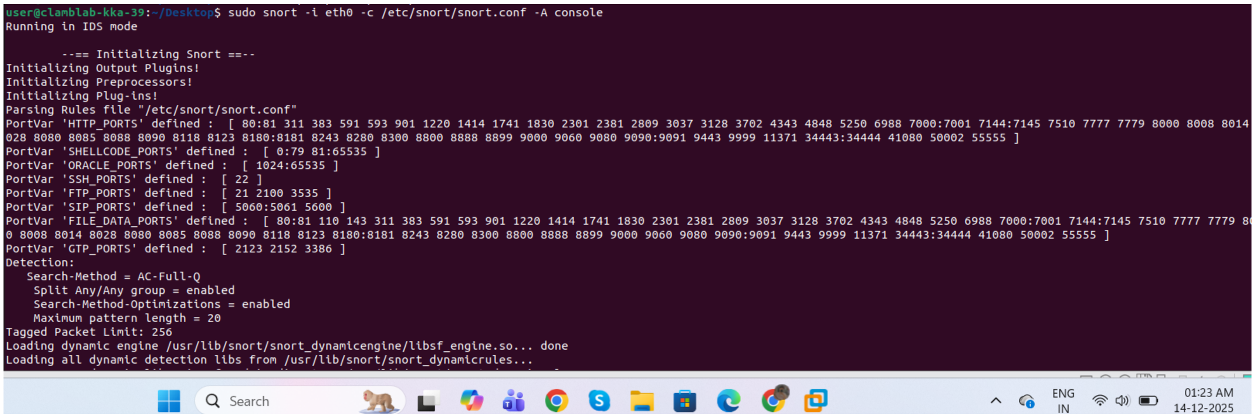
Snort IDS Lab

- Snort was deployed as an Intrusion Detection System (IDS) to monitor network traffic and generate alerts.
- An attacker–defender lab setup was used to simulate real SOC scenarios.
- Ubuntu Linux acted as the IDS host, while Kali Linux was used as the attacker system.
- Custom detection rules were created to identify ICMP attacks and TCP SYN scans.

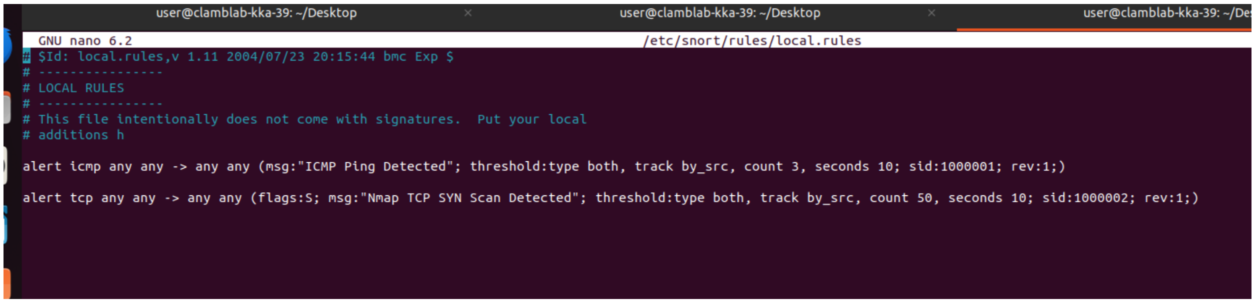
Screenshots

- Snort running in IDS mode on Ubuntu



```
user@clamblab-kka-39:~/Desktop$ sudo snort -i eth0 -c /etc/snort/snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014
028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 80
0 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

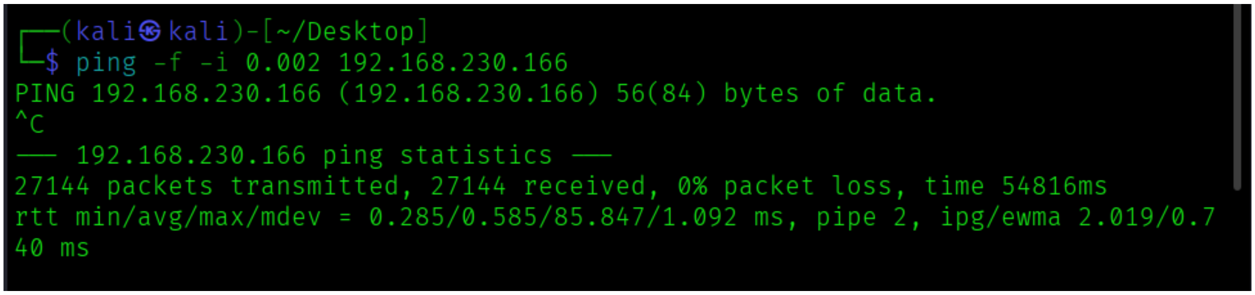
- local.rules file showing both ICMP and TCP SYN rules



user@clamblab-kka-39: ~/Desktop
user@clamblab-kka-39: ~/Desktop
user@clamblab-kka-39: ~/De

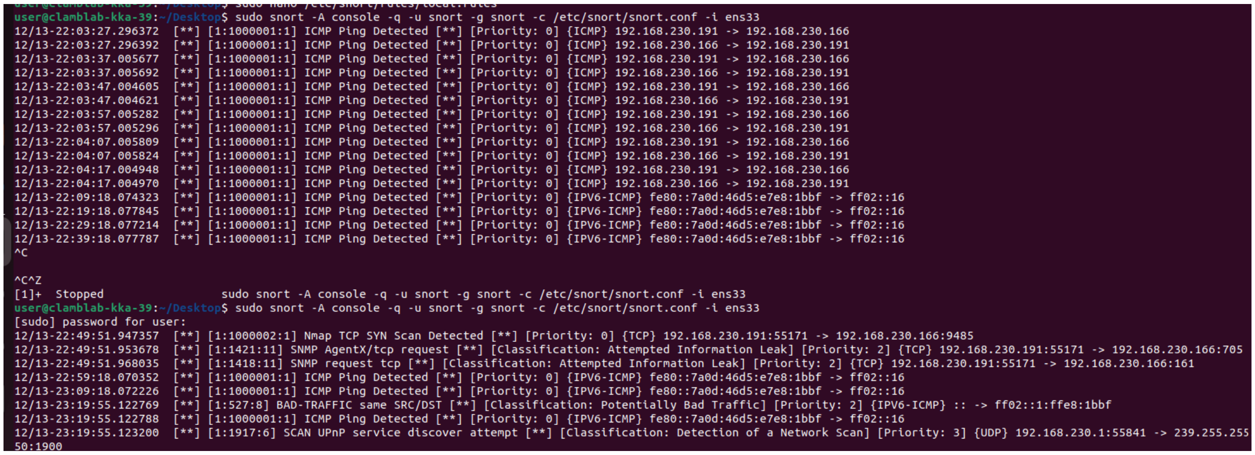
```
GNU nano 6.2                                        /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions h

alert icmp any any -> any any (msg:"ICMP Ping Detected"; threshold:type both, track by_src, count 3, seconds 10; sid:1000001; rev:1;)

alert tcp any any -> any any (flags:S; msg:"Nmap TCP SYN Scan Detected"; threshold:type both, track by_src, count 50, seconds 10; sid:1000002; rev:1;)
```

- Attack simulation from Kali Linux (ping or nmap -sS)



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -f -i 0.002 192.168.230.166
PING 192.168.230.166 (192.168.230.166) 56(84) bytes of data.
^C
--- 192.168.230.166 ping statistics ---
27144 packets transmitted, 27144 received, 0% packet loss, time 54816ms
rtt min/avg/max/mdev = 0.285/0.585/85.847/1.092 ms, pipe 2, ipg/ewma 2.019/0.7
40 ms
```

- Snort alert output confirming detection



```
user@clamblab-kka-39:~/Desktop$ sudo nano /etc/snort/rules/local.rules
user@clamblab-kka-39:~/Desktop$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
12/13-22:03:27.296372  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:03:27.296392  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:03:37.005677  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:03:37.005692  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:03:47.004605  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:03:47.004621  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:03:57.005282  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:03:57.005296  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:04:07.005809  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:04:07.005824  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:04:17.004948  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.191 -> 192.168.230.166
12/13-22:04:17.004970  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.230.166 -> 192.168.230.191
12/13-22:09:18.074323  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-22:19:18.077845  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-22:29:18.077214  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-22:39:18.077787  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
^C

^C^Z
[1]+  Stopped                 sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
user@clamblab-kka-39:~/Desktop$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
[sudo] password for user:
12/13-22:49:51.947357  [**] [1:1000002:1] Nmap TCP SYN Scan Detected [**] [Priority: 0] {TCP} 192.168.230.191:55171 -> 192.168.230.166:9485
12/13-22:49:51.953678  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.230.191:55171 -> 192.168.230.166:705
12/13-22:49:51.968035  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.230.191:55171 -> 192.168.230.166:161
12/13-22:59:18.070352  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-23:09:18.072226  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-23:19:55.122769  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ffe8:1bbf
12/13-23:19:55.122788  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::7a0d:46d5:e7e8:1bbf -> ff02::16
12/13-23:19:55.123200  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.230.1:55841 -> 239.255.255
50:1900
```

Lab Outcome

Snort successfully detected malicious ICMP traffic and TCP SYN scan activity generated from the Kali Linux machine. Real-time alerts confirmed correct IDS configuration and rule effectiveness.