Snort: Intrusion Detection System

December 2023

Wissal BOUTAYEB
Fatima BOUYARMANE

Mr MHAMED ZINEDDINE

PLAN

- Introduction
- Objectives
- Snort Architecture
- Rules
- Detection Attacks using Snort

Introduction:

Snort, an Intrusion Detection System created by Martin Roesch in 1998. Snort is an open-source powerhouse designed to protect networks from cyber threats. It works by analyzing network traffic against predefined rules, swiftly identifying potential security issues. Notably, Snort excels in protocol analysis, allowing it to detect anomalies in packet structures that may indicate malicious activities. With its flexibility, community support, and cross-platform compatibility, Snort has become an essential tool in the ever-changing world of network security.

Objectives:

Attack Detection:

Develop or configure Snort rules to detect a range of common cyber attacks, such as port scans, denial-of-service (DoS) attacks, SQL injection attempts, or malware communication patterns.

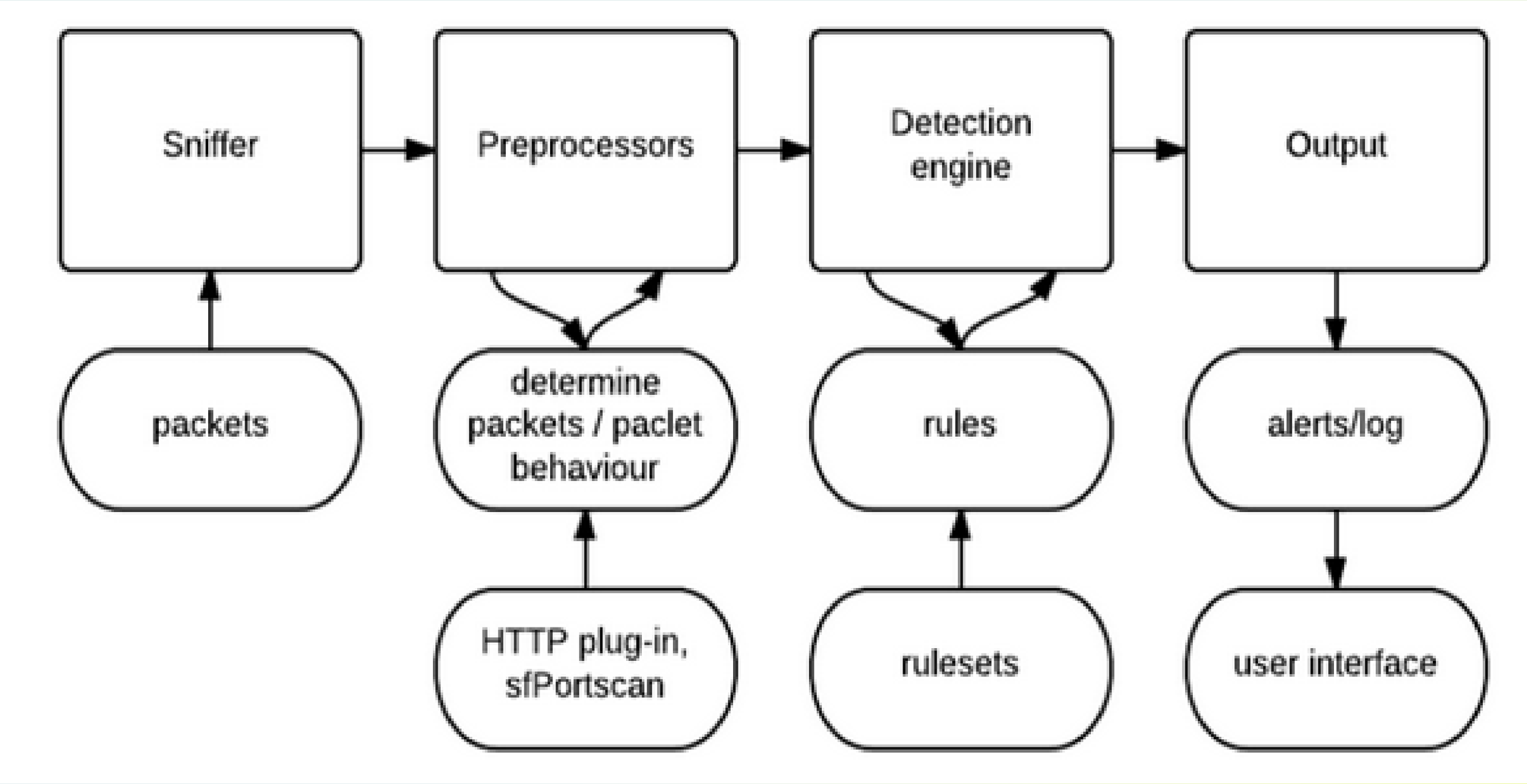
Real-Time Alerting:

Implement a real-time alerting mechanism within Snort to immediately notify administrators when suspicious or malicious activities are detected. Alerts should be clear, actionable, and configurable.

Logging and Event Recording:

Enhance Snort's logging capabilities to record detailed information about detected events. This information should include source and destination IP addresses, timestamp, the nature of the attack, and any relevant payload data.

Snort Architecture:



Rules:

1-Header Rule

Header rules specify the protocol, source and destination IP addresses, and port numbers for the traffic to match. These rules are fundamental in defining the scope of the traffic to be inspected.

2-Option Rule

Option rules specify additional criteria or conditions for triggering an alert. This may include checking for specific TCP flags, IP header information, or other packet attributes.

3-Metadata Rule

Metadata rules provide additional information about the rule itself. This can include details about the rule's author, references to external resources, or any other relevant metadata.

4-Content Rule

Content rules check for specific patterns or signatures within the payload of packets. These rules are crucial for detecting known malicious content or attack patterns.

Syntaxes:

1- alert tcp any any -> 192.168.1.1 80 (msg:"Possible HTTP Attack"; sid:1001;)
2- alert tcp any any -> any any (msg:"SYN Flood Attack Detected"; flags:S; threshold: type threshold, track by_src, count 10, seconds 1; sid:1004;)
3- alert tcp any any -> any any (msg:"Potential Vulnerability Exploitation"; sid:1006;)
4- alert tcp any any -> any any (content:"malware"; msg:"Malware Detected"; sid:1002;)

DETECTING ATTACKS BY SNORT

TCP SYN FLOOD ATTACK:

Configuration of rules:

```
WissalBOUTAYEB@ubuntu:~$ sudo nano /etc/snort/rules/local.rules
WissalBOUTAYEB@ubuntu:~$
```

```
  GNU nano 4.8                                                    /etc/snort/rules/local.rules
# $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
alert tcp any any -> $HOME_NET 80 (threshold: type threshold, track by_dst, count 20, seconds 60; msg: “Possible TCP SYN Flood attack detected”; sid: 10000009; rev: 1;)
```

Target system

```
WissalBOUTAYEB@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.23.129  netmask 255.255.255.0  broadcast 192.168.23.255
        inet6 fe80::d21c:2899:c7f4:1da5  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:02:92:78  txqueuelen 1000  (Ethernet)
        RX packets 32579  bytes 32829734 (32.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2297  bytes 162308 (162.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 196  bytes 17313 (17.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 196  bytes 17313 (17.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

WissalBOUTAYEB@ubuntu:~$
```

Attacker system

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.23.128  netmask 255.255.255.0  broadcast 192.168.23.255
        inet6 fe80::ae46:62d4:cd0:ec92  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c9:13:1f  txqueuelen 1000  (Ethernet)
        RX packets 47576  bytes 38606305 (36.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30365  bytes 5920094 (5.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 340 (340.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 340 (340.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
```

Performing the attack

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood -V -p 80 192.168.23.129
[sudo] password for kali:
using eth0, addr: 192.168.23.128, MTU: 1500
HPING 192.168.23.129 (eth0 192.168.23.129): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

The reaction of snort

```
WissalBOUTAYEB@ubuntu:~$ sudo snort -A console -c /etc/snort/snort.conf -i ens33
12/12-10:10:39.369918  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38391 -> 192.168.23.1
12/12-10:10:39.370358  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38411 -> 192.168.23.1
12/12-10:10:39.377816  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38431 -> 192.168.23.1
12/12-10:10:39.378146  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38451 -> 192.168.23.1
12/12-10:10:39.378633  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38471 -> 192.168.23.1
12/12-10:10:39.379082  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38491 -> 192.168.23.1
12/12-10:10:39.379596  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38511 -> 192.168.23.1
12/12-10:10:39.379913  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38531 -> 192.168.23.1
12/12-10:10:39.380569  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38551 -> 192.168.23.1
12/12-10:10:39.380903  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38571 -> 192.168.23.1
12/12-10:10:39.381430  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38591 -> 192.168.23.1
12/12-10:10:39.381782  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38611 -> 192.168.23.1
12/12-10:10:39.382241  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38631 -> 192.168.23.1
12/12-10:10:39.382547  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38651 -> 192.168.23.1
12/12-10:10:39.385099  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38671 -> 192.168.23.1
12/12-10:10:39.385556  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38691 -> 192.168.23.1
12/12-10:10:39.385973  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38711 -> 192.168.23.1
12/12-10:10:39.386300  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38731 -> 192.168.23.1
12/12-10:10:39.387041  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38751 -> 192.168.23.1
12/12-10:10:39.387370  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38771 -> 192.168.23.1
12/12-10:10:39.387787  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38791 -> 192.168.23.1
12/12-10:10:39.388312  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38811 -> 192.168.23.1
12/12-10:10:39.388719  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38831 -> 192.168.23.1
12/12-10:10:39.388997  [**] [1:10000009:1] “Possible TCP SYN Flood attack detected” [**] [Priority: 0] {TCP} 192.168.23.128:38851 -> 192.168.23.1
```

ICMP ATTACK:

```
WissalBOUTAYEB@ubuntu:~$ cd /etc/snort/rules/
WissalBOUTAYEB@ubuntu:/etc/snort/rules$ ls
attack-responses.rules          community-web-dos.rules    policy.rules
backdoor.rules                  community-web-iis.rules    pop2.rules
bad-traffic.rules               community-web-misc.rules   pop3.rules
chat.rules                      community-web-php.rules    porn.rules
community-bot.rules             ddos.rules                 rpc.rules
community-deleted.rules         deleted.rules              rservices.rules
community-dos.rules             dns.rules                  scan.rules
community-exploit.rules         dos.rules                  shellcode.rules
community-ftp.rules             experimental.rules         smtp.rules
community-game.rules            exploit.rules              snmp.rules
community-icmp.rules            finger.rules               sql.rules
community-imap.rules            ftp.rules                  telnet.rules
community-inappropriate.rules   icmp-info.rules           tftp.rules
community-mail-client.rules     icmp.rules                 virus.rules
community-misc.rules            imap.rules                 web-attacks.rules
community-nntp.rules            info.rules                 web-cgi.rules
community-oracle.rules          local.rules                web-client.rules
community-policy.rules          misc.rules                 web-coldfusion.rules
community-sip.rules             multimedia.rules           web-frontpage.rules
community-smtp.rules            mysql.rules                web-iis.rules
community-sql-injection.rules   netbios.rules              web-misc.rules
community-virus.rules           nntp.rules                 web-php.rules
community-web-attacks.rules     oracle.rules               x11.rules
community-web-cgi.rules         other-ids.rules
community-web-client.rules      p2p.rules
WissalBOUTAYEB@ubuntu:/etc/snort/rules$ sudo nano icmp.rules
[sudo] password for wissal:
```

Configuring rules

```
 GNU nano 4.8                                icmp.rules
#
#
# $Id: icmp.rules,v 1.25.2.1.2.2 2005/05/16 22:17:51 mwatchinski Exp $
#-----------
# ICMP RULES
#-----------
#
# Description:
# These rules are potentially bad ICMP traffic.  They include most of the
# ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
#
# Other ICMP rules are included in icmp-info.rules
alert icmp any any -> 192.168.23.129 any (msg:"ICMP Packet found"; sid:1000000>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8;>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; ic>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; d>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; >
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsi>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsiz>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; i>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; i>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scann>

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.23.129
PING 192.168.23.129 (192.168.23.129) 56(84) bytes of data.
64 bytes from 192.168.23.129: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 192.168.23.129: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 192.168.23.129: icmp_seq=3 ttl=64 time=1.33 ms
64 bytes from 192.168.23.129: icmp_seq=4 ttl=64 time=1.16 ms
64 bytes from 192.168.23.129: icmp_seq=5 ttl=64 time=0.458 ms
64 bytes from 192.168.23.129: icmp_seq=6 ttl=64 time=0.436 ms
64 bytes from 192.168.23.129: icmp_seq=7 ttl=64 time=0.767 ms
64 bytes from 192.168.23.129: icmp_seq=8 ttl=64 time=1.05 ms
64 bytes from 192.168.23.129: icmp_seq=9 ttl=64 time=1.13 ms
64 bytes from 192.168.23.129: icmp_seq=10 ttl=64 time=1.16 ms
```

Sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -I ens33

```
12/12-10:45:13.590278  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:13.590321  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.129 -> 192.168.23.128
12/12-10:45:14.123535  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 1
12/12-10:45:14.616948  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:14.616948  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:14.616948  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:14.617039  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.129 -> 192.168.23.128
12/12-10:45:15.127356  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 1
12/12-10:45:15.593647  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.
12/12-10:45:15.593653  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.
12/12-10:45:15.618666  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:15.618666  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:15.618666  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:15.618757  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.129 -> 192.168.23.128
12/12-10:45:16.621717  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:16.621717  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:16.621717  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:16.621858  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.129 -> 192.168.23.128
12/12-10:45:17.624381  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:17.624381  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:17.624381  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
12/12-10:45:17.624469  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.129 -> 192.168.23.128
12/12-10:45:18.626892  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.23.128 -> 192.168.23.129
```

SSH CONNECTION:

```
# SSH Connection
alert tcp any any -> any 443 (msg: "SSH Detected"; sid: 1000002; rev:1)
```

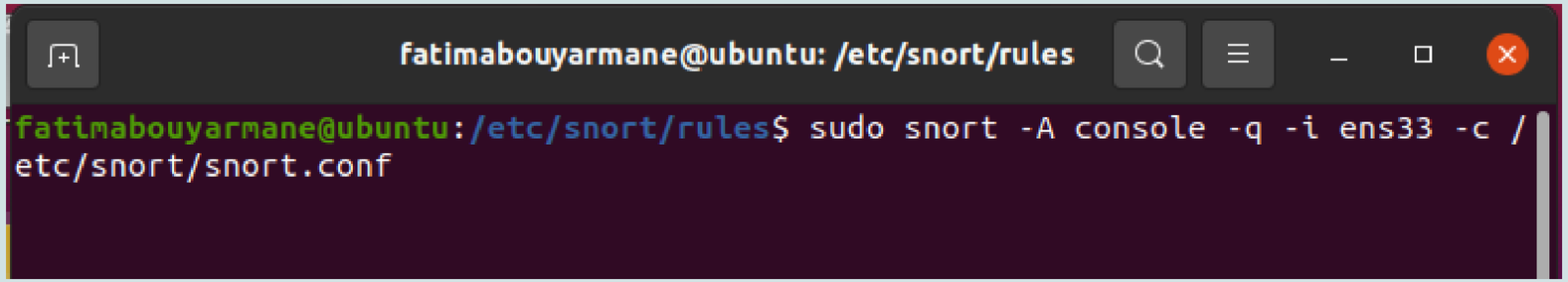
In the file /etc/snort/rules/local.rules

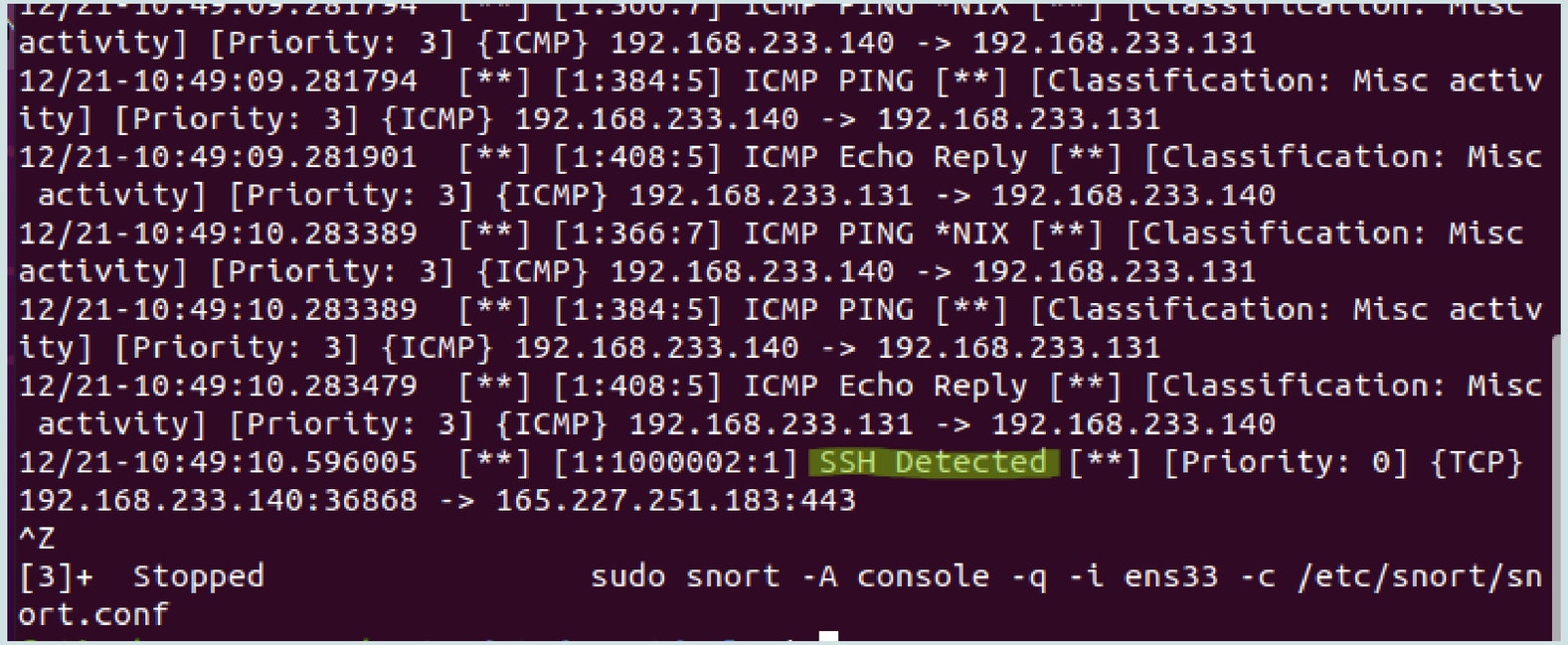
Creating new rule file for SSH traffic

Performing the attack

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.233.131
PING 192.168.233.131 (192.168.233.131) 56(84) bytes of data.
64 bytes from 192.168.233.131: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.233.131: icmp_seq=2 ttl=64 time=1.08 ms
64 bytes from 192.168.233.131: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 192.168.233.131: icmp_seq=4 ttl=64 time=1.38 ms
```

Running Snort to monitor traffic in console mode





Explore the cyber world with a careful look, Make new things in code, like a safety book. Build a future where Snort keeps things secure, A safe place we make, where dangers blur.

Q&A