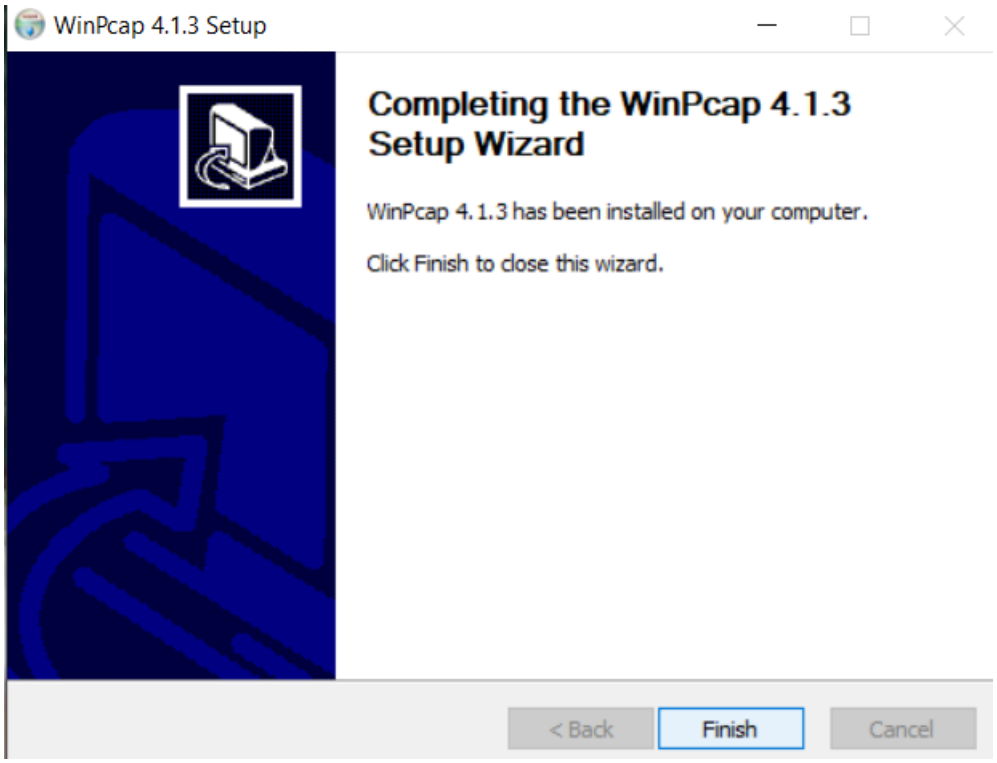
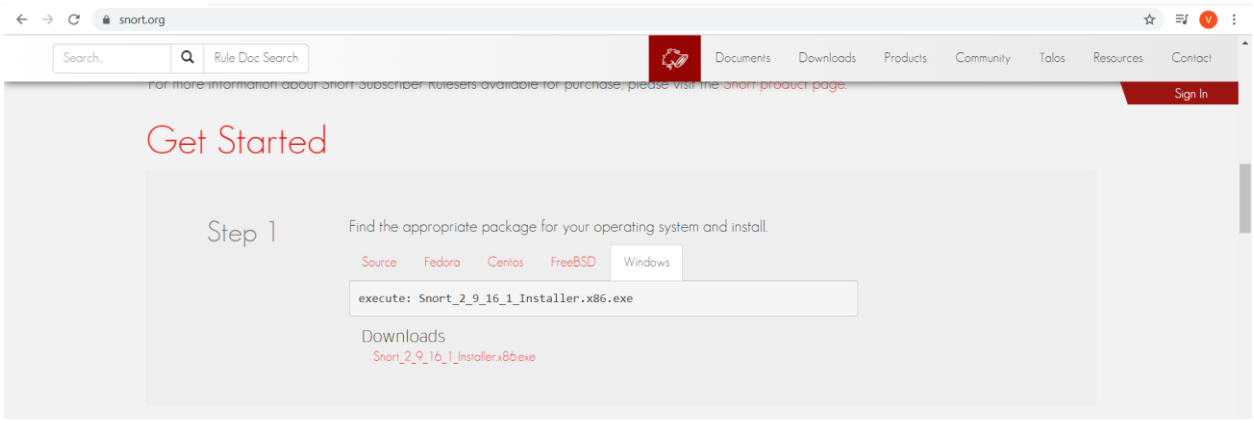
Exercise 10:

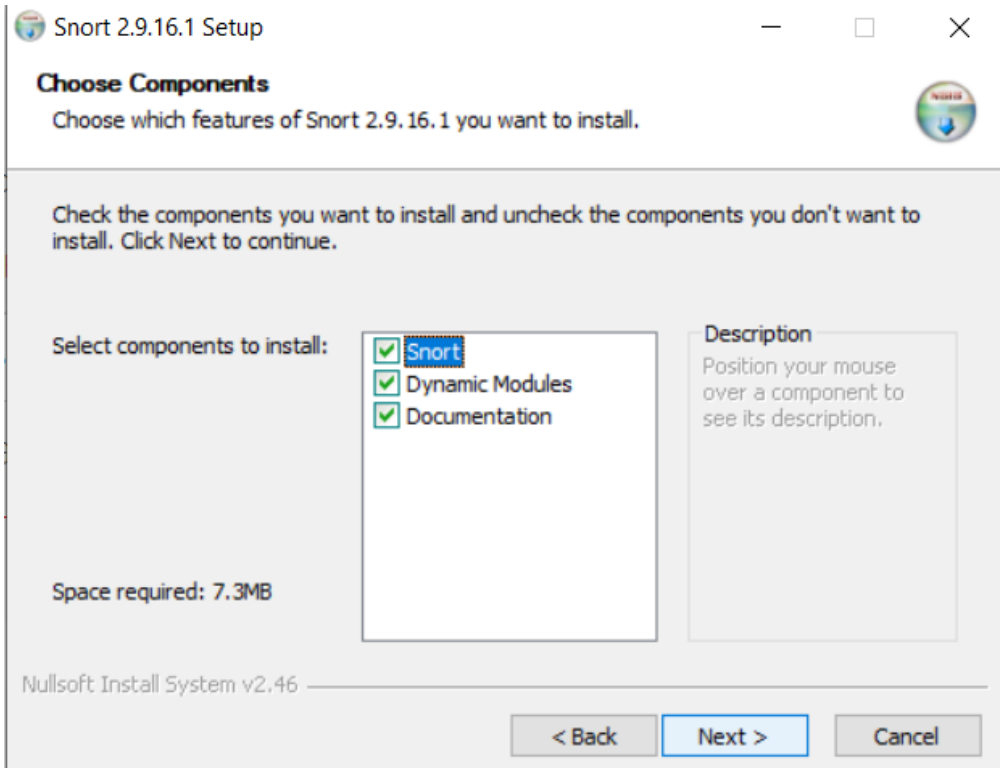
To demonstrate intrusion detection system (ids) using any snort.

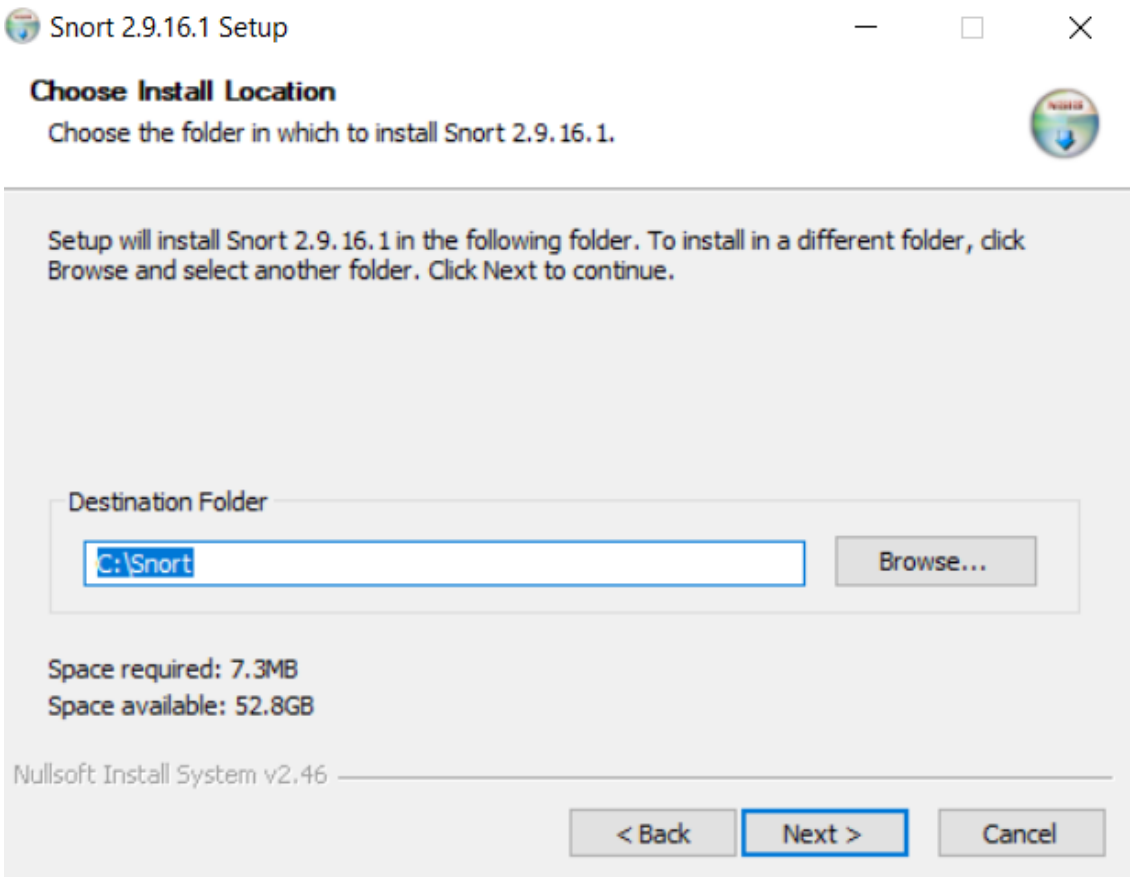
1) Installing WinPcap in Windows:.

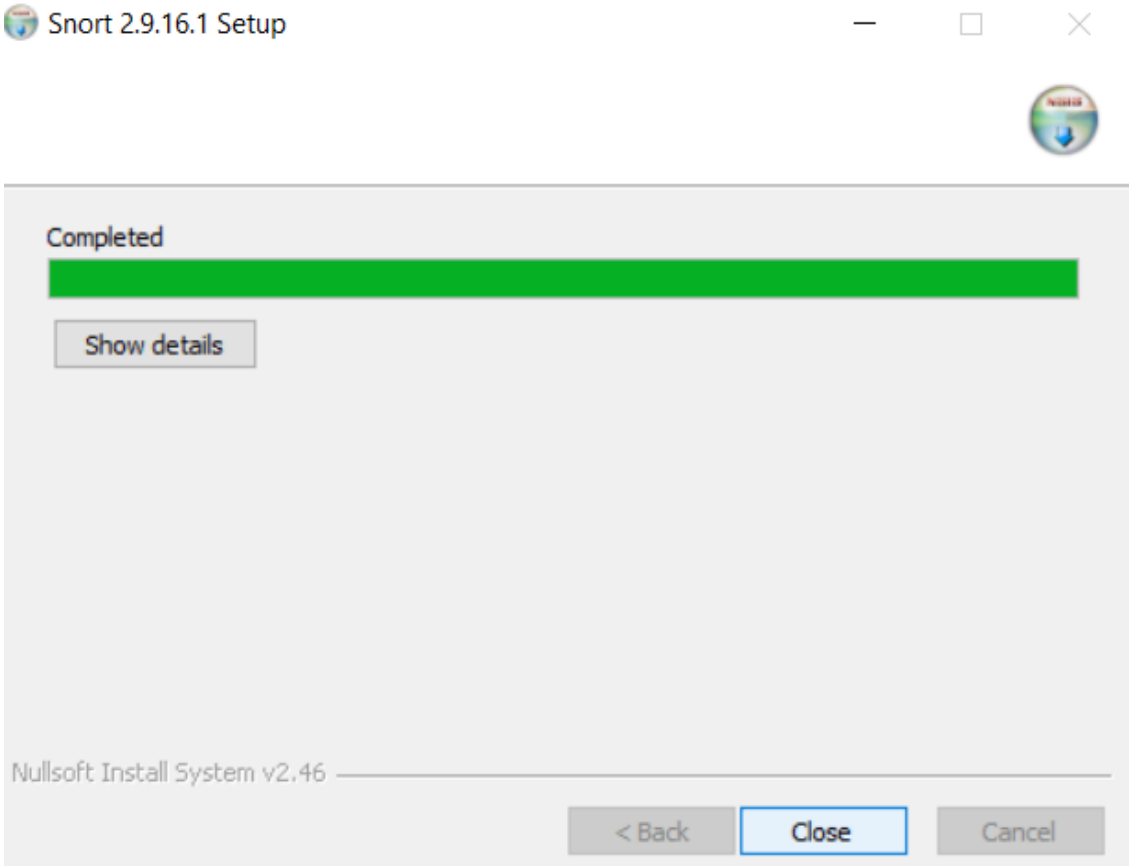


2) Installing Snort in Windows:

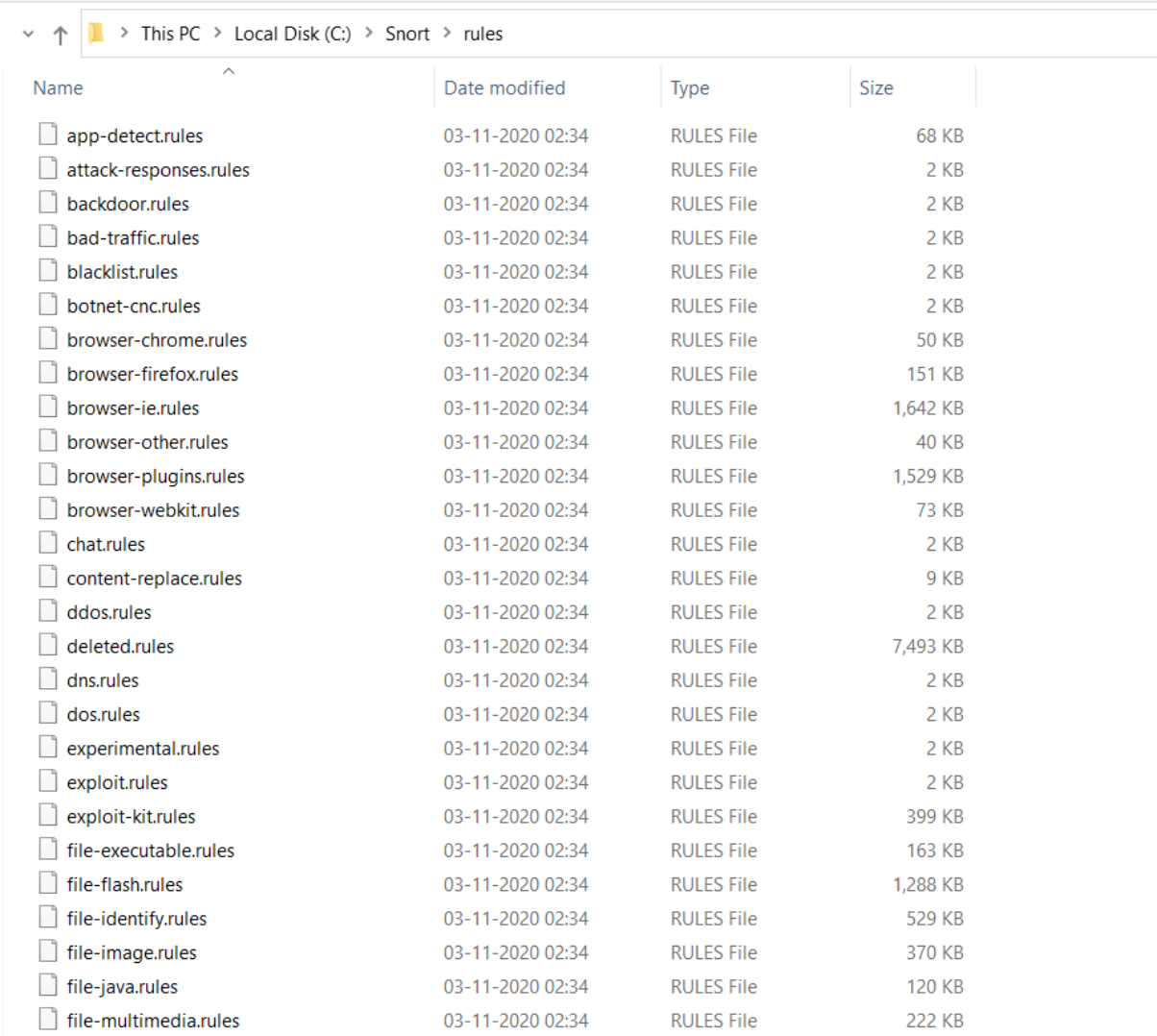


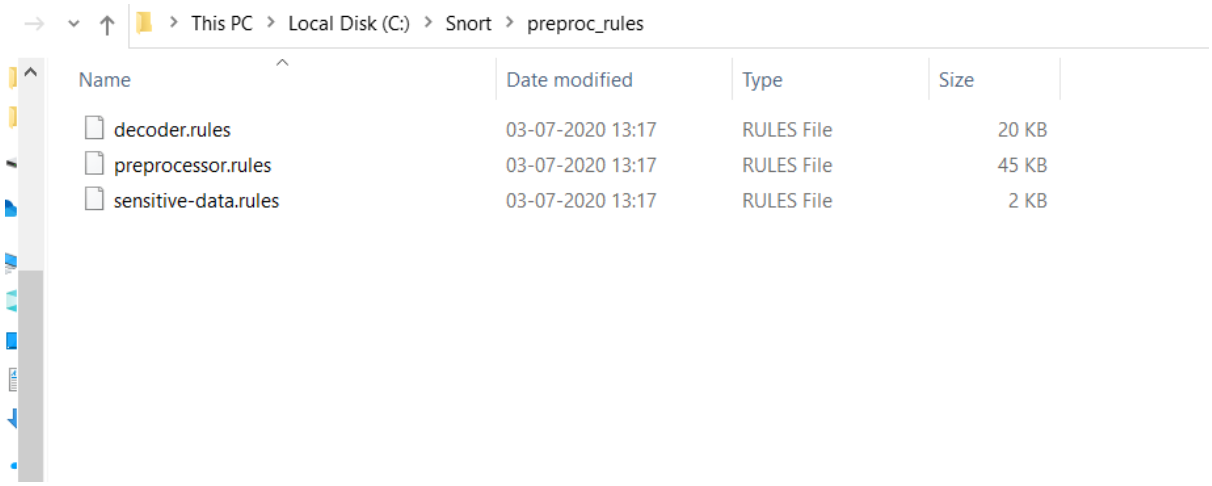



Snort 2.9.16.1 Setup
Choose Install Location
Choose the folder in which to install Snort 2.9.16.1.
Setup will install Snort 2.9.16.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Snort
Browse...
Space required: 7.3MB
Space available: 52.8GB
Nullsoft Install System v2.46
< Back
Next >
Cancel


Snort 2.9.16.1 Setup
Completed
Show details
Nullsoft Install System v2.46
< Back
Close
Cancel

3) Download snort rules:





4) Check snort installation

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16.1-WIN32 GRE (Build 140)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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: 1.2.3


C:\Snort\bin>
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1d3b:6625:c2e2:78a%22
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

```
C:\WINDOWS\system32>cd c:\snort\bin

c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16.1-WIN32 GRE (Build 140)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:69ba:c5a8 \Device\NPF_{0A0B9FCE-C1FE-49C2-B816-04C06A7271AD}  Oracle
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:1d3b:6625 \Device\NPF_{DA7A9A07-22CB-4D9A-A9BA-F5886083E218}  Microsoft
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:8c46:079f \Device\NPF_{A56EB12D-21C0-4739-988A-B493FE0BB0F9}  Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:91c6:101a \Device\NPF_{FF97BBEF-E6B5-417F-86A5-19DFCBEDC843}  Microsoft
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:7c05:ca13 \Device\NPF_{9755E343-B4E8-46D8-83F1-FAB013293E20}  Microsoft Corporation
    6   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:1544:d1ff \Device\NPF_{62273136-FE1D-47CC-82D8-60D8E75F75F9}  Realtek Ethernet Controller

c:\Snort\bin>
```

5) Modify the c:/snort/etc/snort.conf file as required

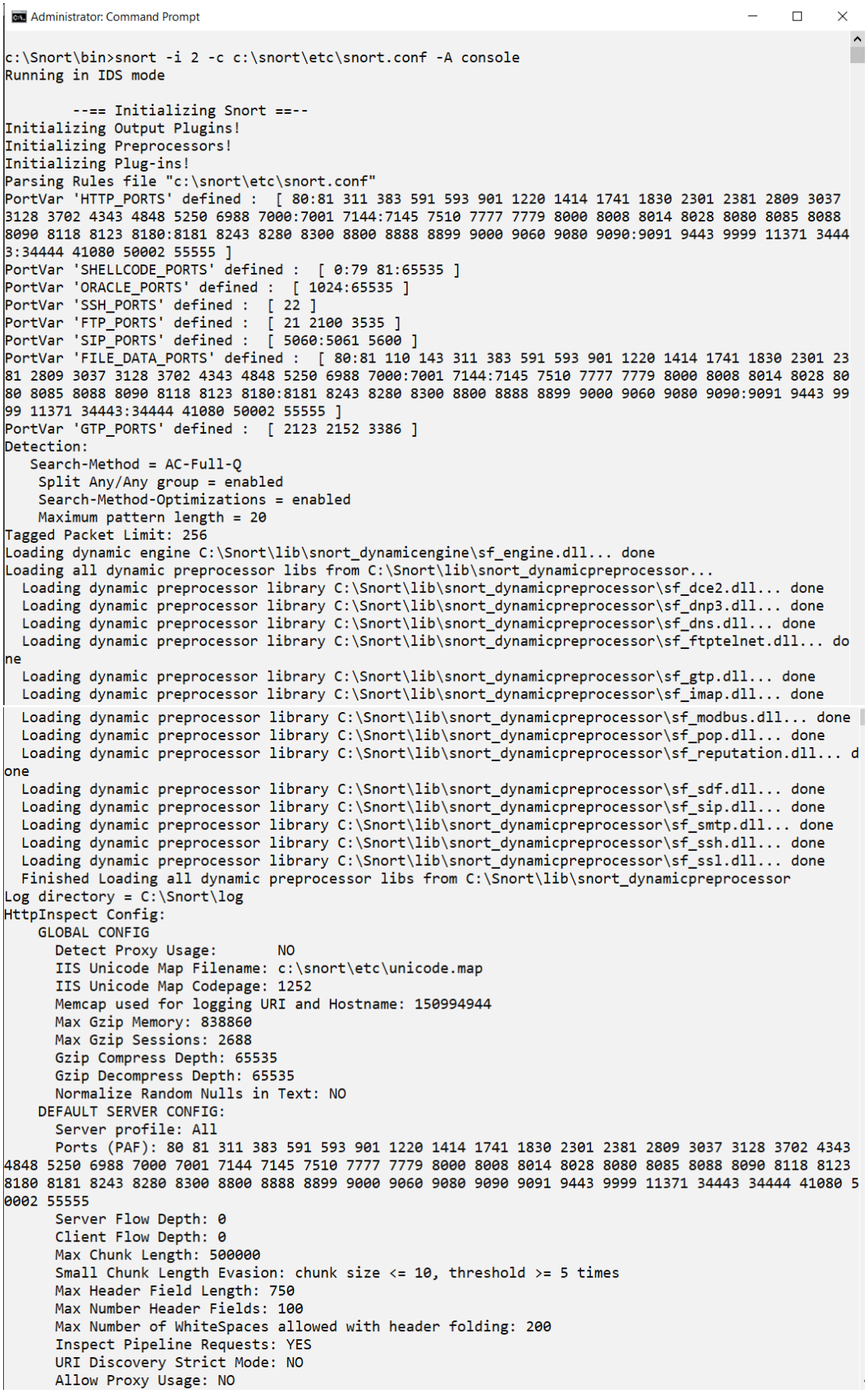
6) Modify the c:/rules/snort/local.rules file to generate alerts

snort.conf | local.rules

C: > Snort > rules > local.rules

```
1   # Copyright 2001-2020 Sourcefire, Inc. All Rights Reserved.
2   #
3   # This file contains (i) proprietary rules that were created, tested and certified by
4   # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5   # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6   # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7   # GNU General Public License (GPL), v2.
8   #
9   # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10  # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11  # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12  # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13  # list of third party owners and their respective copyrights.
14  #
15  # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16  # to the VRT Certified Rules License Agreement (v2.0).
17  #
18  #-------------
19  # LOCAL RULES
20  #-------------
21
22  alert icmp any any -> any any (msg:"ICMP Testing Rule";sid:1000001;rev:1;)
23  alert tcp any any -> any 80 (msg:"TCP Testing Rule";sid:1000002;rev:1;)
24  alert udp any any -> any any (msg:"UDP Testing Rule";sid:1000003;rev:1;)
```

7) Run snort with –A option



```
Administrator: Command Prompt

c:\Snort\bin>snort -i 2 -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 :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088
8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3444
3:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 23
81 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 80
80 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 99
99 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... do
ne
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... d
one
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: c:\snort\etc\unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 838860
      Max Gzip Sessions: 2688
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
      Normalize Random Nulls in Text: NO
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343
4848 5250 6988 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123
8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090 9091 9443 9999 11371 34443 34444 41080 5
0002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
```

Administrator: Command Prompt

```
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Inspect HTTP Cookies: YES
      Inspect HTTP Responses: YES
      Extract Gzip from responses: YES
      Decompress response files:
      Unlimited decompression of gzip data from responses: YES
      Normalize Javascripts in HTTP Responses: YES
      Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP responses: 200
      Normalize HTTP Cookies: NO
      Enable XFF and True Client IP: NO
      Log HTTP URI data: NO
      Log HTTP Hostname data: NO
      Extended ASCII code support in URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: NO
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: NO
      UTF 8: YES alert: NO
      IIS Unicode: YES alert: NO
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: NO
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
      Legacy mode: NO
rpc_decode arguments:
    Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779
    alert_fragments: INACTIVE
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
```

Administrator: Command Prompt

```
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: NO
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAI
L NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK TIME TURN TURNME VERB VRFY X-EXPS XADR
XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EX
CH50
    Ignore Data: No
    Ignore TLS Data: No
    Ignore SMTP Alerts: No
    Max Command Line Length: 512
    Max auth Command Line Length: 1000
    Max Specific Command Line Length:
       ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
       EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
```

```
       ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
       EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
       ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
       IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
       QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
       SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
       TURN:246 TURNME:246 VERB:246 VRFY:255 X-EXPS:246
       XADR:246 XAUTH:246 XCIR:246 XEXCH50:246 XGEN:246
       XLICENSE:246 X-LINK2STATE:246 XQUE:246 XSTA:246 XTRN:246
       XUSR:246
    Max Header Line Length: 1000
    Max Response Line Length: 512
    X-Link2State Alert: Yes
    Drop on X-Link2State Alert: No
    Alert on commands: None
    Alert on unknown commands: No
    SMTP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
    Log Attachment filename: Enabled
    Log MAIL FROM Address: Enabled
    Log RCPT TO Addresses: Enabled
    Log Email Headers: Enabled
    Email Hdrs Log Depth: 1464
SSH config:
    Autodetection: ENABLED
    Challenge-Response Overflow Alert: ENABLED
    SSH1 CRC32 Alert: ENABLED
    Server Version String Overflow Alert: ENABLED
    Protocol Mismatch Alert: ENABLED
    Bad Message Direction Alert: DISABLED
    Bad Payload Size Alert: DISABLED
```

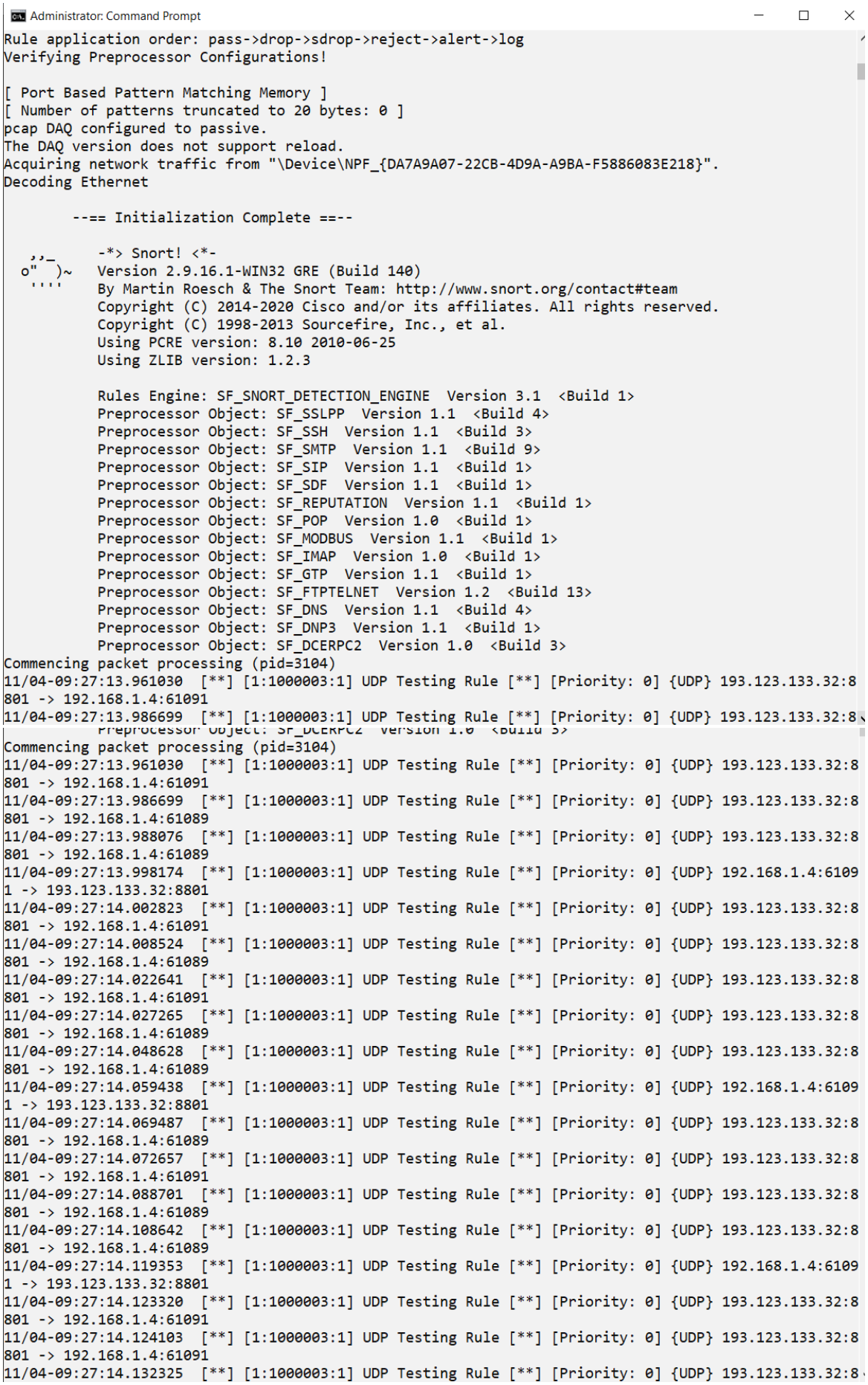
```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
444 Snort rules read
    3 detection rules
    153 decoder rules
    288 preprocessor rules
444 Option Chains linked into 4 Chain Headers
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       1       0       0       0
|     any     441       1       1       0
|      nc     442       1       1       0
|     s+d       0       0       0       0
+-----------------------------------------------------------------------------

+-----------------------[detection-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]---------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[rate-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]------------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[event-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]----------------------------------
+-----------------------[event-filter-local]-----------------------------------
| none
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: pass->drop->sdrop->reject->alert->log
```


Administrator: Command Prompt
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
[Number of patterns truncated to 20 bytes: 0]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{DA7A9A07-22CB-4D9A-A9BA-F5886083E218}".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.16.1-WIN32 GRE (Build 140)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 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: 1.2.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=3104)
11/04-09:27:13.961030 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:13.986699 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
Commencing packet processing (pid=3104)
11/04-09:27:13.961030 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:13.986699 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:13.988076 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:13.998174 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 192.168.1.4:6109
1 -> 193.123.133.32:8801
11/04-09:27:14.002823 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:14.008524 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.022641 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:14.027265 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.048628 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.059438 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 192.168.1.4:6109
1 -> 193.123.133.32:8801
11/04-09:27:14.069487 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.072657 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:14.088701 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.108642 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61089
11/04-09:27:14.119353 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 192.168.1.4:6109
1 -> 193.123.133.32:8801
11/04-09:27:14.123320 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:14.124103 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8
801 -> 192.168.1.4:61091
11/04-09:27:14.132325 [**] [1:1000003:1] UDP Testing Rule [**] [Priority: 0] {UDP} 193.123.133.32:8

```
===============================================================================
Run time for packet processing was 14.430000 seconds
Snort processed 3141 packets.
Snort ran for 0 days 0 hours 0 minutes 14 seconds
   Pkts/sec:          224
===============================================================================
Packet I/O Totals:
   Received:         3508
   Analyzed:         3141 ( 89.538%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:          367 ( 10.462%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         3141 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         3134 ( 99.777%)
       Frag:            0 (  0.000%)
       ICMP:            8 (  0.255%)
        UDP:         2259 ( 71.920%)
        TCP:          867 ( 27.603%)
        IP6:            7 (  0.223%)
    IP6 Ext:            7 (  0.223%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            1 (  0.032%)
       UDP6:            6 (  0.191%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:         3141
===============================================================================
Action Stats:
     Alerts:         2274 ( 72.397%)
     Logged:         2274 ( 72.397%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
```

```
      Alert:            0
Verdicts:
      Allow:         3141 ( 89.538%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
===============================================================================
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                   : 0
  Max concurrent sessions                          : 0
===============================================================================
Snort exiting

c:\Snort\bin>
c:\Snort\bin>
```

```
C:\Users\WELCOME>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=21ms TTL=64
Reply from 192.168.1.1: bytes=32 time=20ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 10ms
```