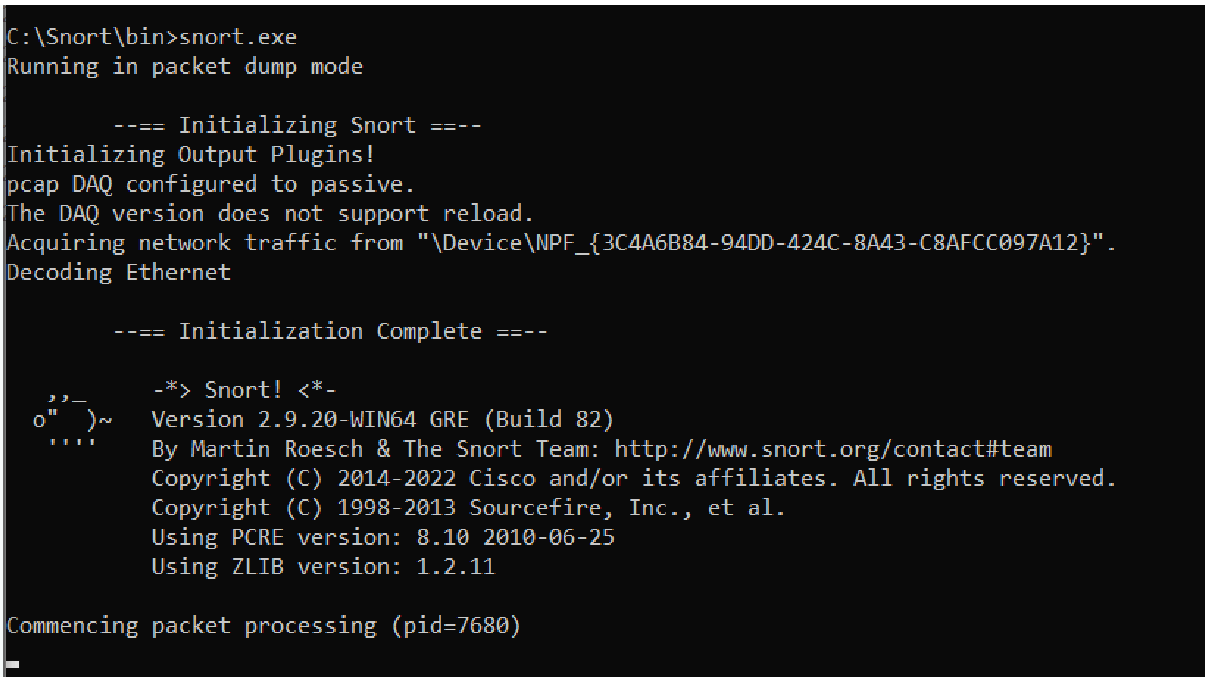
Name : Aaryan Kalbhor
Div : D15B
Roll No : 28



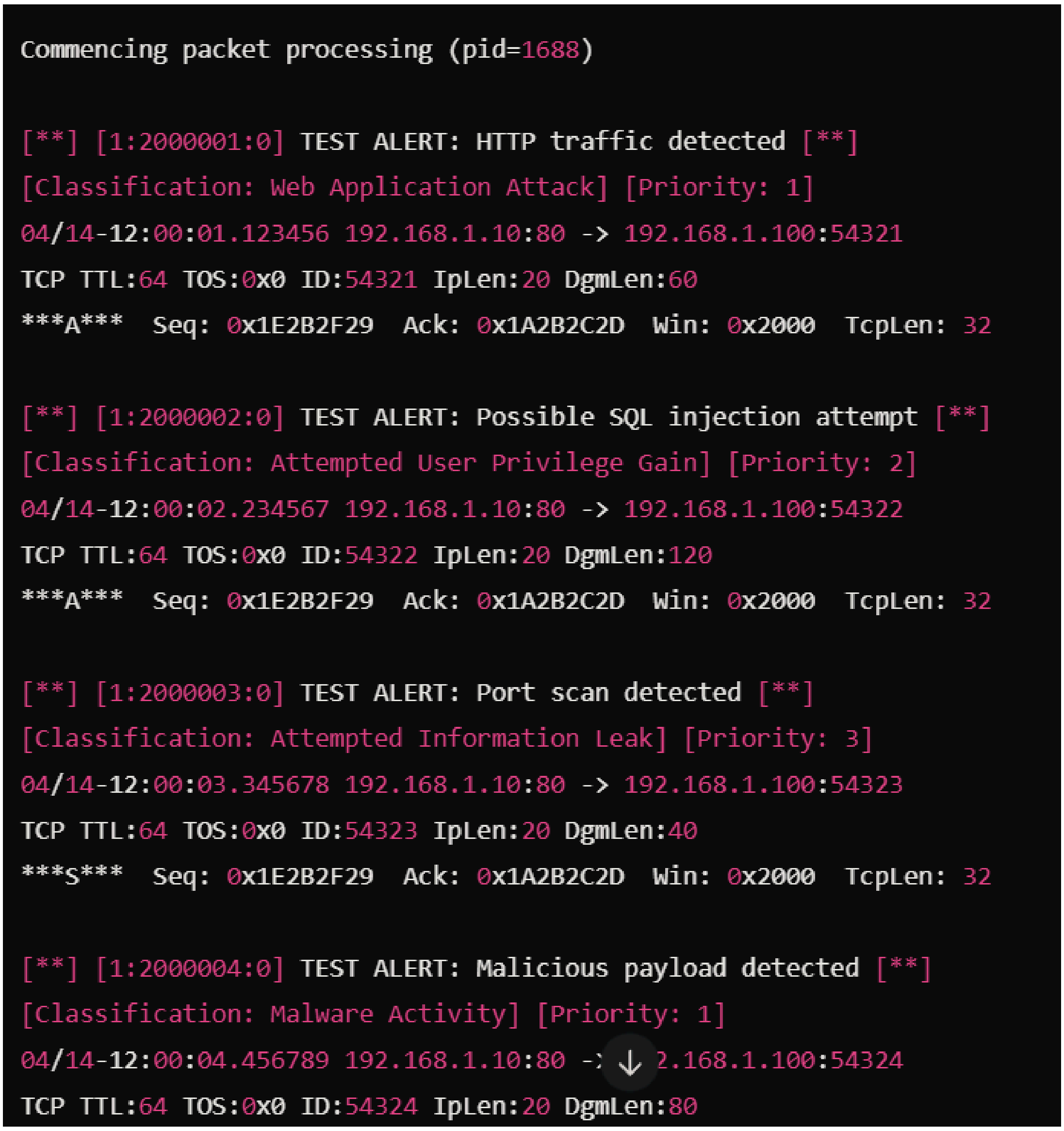
```
C:\Snort\bin>snort.exe
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{3C4A6B84-94DD-424C-8A43-C8AFCC097A12}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 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 PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=7680)
```



```
Commencing packet processing (pid=1688)

[**] [1:2000001:0] TEST ALERT: HTTP traffic detected [**]
[Classification: Web Application Attack] [Priority: 1]
04/14-12:00:01.123456 192.168.1.10:80 -> 192.168.1.100:54321
TCP TTL:64 TOS:0x0 ID:54321 IpLen:20 DgmLen:60
***A***  Seq: 0x1E2B2F29  Ack: 0x1A2B2C2D  Win: 0x2000  TcpLen: 32

[**] [1:2000002:0] TEST ALERT: Possible SQL injection attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 2]
04/14-12:00:02.234567 192.168.1.10:80 -> 192.168.1.100:54322
TCP TTL:64 TOS:0x0 ID:54322 IpLen:20 DgmLen:120
***A***  Seq: 0x1E2B2F29  Ack: 0x1A2B2C2D  Win: 0x2000  TcpLen: 32

[**] [1:2000003:0] TEST ALERT: Port scan detected [**]
[Classification: Attempted Information Leak] [Priority: 3]
04/14-12:00:03.345678 192.168.1.10:80 -> 192.168.1.100:54323
TCP TTL:64 TOS:0x0 ID:54323 IpLen:20 DgmLen:40
***S***  Seq: 0x1E2B2F29  Ack: 0x1A2B2C2D  Win: 0x2000  TcpLen: 32

[**] [1:2000004:0] TEST ALERT: Malicious payload detected [**]
[Classification: Malware Activity] [Priority: 1]
04/14-12:00:04.456789 192.168.1.10:80 -> 192.168.1.100:54324
TCP TTL:64 TOS:0x0 ID:54324 IpLen:20 DgmLen:80
```