IT8761 – Security Laboratory

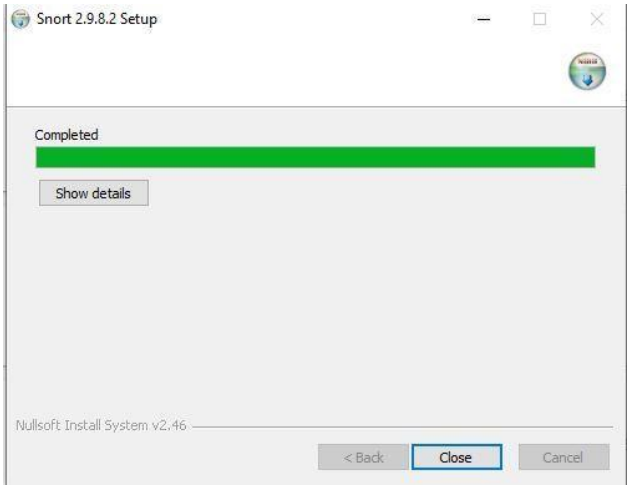
Reshma Ramesh Babu

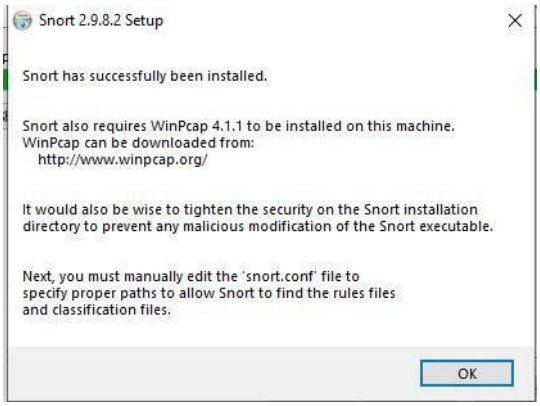
312217104129

Exercise 10

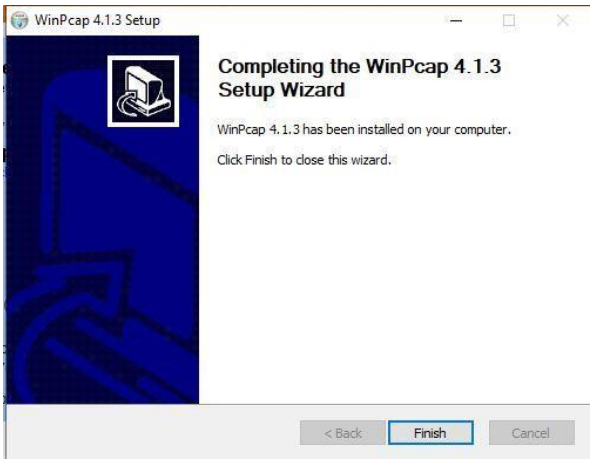
Aim: Intrusion Detection System (ids) using snort

Step 1: Installing Snort 2.9.8.2

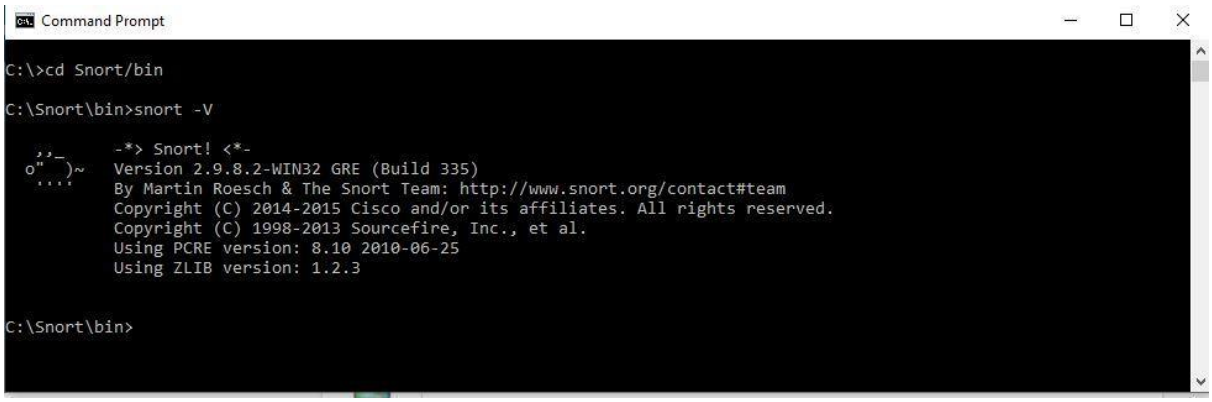




Step 2: Snort requires Wincap to be installed, so install wincap and restart the system



Step 3: Open command prompt and navigate to C:\Snort\bin and run the command: **snort -V** to check if installation was successful



Step 4: Download the snortrules-snapshot-2900.tar.gz file and extract it, replace the rules, preproc_rules folder in C:\Snort with the corresponding folders that were extracted.

Step 5: Open the C:\Snort\etc\snort.conf file and make the following changes in order to configure snort to match your local environment and operational preferences.

Note: Remember to change all '/' to '\' (for Windows)

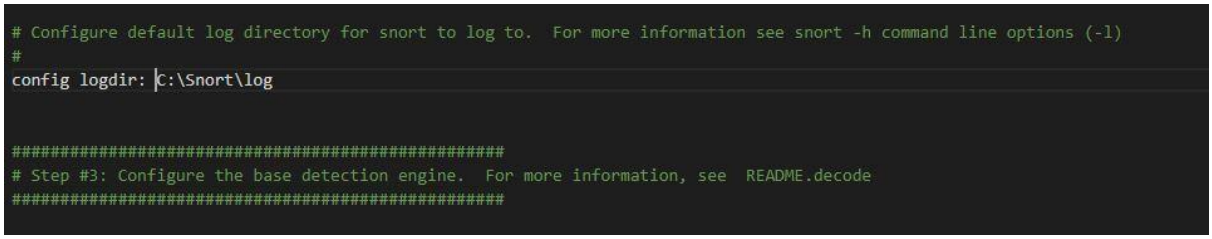
Make HOME_NET reflect the system's ip address and EXTERNAL_NET is any ip that is not HOME_NET

```
##################################################
# Step #1: Set the network variables.  For more information, see README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.113/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

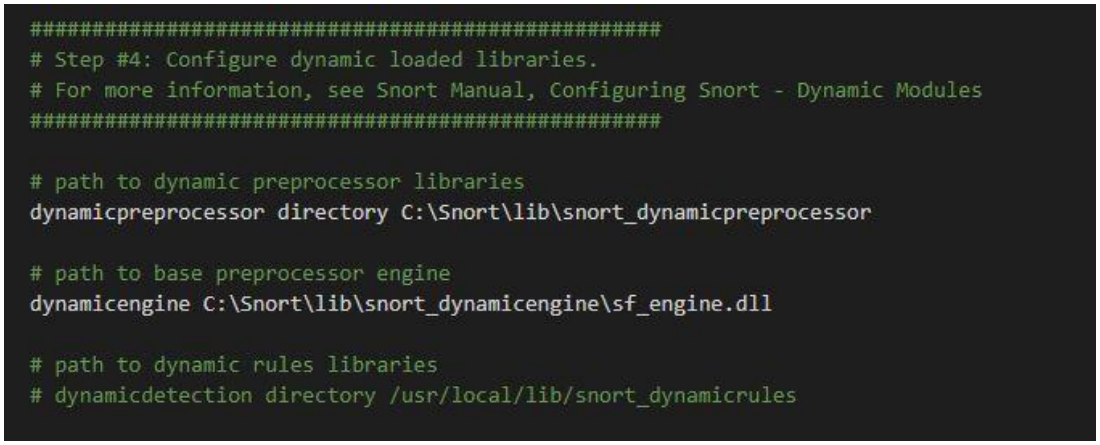
Set appropriate paths

```
101  # Path to your rules files (this can be a relative path)
102  # Note for Windows users:  You are advised to make this an absolute path,
103  # such as:  c:\snort\rules
104  var RULE_PATH C:\Snort\rules
105  var SO_RULE_PATH C:\Snort\so_rules
106  var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108  # If you are using reputation preprocessor set these
109  # Currently there is a bug with relative paths, they are relative to where snort is
110  # not relative to snort.conf like the above variables
111  # This is completely inconsistent with how other vars work, BUG 89986
112  # Set the absolute path appropriately
113  var WHITE_LIST_PATH C:\Snort\rules
114  var BLACK_LIST_PATH C:\Snort\rules
```

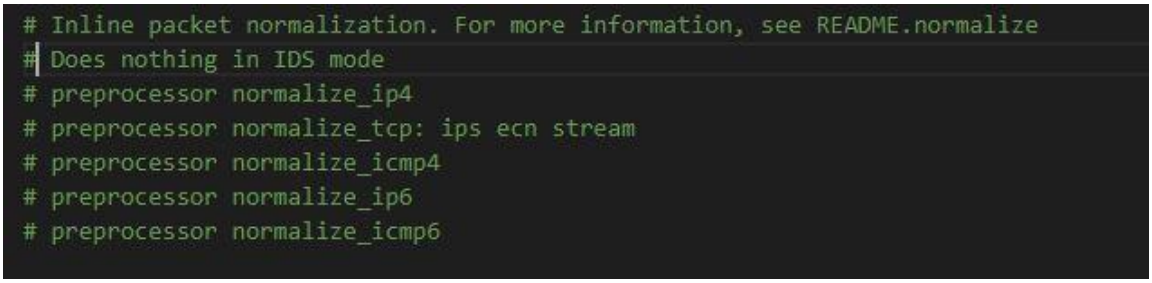
Set log dir path



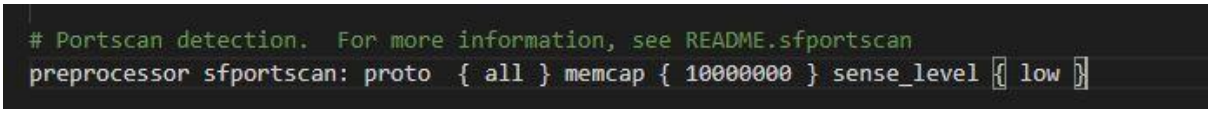
Set appropriate paths



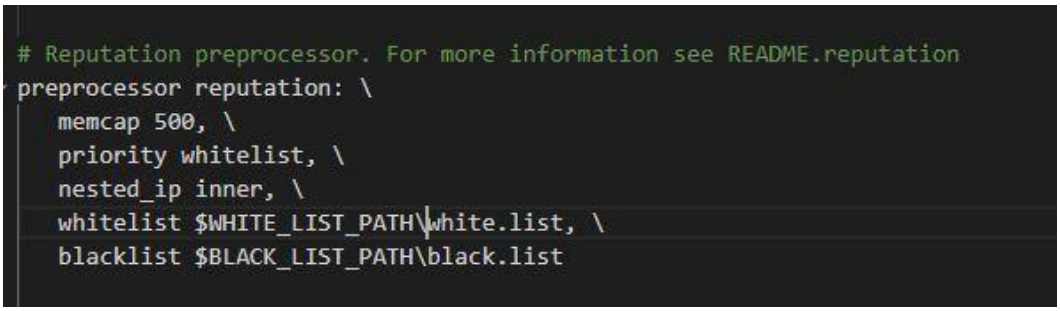
Comment the following lines as we are using only IDS mode on Windows



Enable portscan detection



Set appropriate paths for whitelist and blacklist ip addresses and enable repudiation preprocessor



Include only local.rules, can include others as well.

```
# site specific rules
include $RULE_PATH\local.rules

# include $RULE_PATH/app-detect.rules
# include $RULE_PATH/attack-responses.rules
# include $RULE_PATH/backdoor.rules
# include $RULE_PATH/bad-traffic.rules
# include $RULE_PATH/blacklist.rules
# include $RULE_PATH/botnet-cnc.rules
# include $RULE_PATH/browser-chrome.rules
# include $RULE_PATH/browser-firefox.rules
# include $RULE_PATH/browser-ie.rules
# include $RULE_PATH/browser-other.rules
# include $RULE_PATH/browser-plugins.rules
# include $RULE_PATH/browser-webkit.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/content-replace.rules
# include $RULE_PATH/ddos.rules
# include $RULE_PATH/dns.rules
# include $RULE_PATH/dos.rules
# include $RULE_PATH/experimental.rules
# include $RULE_PATH/exploit-kit.rules
# include $RULE_PATH/exploit.rules
# include $RULE_PATH/file-executable.rules
```

Uncomment pre-processor and decoder alerts and set appropriate paths

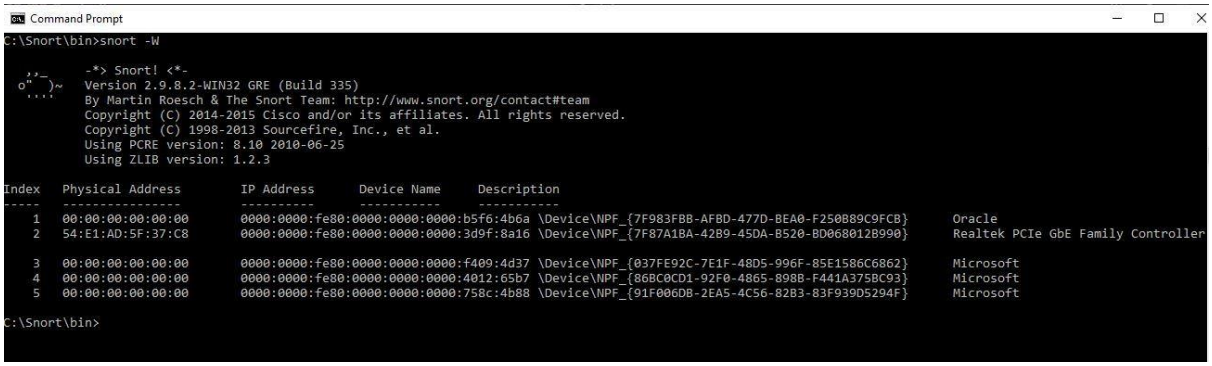
```
##################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
##################################################

# decoder and preprocessor event rules
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
include $PREPROC_RULE_PATH\sensitive-data.rules
```

Step 6: Updating local.rules, this is where we will write our own rules, and create empty files white.list and black.list in C:\Snort\rules.

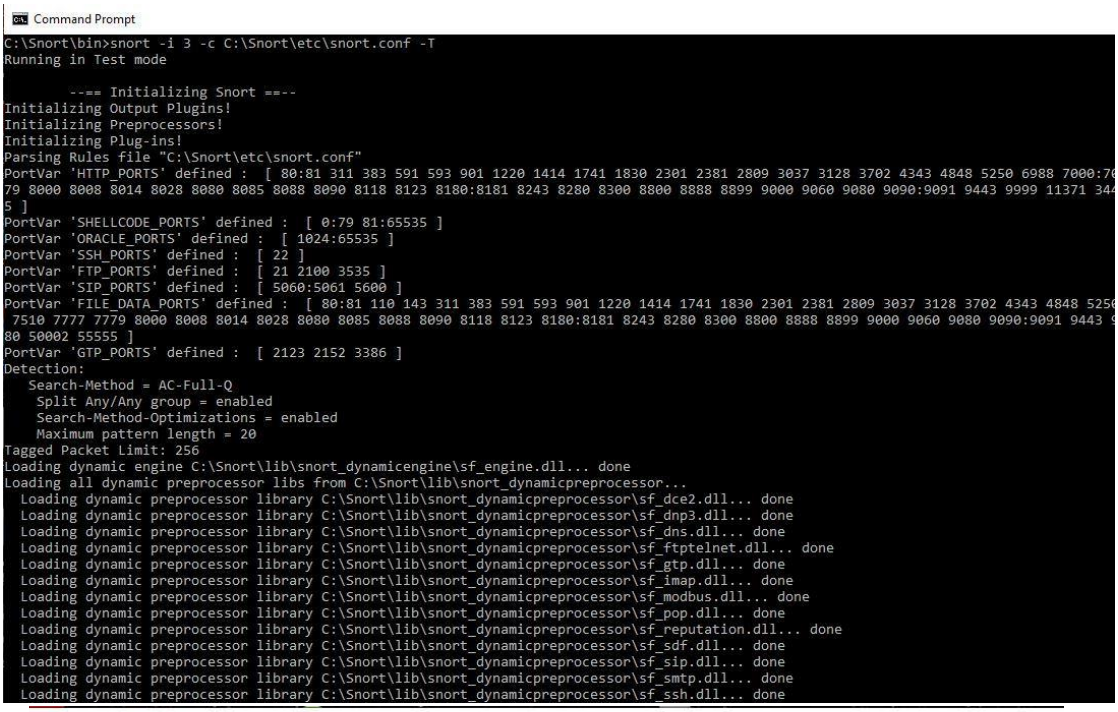
C: > Snort > rules > local.rules

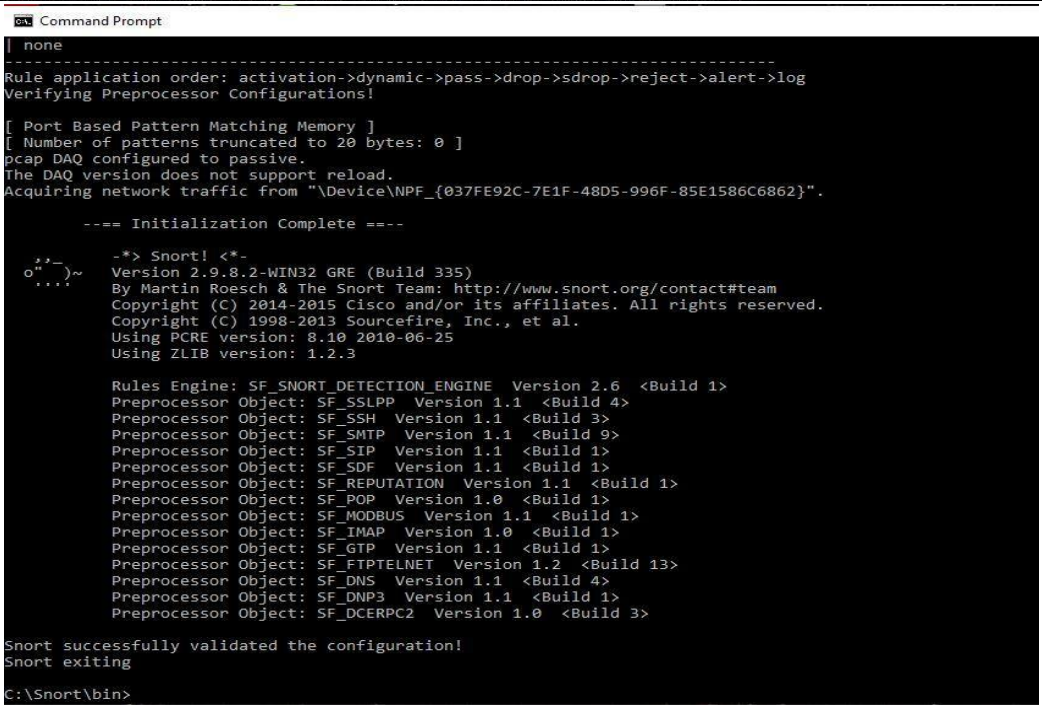
```
1   # $Id: local.rules,v 1.13 2005/02/10 01:11:04 bmc Exp $
2   # ----------------
3   # LOCAL RULES
4   # ----------------
5   # This file intentionally does not come with signatures.  Put your local
6   # additions here.
7
8   alert icmp any any -> any any (msg:"TESTING ICMP alert";sid:10000001;)
9   alert udp any any -> any any (msg:"TESTING UDP alert";sid:10000002;)
10  alert tcp any any -> any any (msg:"TESTING TCP alert";sid:10000003;)
```

Step 7: Check the list available interfaces snort can listen to and choose the appropriate one.



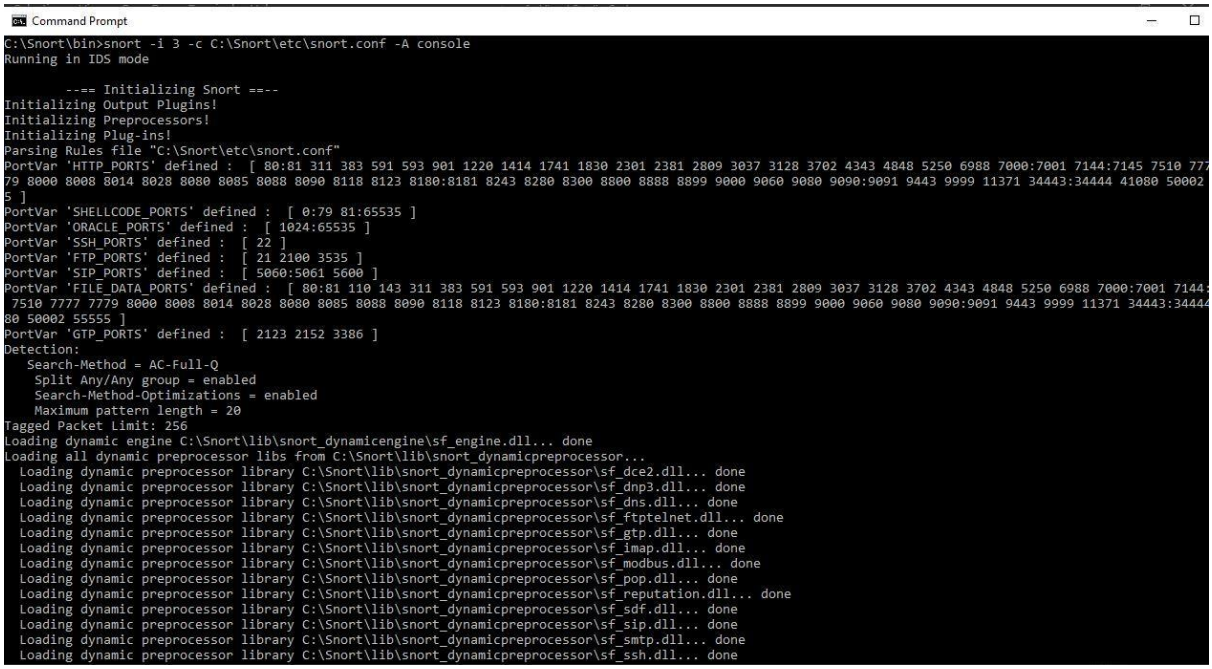
Step 8: Test if the configuration set for snort is valid using the command **snort -i 3 -c C:\Snort\etc\snort.conf -T**



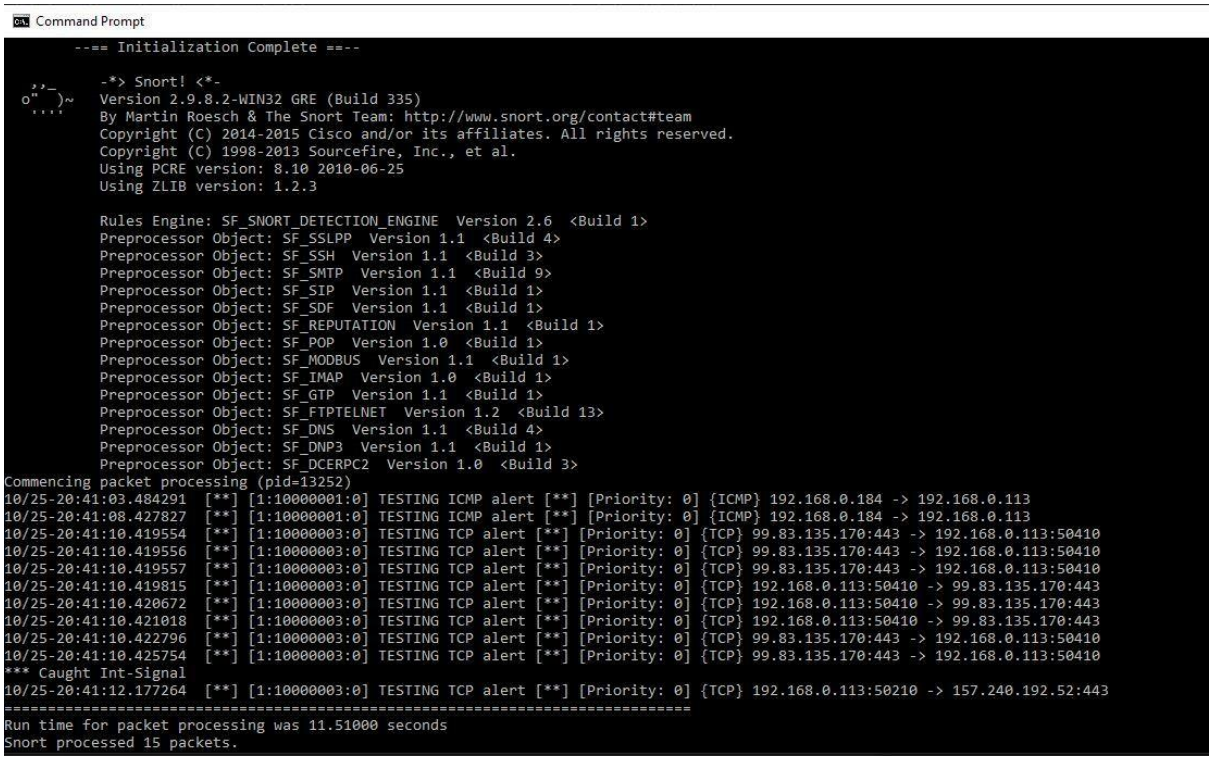


Step 9: Start snort using the command **snort -i 3**

-c C:\Snort\etc\snort.conf -A console


Command Prompt
C:\Snort\bin>snort -i 3 -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 777
79 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 50002
5]
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 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:
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
80 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... done
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... done
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

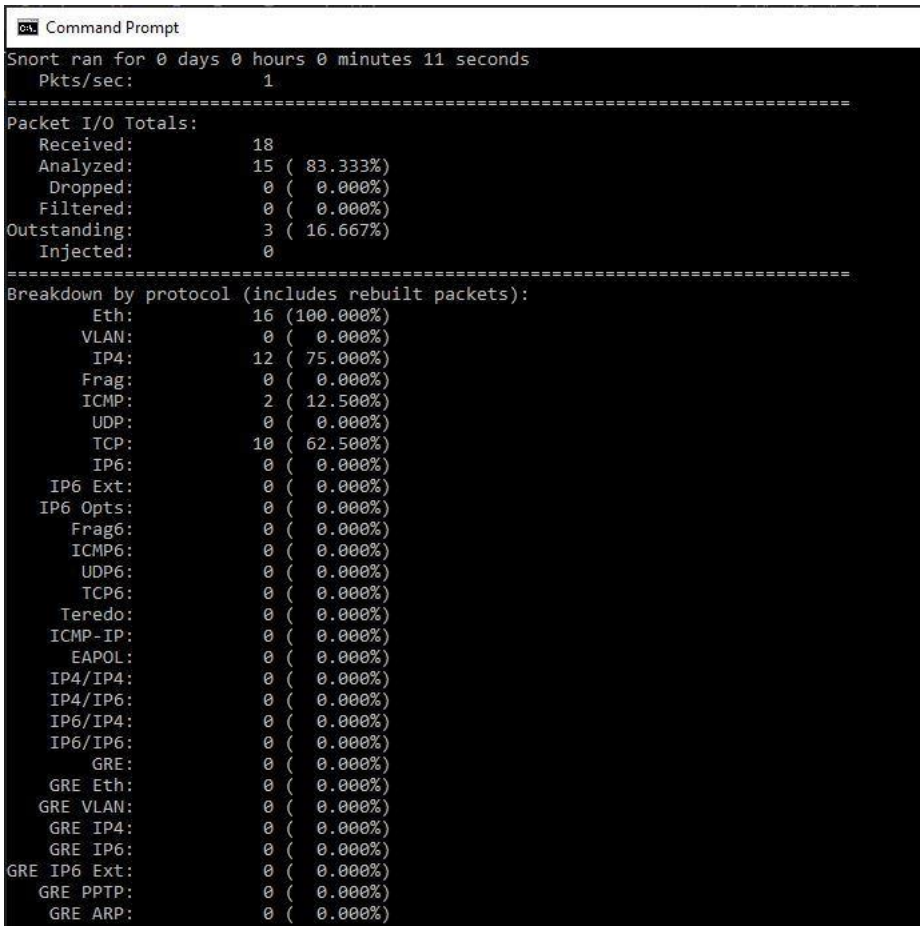
Command Prompt
Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Frag3 engine config:
Bound Address: default
Target-based policy: WINDOWS
Fragment timeout: 180 seconds
Fragment min_ttl: 1
Fragment Anomalies: Alert
Overlap Limit: 10
Min fragment Length: 100
Max Expected Streams: 768
Stream global config:
Track TCP sessions: ACTIVE
Max TCP sessions: 262144
TCP cache pruning timeout: 30 seconds
TCP cache nominal timeout: 3600 seconds
Memcap (for reassembly packet storage): 8388608
Track UDP sessions: ACTIVE
Max UDP sessions: 131072
UDP cache pruning timeout: 30 seconds
UDP cache nominal timeout: 180 seconds
Track ICMP sessions: INACTIVE
Track IP sessions: INACTIVE
Log info if session memory consumption exceeds 1048576
Send up to 2 active responses
Wait at least 5 seconds between responses
Protocol Aware Flushing: ACTIVE
Maximum Flush Point: 16000
Stream TCP Policy config:
Bound Address: default
Reassembly Policy: WINDOWS
Timeout: 180 seconds
Limit on TCP Overlaps: 10
Maximum number of bytes to queue per session: 1048576
Maximum number of segs to queue per session: 2621
Options:
Require 3-Way Handshake: YES

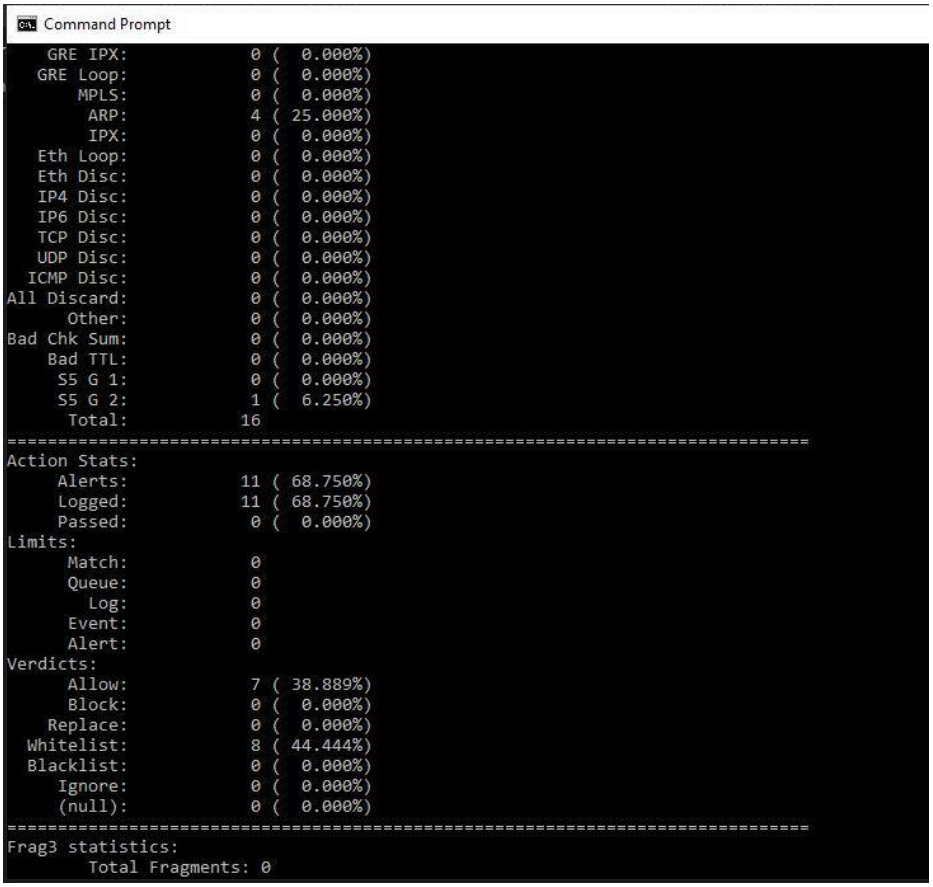


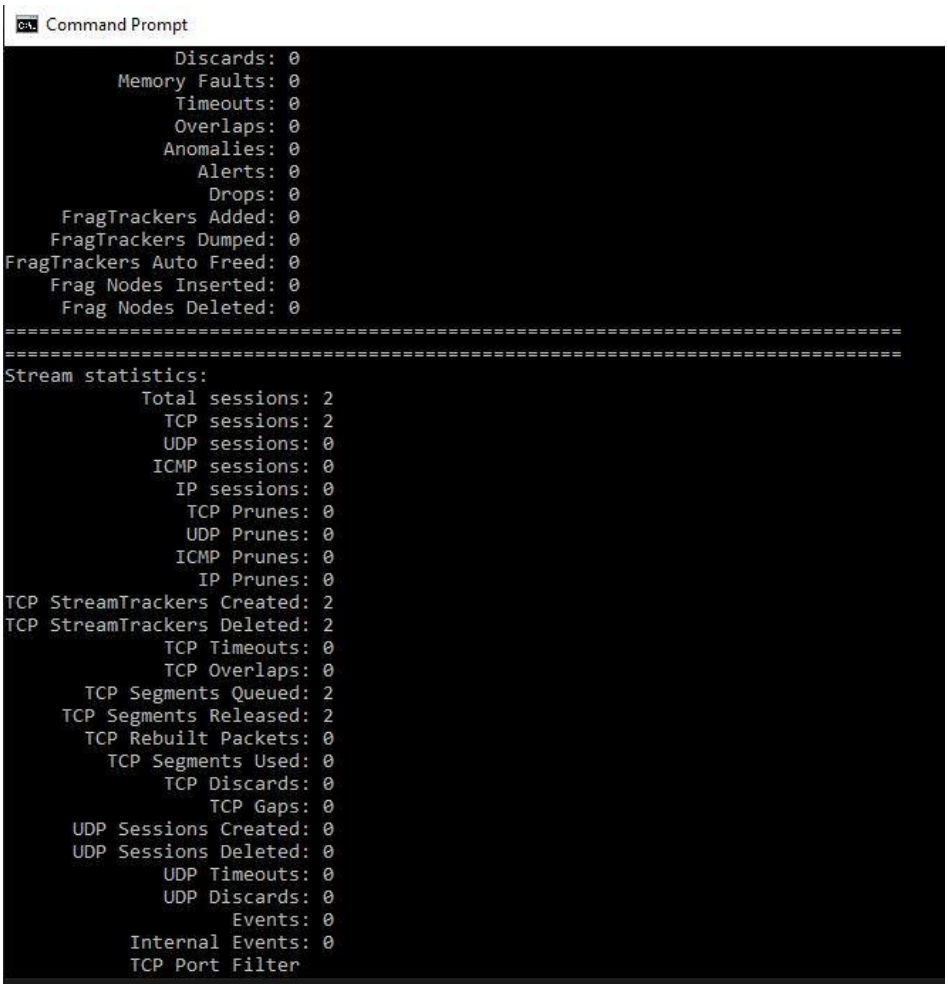
The system with snort was pinged with another system on the same network with an ip address 192.168.0.184 as can be seen from the ICMP alert generated by snort.

To exit snort press **cntl+c**

A summary of all packets processed is presented.




Command Prompt
GRE IPX: 0 (0.000%)
GRE Loop: 0 (0.000%)
MPLS: 0 (0.000%)
ARP: 4 (25.000%)
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: 1 (6.250%)
Total: 16
Action Stats:
Alerts: 11 (68.750%)
Logged: 11 (68.750%)
Passed: 0 (0.000%)
Limits:
Match: 0
Queue: 0
Log: 0
Event: 0
Alert: 0
Verdicts:
Allow: 7 (38.889%)
Block: 0 (0.000%)
Replace: 0 (0.000%)
Whitelist: 8 (44.444%)
Blacklist: 0 (0.000%)
Ignore: 0 (0.000%)
(null): 0 (0.000%)
Frag3 statistics:
Total Fragments: 0


Command Prompt
Discards: 0
Memory Faults: 0
Timeouts: 0
Overlaps: 0
Anomalies: 0
Alerts: 0
Drops: 0
FragTrackers Added: 0
FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
Frag Nodes Inserted: 0
Frag Nodes Deleted: 0
Stream statistics:
Total sessions: 2
TCP sessions: 2
UDP sessions: 0
ICMP sessions: 0
IP sessions: 0
TCP Prunes: 0
UDP Prunes: 0
ICMP Prunes: 0
IP Prunes: 0
TCP StreamTrackers Created: 2
TCP StreamTrackers Deleted: 2
TCP Timeouts: 0
TCP Overlaps: 0
TCP Segments Queued: 2
TCP Segments Released: 2
TCP Rebuilt Packets: 0
TCP Segments Used: 0
TCP Discards: 0
TCP Gaps: 0
UDP Sessions Created: 0
UDP Sessions Deleted: 0
UDP Timeouts: 0
UDP Discards: 0
Events: 0
Internal Events: 0
TCP Port Filter

```
Command Prompt
                Inspected: 0
                  Tracked: 9
          UDP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 0
===============================================================================
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                : 0
  Max concurrent sessions                       : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 2
          Client Hello: 0
          Server Hello: 0
           Certificate: 0
           Server Done: 0
   Client Key Exchange: 0
   Server Key Exchange: 0
         Change Cipher: 0
              Finished: 0
    Client Application: 1
    Server Application: 1
                 Alert: 0
  Unrecognized records: 0
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 1
    Detection disabled: 0
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Reputation Preprocessor Statistics
  Total Memory Allocated: 0
===============================================================================
Snort exiting
```

Step 10: Detecting access by a black listed ip. In the C:\Snort\etc\snort.conf file ensure scan_local is added (since the blacklisted ip will be a local one).

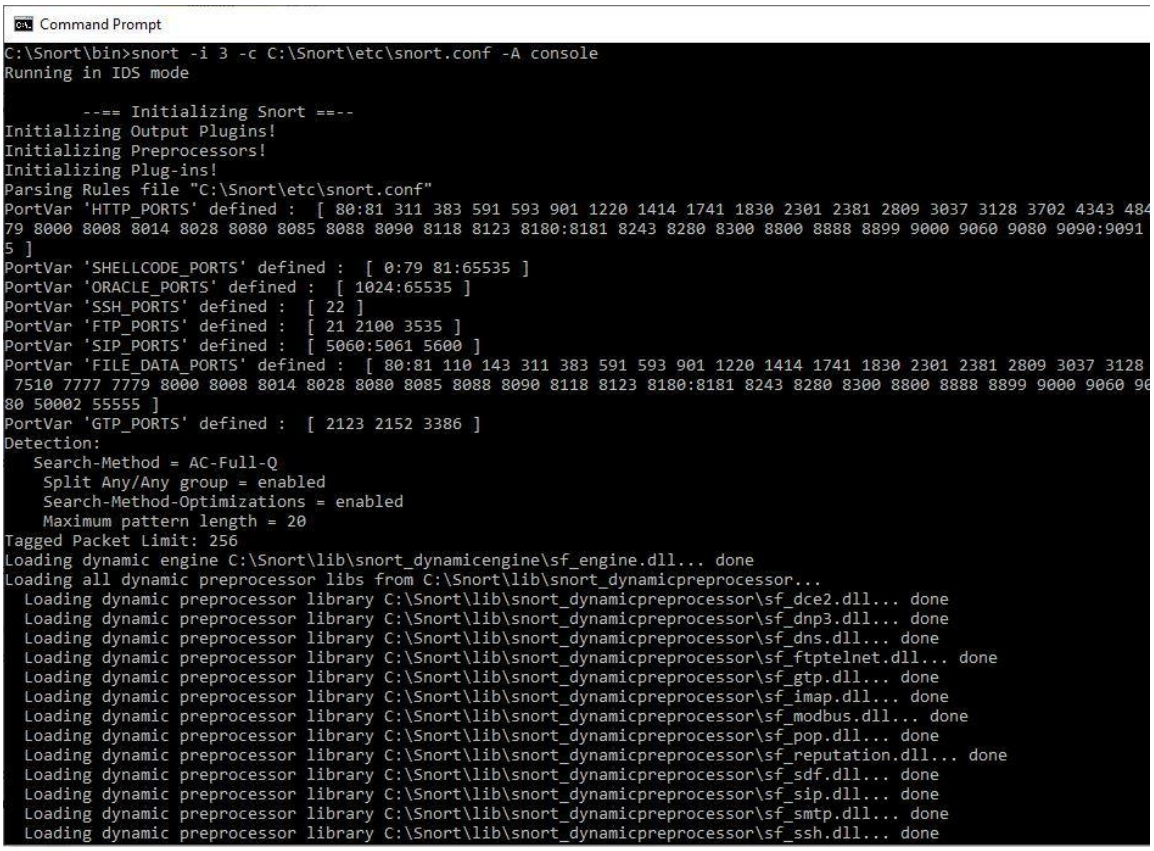
```
# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   scan_local,\
   whitelist $WHITE_LIST_PATH\white.list, \
   blacklist $BLACK_LIST_PATH\black.list
```

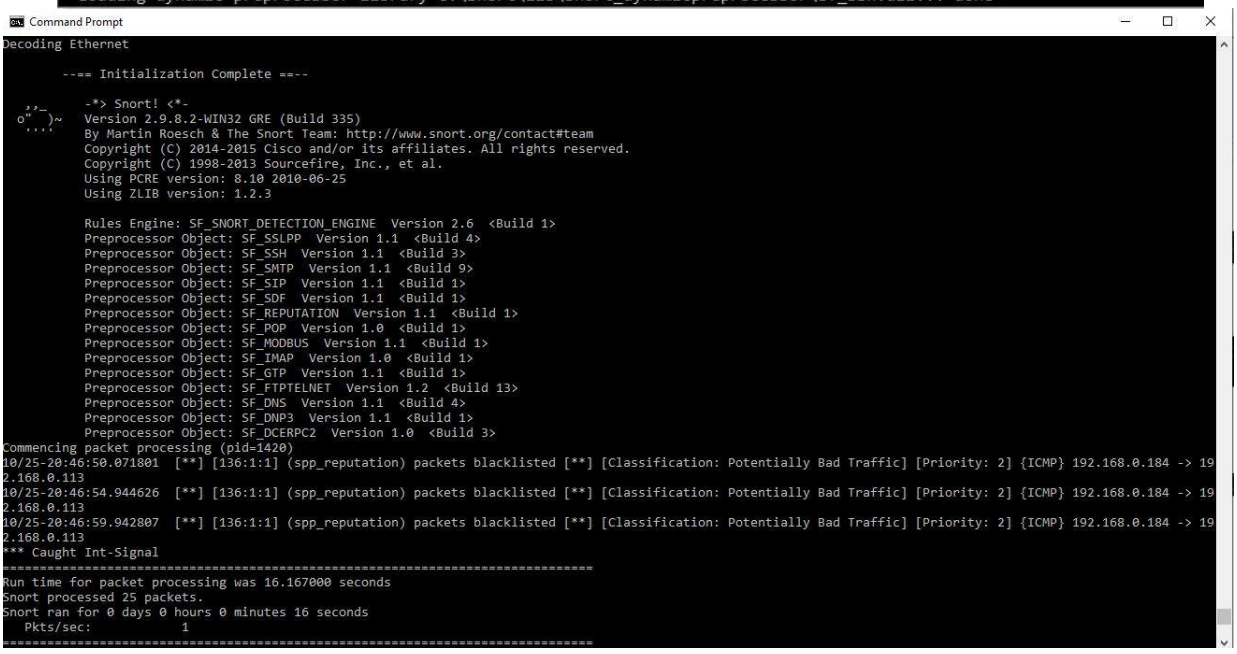
Add the following lines to C:\Snort\rules\black.list file

```
C: > Snort > rules > black.list
1   #Snort Black List file
2   #List of ip address 1 per line
3   192.168.0.184
```

Edit C:\Snort\rules\local.rules to include the following 2 rules.

Run snort using **snort -i 3 -c C:\Snort\etc\snort.conf -A console** command





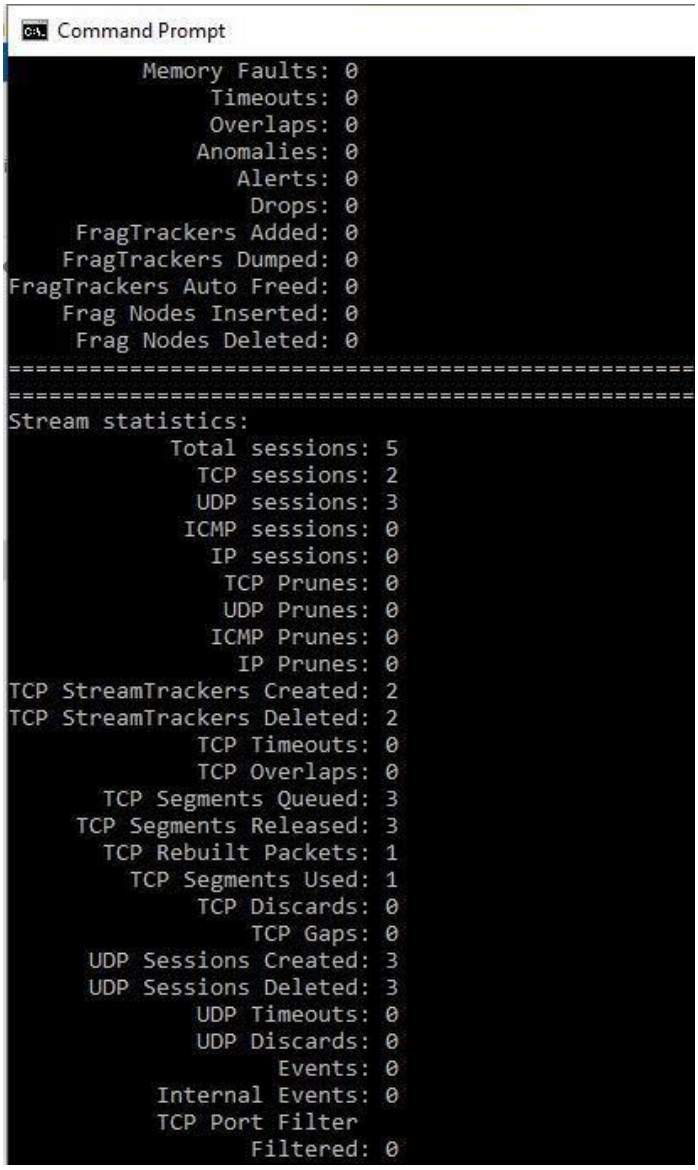
As seen above when the machine was pinged with another on the local network with the blacklisted ip 192.168.0.184 snort raised an alert. Exit by pressing **cntl+c**

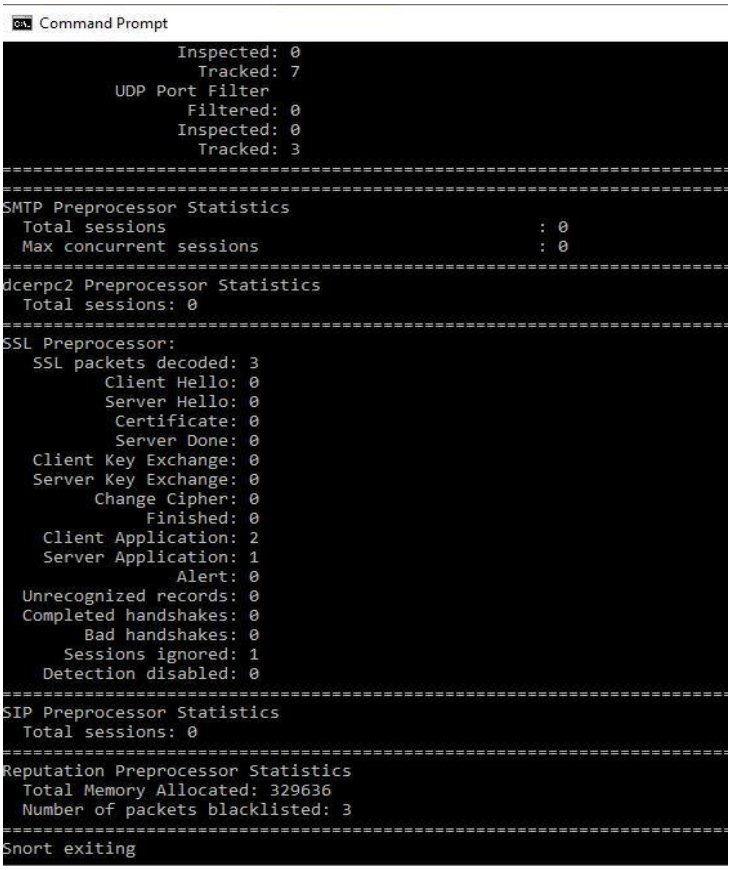
Command Prompt

```
===============================================================
Packet I/O Totals:
   Received:           26
   Analyzed:           25 ( 96.154%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            1 (  3.846%)
   Injected:            0
===============================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           25 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:           19 ( 76.000%)
       Frag:            0 (  0.000%)
       ICMP:            3 ( 12.000%)
        UDP:            9 ( 36.000%)
        TCP:            7 ( 28.000%)
        IP6:            1 (  4.000%)
    IP6 Ext:            1 (  4.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            1 (  4.000%)
       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 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%)
```

Command Prompt

```
       MPLS:            0 (  0.000%)
        ARP:            5 ( 20.000%)
        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:           25
===============================================================
Action Stats:
     Alerts:            3 ( 12.000%)
     Logged:            3 ( 12.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:           23 ( 88.462%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:            2 (  7.692%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
===============================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
                Discards: 0
```


Command Prompt
Memory Faults: 0
Timeouts: 0
Overlaps: 0
Anomalies: 0
Alerts: 0
Drops: 0
FragTrackers Added: 0
FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
Frag Nodes Inserted: 0
Frag Nodes Deleted: 0
Stream statistics:
Total sessions: 5
TCP sessions: 2
UDP sessions: 3
ICMP sessions: 0
IP sessions: 0
TCP Prunes: 0
UDP Prunes: 0
ICMP Prunes: 0
IP Prunes: 0
TCP StreamTrackers Created: 2
TCP StreamTrackers Deleted: 2
TCP Timeouts: 0
TCP Overlaps: 0
TCP Segments Queued: 3
TCP Segments Released: 3
TCP Rebuilt Packets: 1
TCP Segments Used: 1
TCP Discards: 0
TCP Gaps: 0
UDP Sessions Created: 3
UDP Sessions Deleted: 3
UDP Timeouts: 0
UDP Discards: 0
Events: 0
Internal Events: 0
TCP Port Filter
Filtered: 0


Command Prompt
Inspected: 0
Tracked: 7
UDP Port Filter
Filtered: 0
Inspected: 0
Tracked: 3
SMTP Preprocessor Statistics
Total sessions : 0
Max concurrent sessions : 0
dcerpc2 Preprocessor Statistics
Total sessions: 0
SSL Preprocessor:
SSL packets decoded: 3
Client Hello: 0
Server Hello: 0
Certificate: 0
Server Done: 0
Client Key Exchange: 0
Server Key Exchange: 0
Change Cipher: 0
Finished: 0
Client Application: 2
Server Application: 1
Alert: 0
Unrecognized records: 0
Completed handshakes: 0
Bad handshakes: 0
Sessions ignored: 1
Detection disabled: 0
SIP Preprocessor Statistics
Total sessions: 0
Reputation Preprocessor Statistics
Total Memory Allocated: 329636
Number of packets blacklisted: 3
Snort exiting