NAME: Divyang Bagla

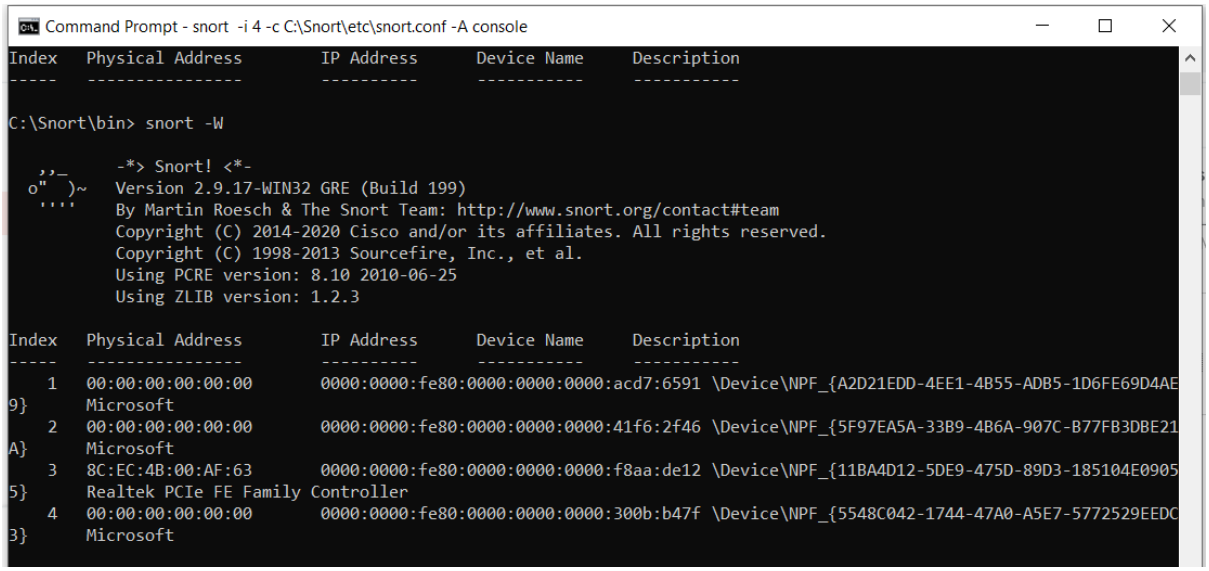
PANEL: D (D2)

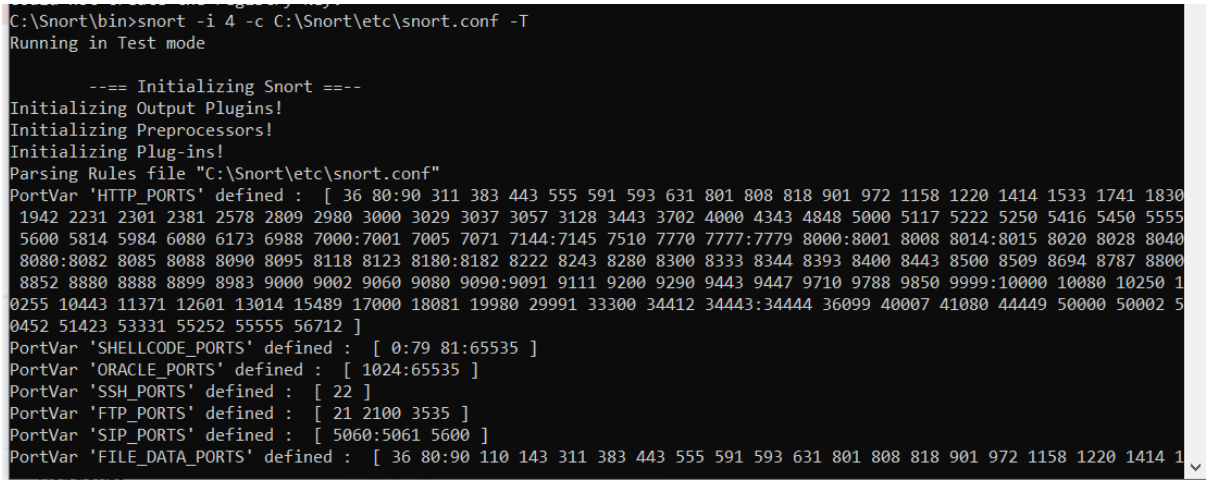
ROLL NO.: PD32

SUBJECT: IS

LAB ASSIGNMENT 6

SNORT IMPLEMENTATION:-





ALERT MESSAGES in local rules file:-

```
#--------------
alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001;)
alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002;)
alert udp any any -> any any (msg:"Testing UDP"; sid:1000003;)
```

```
C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 383 443 555 591 593 631 801 808 818 901 972 1158 1220 1414 1533 1741 1830
 1942 2231 2301 2381 2578 2809 2980 3000 3029 3037 3057 3128 3443 3702 4000 4343 4848 5000 5117 5222 5250 5416 5450 5555
 5600 5814 5984 6080 6173 6988 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040
 8080:8082 8085 8088 8090 8095 8118 8123 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8500 8509 8694 8787 8800
 8852 8880 8888 8899 8983 9000 9002 9060 9080 9090:9091 9111 9200 9290 9443 9447 9710 9788 9850 9999:10000 10080 10250 1
0255 10443 11371 12601 13014 15489 17000 18081 19980 29991 33300 34412 34443:34444 36099 40007 41080 44449 50000 50002 5
PAGE 1 OF 1   198 WORDS   ENGLISH (INDIA)
```

```
Commencing packet processing (pid=11320)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 646.396000 seconds
Snort processed 0 packets.
Snort ran for 0 days 0 hours 10 minutes 46 seconds
   Pkts/min:           0
   Pkts/sec:           0
===============================================================================
Packet I/O Totals:
   Received:           0
   Analyzed:           0 (  0.000%)
    Dropped:           0 (  0.000%)
   Filtered:           0 (  0.000%)
Outstanding:           0 (  0.000%)
   Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           0 (  0.000%)
       VLAN:           0 (  0.000%)
        IP4:           0 (  0.000%)
       Frag:           0 (  0.000%)
       ICMP:           0 (  0.000%)
        UDP:           0 (  0.000%)
        TCP:           0 (  0.000%)
        IP6:           0 (  0.000%)
    IP6 Ext:           0 (  0.000%)
   IP6 Opts:           0 (  0.000%)
      Frag6:           0 (  0.000%)
```

```
===============================================================================
Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:            0 (  0.000%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
     Frags Reassembled: 0
              Discards: 0
         Memory Faults: 0
              Timeouts: 0
              Overlaps: 0
             Anomalies: 0
                Alerts: 0
```

```
    Maximum initialization total: 4514
===============================================================================
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                          : 0
  Max concurrent sessions                 : 0
===============================================================================
POP Preprocessor Statistics
  Total sessions                          : 0
  Max concurrent sessions                 : 0
===============================================================================
Snort exiting

C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
```