

IDS_using_SNORT tool

IDS (Intrusion Detection System):

An Intrusion Detection System (IDS) is a security mechanism designed to detect unauthorized access, potential attacks, or suspicious activities within a network or system. The purpose of an IDS is to monitor traffic and identify malicious activities, security breaches, or violations of security policies in real-time, providing alerts for further action.

Key Functions of IDS

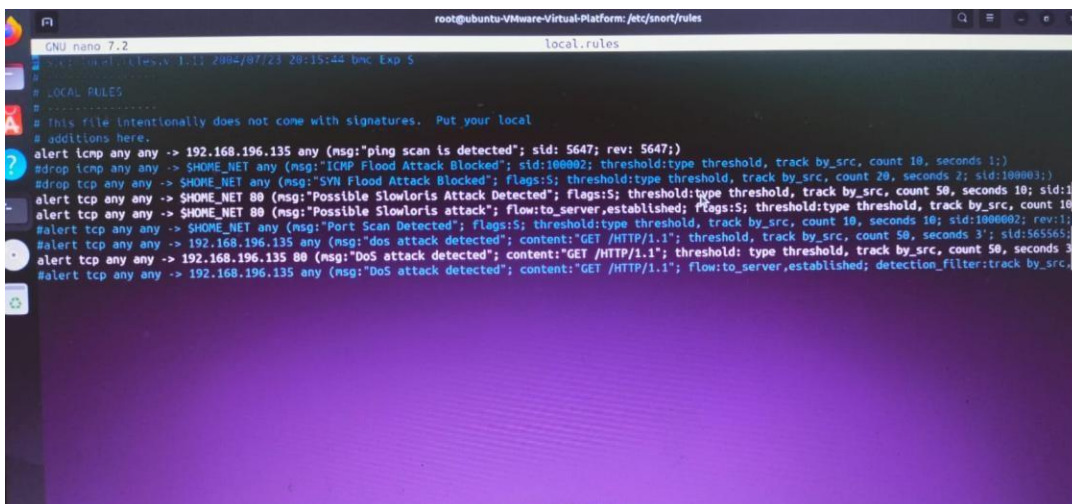
- **Monitoring Traffic:** IDS continually monitors network or system traffic to detect abnormal patterns that could suggest an attack or security breach.
- **Alerting:** When an intrusion or potential security threat is detected, the IDS generates alerts or notifications to security personnel, enabling them to take immediate action.
- **Recording Events:** IDS can log all network activities or system events for future analysis, helping in forensic investigations and improving security policies.

Proof of concept:

Step-1: on the ubuntu terminal

open the rules as `cd/etc/snort/rules`

In `local.rules`: `alert icmp any any -> 192.168.1.109 any (msg:" PING SCAN IS DETECTED"; sid: 569847; rev: 547;)`



```
root@ubuntu-Virtual-Platform: /etc/snort/rules
GNU nano 7.2 local.rules
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> 192.168.196.135 any (msg:"ping scan is detected"; sid: 5647; rev: 5647;)
#drop icmp any any -> SHOME_NET any (msg:"ICMP Flood Attack Blocked"; sid:100002; threshold:type threshold, track by_src, count 10, seconds 1;)
#drop tcp any any -> SHOME_NET any (msg:"SYN Flood Attack Blocked"; flags:S; threshold:type threshold, track by_src, count 20, seconds 2; sid:100003;)
alert tcp any any -> SHOME_NET 80 (msg:"Possible Slowloris Attack Detected"; flags:S; threshold:type threshold, track by_src, count 50, seconds 10; sid:100004;)
alert tcp any any -> SHOME_NET 80 (msg:"Possible Slowloris attack"; flow:to_server,established; flags:S; threshold:type threshold, track by_src, count 10; sid:100005;)
#alert tcp any any -> SHOME_NET any (msg:"Port Scan Detected"; flags:S; threshold:type threshold, track by_src, count 10, seconds 10; sid:100006; rev:1;)
#alert tcp any any -> 192.168.196.135 any (msg:"dos attack detected"; content:"GET /HTTP/1.1"; threshold: type threshold, track by_src, count 50, seconds 3; sid:565565;)
alert tcp any any -> 192.168.196.135 80 (msg:"DoS attack detected"; content:"GET /HTTP/1.1"; threshold: type threshold, track by_src, count 50, seconds 3; sid:565566;)
#alert tcp any any -> 192.168.196.135 any (msg:"DoS attack detected"; content:"GET /HTTP/1.1"; flow:to_server,established; detection_filter:track by_src, count 10, seconds 10; sid:565567; rev:1;)
```

STEP-2: snort -A console -q -c /etc/snort/snort.conf

1. snort

- This is the Snort command itself, which is used to start the Snort IDS/IPS process.

2. -A console

- The -A option specifies the alert output method.
- console means that Snort will display alerts directly to the console (i.e., standard output).
- This is often used for testing purposes or when you want to monitor alerts in real time directly on the terminal. When Snort detects an intrusion or suspicious activity, it will print an alert to the screen.

3. -q

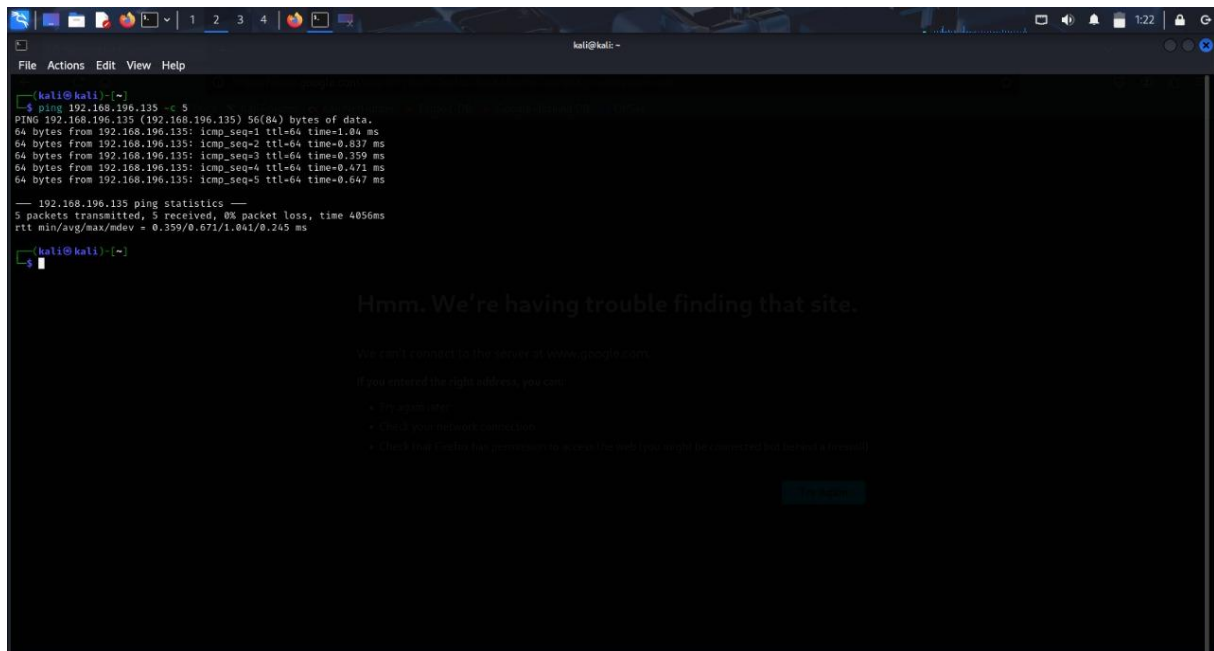
- The -q option stands for "quiet mode".
- When -q is used, Snort reduces the verbosity of its output, showing only alerts and critical information. This means Snort won't output verbose information about the packets it's processing; it will only show the alerts that match your configured rules.
- Without this flag, Snort would typically print more detailed logs and packet information, which might include lots of data that's not always useful for quick monitoring.

4. -c /etc/snort/snort.conf

- The -c option specifies the path to the Snort configuration file.
- /etc/snort/snort.conf is the typical location for the Snort configuration file on many Linux distributions.
- This configuration file contains the rules, settings, and parameters that define how Snort analyzes network traffic. It includes network variables, rule sets, logging options, and other settings.

Step-3:

The target machine is kali Linux ,here we are performing the PING scan



The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window is open with the following output:

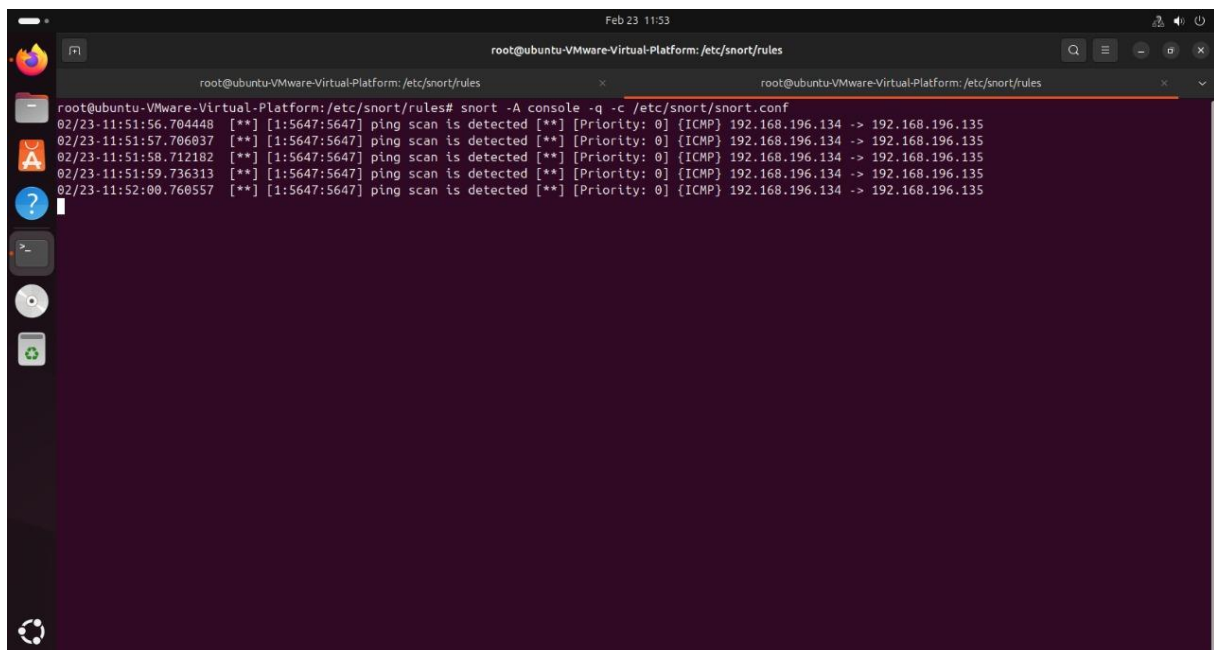
```
kali@kali:~$ ping 192.168.196.135 -c 5
PING 192.168.196.135 (192.168.196.135) 56(84) bytes of data:
64 bytes from 192.168.196.135: icmp_seq=1 ttl=64 time=1.04 ms
64 bytes from 192.168.196.135: icmp_seq=2 ttl=64 time=0.837 ms
64 bytes from 192.168.196.135: icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from 192.168.196.135: icmp_seq=4 ttl=64 time=0.421 ms
64 bytes from 192.168.196.135: icmp_seq=5 ttl=64 time=0.647 ms

--- 192.168.196.135 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.359/0.671/1.041/0.245 ms

kali@kali:~$
```

In the background, a web browser window is open, displaying a 404 error message: "Hmm. We're having trouble finding that site." The message indicates that the user cannot connect to the server at www.google.com and suggests checking the address, connection, or permissions.

Step-4:finally alert appeared



The screenshot shows a terminal window on a Ubuntu VM. The user has run the command `snort -A console -q -c /etc/snort/snort.conf` to display alerts. The output shows four alerts, all indicating a ping scan detected from 192.168.196.134 to 192.168.196.135.

```
root@ubuntu-VMware-Virtual-Platform:/etc/snort/rules# snort -A console -q -c /etc/snort/snort.conf
02/23-11:51:56.704448  [**] [1:5647:5647] ping scan is detected [**] [Priority: 0] [ICMP] 192.168.196.134 -> 192.168.196.135
02/23-11:51:57.706037  [**] [1:5647:5647] ping scan is detected [**] [Priority: 0] [ICMP] 192.168.196.134 -> 192.168.196.135
02/23-11:51:58.712182  [**] [1:5647:5647] ping scan is detected [**] [Priority: 0] [ICMP] 192.168.196.134 -> 192.168.196.135
02/23-11:51:59.736313  [**] [1:5647:5647] ping scan is detected [**] [Priority: 0] [ICMP] 192.168.196.134 -> 192.168.196.135
02/23-11:52:00.760557  [**] [1:5647:5647] ping scan is detected [**] [Priority: 0] [ICMP] 192.168.196.134 -> 192.168.196.135
```