Network Security Lab (CY-331L)

Lab #06 Task

Name: Rooshan Riaz
Reg No: 2022506

Installing snort

```
rooshan@rooshan:~$ sudo apt-get install snort
```

Configuring Snort

```
ipvar HOME_NET 192.168.80.128
```

Task 1:

Snort Rule for ICMP Traffic:

This rule will detect ICMP echo requests (ping requests) from any source to any destination. When a ping request is sent from any device to any IP address, the rule triggers an alert, generating a message "ICMP Ping Request Detected" in the logs.

The logs will display an alert for each ICMP echo request detected, including the source and destination IPs, timestamp, and the message defined in the rule.

Configuring Snort rule for ICMP

```
# LOCAL RULES
alert icmp any any -> any any (msg:"ICMP ping request Detected"; itype:8; sid:1000001; rev:1;)
```

Pinging Virtual Machine from a different machine

```
C:\Users\riazr>ping 192.168.80.128

Pinging 192.168.80.128 with 32 bytes of data:
Reply from 192.168.80.128: bytes=32 time<1ms TTL=64
Reply from 192.168.80.128: bytes=32 time<1ms TTL=64
Reply from 192.168.80.128: bytes=32 time<1ms TTL=64
Reply from 192.168.80.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.80.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Snort Ping Detected

```
rooshan@rooshan:/etc/snort$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
10/17-15:50:58.939052  [**] [1:1000001:1] ICMP Traffic Requested Detected [**] [Priority: 0] {ICMP} 192.168.80.1 -> 192.168.80.128
10/17-15:50:59.953469  [**] [1:1000001:1] ICMP Traffic Requested Detected [**] [Priority: 0] {ICMP} 192.168.80.1 -> 192.168.80.128
10/17-15:51:00.971618  [**] [1:1000001:1] ICMP Traffic Requested Detected [**] [Priority: 0] {ICMP} 192.168.80.1 -> 192.168.80.128
10/17-15:51:01.990091  [**] [1:1000001:1] ICMP Traffic Requested Detected [**] [Priority: 0] {ICMP} 192.168.80.1 -> 192.168.80.128
```

Task 2:

Configuring Snort rule for HTTP and HTTPS:

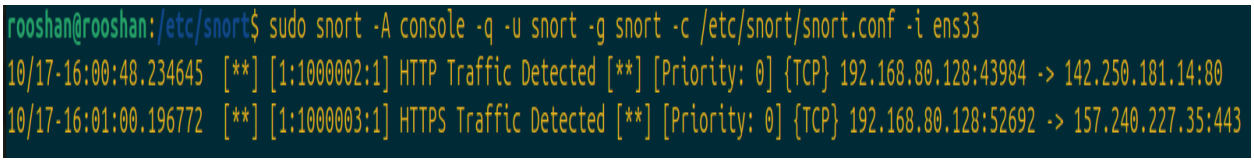
This rule detects TCP traffic sent to port 80 (HTTP) and port 443 (HTTPS) from any source.

```
alert tcp any any -> any 80 (msg: "HTTP Traffic Detected"; sid:1000002; rev:1;)
alert tcp any any -> any 443 (msg: "HTTPS Traffic Detected"; sid:1000003; rev:1;)
```

Testing HTTP & HTTPS Traffic

```
rooshan@rooshan:~$ curl http://google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
rooshan@rooshan:~$ curl https://facebook.com
rooshan@rooshan:~$
```

Detecting HTTP & HTTPS Traffic



Each time HTTP or HTTPS traffic is detected, the logs will display an alert with the message "HTTP Traffic Detected" or “HTTPS Traffic Detected”, including source and destination IPs, the destination port (80) or port (443), and the timestamp.