LAB ASSIGNMENT - 6

Name: Ashwin Balaji
Roll Number: 2020PMD4221
Course: M.Tech (Mobile Computing and Data Analytics)

Title: To work with Snort tool to demonstrate Intrusion Detection System

Software Requirements: Snort IDS 2.9, NpCap 1.31

Theory:

Snort uses a simple, lightweight rules description language that is flexible and quite powerful. There are a number of simple guidelines to remember when developing Snort rules. The first is that Snort rules must be completely contained on a single line, the Snort rule parser doesn't know how to handle rules on multiple lines.

Snort rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information. The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

Rule_actions Protocols Source_address Source_port ***->/<>*** *Destination_address Destination_port* ***(****Rule_actions* ***: " " ;)***

Rule Actions: The rule header contains the information that defines the "who, where, and what" of a packet, as well as what to do in the event that a packet with all the attributes indicated in the rule should show up. The first item in a rule is the rule action. The rule action tells Snort what to do when it finds a packet that matches the rule criteria. There are five available default actions in Snort, alert, log, pass, activate, and dynamic.

- **alert** - generate an alert using the selected alert method, and then log the packet
- **log** - log the packet
- **pass** - ignore the packet
- **activate** - alert and then turn on another dynamic rule
- **dynamic** - remain idle until activated by an activate rule, then act as a log rule
- **drop** - block and log the packet
- **reject** - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
- **sdrop** - block the packet but do not log it.

Protocols: The next field in a rule is the protocol. There are three IP protocols that Snort currently analyzes for suspicious behavior, tcp, udp, and icmp. In the future there may be more, such as ARP, IGRP, GRE, OSPF, RIP, IPX, etc.

- tcp
- udp
- icmp

Direction Operator: The direction operator **"->"** indicates the orientation, or "direction", of the traffic that the rule applies to. The IP address and port numbers on the left side of the direction operator is considered to be the traffic coming from the source host, and the address and port information on the right side of the operator is the destination host. There is also a bidirectional operator, which is indicated with a **"<>"** symbol. This tells Snort to consider the address/port pairs in either the source or destination orientation.

Rule Options: Rule options form the heart of Snort's intrusion detection engine, combining ease of use with power and flexibility. All Snort rule options are separated from each other using the semicolon ";" character. Rule option keywords are separated from their arguments with a colon **":"** character. As of this writing, there are fifteen rule option keywords available for Snort:

- **msg** - prints a message in alerts and packet logs
- **logto** - log the packet to a user specified filename instead of the standard output file
- **ttl** - test the IP header's TTL field value
- **tos** - test the IP header's TOS field value
- **id** - test the IP header's fragment ID field for a specific value
- **ipoption** - watch the IP option fields for specific codes
- **fragbits** - test the fragmentation bits of the IP header
- **dsize** - test the packet's payload size against a value
- **flags** - test the TCP flags for certain values
- **seq** - test the TCP sequence number field for a specific value
- **ack** - test the TCP acknowledgement field for a specific value
- **itype** - test the ICMP type field against a specific value
- **icode** - test the ICMP code field against a specific value
- **icmp_id** - test the ICMP ECHO ID field against a specific value
- **icmp_seq** - test the ICMP ECHO sequence number against a specific value
- **content** - search for a pattern in the packet's payload
- **content-list** - search for a set of patterns in the packet's payload
- **offset** - modifier for the content option, sets the offset to begin attempting a pattern match
- **depth** - modifier for the content option, sets the maximum search depth for a pattern match attempt
- **nocase** - match the preceeding content string with case insensitivity

- **session** - dumps the application layer information for a given session
- **rpc** - watch RPC services for specific application/proceedure calls
- **resp** - active response (knock down connections, etc)
- **react** - active response (block web sites)

Procedure:

1. Download and Install Snort IDS.
   Follow: https://www.youtube.com/watch?v=-AkUidedDlY

```
07/16-14:44:49.585025  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.1:60705 -> 239.255.255.25
0:1900
07/16-14:44:49.686959  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.1:60705 -> 239.255.255.25
0:1900
07/16-14:44:49.790646  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.1:60705 -> 239.255.255.25
0:1900
07/16-14:44:49.892130  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.1:60705 -> 239.255.255.25
0:1900
07/16-14:44:49.994167  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.1:60705 -> 239.255.255.25
0:1900
07/16-14:44:56.242141  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.102:50706 -> 172.217.166.
206:443
07/16-14:44:56.249480  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 172.217.166.206:443 -> 192.168.0.10
2:50706
07/16-14:44:56.275294  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.102:50706 -> 172.217.166.
206:443
07/16-14:44:56.324463  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 172.217.166.206:443 -> 192.168.0.10
2:50706
07/16-14:44:56.324463  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 172.217.166.206:443 -> 192.168.0.10
2:50706
07/16-14:44:56.324829  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.102:50706 -> 172.217.166.
206:443
07/16-14:44:56.350462  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.0.102:50706 -> 172.217.166.
206:443
07/16-14:44:56.353496  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 172.217.166.206:443 -> 192.168.0.10
2:50706
```

```
===============================================================================
Packet I/O Totals:
   Received:       435632
   Analyzed:       432547 ( 99.292%)
    Dropped:         3085 (  0.703%)
   Filtered:            0 (  0.000%)
Outstanding:         3085 (  0.708%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:       432591 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:       431590 ( 99.769%)
       Frag:            0 (  0.000%)
       ICMP:           34 (  0.008%)
        UDP:       300363 ( 69.433%)
        TCP:       124245 ( 28.721%)
        IP6:          364 (  0.084%)
    IP6 Ext:          412 (  0.095%)
   IP6 Opts:           48 (  0.011%)
      Frag6:            0 (  0.000%)
```

```
===============================================================================

Memory Statistics for File at:Fri Jul 16 18:42:33 2021

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
          Total Statistics:
               Memory in use:            280 bytes
                No of allocs:              6
                 No of frees:              1
        Session Statistics:
               Memory in use:              0 bytes
                No of allocs:              1
                 No of frees:              1
        Mempool Statistics:
               Memory in use:            280 bytes
                No of allocs:              5
                 No of frees:              0
===============================================================================
```

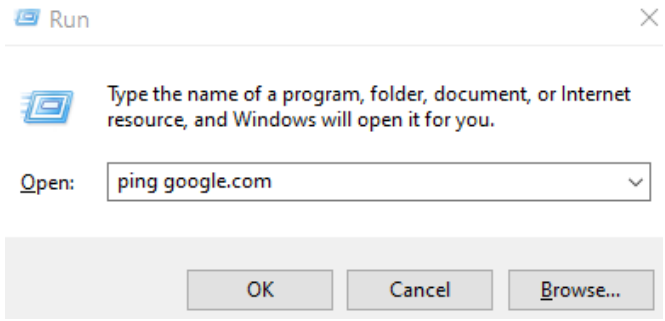
2. Restart the machine after installation.
3. Run **cmd as Administrator**
4. To test packet (i.e., TCP, ICMP, UDP) detection and its flow:
   a) **C:\snort\etc\local.rules** to edit rules
   b) **Defined Rules:**

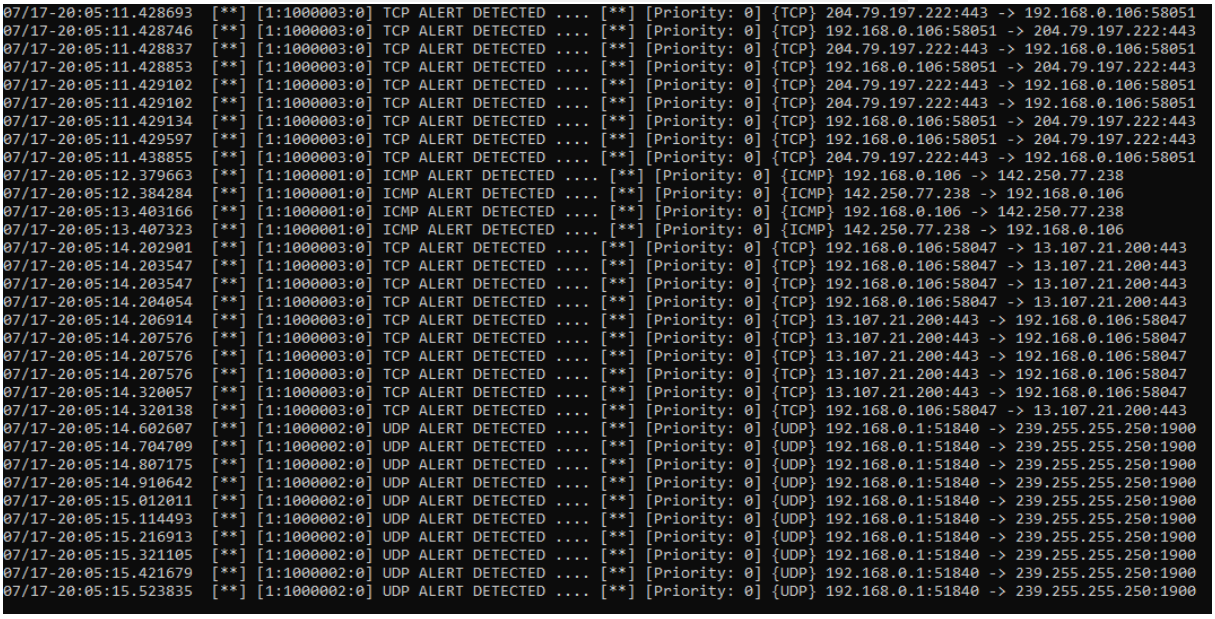
```
alert icmp any any -> any any (msg:"ICMP ALERT DETECTED ...."; sid:1000001;)

alert udp any any -> any any (msg:"UDP ALERT DETECTED ...."; sid:1000002;)

alert tcp any any -> any any (msg:"TCP ALERT DETECTED ...."; sid:1000003;)
```

   c) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**
   d) To test ICMP packet flow, click on **RUN** and enter **ping <website.com>**

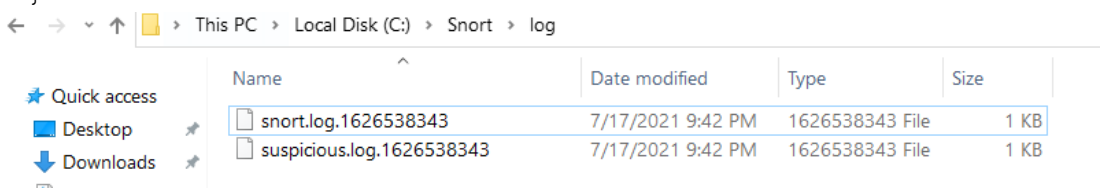




```
07/17-20:05:11.428693  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 204.79.197.222:443 -> 192.168.0.106:58051
07/17-20:05:11.428746  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58051 -> 204.79.197.222:443
07/17-20:05:11.428837  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 204.79.197.222:443 -> 192.168.0.106:58051
07/17-20:05:11.428853  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58051 -> 204.79.197.222:443
07/17-20:05:11.429102  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 204.79.197.222:443 -> 192.168.0.106:58051
07/17-20:05:11.429102  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 204.79.197.222:443 -> 192.168.0.106:58051
07/17-20:05:11.429134  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58051 -> 204.79.197.222:443
07/17-20:05:11.429597  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58051 -> 204.79.197.222:443
07/17-20:05:11.438855  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 204.79.197.222:443 -> 192.168.0.106:58051
07/17-20:05:12.379663  [**] [1:1000001:0] ICMP ALERT DETECTED .... [**] [Priority: 0] {ICMP} 192.168.0.106 -> 142.250.77.238
07/17-20:05:12.384284  [**] [1:1000001:0] ICMP ALERT DETECTED .... [**] [Priority: 0] {ICMP} 142.250.77.238 -> 192.168.0.106
07/17-20:05:13.403166  [**] [1:1000001:0] ICMP ALERT DETECTED .... [**] [Priority: 0] {ICMP} 192.168.0.106 -> 142.250.77.238
07/17-20:05:13.407323  [**] [1:1000001:0] ICMP ALERT DETECTED .... [**] [Priority: 0] {ICMP} 142.250.77.238 -> 192.168.0.106
07/17-20:05:14.202901  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58047 -> 13.107.21.200:443
07/17-20:05:14.203547  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58047 -> 13.107.21.200:443
07/17-20:05:14.203547  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58047 -> 13.107.21.200:443
07/17-20:05:14.204054  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58047 -> 13.107.21.200:443
07/17-20:05:14.206914  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.0.106:58047
07/17-20:05:14.207576  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.0.106:58047
07/17-20:05:14.207576  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.0.106:58047
07/17-20:05:14.207576  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.0.106:58047
07/17-20:05:14.320057  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.0.106:58047
07/17-20:05:14.320138  [**] [1:1000003:0] TCP ALERT DETECTED .... [**] [Priority: 0] {TCP} 192.168.0.106:58047 -> 13.107.21.200:443
07/17-20:05:14.602607  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:14.704709  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:14.807175  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:14.910642  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.012011  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.114493  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.216913  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.321105  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.421679  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
07/17-20:05:15.523835  [**] [1:1000002:0] UDP ALERT DETECTED .... [**] [Priority: 0] {UDP} 192.168.0.1:51840 -> 239.255.255.250:1900
```

5. To **log suspicious traffic in the network.**
   a) **C:\snort\etc\local.rules** to edit rules
   b) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**

```
ruletype suspicious
{
   type log
   output log_tcpdump: suspicious.log
}
  ruletype codered
  {
        type alert
        output alert_syslog: LOG_AUTH LOG_ALERT
        output log_tcpdump: suspicious.log
  }
```



6. To **log/alert certain suspicious/restricted keyword request from the browser.**
   a) Alert protocol request with the request content and the message to be logged.
   b) **C:\snort\etc\local.rules** to edit rules

```
alert tcp any any -> any any (content:"instagram"; msg:"Alert ... Social Network ping addresses"; sid:1000004; rev:1;)

alert tcp any any -> any any (content:"malware"; msg:"Alert... Suspicious Keyword request !!!"; sid:1000005; rev:1;)
```

   c) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**
   d) Run the rules tagged content in the browser to test IDS.

```
Commencing packet processing (pid=3040)
07/17-23:25:21.399686  [**] [1:1000004:1] Alert ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:60916 -> 157.240.198.17:443
07/17-23:25:22.059177  [**] [1:1000004:1] Alert ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:64044 -> 157.240.198.10:443
07/17-23:28:48.062335  [**] [1:1000005:1] Alert... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:53812 -> 13.35.190.75:443
07/17-23:28:51.256195  [**] [1:1000005:1] Alert... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:53850 -> 18.205.201.184:443
07/17-23:28:51.477766  [**] [1:1000005:1] Alert... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:51231 -> 18.205.201.184:443
07/17-23:28:51.486890  [**] [1:1000005:1] Alert... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 18.205.201.184:443 -> 192.168.0.106:53850
07/17-23:28:51.711475  [**] [1:1000005:1] Alert... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 18.205.201.184:443 -> 192.168.0.106:51231
```

   e) Snort successfully detected the keyword entered, showing the **date, time, message, alert priority, source->destination address**.

7. To **reject certain suspicious/restricted keyword response/request to/from the browser**.
   a) **C:\snort\etc\local.rules** to edit rules

```
reject tcp any any <> any any (content:"TCP instagram"; msg:"Alert ... Social Network ping addresses"; sid:1000004; rev:1;)

reject tcp any any <> any any (content:"TCP malware"; msg:"Alert... Suspicious Keyword request !!!"; sid:1000005; rev:1;)

reject udp any any <> any any (content:"instagram"; msg:"UDP Rejected Request ... Social Network ping addresses"; sid:1000006; rev:1;)
```

b) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**

c) Run the rules tagged content in the browser to test IDS.

```
Commencing packet processing (pid=3784)
07/17-23:55:56.240964  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:54812 -> 157.240.198.35:443
07/17-23:55:56.334796  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:57170 -> 157.240.198.35:443
07/17-23:55:59.883142  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:60283 -> 192.168.0.1:53
07/17-23:55:59.884703  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:60283
07/17-23:55:59.889196  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:55223 -> 157.240.198.17:443
07/17-23:56:00.681825  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:56252 -> 192.168.0.1:53
07/17-23:56:00.683501  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:56252
07/17-23:56:00.689583  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:59047 -> 157.240.198.10:443
07/17-23:56:00.972647  [**] [1:1000006:1] TCP Rejected Request... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:61197 -> 13.35.190.75:443
07/17-23:56:03.160907  [**] [1:1000006:1] TCP Rejected Request... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:54711 -> 18.205.201.184:443
07/17-23:56:03.429248  [**] [1:1000006:1] TCP Rejected Request... Suspicious Keyword request !!! [**] [Priority: 0] {TCP} 192.168.0.106:61457 -> 18.205.201.184:443
07/17-23:56:26.683184  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:64290 -> 192.168.0.1:53
07/17-23:56:26.685717  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:64290
07/17-23:56:28.942639  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:52353 -> 157.240.198.17:443
07/17-23:56:29.672994  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:61282 -> 157.240.198.10:443
07/17-23:56:51.166799  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:51939 -> 157.240.198.17:443
07/17-23:56:51.882164  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:53171 -> 157.240.198.10:443
07/17-23:56:55.885222  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:52738 -> 157.240.198.17:443
07/17-23:56:56.643284  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:51998 -> 157.240.198.10:443
07/17-23:57:38.982436  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:63554 -> 192.168.0.1:53
07/17-23:57:38.985816  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:63554
07/17-23:57:41.665587  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:59108 -> 192.168.0.1:53
07/17-23:57:41.668913  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:59108
07/17-23:57:41.676162  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:54370 -> 157.240.198.17:443
07/17-23:57:42.257621  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.106:53112 -> 192.168.0.1:53
07/17-23:57:42.259244  [**] [1:1000005:1] UDP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {UDP} 192.168.0.1:53 -> 192.168.0.106:53112
07/17-23:57:42.263579  [**] [1:1000004:1] TCP Rejected Request ... Social Network ping addresses [**] [Priority: 0] {TCP} 192.168.0.106:63001 -> 157.240.198.10:443
```

8. To **pass certain suspicious/restricted keyword response/request to/from the browser.**

a) **C:\snort\etc\local.rules** to edit rules

```
pass tcp any any <> any any (content:"TCP instagram"; msg:"Alert ... Social Network ping addresses"; sid:1000004; rev:1;)

pass tcp any any <> any any (content:"TCP malware"; msg:"Alert... Suspicious Keyword request !!!"; sid:1000005; rev:1;)

pass udp any any <> any any (content:"instagram"; msg:"UDP Pass Request ... Social Network ping addresses"; sid:1000006; rev:1;)
```

b) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**

c) Run the rules tagged content in the browser to test IDS.\
d) No request/response can be seen recorded in the cmd as those requests/response has been ignored by the IDS

```
Commencing packet processing (pid=12272)
```

9. To **drop/sdrop certain suspicious/restricted keyword response/request to/from the browser.**
   e) **C:\snort\etc\local.rules** to edit rules

   Note: Change drop to sdrop to check for results

```
drop tcp any any <> any any (content:"TCP instagram"; msg:"Drop/SDrop ... Social Network ping addresses"; sid:1000004; rev:1;)

drop tcp any any <> any any (content:"TCP malware"; msg:"Drop/SDrop... Suspicious Keyword request !!!"; sid:1000005; rev:1;)

drop udp any any <> any any (content:"instagram"; msg:"UDP Drop/SDrop... Social Network ping addresses"; sid:1000006; rev:1;)
```

   f) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**
   g) Run the rules tagged content in the browser to test IDS.
   h) No request/response can be seen recorded in the cmd as those requests/response has been ignored by the IDS but the log has been recorded (in the case of drop, but not recorded in the case of sdrop)

```
Commencing packet processing (pid=12272)
```

snort.log.1626549389	7/18/2021 12:46 A...	1626549389 File	1 KB

10. To **log certain suspicious/restricted keyword response/request to/from the browser.**
    a) **C:\snort\etc\local.rules** to edit rules

```
log tcp any any <> any any (content:"instagram"; msg:"TCP Log Request ... Social Network ping addresses"; sid:1000004; rev:1;)
```

```
log udp any any <> any any (content:"instagram"; msg:"UDP Log Request ... Social Network ping addresses"; sid:1000005; rev:1;)

log tcp any any <> any any (content:"malware"; msg:"TCP Log Request... Suspicious Keyword request !!!"; sid:1000006; rev:1;)
```

b) Run **C:\snort\bin\snort -i 5 -c C:\Snort\etc\snort.conf -A console**

c) Run the rules tagged content in the browser to test IDS.

d) No request/response can be seen recorded in the cmd, as those requests/response has been ignored by the IDS but the log has been recorded.

snort.log.1626549948	7/18/2021 1:02 AM	1626549948 File	8 KB

11. Flags in Snort.

```
alert tcp any any <> any any (flags: AP; msg: "Possible ACK PUSH scan"; sid: 1000045;)

alert tcp any any <> any any (flags: AU; msg: "Possible ACK URG scan"; sid: 1000046;)

alert tcp any any <> any any (flags: AR; msg: "Possible ACK RST scan"; sid: 1000047;)

alert tcp any any <> any any (flags: AS; msg: "Possible ACK SYN scan"; sid: 1000048;)

alert tcp any any <> any any (flags: AF; msg: "Possible ACK FIN scan"; Priority: 1; sid: 1000049;)
```

```
07/18-01:18:48.343837  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.17:443 -> 192.168.0.106:63000
07/18-01:18:49.080181  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:61058 -> 157.240.198.10:443
07/18-01:18:49.381500  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 99.86.46.98:443 -> 192.168.0.106:55373
07/18-01:18:49.383014  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 99.86.46.98:443 -> 192.168.0.106:55373
07/18-01:18:49.383014  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.10:443 -> 192.168.0.106:61058
07/18-01:18:49.383436  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 99.86.46.98:443 -> 192.168.0.106:55373
07/18-01:18:49.396988  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.10:443 -> 192.168.0.106:61058
07/18-01:18:52.471887  [**] [1:1000048:0] Possible ACK SYN scan [**] [Priority: 0] {TCP} 137.116.139.120:443 -> 192.168.0.106:60905
07/18-01:18:52.474685  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:60905 -> 137.116.139.120:443
```

```
07/18-01:19:25.823597  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 3.82.237.115:443 -> 192.168.0.106:59659
07/18-01:19:25.824833  [**] [1:1000047:0] Possible ACK RST scan [**] [Priority: 0] {TCP} 192.168.0.106:59659 -> 3.82.237.115:443
07/18-01:19:27.075267  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:58158 -> 157.240.198.10:443
07/18-01:19:27.304684  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.10:443 -> 192.168.0.106:58158
07/18-01:19:29.610779  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 192.168.0.106:55373 -> 99.86.46.98:443
07/18-01:19:30.599231  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.3.29:443 -> 192.168.0.106:61605
07/18-01:19:30.599231  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 157.240.3.29:443 -> 192.168.0.106:61605
07/18-01:19:31.481542  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:63000 -> 157.240.198.17:443
07/18-01:19:31.762922  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.17:443 -> 192.168.0.106:63000
07/18-01:19:31.833364  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:61058 -> 157.240.198.10:443
07/18-01:19:32.056533  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.10:443 -> 192.168.0.106:61058
07/18-01:19:32.194248  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.3.29:443 -> 192.168.0.106:52924
07/18-01:19:32.194632  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 192.168.0.106:52924 -> 157.240.3.29:443
07/18-01:19:32.195809  [**] [1:1000049:0] Possible ACK FIN scan [**] [Priority: 0] {TCP} 157.240.3.29:443 -> 192.168.0.106:52924
07/18-01:19:38.078594  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 192.168.0.106:58158 -> 157.240.198.10:443
07/18-01:19:38.315578  [**] [1:1000045:0] Possible ACK PUSH scan [**] [Priority: 0] {TCP} 157.240.198.10:443 -> 192.168.0.106:58158
07/18-01:18:19.282583  [**] [1:1000047:0] Possible ACK RST scan [**] [Priority: 0] {TCP} 192.168.0.106:55373 -> 99.86.46.98:443
07/18-01:19:39.211873  [**] [1:1000047:0] Possible ACK RST scan [**] [Priority: 0] {TCP} 192.168.0.106:55373 -> 99.86.46.98:443
```

Help Links:

1. https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm

2. https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210717%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210717T192334Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=ed8992eaa13ae7a9ef9e139863b12cf62aab017550fbb16a90b30104598985a1

3. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node29.html#SECTION00424000000000000000