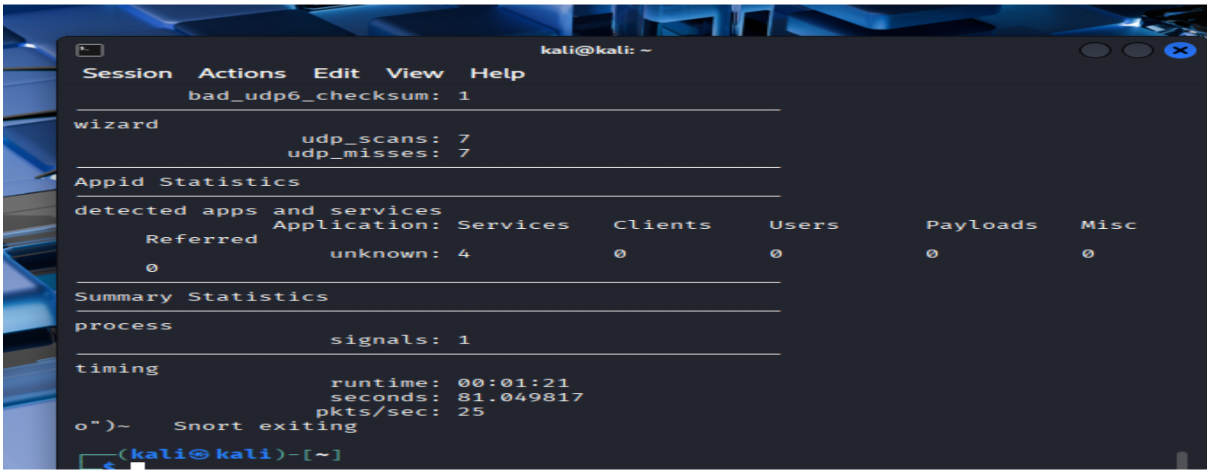
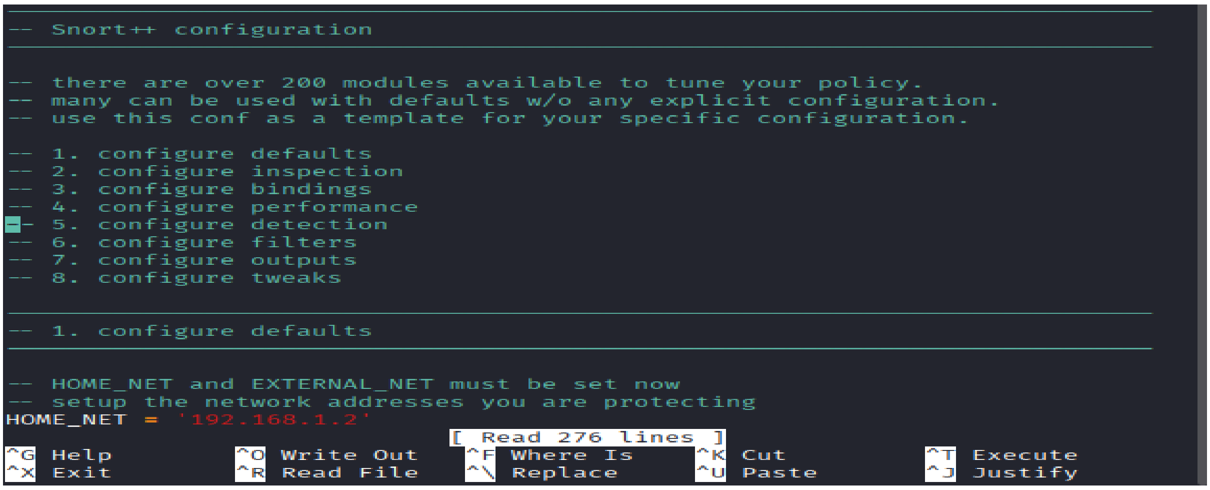
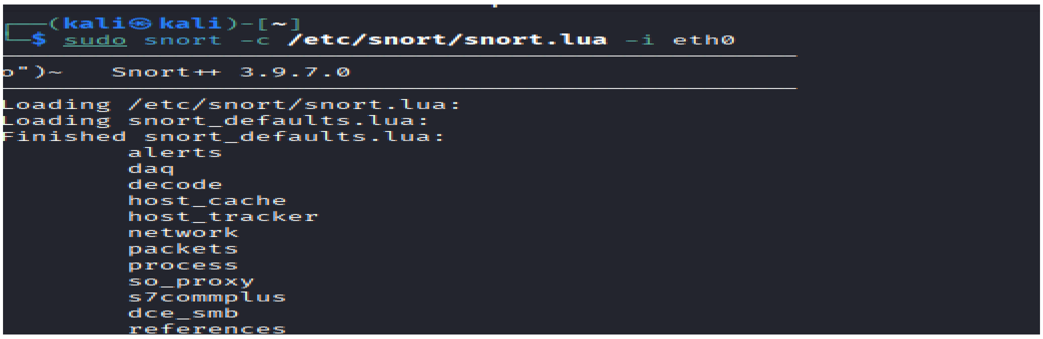


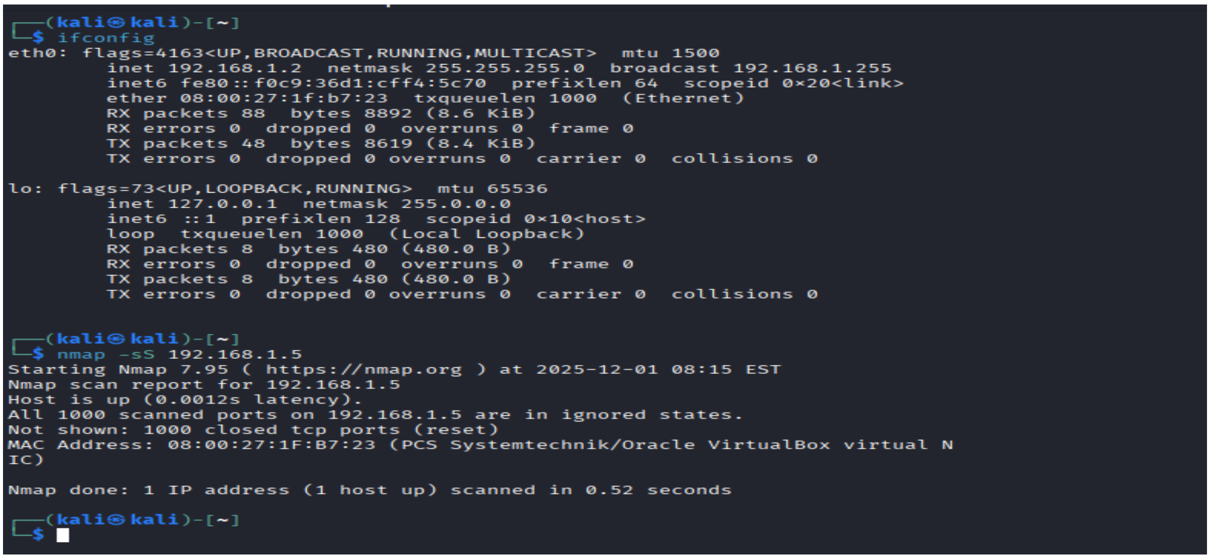
```
        bad_udp6_checksum: 1
--------------------------------------------------------------------------------
wizard
                udp_scans: 7
              udp_misses: 7
--------------------------------------------------------------------------------
Appid Statistics
--------------------------------------------------------------------------------
detected apps and services
              Application: Services    Clients    Users      Payloads    Misc
     Referred
                  unknown: 4           0          0          0           0
     0
--------------------------------------------------------------------------------
Summary Statistics
--------------------------------------------------------------------------------
process
                  signals: 1
--------------------------------------------------------------------------------
timing
                  runtime: 00:01:21
                  seconds: 81.049817
                pkts/sec: 25
o")~   Snort exiting

┌──(kali㉿kali)-[~]
```



```
---------------------------------------------------------------------------
-- Snort++ configuration
---------------------------------------------------------------------------

-- there are over 200 modules available to tune your policy.
-- many can be used with defaults w/o any explicit configuration.
-- use this conf as a template for your specific configuration.

-- 1. configure defaults
-- 2. configure inspection
-- 3. configure bindings
-- 4. configure performance
-- 5. configure detection
-- 6. configure filters
-- 7. configure outputs
-- 8. configure tweaks

---------------------------------------------------------------------------
-- 1. configure defaults
---------------------------------------------------------------------------

-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = '192.168.1.2'
                                        [ Read 276 lines ]
^G Help           ^O Write Out      ^F Where Is       ^K Cut            ^T Execute
^X Exit           ^R Read File      ^\ Replace        ^U Paste          ^J Justify
```



```
┌──(kali㉿kali)-[~]
└─$ sudo snort -c /etc/snort/snort.lua -i eth0
--------------------------------------------------
o")~   Snort++ 3.9.7.0
--------------------------------------------------
Loading /etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        alerts
        daq
        decode
        host_cache
        host_tracker
        network
        packets
        process
        so_proxy
        s7commplus
        dce_smb
        references
```



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f0c9:36d1:cff4:5c70  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:b7:23  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 8892 (8.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 8619 (8.4 KiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 08:15 EST
Nmap scan report for 192.168.1.5
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:1F:B7:23 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

┌──(kali㉿kali)-[~]
└─$ 
```