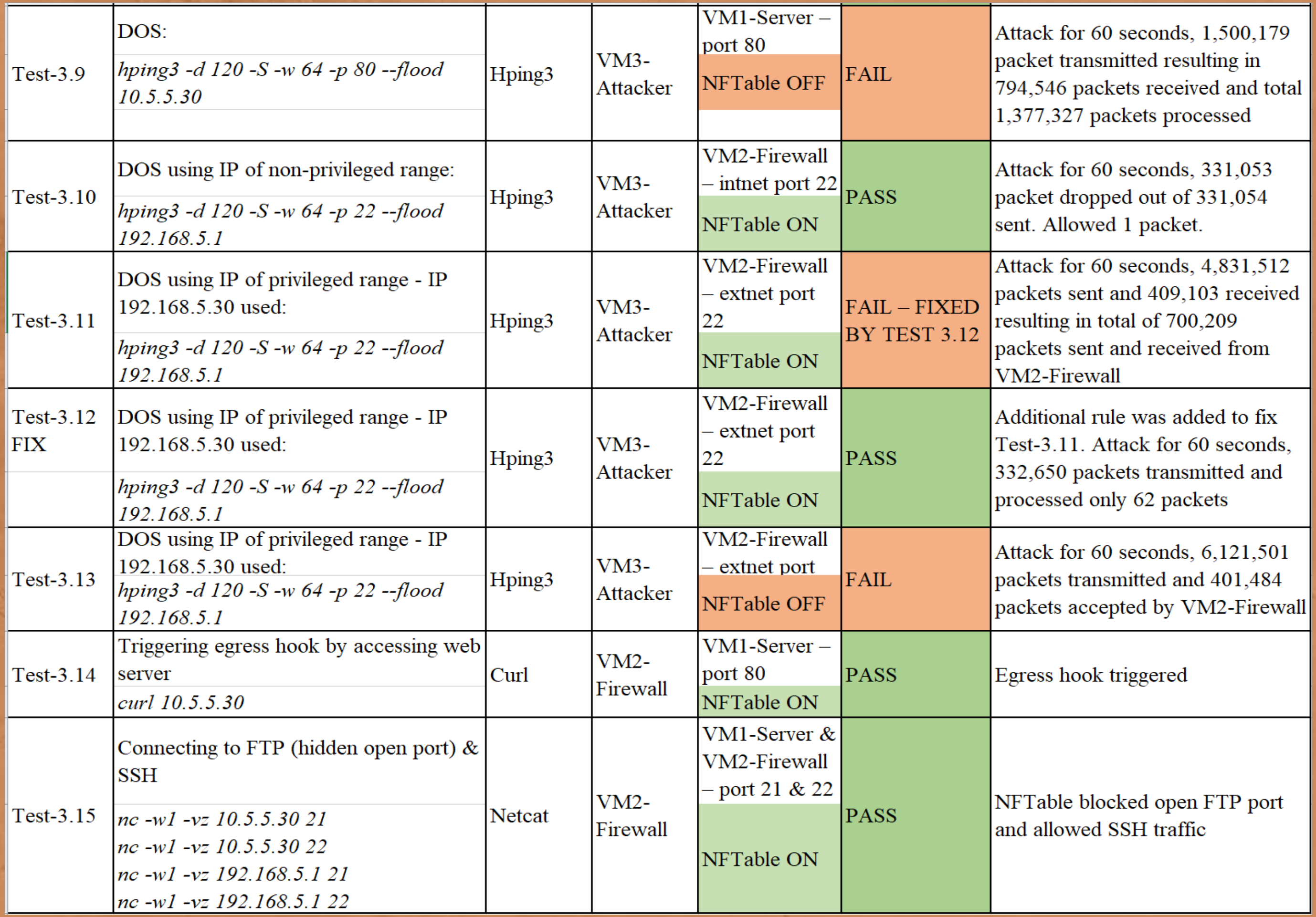
Summary of tests:



Author: Sebastian Konefal student no:b00168561

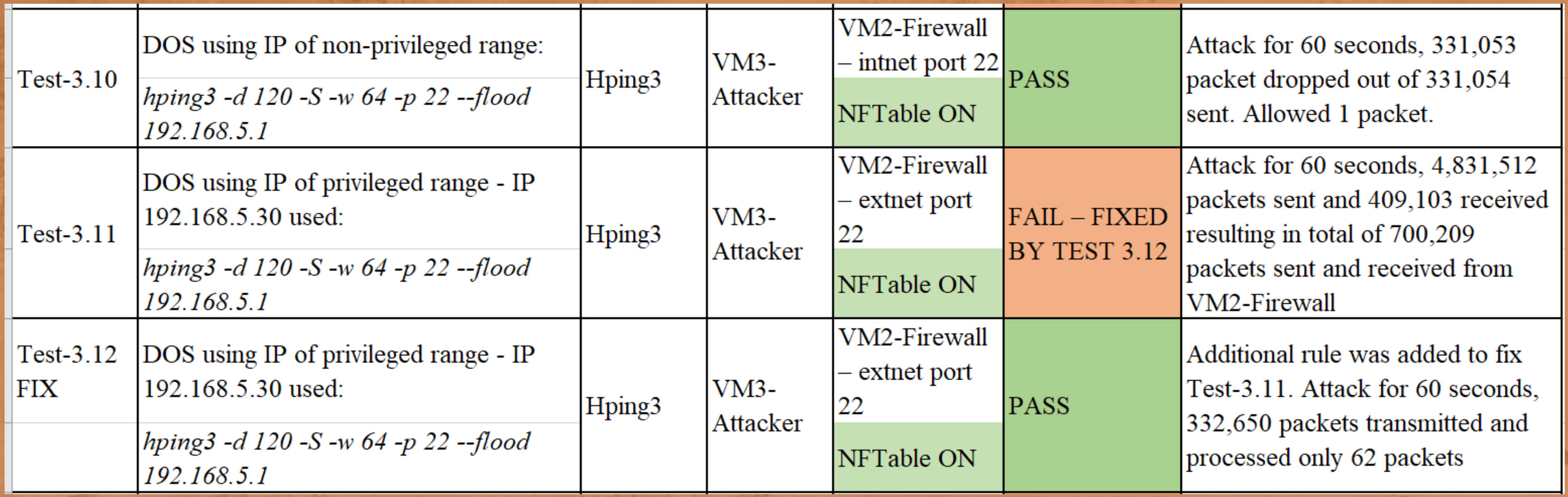
Tests of Nftable

Number	Type	Tool	Source	Destination	Result	Comment
Test-3.1	Open ports scan *nmap -p 1-65535 10.5.5.30*	Nmap	VM3-Attacker	VM1-Server NFTable ON	PASS	NFTable blocked port scan discovery by frequent sources timeouts
Test-3.2	Open ports scan *nmap -p 1-65535 10.5.5.30*	Nmap	VM3-Attacker	VM1-Server NFTable OFF	FAIL	NFTable was turned off and the scan revealed open services
Test-3.3	Open ports scan: *nmap -p 1-65535 192.168.5.1*	Nmap	VM3-Attacker	VM1-Firewall NFTable ON	PASS	NFTable blocked port scan discovery by frequent sources timeouts
Test-3.4	Open ports scan: *nmap -p 1-65535 192.168.5.1*	Nmap	VM3-Attacker	VM1-Firewall NFTable OFF	FAIL	NFTable was turned off and the scan revealed open services
Test-3.5	IPv6 open port scan on *nmap -6 -p 1-65535 fe80::e021:3ee8:35dc:c95e/64* *ping fe80::e021:3ee8:35dc:c95e*	Nmap & ping	VM3-Attacker	VM-Firewall NFTable ON	PASS	No connection via IPv6
Test-3.6	IPv6 open port scan on *ping6 fe80::43eb:1933:6699:4ab2%enp0s3*	Ping6	VM3-Attacker	VM1-Server NFTable ON	PASS	No connection via IPv6
Test-3.7	Accessing web server using IP: 192.168.5.30 & 192.168.5.190 *curl 10.5.5.30*	Curl	VM3-Attacker	VM1-Server NFTable ON	PASS	Packets sent and reply received
Test-3.8	DOS: *hping3 -d 120 -S -w 64 -p 80 --flood 10.5.5.30*	Hping3	VM3-Attacker	VM1- Server – port 80 NFTable ON	PASS	Attack for 60 seconds, 1,540,273 packets transmitted but only 122 processed (sent and received)



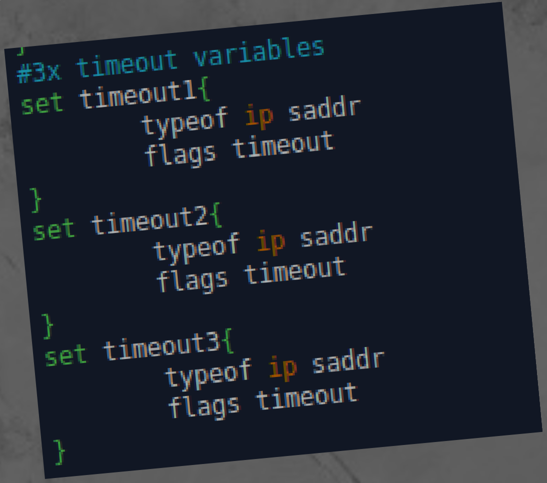
Test-3.9	DOS: *hping3 -d 120 -S -w 64 -p 80 --flood 10.5.5.30*	Hping3	VM3-Attacker	VM1-Server – port 80 NFTable OFF	FAIL	Attack for 60 seconds, 1,500,179 packet transmitted resulting in 794,546 packets received and total 1,377,327 packets processed
Test-3.10	DOS using IP of non-privileged range: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – intnet port 22 NFTable ON	PASS	Attack for 60 seconds, 331,053 packet dropped out of 331,054 sent. Allowed 1 packet.
Test-3.11	DOS using IP of privileged range - IP 192.168.5.30 used: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – extnet port 22 NFTable ON	FAIL – FIXED BY TEST 3.12	Attack for 60 seconds, 4,831,512 packets sent and 409,103 received resulting in total of 700,209 packets sent and received from VM2-Firewall
Test-3.12 FIX	DOS using IP of privileged range - IP 192.168.5.30 used: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – extnet port 22 NFTable ON	PASS	Additional rule was added to fix Test-3.11. Attack for 60 seconds, 332,650 packets transmitted and processed only 62 packets
Test-3.13	DOS using IP of privileged range - IP 192.168.5.30 used: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – extnet port NFTable OFF	FAIL	Attack for 60 seconds, 6,121,501 packets transmitted and 401,484 packets accepted by VM2-Firewall
Test-3.14	Triggering egress hook by accessing web server *curl 10.5.5.30*	Curl	VM2-Firewall	VM1-Server – port 80 NFTable ON	PASS	Egress hook triggered
Test-3.15	Connecting to FTP (hidden open port) & SSH *nc -w1 -vz 10.5.5.30 21* *nc -w1 -vz 10.5.5.30 22* *nc -w1 -vz 192.168.5.1 21* *nc -w1 -vz 192.168.5.1 22*	Netcat	VM2-Firewall	VM1-Server & VM2-Firewall – port 21 & 22 NFTable ON	PASS	NFTable blocked open FTP port and allowed SSH traffic

Test case example

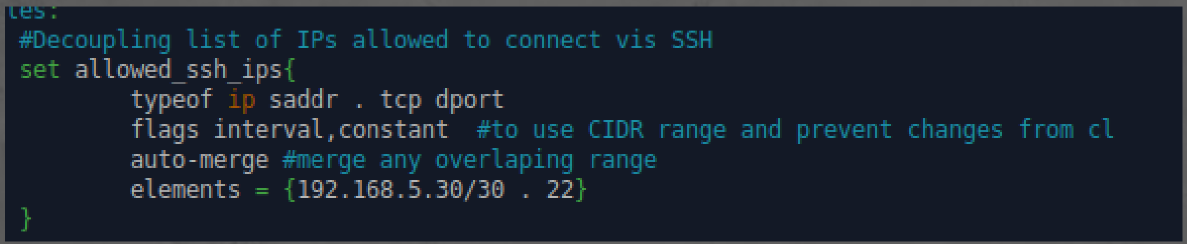


Test-3.10	DOS using IP of non-privileged range: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – intnet port 22 NFTable ON	PASS	Attack for 60 seconds, 331,053 packet dropped out of 331,054 sent. Allowed 1 packet.
Test-3.11	DOS using IP of privileged range - IP 192.168.5.30 used: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – extnet port 22 NFTable ON	FAIL – FIXED BY TEST 3.12	Attack for 60 seconds, 4,831,512 packets sent and 409,103 received resulting in total of 700,209 packets sent and received from VM2-Firewall
Test-3.12 FIX	DOS using IP of privileged range - IP 192.168.5.30 used: *hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1*	Hping3	VM3-Attacker	VM2-Firewall – extnet port 22 NFTable ON	PASS	Additional rule was added to fix Test-3.11. Attack for 60 seconds, 332,650 packets transmitted and processed only 62 packets

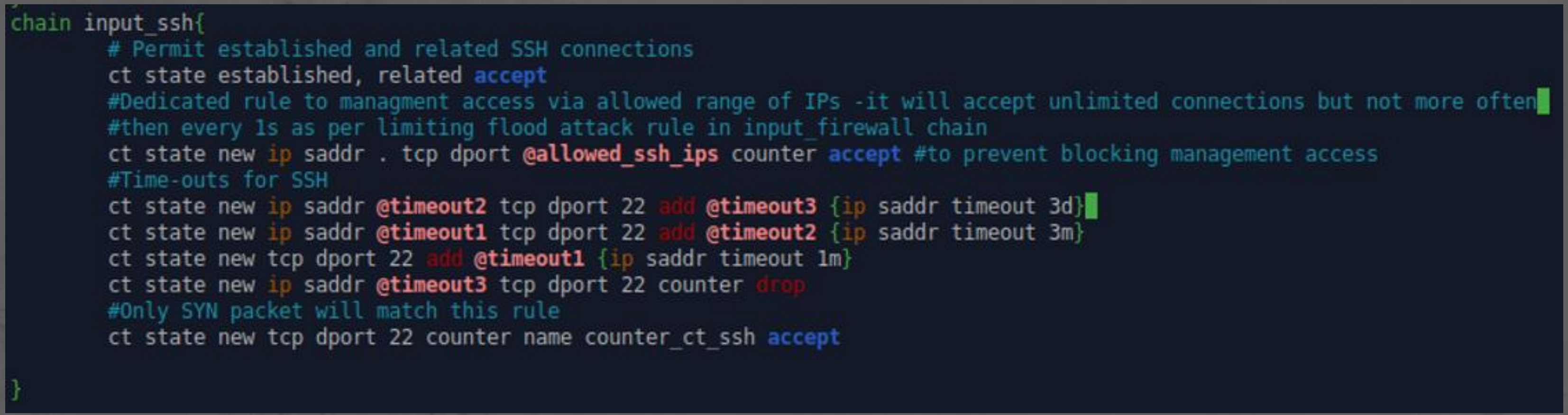
Initial script:



```
#3x timeout variables
set timeout1{
        typeof ip saddr
        flags timeout

}
set timeout2{
        typeof ip saddr
        flags timeout

}
set timeout3{
        typeof ip saddr
        flags timeout

}
```



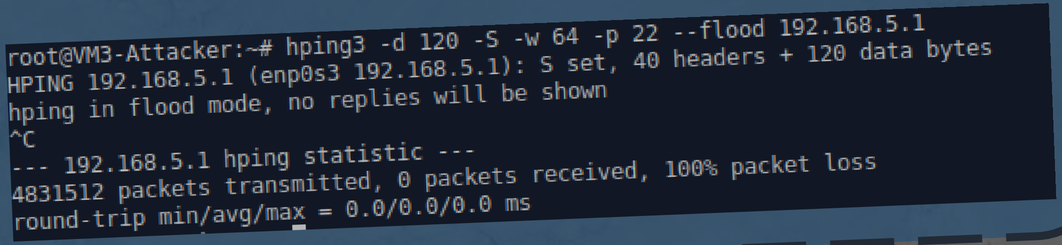
```
les:
 #Decoupling list of IPs allowed to connect vis SSH
 set allowed_ssh_ips{
         typeof ip saddr . tcp dport
         flags interval,constant  #to use CIDR range and prevent changes from cl
         auto-merge #merge any overlaping range
         elements = {192.168.5.30/30 . 22}
 }
```



```
chain input_ssh{
        # Permit established and related SSH connections
        ct state established, related accept
        #Dedicated rule to managment access via allowed range of IPs -it will accept unlimited connections but not more often
        #then every 1s as per limiting flood attack rule in input_firewall chain
        ct state new ip saddr . tcp dport @allowed_ssh_ips counter accept #to prevent blocking management access
        #Time-outs for SSH
        ct state new ip saddr @timeout2 tcp dport 22 add @timeout3 {ip saddr timeout 3d}
        ct state new ip saddr @timeout1 tcp dport 22 add @timeout2 {ip saddr timeout 3m}
        ct state new tcp dport 22 add @timeout1 {ip saddr timeout 1m}
        ct state new ip saddr @timeout3 tcp dport 22 counter drop
        #Only SYN packet will match this rule
        ct state new tcp dport 22 counter name counter_ct_ssh accept

}
```

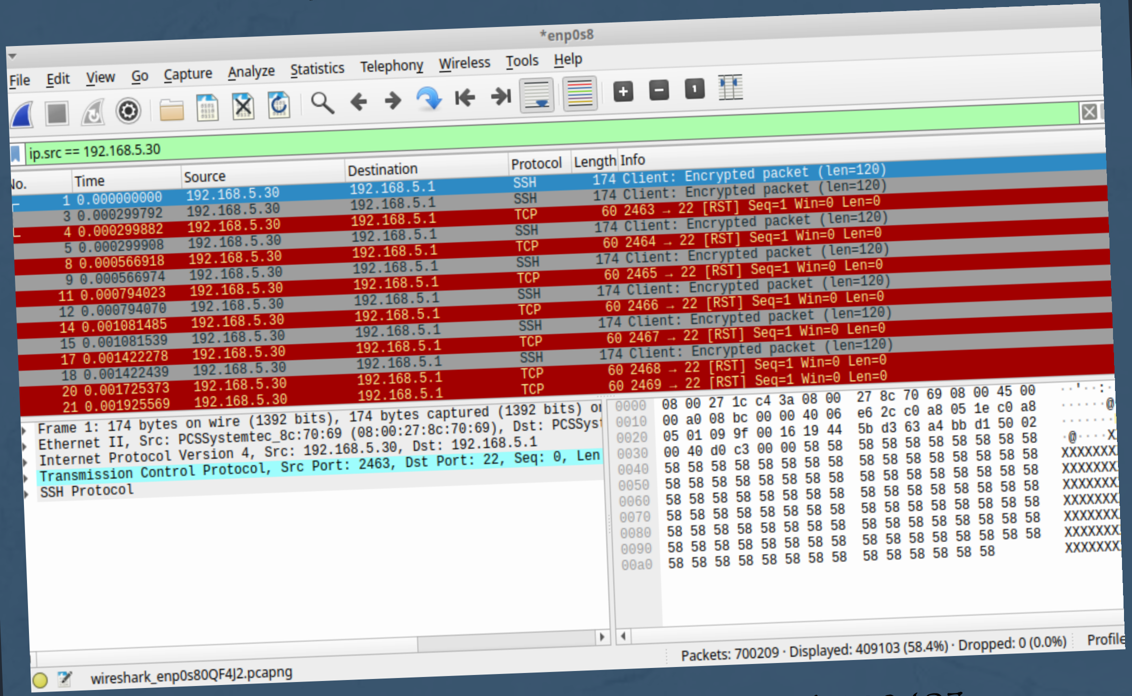
Test-3.11 - FAIL

Flood attack from VM3-Attacker sending 4,831,512 packets:



```
root@VM3-Attacker:~# hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1
HPING 192.168.5.1 (enp0s3 192.168.5.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.5.1 hping statistic ---
4831512 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Wireshark capture on VM-Firewall 192.168.5.1 registering incoming traffic:

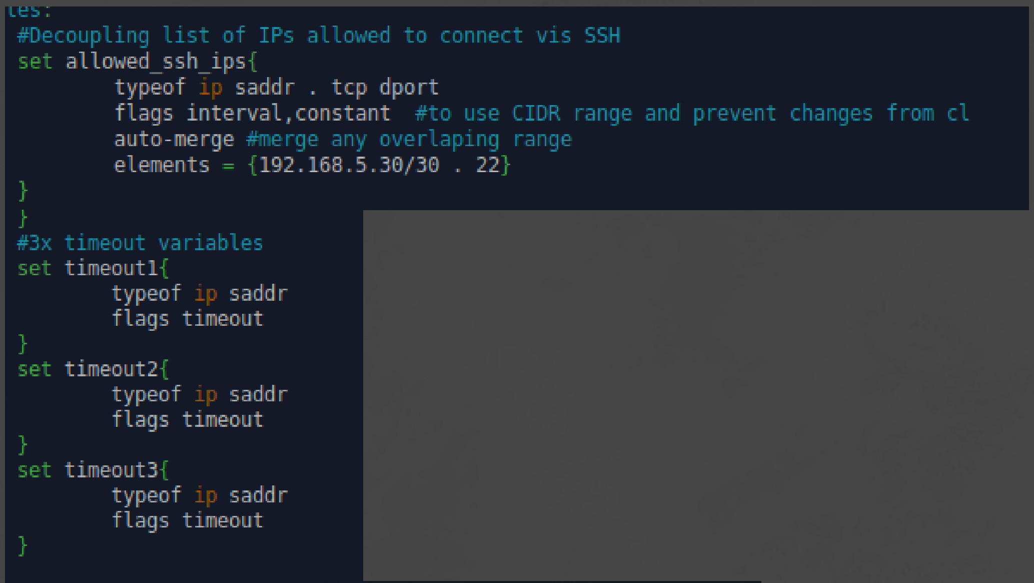


*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

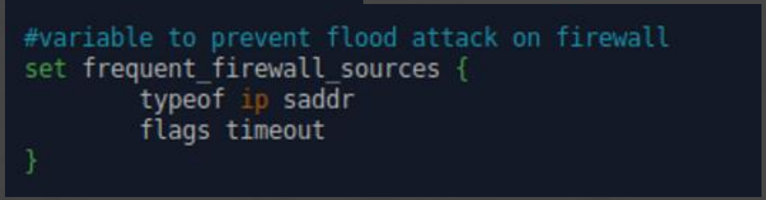
```
ip.src == 192.168.5.30

No.  Time         Source        Destination  Protocol Length Info
  1 0.000000000  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
  3 0.000299792  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
  4 0.000299882  192.168.5.30  192.168.5.1  TCP       60 2463 → 22 [RST] Seq=1 Win=0 Len=0
  5 0.000299908  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
  8 0.000566918  192.168.5.30  192.168.5.1  TCP       60 2464 → 22 [RST] Seq=1 Win=0 Len=0
  9 0.000566974  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
 11 0.000794023  192.168.5.30  192.168.5.1  TCP       60 2465 → 22 [RST] Seq=1 Win=0 Len=0
 12 0.000794070  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
 14 0.001081485  192.168.5.30  192.168.5.1  TCP       60 2466 → 22 [RST] Seq=1 Win=0 Len=0
 15 0.001081539  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
 17 0.001422278  192.168.5.30  192.168.5.1  TCP       60 2467 → 22 [RST] Seq=1 Win=0 Len=0
 18 0.001422439  192.168.5.30  192.168.5.1  SSH      174 Client: Encrypted packet (len=120)
 20 0.001725373  192.168.5.30  192.168.5.1  TCP       60 2468 → 22 [RST] Seq=1 Win=0 Len=0
 21 0.001925569  192.168.5.30  192.168.5.1  TCP       60 2469 → 22 [RST] Seq=1 Win=0 Len=0

Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) o
Ethernet II, Src: PCSSystemtec_8c:70:69 (08:00:27:8c:70:69), Dst: PCSSys
Internet Protocol Version 4, Src: 192.168.5.30, Dst: 192.168.5.1
Transmission Control Protocol, Src Port: 2463, Dst Port: 22, Seq: 0, Len
SSH Protocol

0000  08 00 27 1c c4 3a 08 00  27 8c 70 69 08 00 45 00   ··'··:·
0010  00 a0 08 bc 00 00 40 06  e6 2c c0 a8 05 1e c0 a8   ······@
0020  05 01 09 9f 00 16 19 44  5b d3 63 a4 bb d1 50 02   ·······
0030  00 40 d0 c3 00 00 58 58  58 58 58 58 58 58 58 58   ·@····X
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXX
00a0  58 58 58 58 58 58 58 58  58 58 58 58 58 58

wireshark_enp0s80QF4J2.pcapng    Packets: 700209 · Displayed: 409103 (58.4%) · Dropped: 0 (0.0%)    Profile
```

RESULT: FAIL 4,831,000 packets sent and 409,103 received resulting in total of 700,209 packets sent and received by VM2-Firewall

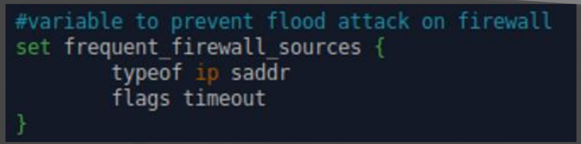
Final script:



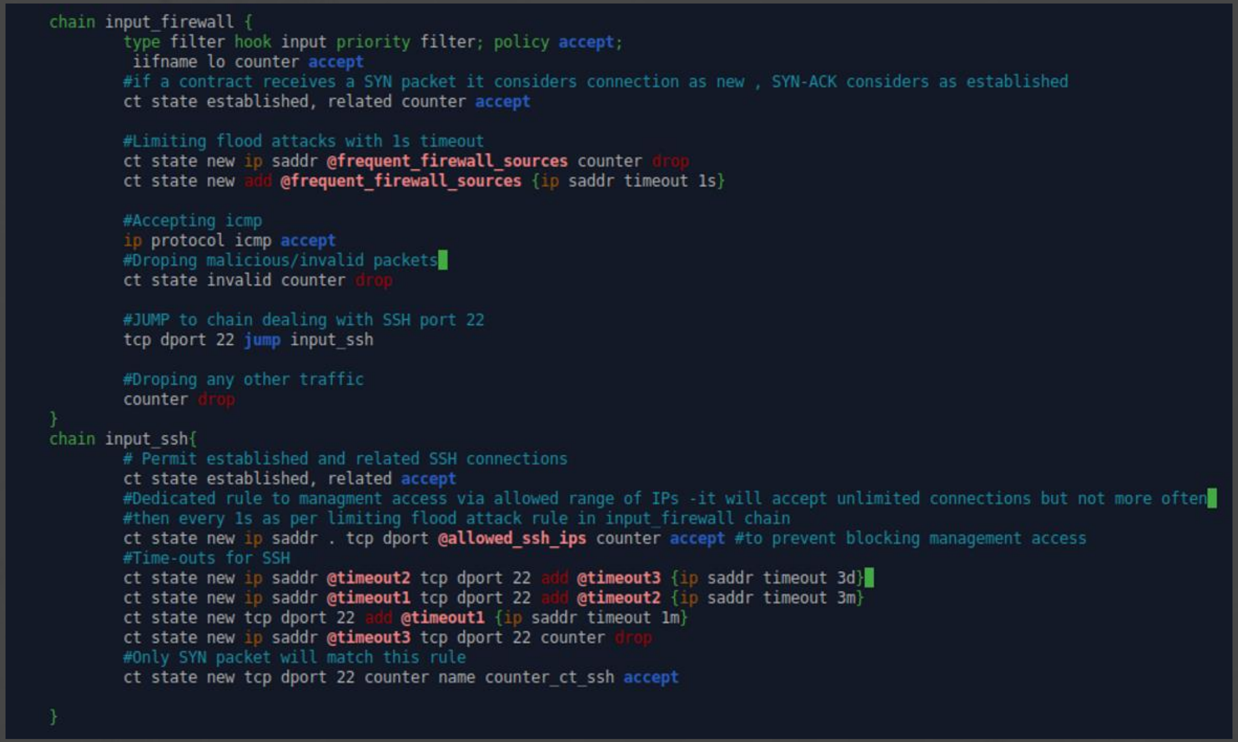
```
les:
 #Decoupling list of IPs allowed to connect vis SSH
 set allowed_ssh_ips{
         typeof ip saddr . tcp dport
         flags interval,constant  #to use CIDR range and prevent changes from cl
         auto-merge #merge any overlaping range
         elements = {192.168.5.30/30 . 22}
 }
 }
 #3x timeout variables
 set timeout1{
         typeof ip saddr
         flags timeout
 }
 set timeout2{
         typeof ip saddr
         flags timeout
 }
 set timeout3{
         typeof ip saddr
         flags timeout
 }
```



```
 #variable to prevent flood attack on firewall
 set frequent_firewall_sources {
         typeof ip saddr
         flags timeout
 }
```



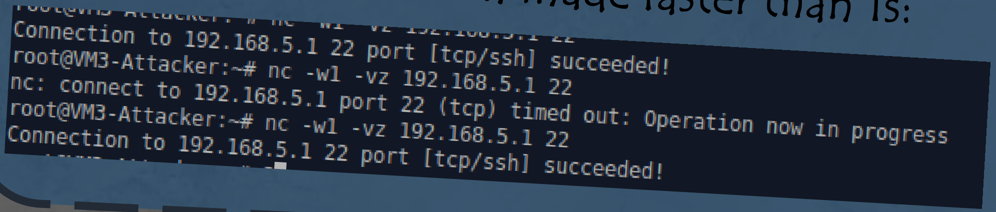
```
#variable to prevent flood attack on firewall
set frequent_firewall_sources {
        typeof ip saddr
        flags timeout
}
```



```
    chain input_firewall {
            type filter hook input priority filter; policy accept;
             iifname lo counter accept
            #if a contract receives a SYN packet it considers connection as new , SYN-ACK considers as established
            ct state established, related counter accept

            #Limiting flood attacks with 1s timeout
            ct state new ip saddr @frequent_firewall_sources counter drop
            ct state new add @frequent_firewall_sources {ip saddr timeout 1s}

            #Accepting icmp
            ip protocol icmp accept
            #Droping malicious/invalid packets
            ct state invalid counter drop

            #JUMP to chain dealing with SSH port 22
            tcp dport 22 jump input_ssh

            #Droping any other traffic
            counter drop
    }
    chain input_ssh{
            # Permit established and related SSH connections
            ct state established, related accept
            #Dedicated rule to managment access via allowed range of IPs -it will accept unlimited connections but not more often
            #then every 1s as per limiting flood attack rule in input_firewall chain
            ct state new ip saddr . tcp dport @allowed_ssh_ips counter accept #to prevent blocking management access
            #Time-outs for SSH
            ct state new ip saddr @timeout2 tcp dport 22 add @timeout3 {ip saddr timeout 3d}
            ct state new ip saddr @timeout1 tcp dport 22 add @timeout2 {ip saddr timeout 3m}
            ct state new tcp dport 22 add @timeout1 {ip saddr timeout 1m}
            ct state new ip saddr @timeout3 tcp dport 22 counter drop
            #Only SYN packet will match this rule
            ct state new tcp dport 22 counter name counter_ct_ssh accept

    }
```

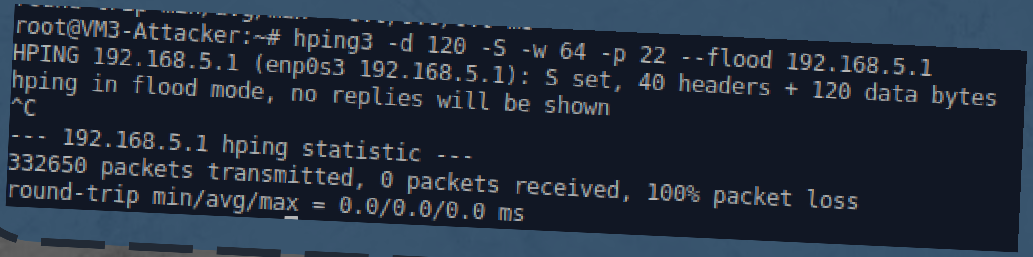
TEST 3.12 – Success

Verified that connection is possible from VM3-Attacker privileged IP range but blocked on connection made faster than 1s:



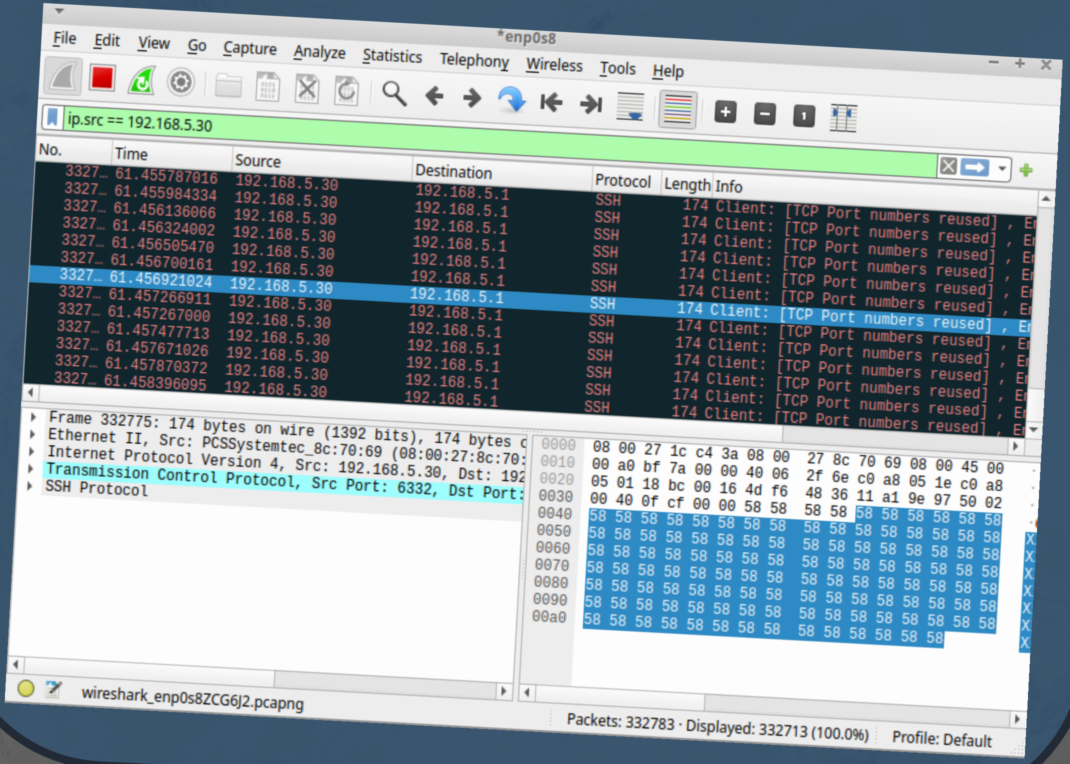
```
root@VM3-Attacker:~# nc -w1 -vz 192.168.5.1 22
Connection to 192.168.5.1 22 port [tcp/ssh] succeeded!
root@VM3-Attacker:~# nc -w1 -vz 192.168.5.1 22
nc: connect to 192.168.5.1 port 22 (tcp) timed out: Operation now in progress
root@VM3-Attacker:~# nc -w1 -vz 192.168.5.1 22
Connection to 192.168.5.1 22 port [tcp/ssh] succeeded!
root@VM3-Attacker:~#
```

Flood attack from VM3-Attacker sending 332,650 packets:



```
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@VM3-Attacker:~# hping3 -d 120 -S -w 64 -p 22 --flood 192.168.5.1
HPING 192.168.5.1 (enp0s3 192.168.5.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.5.1 hping statistic ---
332650 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Wireshark capture on VM-Firewall 192.168.5.1 registering incoming traffic:



Filter: ip.src == 192.168.5.30

```
No.     Time         Source         Destination   Protocol Length Info
3327…   61.455787016 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.455984334 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.456136066 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.456324002 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.456505470 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.456700161 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.456921024 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.457266911 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.457267000 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.457477713 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.457671026 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.457870372 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
3327…   61.458396095 192.168.5.30   192.168.5.1   SSH      174 Client: [TCP Port numbers reused] , E
```

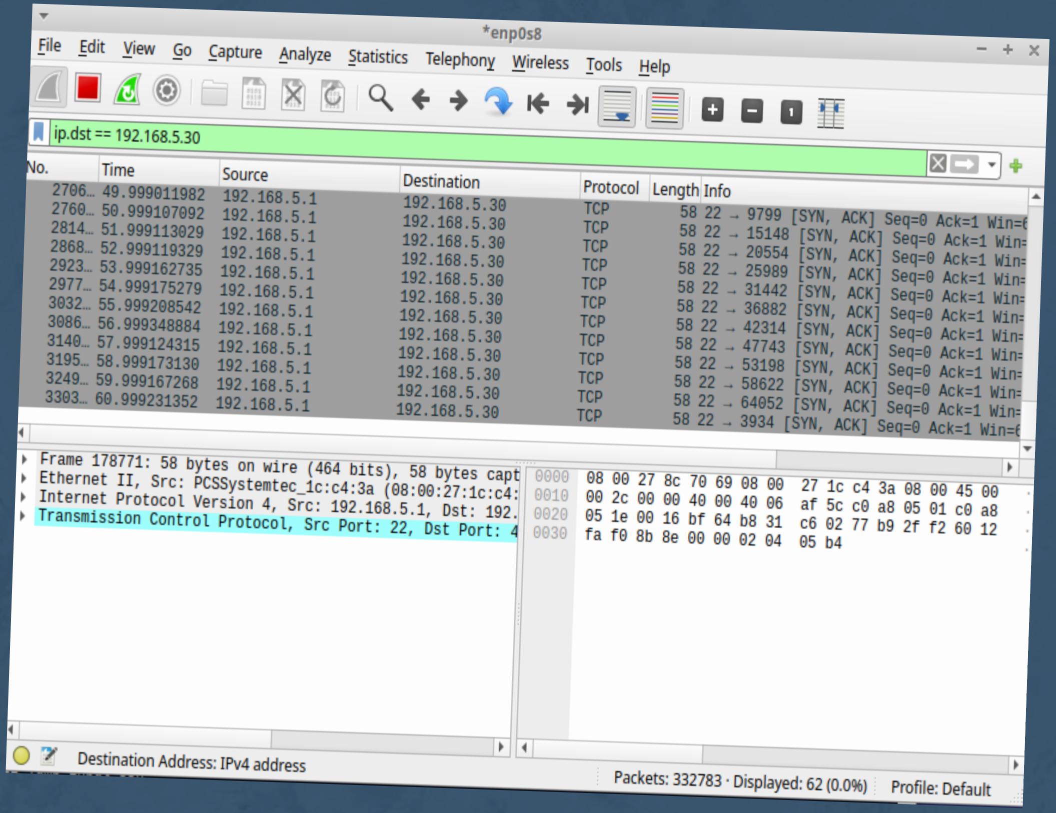
```
▸ Frame 332775: 174 bytes on wire (1392 bits), 174 bytes c
▸ Ethernet II, Src: PCSSystemtec_8c:70:69 (08:00:27:8c:70:
▸ Internet Protocol Version 4, Src: 192.168.5.30, Dst: 192
▸ Transmission Control Protocol, Src Port: 6332, Dst Port:
▸ SSH Protocol
```

```
0000  08 00 27 1c c4 3a 08 00  27 8c 70 69 08 00 45 00
0010  00 a0 bf 7a 00 00 40 06  2f 6e c0 a8 05 1e c0 a8
0020  05 01 18 bc 00 16 4d f6  48 36 11 a1 9e 97 50 02
0030  00 40 0f cf 00 00 58 58  58 58 58 58 58 58 58 58
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58
00a0  58 58 58 58 58 58 58 58  58 58 58 58 58 58
```

wireshark_enp0s8ZCG6J2.pcapng

Packets: 332783 · Displayed: 332713 (100.0%)   Profile: Default

Wireshark capture on VM-Firewall 192.168.5.1 registering outgoing traffic: of 62 packets out of total 332783 packets:


*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 192.168.5.30

No.	Time	Source	Destination	Protocol	Length	Info
2706…	49.999011982	192.168.5.1	192.168.5.30	TCP	58	22 → 9799 [SYN, ACK] Seq=0 Ack=1 Win=6
2760…	50.999107092	192.168.5.1	192.168.5.30	TCP	58	22 → 15148 [SYN, ACK] Seq=0 Ack=1 Win=
2814…	51.999113029	192.168.5.1	192.168.5.30	TCP	58	22 → 20554 [SYN, ACK] Seq=0 Ack=1 Win=
2868…	52.999119329	192.168.5.1	192.168.5.30	TCP	58	22 → 25989 [SYN, ACK] Seq=0 Ack=1 Win=
2923…	53.999162735	192.168.5.1	192.168.5.30	TCP	58	22 → 31442 [SYN, ACK] Seq=0 Ack=1 Win=
2977…	54.999175279	192.168.5.1	192.168.5.30	TCP	58	22 → 36882 [SYN, ACK] Seq=0 Ack=1 Win=
3032…	55.999208542	192.168.5.1	192.168.5.30	TCP	58	22 → 42314 [SYN, ACK] Seq=0 Ack=1 Win=
3086…	56.999348884	192.168.5.1	192.168.5.30	TCP	58	22 → 47743 [SYN, ACK] Seq=0 Ack=1 Win=
3140…	57.999124315	192.168.5.1	192.168.5.30	TCP	58	22 → 53198 [SYN, ACK] Seq=0 Ack=1 Win=
3195…	58.999173130	192.168.5.1	192.168.5.30	TCP	58	22 → 58622 [SYN, ACK] Seq=0 Ack=1 Win=
3249…	59.999167268	192.168.5.1	192.168.5.30	TCP	58	22 → 64052 [SYN, ACK] Seq=0 Ack=1 Win=
3303…	60.999231352	192.168.5.1	192.168.5.30	TCP	58	22 → 3934 [SYN, ACK] Seq=0 Ack=1 Win=6

```
▸ Frame 178771: 58 bytes on wire (464 bits), 58 bytes capt
▸ Ethernet II, Src: PCSSystemtec_1c:c4:3a (08:00:27:1c:c4:
▸ Internet Protocol Version 4, Src: 192.168.5.1, Dst: 192.
▸ Transmission Control Protocol, Src Port: 22, Dst Port: 4
```

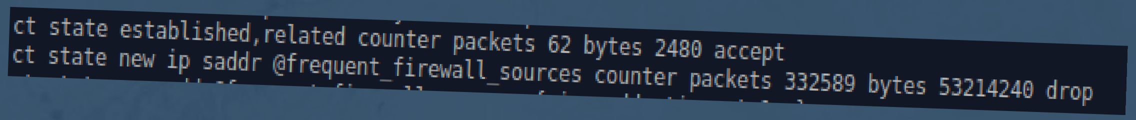
```
0000  08 00 27 8c 70 69 08 00  27 1c c4 3a 08 00 45 00
0010  00 2c 00 00 40 00 40 06  af 5c c0 a8 05 01 c0 a8
0020  05 1e 00 16 bf 64 b8 31  c6 02 77 b9 2f f2 60 12
0030  fa f0 8b 8e 00 00 02 04  05 b4
```

Destination Address: IPv4 address

Packets: 332783 · Displayed: 62 (0.0%)

Profile: Default

Received on VM2-Firewall and blocked by rule:



```
ct state established,related counter packets 62 bytes 2480 accept
ct state new ip saddr @frequent_firewall_sources counter packets 332589 bytes 53214240 drop
```

RESULT: PASS – 332650 packets transmitted by VM3-Attaccker and only 62 packets processed by VM2-Firewall

Thank You!