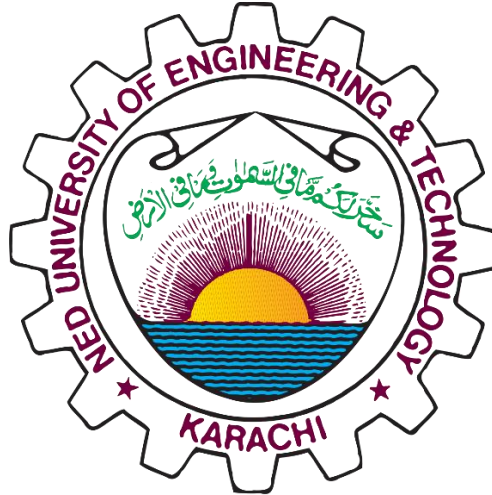


Intrusion Detection & Prevention System Using Snort on Ubuntu



Group Members	Uzma Haneef Sarah Zafar Hashem Al-Sakkaf
Course Instructor	Prof. Dr. Muhammad Mubashir
Course Title	Information Security
Course Code	CT-355

Introduction:

Snort is a widely used open-source intrusion detection system (IDS) designed to analyze network traffic in real-time and identify potential threats by matching traffic patterns against predefined rules. For this project, we installed and configured Snort on Ubuntu, a user-friendly Linux distribution, to serve as the platform for implementing a basic IDS and IPS. The setup involved configuring Snort rules to specifically detect ICMP packets, such as ping requests, and SSH login attempts, which are common in network reconnaissance and unauthorized access attempts. By customizing Snort's rule set and optimizing its configuration on Ubuntu, the system was fine-tuned to monitor network activity effectively and log potential security events for analysis.

Commands used:

To install snort:

```
sudo apt-get install snort
```

Change snort.conf home_net directory to:

```
ipvar HOME_NET 192.168.0.0/24
```

To configure Snort:

```
cd/ etc/snort
```

```
ls
```

```
sudo cp snort.conf snort.conf.backup
```

```
ls
```

```
sudo nano snort.conf
```

```
sudo snort -T -l enp0s8 -c etc/snort/snort.conf
```

Setting up custom rules on Snort:

```
sudo nano local.rules
```

```
alert icmp any any -> $HOME_NET any (msg: "ICMP Detected"; sid: 1000001; rev: 1)
```

```
alert tcp any any -> any443 (msg: "SSH Detected"; sid: 1000002; rev: 1)
```

```
ls
```

```
sudo snort -A console -q -i enp0s8 -c etc/snort/snort.conf -K ascii
```

On new terminal: -For ICMP packet detection

```
sudo nano /var/log/snort/snort.alert.fast
```

```
ping google.com
```

On new terminal: -For SSH login attempt detection

```
sudo su
```

```
sudo nano /var/log/snort/snort.alert.fast
```

```
sudo snort -A console -q -i enp0s8 -c etc/snort/snort.conf -K ascii
```

Ping google.com results:

```
sarah@sarah-VirtualBox:~$ ping google.com
PING google.com (142.250.181.78) 56(84) bytes of data.
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=1 ttl=60 time=30.9 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=2 ttl=60 time=28.6 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=3 ttl=60 time=30.0 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=4 ttl=60 time=28.7 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=5 ttl=60 time=28.7 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=6 ttl=60 time=32.2 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=7 ttl=60 time=31.8 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=8 ttl=60 time=44.3 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=9 ttl=60 time=28.7 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=10 ttl=60 time=29.0 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=11 ttl=60 time=29.6 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=12 ttl=60 time=29.1 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=13 ttl=60 time=29.2 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=14 ttl=60 time=29.4 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=15 ttl=60 time=39.6 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=16 ttl=60 time=32.6 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=17 ttl=60 time=27.3 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=18 ttl=60 time=44.3 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=19 ttl=60 time=33.4 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=20 ttl=60 time=30.0 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=21 ttl=60 time=28.5 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=22 ttl=60 time=27.3 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=23 ttl=60 time=27.5 ms
64 bytes from fjr04s07-in-f14.1e100.net (142.250.181.78): icmp_seq=24 ttl=60 time=28.6 ms
^C
--- google.com ping statistics ---
24 packets transmitted, 24 received, 0% packet loss, time 23022ms
rtt min/avg/max/mdev = 27.275/31.212/44.332/4.699 ms
sarah@sarah-VirtualBox:~$
```

ICMP packet & SSH login attempt detection:

```
root@sarah-VirtualBox:/home/sarah# sudo snort -A console -q -i enp0s8 -c /etc/snort/snort.conf -K ascii
11/17-20:36:06.083863 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:49878 -> 138.199.14.80:443
11/17-20:36:06.087228 [[*] [1:1000001:1] ICMP Detected [[*] [Priority: 0] {IPV6-ICMP} fe80::a666:1be6:e03e:be66 -> fe80::1
11/17-20:36:06.092648 [[*] [1:1000001:1] ICMP Detected [[*] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a666:1be6:e03e:be66
11/17-20:36:06.398046 [[*] [1:1000001:1] ICMP Detected [[*] [Priority: 0] {IPV6-ICMP} fe80::1ba:bf51:41b0:2a9f -> fe80::1
11/17-20:36:06.404791 [[*] [1:1000001:1] ICMP Detected [[*] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::1ba:bf51:41b0:2a9f
11/17-20:36:14.550537 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.662532 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.698600 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.700145 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.700413 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.701031 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.702025 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.707086 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.719316 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.757906 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.759744 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.761502 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.762070 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.762572 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.763921 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.764684 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.765145 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.765417 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.765779 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.766582 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.766939 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.767216 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.769073 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.769873 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:15.770036 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60042 -> 172.217.21.54:443
11/17-20:36:16.197490 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:49878 -> 138.199.14.80:443
11/17-20:36:16.288600 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:49878 -> 138.199.14.80:443
11/17-20:36:16.424404 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60501 -> 74.125.98.202:443
11/17-20:36:16.457875 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60501 -> 74.125.98.202:443
11/17-20:36:16.494947 [[*] [1:1000002:1] SSH Detected [[*] [Priority: 0] {TCP} 192.168.100.43:60501 -> 74.125.98.202:443
```

