

# CSEC Week 07 Lab

## Task 1 - Adding a Rule for ICMP Packets

```
csec-server x csec-attacker x csec-client x
cybersec-server@ubuntu: ~
09/18-22:00:01.704434 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:53792 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:4 ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:02.704707 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:15187 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:2907 Seq:5 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:02.704735 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:53930 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:5 ECHO REPLY

^X[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:03.703899 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:15188 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:2907 Seq:6 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:03.703935 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:54045 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:6 ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:04.704470 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:15295 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:2907 Seq:7 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:04.704505 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:54229 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:7 ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:05.704330 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:15343 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:2907 Seq:8 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:05.704353 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:54418 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:8 ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:06.704515 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:15383 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:2907 Seq:9 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:00:06.704539 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:54548 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:2907 Seq:9 ECHO REPLY

^C
cybersec-server@ubuntu:~$ alexander t
```

## Task 2 - Snort in IDS mode and displaying alerts to the console.

```
nc
cybersec-server@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -l eth0
09/18-22:02:10.911661 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:10.911661 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:10.911661 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:10.911698 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:10.911698 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:11.914221 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:11.914221 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:11.914221 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:11.914257 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:11.914257 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:12.925170 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:12.925170 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:12.925170 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:12.925206 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:12.925206 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:13.938374 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:13.938374 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:13.938374 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:13.938424 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:13.938424 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:14.937320 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:14.937320 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:14.937320 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:14.937348 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:15.936409 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:15.936409 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:15.936409 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:15.936442 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:15.936442 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:16.936995 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:16.936995 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:16.936995 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:16.937037 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:16.937037 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:17.936433 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:17.936433 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:17.936433 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
09/18-22:02:17.936470 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
09/18-22:02:17.936470 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
^C*** Caught Int-Signal
cybersec-server@ubuntu:~$ alexander
```

### Task 3 - Generating alerts for web service

```
csec-server x csec-attacker x csec-client x
cybersec-server@ubuntu: ~
09/18-22:05:52.002799 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0xC0 ID:54895 IpLen:20 DgmLen:97
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
10.0.2.6:53 -> 10.0.2.7:44231
UDP TTL:64 TOS:0x0 ID:13927 IpLen:20 DgmLen:69
Len: 41 Csum: 42718
(41 more bytes of original packet)
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:05:52.056070 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0xC0 ID:54905 IpLen:20 DgmLen:97
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
10.0.2.6:53 -> 10.0.2.7:46438
UDP TTL:64 TOS:0x0 ID:13934 IpLen:20 DgmLen:69
Len: 41 Csum: 29151
(41 more bytes of original packet)
** END OF DUMP

[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:54.496270 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6153 IpLen:20 DgmLen:60 DF
*****S Seq: 0xEA678B52 Ack: 0x0 Win: 0x7210 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 103259 0 NOP WS: 7

[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:54.496440 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6154 IpLen:20 DgmLen:52 DF
****A**** Seq: 0xEA678B53 Ack: 0xDCEB9D67 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 103259 105641

[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:54.496534 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6155 IpLen:20 DgmLen:394 DF
***AP*** Seq: 0xEA678B53 Ack: 0xDCEB9D67 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 103259 105641

[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:54.502528 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6156 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEA678CA9 Ack: 0xDCEBA083 Win: 0xF1 TcpLen: 32
TCP Options (3) => NOP NOP TS: 103260 105642

[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:55.231461 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6157 IpLen:20 DgmLen:394 DF
***AP*** Seq: 0xEA678CA9 Ack: 0xDCEBA083 Win: 0xF1 TcpLen: 32
TCP Options (3) => NOP NOP TS: 103442 105642

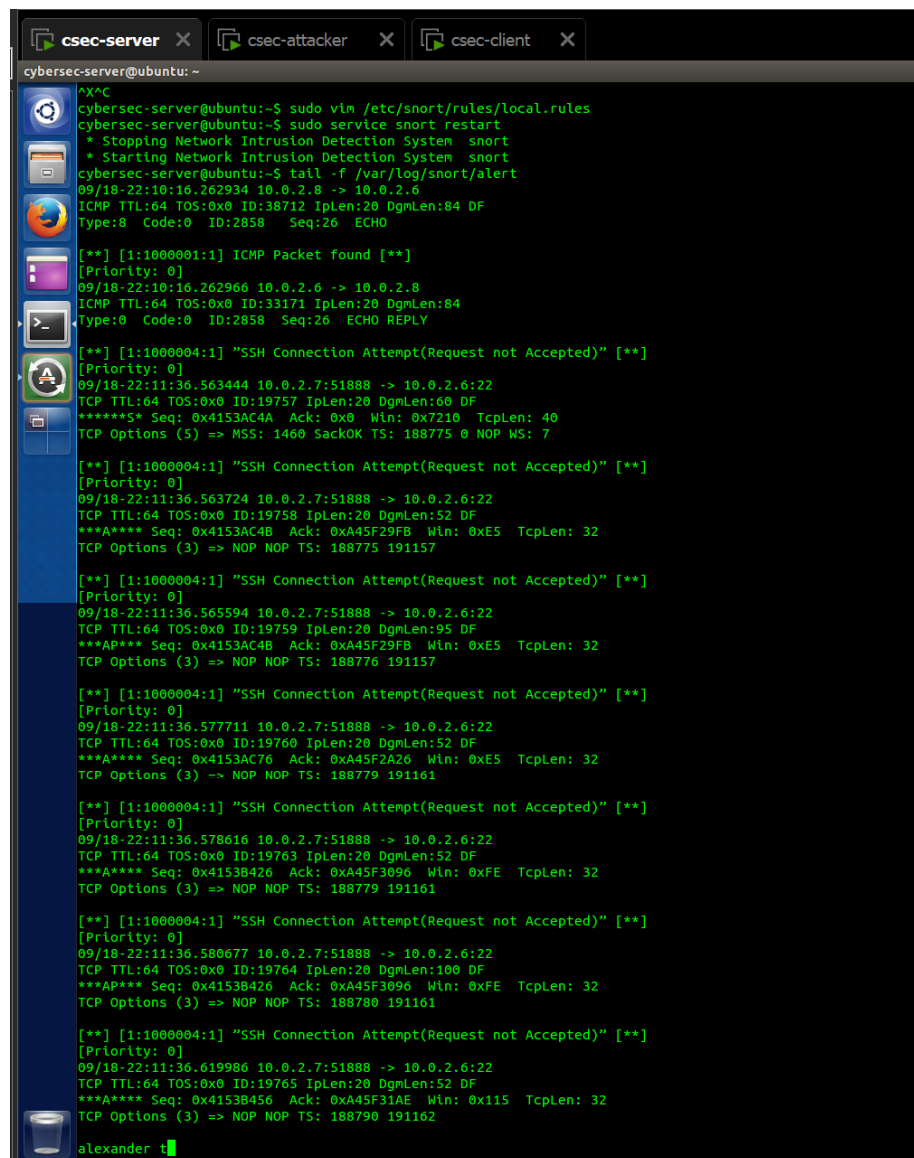
[**] [1:1000002:1] Web Access Request [**]
[Priority: 0]
09/18-22:05:55.232580 10.0.2.7:38698 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:6158 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEA678DFF Ack: 0xDCEBA39E Win: 0xFD TcpLen: 32
TCP Options (3) => NOP NOP TS: 103443 105824

^C
cybersec-server@ubuntu:~$ alexander t
```

## Task 4 - Generating alerts for ICMP Source Quench Packets

```
csec-server x csec-attacker x csec-client x
File Edit View Search Terminal Help
ICMP TTL:64 TOS:0x0 ID:36556 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:2858 Seq:6 ECHO
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:09:56.234073 10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:30245 IpLen:20 DgmLen:84
Type:0 Code:0 ID:2858 Seq:6 ECHO REPLY
[**] [1:1000003:1] ICMP source uench [**]
[Priority: 0]
09/18-22:09:56.237380 10.0.2.6 -> 10.0.2.8
ICMP TTL:255 TOS:0x0 ID:39319 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:36556 IpLen:20 DgmLen:84 DF
Type: 8 Code: 0 Csum: 56571 Id: 2858 SeqNo: 6
** END OF DUMP
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:09:56.237380 10.0.2.6 -> 10.0.2.8
ICMP TTL:255 TOS:0x0 ID:39319 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:36556 IpLen:20 DgmLen:84 DF
Type: 8 Code: 0 Csum: 56571 Id: 2858 SeqNo: 6
** END OF DUMP
[**] [1:1000003:1] ICMP source uench [**]
[Priority: 0]
09/18-22:09:56.237388 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:38670 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:30245 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 58619 Id: 2858 SeqNo: 6
** END OF DUMP
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:09:56.237388 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:38670 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:30245 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 58619 Id: 2858 SeqNo: 6
** END OF DUMP
[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/18-22:09:56.237388 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:38670 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:30245 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 58619 Id: 2858 SeqNo: 6
** END OF DUMP
[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http:
```

## Task 5 - Running Snort as Intrusion Prevention System (IPS)



The screenshot shows a terminal window with three tabs: 'csec-server', 'csec-attacker', and 'csec-client'. The active tab is 'csec-server', which shows the following commands and output:

```
cybersec-server@ubuntu:~$ sudo vim /etc/snort/rules/local.rules
cybersec-server@ubuntu:~$ sudo service snort restart
 * Stopping Network Intrusion Detection System snort
 * Starting Network Intrusion Detection System snort
cybersec-server@ubuntu:~$ tail -f /var/log/snort/alert
09/18-22:10:16.262934 10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:38712 Iplen:20 DgmLen:84 DF
Type:8 Code:0 ID:2858 Seq:26 ECHO
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/18-22:10:16.262966 10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:33171 Iplen:20 DgmLen:84
Type:0 Code:0 ID:2858 Seq:26 ECHO REPLY
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.563444 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19757 Iplen:20 DgmLen:60 DF
*****S* Seq: 0x4153AC4A Ack: 0x0 Wln: 0x7210 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 188775 0 NOP WS: 7
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.563724 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19758 Iplen:20 DgmLen:52 DF
*****S* Seq: 0x4153AC4B Ack: 0xA45F29FB Wln: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 188775 191157
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.565594 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19759 Iplen:20 DgmLen:95 DF
*****S* Seq: 0x4153AC4B Ack: 0xA45F29FB Wln: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 188776 191157
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.577711 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19760 Iplen:20 DgmLen:52 DF
*****S* Seq: 0x4153AC76 Ack: 0xA45F2A26 Wln: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 188779 191161
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.578616 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19763 Iplen:20 DgmLen:52 DF
*****S* Seq: 0x4153B426 Ack: 0xA45F3096 Wln: 0xFE TcpLen: 32
TCP Options (3) => NOP NOP TS: 188779 191161
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.580677 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19764 Iplen:20 DgmLen:100 DF
*****S* Seq: 0x4153B426 Ack: 0xA45F3096 Wln: 0xFE TcpLen: 32
TCP Options (3) => NOP NOP TS: 188780 191161
[**] [1:1000004:1] "SSH Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/18-22:11:36.619986 10.0.2.7:51888 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:19765 Iplen:20 DgmLen:52 DF
*****S* Seq: 0x4153B456 Ack: 0xA45F31AE Wln: 0x115 TcpLen: 32
TCP Options (3) => NOP NOP TS: 188790 191162
alexander t
```