

# Assignment-5

## Question 1

### For ICMP request

- 1) Alert signature: `alert icmp any any -> $HOME_NET any (msg: "ICMP Ping Detected"; sid: 100001; rev:1;)`

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> $HOME_NET any (msg: "ICMP Ping Detected"; sid: 100001; rev:1;)
~
```

- 2) Description: The Ubuntu has started listening to this request using: `sudo snort -q -l /var/log/snort -i enp0s3 -A console -c /etc/snort/snort.conf`. Now we ping the Metasploitable VM from Kali VM using the IP address of the Metasploitable VM.

```
└$ ping 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
64 bytes from 192.168.1.13: icmp_seq=1 ttl=64 time=13.8 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=64 time=0.732 ms
64 bytes from 192.168.1.13: icmp_seq=3 ttl=64 time=0.778 ms
64 bytes from 192.168.1.13: icmp_seq=4 ttl=64 time=1.09 ms
64 bytes from 192.168.1.13: icmp_seq=5 ttl=64 time=0.686 ms
64 bytes from 192.168.1.13: icmp_seq=6 ttl=64 time=0.645 ms
64 bytes from 192.168.1.13: icmp_seq=7 ttl=64 time=0.834 ms
64 bytes from 192.168.1.13: icmp_seq=8 ttl=64 time=0.549 ms
64 bytes from 192.168.1.13: icmp_seq=9 ttl=64 time=0.965 ms
^C
--- 192.168.1.13 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8079ms
rtt min/avg/max/mdev = 0.549/2.236/13.847/4.107 ms
```

And we observe alerts on the Ubuntu Virtual Machine using the ICMP alert we specified in the local.rules file.

```
03/23-23:50:57.334771 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:50:57.335171 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:50:58.328697 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:50:58.328950 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:50:59.359472 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:50:59.359839 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:00.361344 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:00.361913 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:01.362568 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:01.362756 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:02.366786 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:02.367002 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:03.390325 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:03.390888 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:04.391937 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:04.391937 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
03/23-23:51:05.403667 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.12 -> 192.168.1.13
03/23-23:51:05.404115 [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.13 -> 192.168.1.12
^C*** Caught Int-Signal
```

- 3) Alert from log file: In my case, the log of the alert is dumped into `/var/log/snort/snort.log.1679595079`. Reading from this file is done through this command: `sudo tcpdump -r snort.log.1679595079`.

```
reading from file snort.log.1679595079, link-type EN10MB (Ethernet), snapshot length 1514
23:50:57.334771 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 1, length 64
23:50:57.335171 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 1, length 64
23:50:58.328697 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 2, length 64
23:50:58.328950 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 2, length 64
23:50:59.359472 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 3, length 64
23:50:59.359839 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 3, length 64
23:51:00.361344 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 4, length 64
23:51:00.361913 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 4, length 64
23:51:01.362568 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 5, length 64
23:51:01.362756 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 5, length 64
23:51:02.366706 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 6, length 64
23:51:02.367002 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 6, length 64
23:51:03.390325 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 7, length 64
23:51:03.390888 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 7, length 64
23:51:04.391937 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 8, length 64
23:51:04.391937 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 8, length 64
23:51:05.403667 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1204, seq 9, length 64
23:51:05.404115 IP 192.168.1.13 > 192.168.1.12: ICMP echo reply, id 1204, seq 9, length 64
```

### For SSH request

- 1) Alert signature: `alert tcp any any -> $HOME_NET 443 (msg: "HTTPS Request Detected"; sid: 100001; rev:1;)`

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any -> $HOME_NET 22 (msg: "SSH Authentication Detected"; sid: 100002; rev:1;)
```

- 2) Description: The Ubuntu has started listening to this request using: `sudo snort -q -l /var/log/snort -i enp0s3 -A console -c /etc/snort/snort.conf`. Now we will try to ssh the Metasploitable VM from Kali VM using the IP address of the Metasploitable VM.

```
└$ ssh msfadmin@192.168.1.13
Unable to negotiate with 192.168.1.13 port 22: no matching host key type found.
Their offer: ssh-rsa,ssh-dss
```

And we observe alerts on the Ubuntu Virtual Machine using the TCP alert on port 22(SSH port) as we specified in the local.rules file.

```
03/24-01:06:20.515593  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
03/24-01:06:20.516333  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
03/24-01:06:20.516732  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
03/24-01:06:20.519556  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
03/24-01:06:20.520284  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
03/24-01:06:20.520628  [**] [1:100002:1] SSH Authentication Detected [**] [Priority: 0] {TCP} 192.168.1.12:51364 -> 1
92.168.1.13:22
```

- 3) Alert from log file: In my case, the log of the alert is dumped into `/var/log/snort/snort.log.1679600173`. Reading from this file is done through this command: `sudo tcpdump -r snort.log.1679600173`.

```
reading from file snort.log.1679600173, link-type EN10MB (Ethernet), snapshot length 1514
01:06:20.515593 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [S], seq 689861182, win 64240, options [mss 1460,sack
OK,TS val 2864345195 ecr 0,nop,wscale 7], length 0
01:06:20.516333 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [.], ack 3715892710, win 502, options [nop,nop,TS val
2864345196 ecr 6549], length 0
01:06:20.516732 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [P.], seq 0:35, ack 1, win 502, options [nop,nop,TS val
2864345196 ecr 6549], length 35: SSH: SSH-2.0-OpenSSH_9.0pi Debian-1~b2
01:06:20.519556 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [.], ack 39, win 502, options [nop,nop,TS val 2864345
199 ecr 6549], length 0
01:06:20.520284 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [F.], seq 1539, ack 823, win 501, options [nop,nop,TS
val 2864345200 ecr 6549], length 0
01:06:20.520628 IP 192.168.1.12.51364 > 192.168.1.13.ssh: Flags [.], ack 824, win 501, options [nop,nop,TS val 286434
5200 ecr 6549], length 0
```

## Question 2

- 1) Alert signature: `alert tcp any any -> $HOME_NET 443 (msg: "HTTPS Request Detected"; sid: 100001; rev:1;)`

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert tcp any any -> $HOME_NET 443 (msg:"Craigslist website browsing detected"; content: "craigslist.org";
sid: 100000; rev:1;)
```

- 2) Alert from log file: In my case, the log of the alert is dumped into `/var/log/snort/snort.log.1679654014`. Reading from this file is done through this command: `sudo tcpdump -r snort.log.1679654014`.

```
reading from file snort.log.1679654014, link-type EN10MB (Ethernet), snapshot length 1514
16:03:38.320156 IP 20.42.65.85.https > 192.168.1.2.50696: Flags [F.], seq 931909419, ack 4136137144, win 2053, length 0
16:03:38.320156 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [S.], seq 618429759, ack 2897119396, win 65535, options [mss 1440,nop,wscale
8,nop,nop,sackOK], length 0
16:03:38.842373 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [P.], seq 6292:6343, ack 386, win 2051, length 51
16:03:39.158592 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [.], ack 2284, win 2053, length 0
16:03:39.158592 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [.], ack 5164, win 2053, length 0
16:03:39.158592 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [P.], seq 6343:6397, ack 5164, win 2053, length 54
16:03:39.158592 IP 20.42.65.85.https > 192.168.1.2.50701: Flags [P.], seq 6397:6859, ack 6127, win 2049, length 453
16:03:39.742645 IP cities.craigslist.org.https > Himesh.37916: Flags [S.], seq 4107828977, ack 3899532052, win 64240, options [mss 1452,sack
0,eol], length 0
16:03:40.062630 IP cities.craigslist.org.https > Himesh.37928: Flags [S.], seq 2551015906, ack 3035605386, win 64240, options [mss 1452,sack
0,eol], length 0
16:03:40.062630 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1:1381, ack 518, win 19320, length 1380
16:03:40.062630 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1381:1401, ack 518, win 19320, length 1364
16:03:40.062630 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1401:2765, ack 518, win 19320, length 1364
16:03:40.062630 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 2765:2838, ack 518, win 19320, length 73
16:03:40.280146 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1:1381, ack 518, win 19320, length 1380
16:03:40.370358 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1381:1401, ack 518, win 19320, length 20
16:03:40.370359 IP cities.craigslist.org.https > Himesh.37916: Flags [P.], seq 1401:2765, ack 518, win 19320, length 1364
```