local.rules

```
# ================================
# Custom Snort IPS Rules
# Graduation Project
# ================================

# 1. Block ICMP Ping
drop icmp any any -> any any (
    msg:"PING BLOCKED";
    sid:1000001;
    rev:1;
)

# 2. Detect Nmap SYN Scan
drop tcp any any -> any any (
    flags:S;
    msg:"NMAP SYN SCAN DETECTED";
    sid:1000002;
    rev:1;
)

# 3. Detect Nmap OS Detection
alert tcp any any -> any any (
    ttl: < 64;
    msg:"NMAP OS DETECTION ATTEMPT";
    sid:1000003;
    rev:1;
)

# 4. Block Telnet Access
drop tcp any any -> any 23 (
    msg:"TELNET ACCESS BLOCKED";
    sid:1000004;
    rev:1;
)

# 5. SSH Brute Force / Scan Detection
alert tcp any any -> any 22 (
    flow:to_server,established;
    msg:"SSH CONNECTION ATTEMPT DETECTED";
    sid:1000005;
    rev:1;
)
```

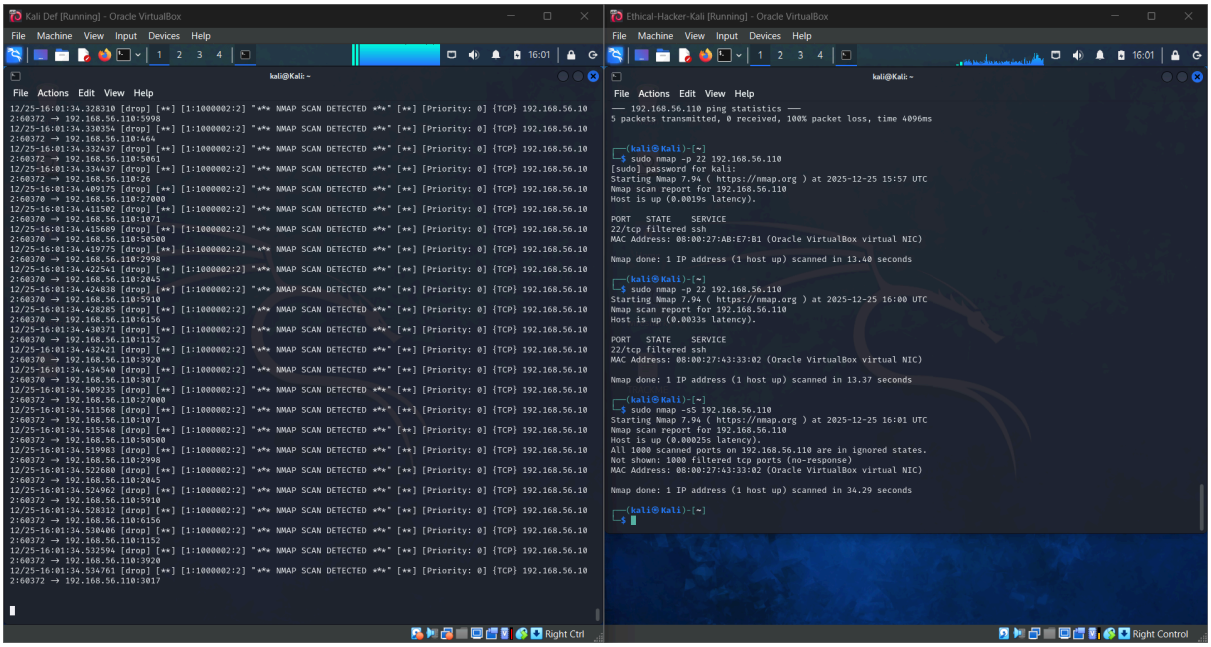
snort_commands

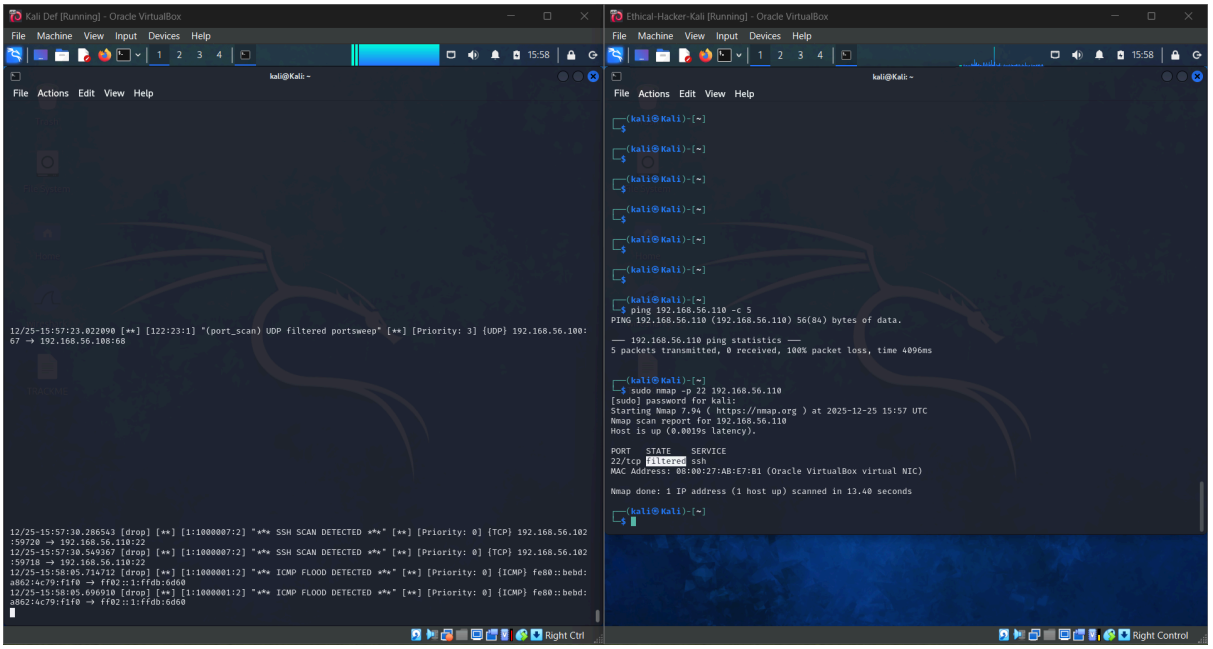
```
# Check Snort Version
snort -V

# Test configuration file
sudo snort -T -c /etc/snort/snort.lua

# Run Snort as IPS (Inline Mode)
sudo snort -Q \
--daq afpacket \
-i eth0:eth1 \
-c /etc/snort/snort.lua \
-A alert_fast

# Alternative (Bridge Interface)
sudo snort -Q \
--daq afpacket \
-i br0 \
-c /etc/snort/snort.lua \
-A alert_fast
```


Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
12/25-16:01:34.328310 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:5998
12/25-16:01:34.330354 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:464
12/25-16:01:34.332437 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:5061
12/25-16:01:34.334437 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:26
12/25-16:01:34.409175 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:27000
12/25-16:01:34.411502 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:1071
12/25-16:01:34.415680 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:50500
12/25-16:01:34.419775 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:2998
12/25-16:01:34.422541 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:2045
12/25-16:01:34.424838 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:5910
12/25-16:01:34.428285 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:6156
12/25-16:01:34.430371 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:1152
12/25-16:01:34.432421 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:3920
12/25-16:01:34.434540 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60370 → 192.168.56.110:3017
12/25-16:01:34.509235 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:27000
12/25-16:01:34.511568 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:1071
12/25-16:01:34.515548 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:50500
12/25-16:01:34.519983 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:2998
12/25-16:01:34.522680 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:2045
12/25-16:01:34.524962 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:5910
12/25-16:01:34.528312 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:6156
12/25-16:01:34.530406 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:1152
12/25-16:01:34.532594 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:3920
12/25-16:01:34.534761 [drop] [**] [1:1000002:2] "a** NMAP SCAN DETECTED a**a" [**] [Priority: 0] {TCP} 192.168.56.10
2:60372 → 192.168.56.110:3017
Right Ctrl
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
— 192.168.56.110 ping statistics —
5 packets transmitted, 0 received, 100% packet loss, time 4096ms
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -p 22 192.168.56.110
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2025-12-25 15:57 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0019s latency).
PORT STATE SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:AB:E7:B1 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -p 22 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-25 16:00 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0033s latency).
PORT STATE SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sS 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-25 16:01 UTC
Nmap scan report for 192.168.56.110
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.56.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 34.29 seconds
┌──(kali㉿Kali)-[~]
└─$
Right Control
Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
12/25-15:56:40.369081 [drop] [**] [1:1000001:2] "a** ICMP FLOOD DETECTED a**a" [**] [Priority: 0] {ICMP} 192.168.56.
102 → 192.168.56.110
12/25-15:56:41.388656 [drop] [**] [1:1000001:2] "a** ICMP FLOOD DETECTED a**a" [**] [Priority: 0] {ICMP} 192.168.56.
102 → 192.168.56.110
12/25-15:56:42.412782 [drop] [**] [1:1000001:2] "a** ICMP FLOOD DETECTED a**a" [**] [Priority: 0] {ICMP} 192.168.56.
102 → 192.168.56.110
12/25-15:56:43.436673 [drop] [**] [1:1000001:2] "a** ICMP FLOOD DETECTED a**a" [**] [Priority: 0] {ICMP} 192.168.56.
102 → 192.168.56.110
12/25-15:56:44.460653 [drop] [**] [1:1000001:2] "a** ICMP FLOOD DETECTED a**a" [**] [Priority: 0] {ICMP} 192.168.56.
102 → 192.168.56.110
12/25-15:56:57.656942 [**] [122:23:1] "(port_scan) UDP filtered portsweep" [**] [Priority: 3] {UDP} 192.168.56.100:
67 → 192.168.56.108:68
Right Ctrl
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
┌──(kali㉿Kali)-[~]
└─$ ping 192.168.56.110 -c 5
PING 192.168.56.110 (192.168.56.110) 56(84) bytes of data.
— 192.168.56.110 ping statistics —
5 packets transmitted, 0 received, 100% packet loss, time 4096ms
┌──(kali㉿Kali)-[~]
└─$
Right Control


Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
12/25-15:57:23.022090 [**] [122:23:1] "(port_scan) UDP filtered portsweep" [**] [Priority: 3] {UDP} 192.168.56.100:67 -> 192.168.56.108:68
12/25-15:57:30.286543 [drop] [**] [1:1000007:2] "**** SSH SCAN DETECTED ****" [**] [Priority: 0] {TCP} 192.168.56.102:59720 -> 192.168.56.110:22
12/25-15:57:30.549367 [drop] [**] [1:1000007:2] "**** SSH SCAN DETECTED ****" [**] [Priority: 0] {TCP} 192.168.56.102:59718 -> 192.168.56.110:22
12/25-15:58:05.714712 [drop] [**] [1:1000001:2] "**** ICMP FLOOD DETECTED ****" [**] [Priority: 0] {ICMP} fe80::bebd:a862:4c79:f1f0 -> ff02::1:ffdb:6d60
12/25-15:58:05.696910 [drop] [**] [1:1000001:2] "**** ICMP FLOOD DETECTED ****" [**] [Priority: 0] {ICMP} fe80::bebd:a862:4c79:f1f0 -> ff02::1:ffdb:6d60
Right Ctrl
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
(kali㉿Kali)-[~]
$ ping 192.168.56.110 -c 5
PING 192.168.56.110 (192.168.56.110) 56(84) bytes of data.
--- 192.168.56.110 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4096ms
(kali㉿Kali)-[~]
$ sudo nmap -p 22 192.168.56.110
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2025-12-25 15:57 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0019s latency).
PORT STATE SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:AB:E7:B1 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
(kali㉿Kali)-[~]
Right Control