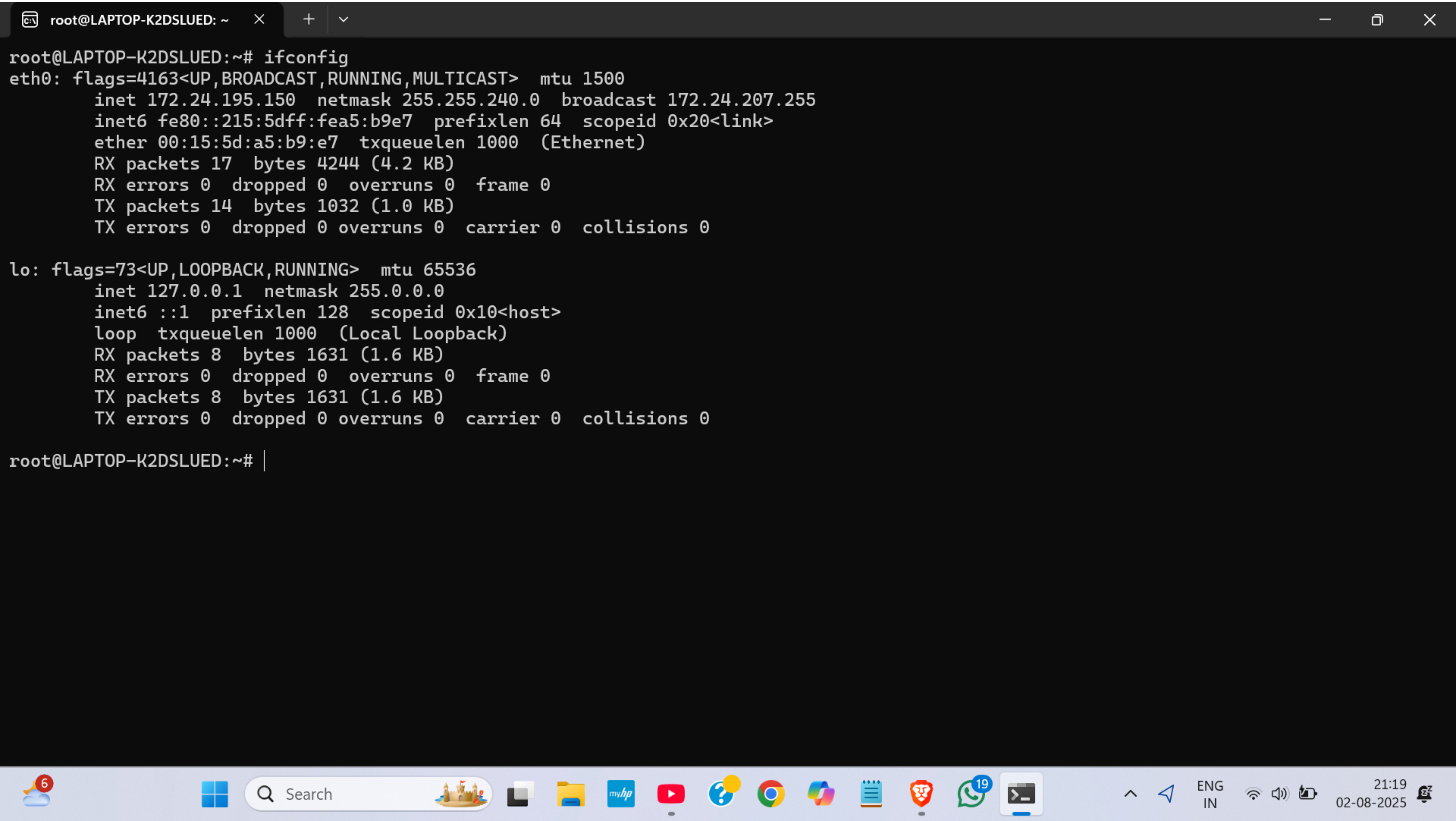
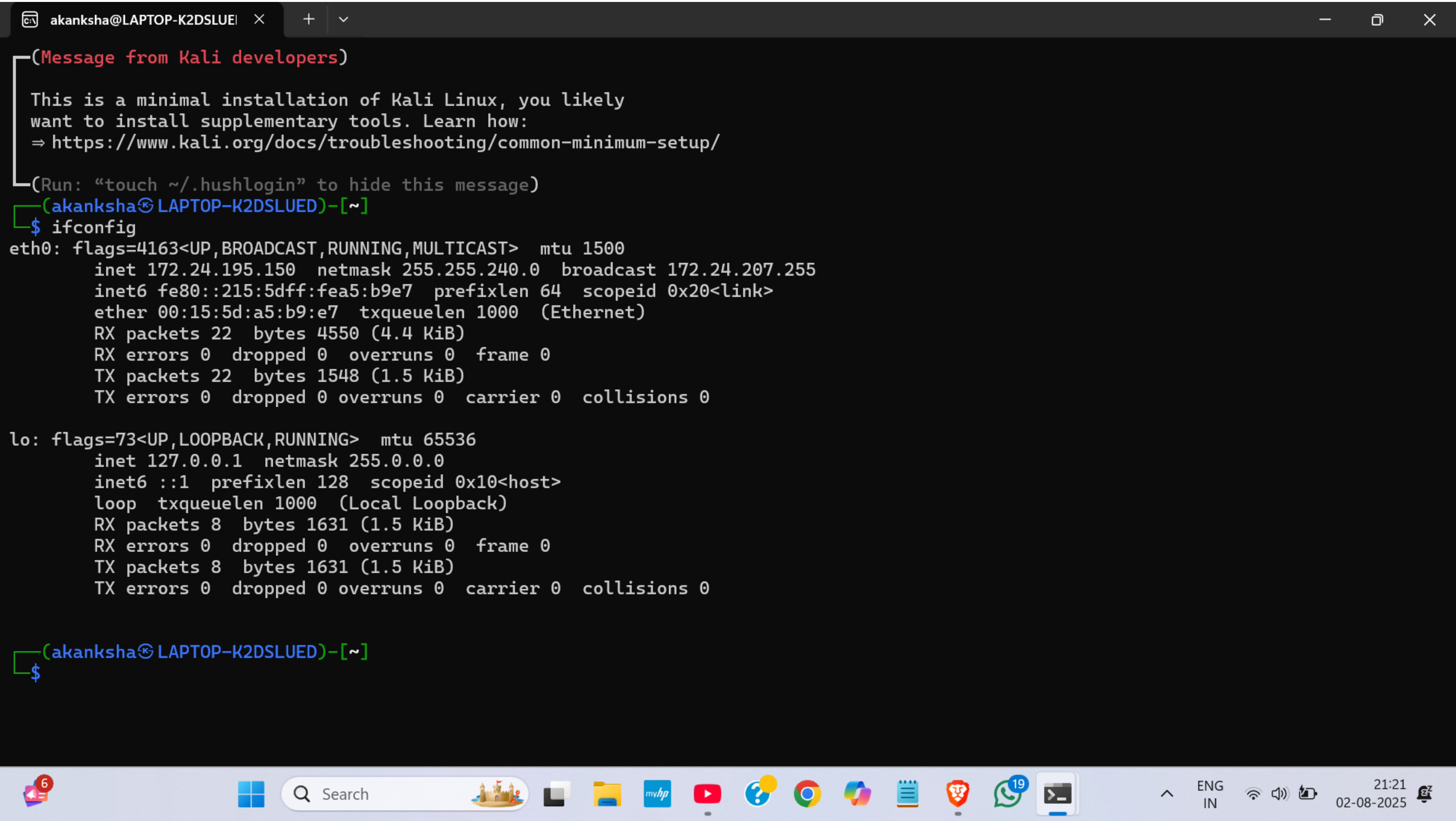
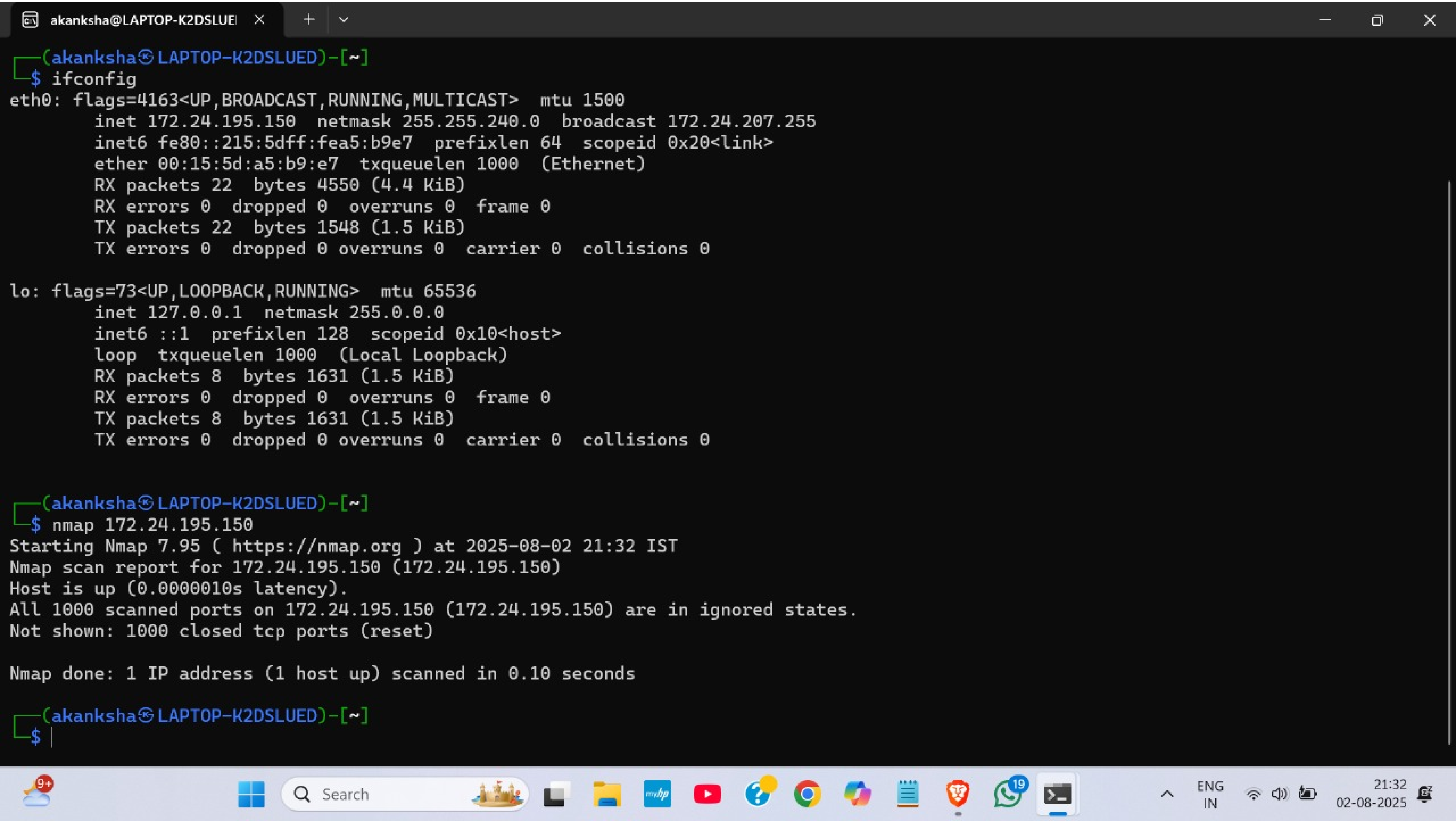


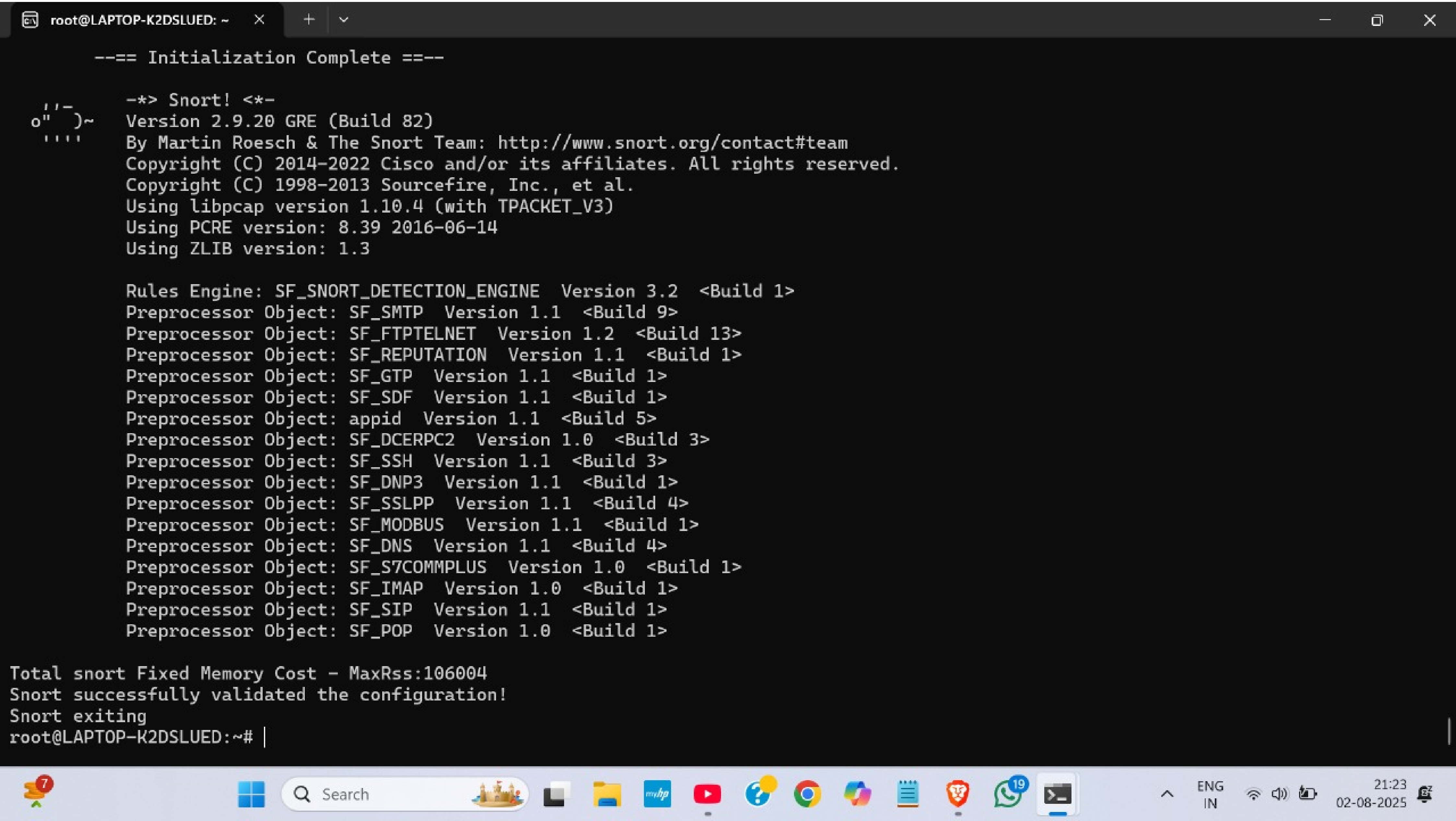
```
root@LAPTOP-K2DSLUED:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.195.150  netmask 255.255.240.0  broadcast 172.24.207.255
        inet6 fe80::215:5dff:fea5:b9e7  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:a5:b9:e7  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 4244 (4.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1032 (1.0 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 8  bytes 1631 (1.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 1631 (1.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@LAPTOP-K2DSLUED:~#
```



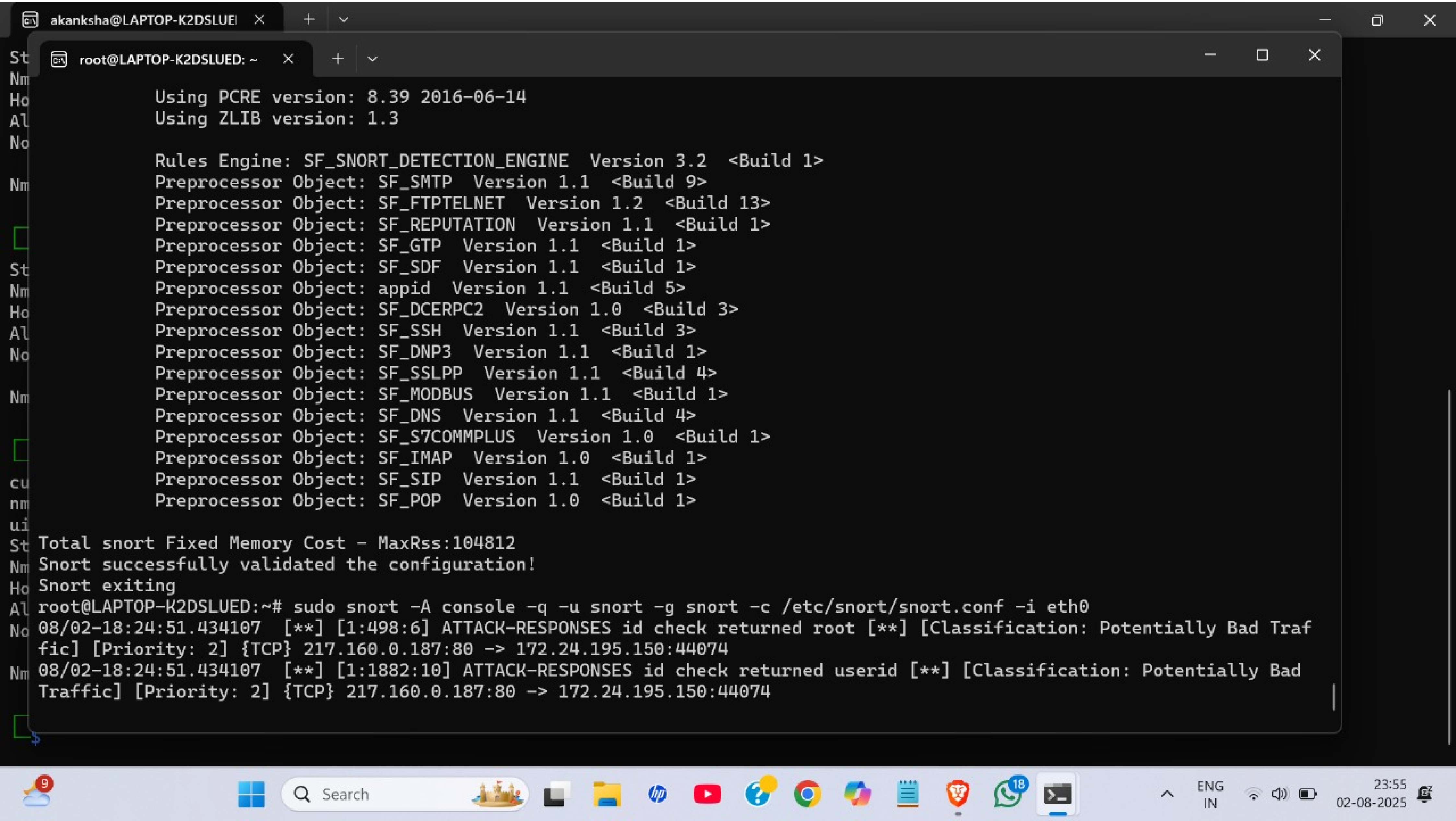
```
┌─(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└─(Run: “touch ~/.hushlogin” to hide this message)
┌──(akanksha㉿LAPTOP-K2DSLUED)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.195.150  netmask 255.255.240.0  broadcast 172.24.207.255
        inet6 fe80::215:5dff:fea5:b9e7  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:a5:b9:e7  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 4550 (4.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 1548 (1.5 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 1631 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 1631 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(akanksha㉿LAPTOP-K2DSLUED)-[~]
└─$
```



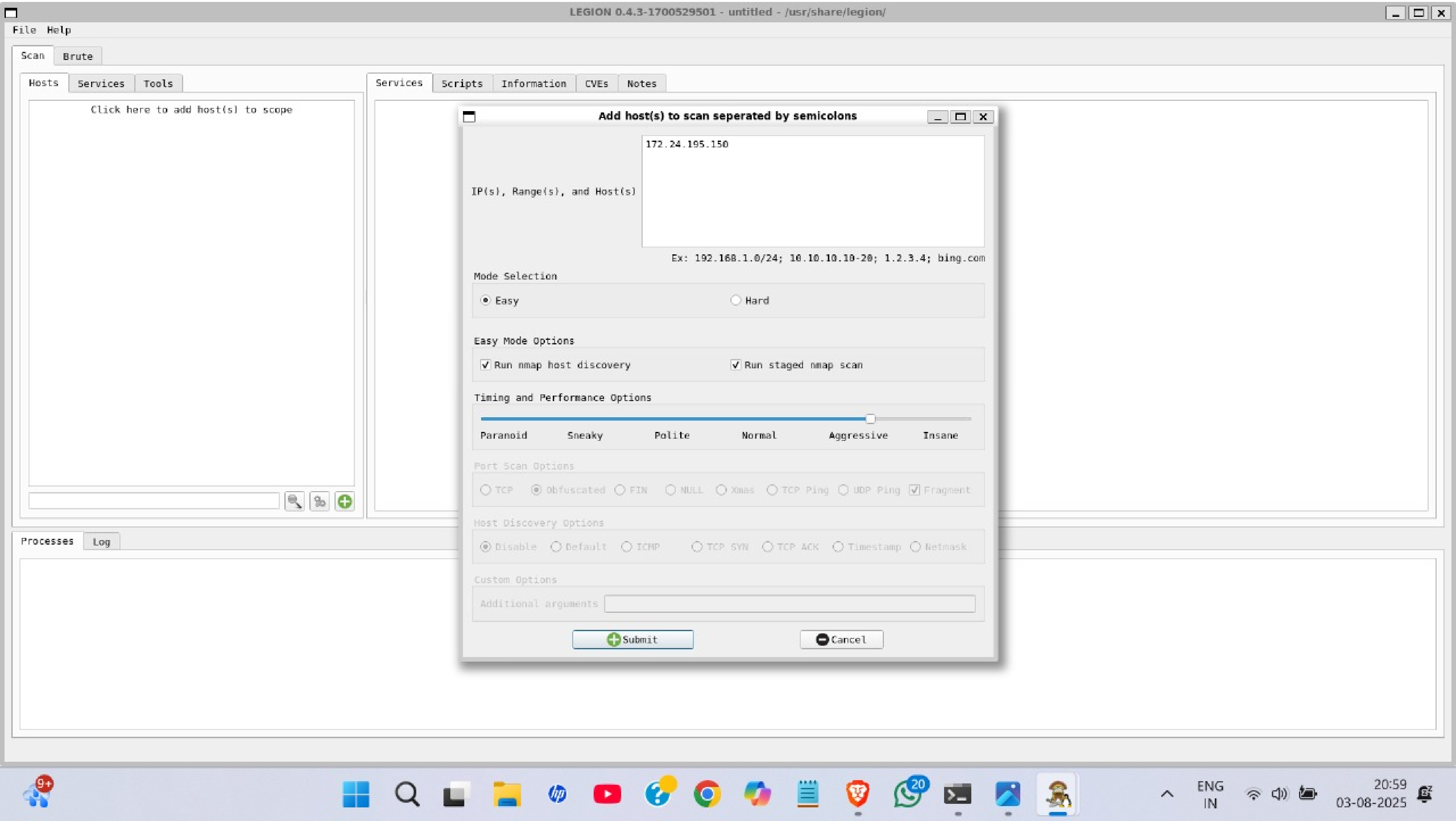
```
┌──(akanksha㉿LAPTOP-K2DSLUED)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.195.150  netmask 255.255.240.0  broadcast 172.24.207.255
        inet6 fe80::215:5dff:fea5:b9e7  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:a5:b9:e7  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 4550 (4.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 1548 (1.5 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 1631 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 1631 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(akanksha㉿LAPTOP-K2DSLUED)-[~]
└─$ nmap 172.24.195.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 21:32 IST
Nmap scan report for 172.24.195.150 (172.24.195.150)
Host is up (0.0000010s latency).
All 1000 scanned ports on 172.24.195.150 (172.24.195.150) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

┌──(akanksha㉿LAPTOP-K2DSLUED)-[~]
└─$
```



```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Total snort Fixed Memory Cost - MaxRss:106004
Snort successfully validated the configuration!
Snort exiting
root@LAPTOP-K2DSLUED:~#
```



```
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Total snort Fixed Memory Cost - MaxRss:104812
Snort successfully validated the configuration!
Snort exiting
root@LAPTOP-K2DSLUED:~# sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
08/02-18:24:51.434107  [**] [1:498:6] ATTACK-RESPONSES id check returned root [**] [Classification: Potentially Bad Traf
fic] [Priority: 2] {TCP} 217.160.0.187:80 -> 172.24.195.150:44074
08/02-18:24:51.434107  [**] [1:1882:10] ATTACK-RESPONSES id check returned userid [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 217.160.0.187:80 -> 172.24.195.150:44074
```



LEGION 0.4.3-1700529501 - untitled - /usr/share/legion/

Click here to add host(s) to scope

Add host(s) to scan seperated by semicolons

IP(s), Range(s), and Host(s): 172.24.195.150

Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com

Mode Selection

● Easy ○ Hard

Easy Mode Options

☑ Run nmap host discovery ☑ Run staged nmap scan

Timing and Performance Options

Paranoid Sneaky Polite Normal Aggressive Insane

Port Scan Options

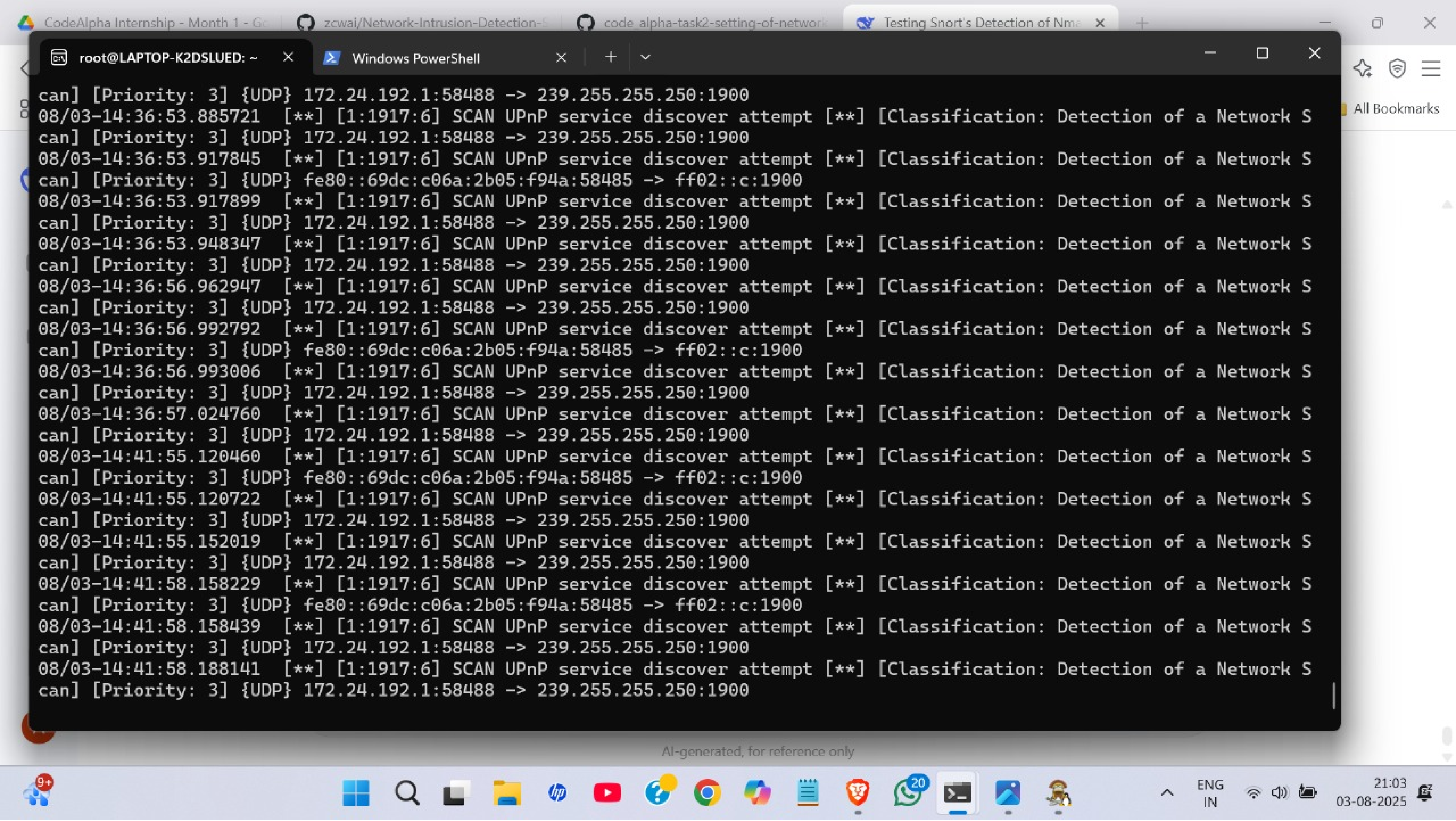
○ TCP ● Obfuscated ○ FIN ○ NULL ○ Xmas ○ TCP Ping ○ UDP Ping ☑ Fragment

Host Discovery Options

● Disable ○ Default ○ ICMP ○ TCP SYN ○ TCP ACK ○ Timestamp ○ Netmask

Custom Options

Additional arguments



CodeAlpha Internship - Month 1 - Go
zcwai/Network-Intrusion-Detection-S
code_alpha-task2-setting-of-network
Testing Snort's Detection of Nma
root@LAPTOP-K2DSLUED: ~
Windows PowerShell
All Bookmarks
AI-generated, for reference only
ENG
IN
21:03
03-08-2025

```
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:53.885721  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:53.917845  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} fe80::69dc:c06a:2b05:f94a:58485 -> ff02::c:1900
08/03-14:36:53.917899  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:53.948347  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:56.962947  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:56.992792  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} fe80::69dc:c06a:2b05:f94a:58485 -> ff02::c:1900
08/03-14:36:56.993006  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:36:57.024760  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:41:55.120460  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} fe80::69dc:c06a:2b05:f94a:58485 -> ff02::c:1900
08/03-14:41:55.120722  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:41:55.152019  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:41:58.158229  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} fe80::69dc:c06a:2b05:f94a:58485 -> ff02::c:1900
08/03-14:41:58.158439  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
08/03-14:41:58.188141  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network S
can] [Priority: 3] {UDP} 172.24.192.1:58488 -> 239.255.255.250:1900
```