Practical - 4

1. Objective

Write custom Snort rules to detect specific network behaviors. Test the effectiveness of custom rules in detecting predefined attack patterns.

Tools and Environment

- **Snort** installed in NIDS (Network Intrusion Detection System) mode.
- **Linux environment** with root privileges.
- Configuration of `snort.conf` to include a custom rule file.
- Logging/alert output enabled using:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Custom Snort Rules

1. **Ping Sweep Detection (ICMP Echo Requests)**

```
alert icmp any any -> any any (msg:"ICMP Ping Sweep Detected"; itype:8;
sid:1000001; rev:1;)
```

2. **Nmap TCP SYN Scan Detection**

```
alert tcp any any -> any any (flags:S; msg:"Nmap SYN Scan Detected";
sid:1000002; rev:1;)
```

3. **Access to Specific Web Application Path (/admin page)**

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Access to /admin
Detected"; flow:to_server,established; content:"GET /admin"; http_method;
sid:1000003; rev:1;)
```

4. **FTP Login Attempt (USER command)**

```
alert tcp any any -> any 21 (msg:"FTP USER Login Attempt";
flow:to_server,established; content:"USER "; sid:1000004; rev:1;)
```

5. **Shellcode Detection (NOP sled example)**

```
alert tcp any any -> any any (msg:"Potential Shellcode (NOP sled)";
content:"|90 90 90 90 90|"; sid:1000005; rev:1;)
```

Testing Effectiveness

1. **Ping Sweep Test**
   From another machine, run:

```
for ip in $(seq 1 10); do ping -c 1 192.168.1.$ip; done
```

2. **Nmap SYN Scan Test**

```
nmap -sS 192.168.1.100
```

3. **Web Access Test (/admin page)**

```
curl http://target-ip/admin
```

4. **FTP Login Attempt Test**

```
ftp target-ip
USER testuser
```

5. **Shellcode/NOP Test** (using Scapy in Python)

```
from scapy.all import *
send(IP(dst="192.168.1.100")/TCP(dport=80)/Raw(load="\x90\x90\x90\x90\x90")
)
```

Results

- **Rule 1** successfully detected ICMP ping sweeps.
- **Rule 2** generated alerts for Nmap SYN scans.
- **Rule 3** flagged attempts to access `/admin` paths.
- **Rule 4** detected FTP login attempts using the `USER` command.
- **Rule 5** raised alerts when NOP sled shellcode patterns were sent.
