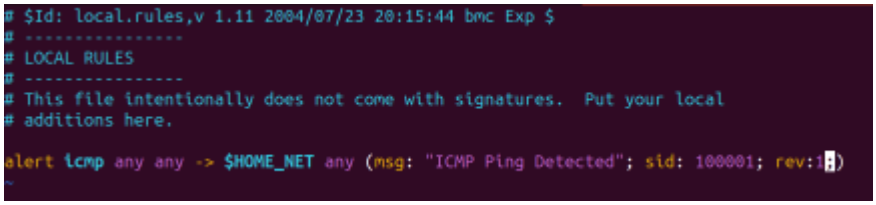
Assignment-5

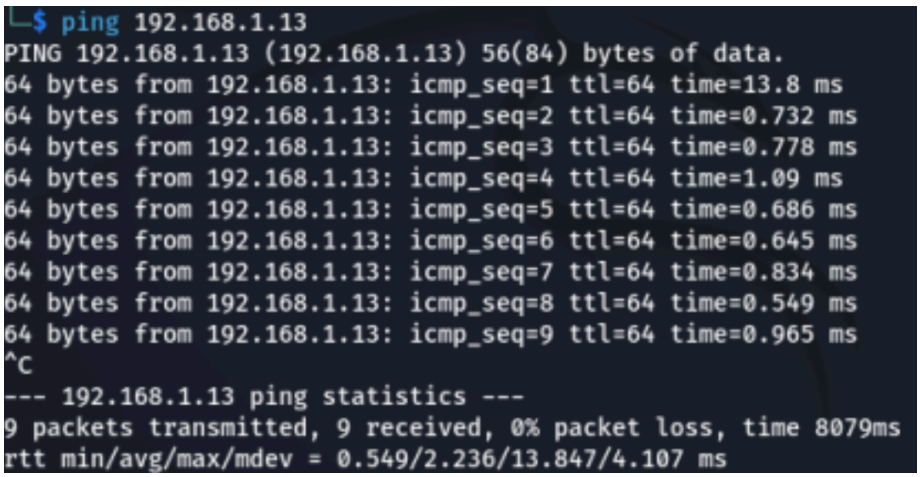
Question 1

For ICMP request

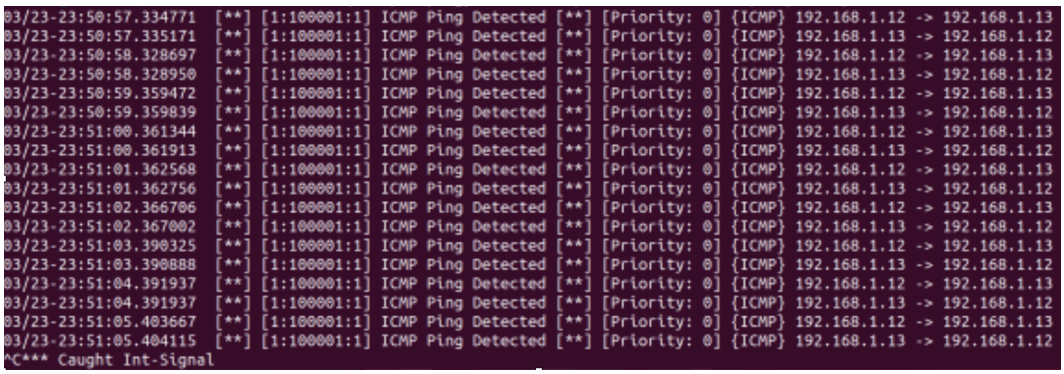
1) Alert signature: *alert icmp any any -> $HOME_NET any (msg: "ICMP Ping Detected"; sid: 100001; rev:1;)*



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.



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



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;)
~
```

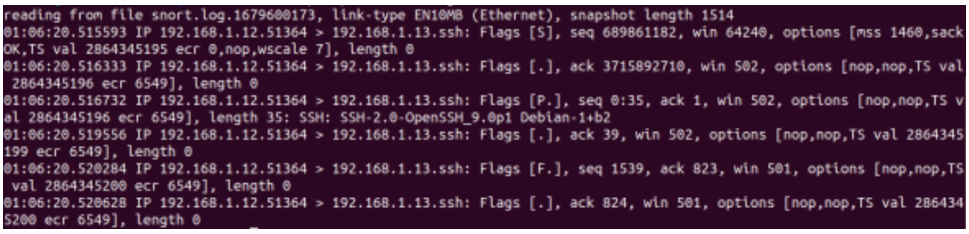
2) Description: The Ubuntu has started listening to this request using: *sudo snort -q -l /var/log/snort -i enp0s3 -A console -c /etc/snort/snort.conf* . Now we will try to ssh the Metasploitable VM from Kali VM using the IP address of the Metasploitable VM.

```
└─$ 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*.*



Question 2

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