Snort Rule Development

A Snort rule, at its core, is a powerful tool that we use to identify and flag potential malicious activity in network traffic.

As already discussed, Snort rules resemble Suricata rules. They are composed of a `rule header` and `rule options`. Even though Snort rules share similarities with Suricata rules, we strongly suggest studying Snort rule writing from the following resources: https://docs.snort.org/, https://docs.suricata.io/en/latest/rules/differences-from-snort.html.

> Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, let's SSH into the Target IP using the provided credentials. The vast majority of the commands covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

Let's move forward and explore some examples of crafting Snort rules to counter real-world malware threats.

Snort Rule Development Example 1: Detecting Ursnif (Inefficiently)

Snort Rule Development

```
alert tcp any any -> any any (msg:"Possible Ursnif C2 Activity"; flow:established,to_server; conten
```

The Snort rule above is designed to detect certain variations of Ursnif malware. The rule is inefficient since it misses HTTP sticky buffers. Let's break down the important parts of this rule to understand its workings.

- `flow:established,to_server;` ensures that this rule only matches established TCP connections where data is flowing from the client to the server.
- `content:"/images/", depth 12;` instructs Snort to look for the string `/images/` within the first `12` bytes of the packet payload.
- `content:"_2F";` and `content:"_2B";` direct Snort to search for the strings `_2F` and `_2B` anywhere in the payload.
- `content:"User-Agent|3a 20|Mozilla/4.0 (compatible|3b| MSIE 8.0|3b| Windows NT";` is looking for a specific `User-Agent`. The `|3a 20|` and `|3b|` in the rule are hexadecimal representations of the `:` and `;` characters respectively.
- `content:!"Accept"; content:!"Cookie|3a|"; content:!"Referer|3a|";` look for the absence of certain standard HTTP headers, such as `Accept`, `Cookie:` and `Referer:`. The `!` indicates negation.

The above rule is already incorporated in the `local.rules` file found in the `/home/htb-student` directory of this section's target. To test it, first, you need to uncomment the rule. Then, execute Snort on the `ursnif.pcap` file, which is located in the `/home/htb-student/pcaps` directory.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ sudo snort -c /root/snorty/etc/snort/snort.lua --daq-dir /usr/local/lib/daq
--------------------------------------------------
o")~   Snort++ 3.1.64.0
--------------------------------------------------
Loading /root/snorty/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        hosts
---SNIP---
```

? Go to Questions

Table of Contents

Introduction To IDS/IPS

Suricata

Suricata Fundamentals

Suricata Rule Development Part 1

Suricata Rule Development Part 2 (Encrypted Traffic)

Snort

Snort Fundamentals

Snort Rule Development

Zeek

Zeek Fundamentals

Intrusion Detection With Zeek

Skills Assessment

Skills Assessment - Suricata

Skills Assessment - Snort

Skills Assessment - Zeek

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

```
        host_tracker
Finished /root/snorty/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Loading rule args:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Finished rule args:
-------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     210       2     210    /root/snorty/etc/snort/snort.lua
-------------------------------------------------
rule counts
       total rules loaded: 210
          duplicate rules: 2
               text rules: 210
             option chains: 210
             chain headers: 5
-------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       1       0       1       0
   total       1       0       1       0
-------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      208     208
                    total:      208     208
-------------------------------------------------
fast pattern groups
                     any: 2
               to_server: 1
               to_client: 1
-------------------------------------------------
search engine (ac_bnfa)
                instances: 3
                 patterns: 417
             pattern chars: 2566
                num states: 1836
         num match states: 371
             memory scale: KB
             total memory: 70.9639
           pattern memory: 18.792
        match list memory: 27.8125
        transition memory: 23.9844
appid: MaxRss diff: 3024
appid: patterns loaded: 300
-------------------------------------------------
pcap DAQ configured to read-file.
Commencing packet processing
++ [0] /home/htb-student/pcaps/ursnif.pcap
07/21-19:27:47.161230 [**] [1:1000002:1] "Possible Ursnif C2 Activity" [**] [Priority: 0] {TCP} 10.
00:1F:E2:10:8B:C9 -> 00:0C:29:C9:67:00 type:0x800 len:0x18C
10.10.10.104:49191 -> 192.42.116.41:80 TCP TTL:128 TOS:0x0 ID:20640 IpLen:20 DgmLen:382 DF
***AP*** Seq: 0x12E06BB  Ack: 0xE061E225  Win: 0x4029  TcpLen: 20

snort.raw[342]:
- - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
47 45 54 20 2F 69 6D 61  67 65 73 2F 70 32 52 55  GET /ima ges/p2RU
52 68 5F 32 2F 42 6B 32  76 72 31 4F 59 52 46 31  Rh_2/Bk2 vr1OYRF1
57 47 75 35 6E 67 5F 32  46 73 66 73 2F 57 4F 57  WGu5ng_2 Fsfs/WOW
72 47 54 45 54 79 4B 2F  37 4D 7A 4D 5F 32 42 6E  rGTETyK/ 7MzM_2Bn
47 5A 51 52 32 6A 73 67  50 2F 73 5F 32 42 70 53  GZQR2jsg P/s_2BpS
34 31 4B 37 41 67 2F 4F  75 4A 6A 51 66 41 61 63  41K7Ag/O uJjQfAac
32 64 2F 76 6D 46 5F 32  46 31 4B 42 50 72 4B 5F  2d/vmF_2 F1KBPrK_
32 2F 46 36 36 38 32 64  67 64 69 61 47 31 7A 75  2/F6682d gdiaG1zu
56 43 7A 37 47 68 64 2F  62 4C 37 36 57 66 35 71  VCz7Ghd/ bL76Wf5q
64 71 77 56 35 76 7A 52  2F 32 65 31 41 38 79 42  dqwV5vzR /2e1A8yB
49 64 6B 6D 49 5F 32 42  2F 6F 67 79 7A 4E 55 57  IdkmI_2B /ogyzNUW
33 47 72 2F 67 4B 42 5A  57 58 78 2E 67 69 66 20  3Gr/gKBZ WXx.gif
48 54 54 50 2F 31 2E 31  0D 0A 55 73 65 72 2D 41  HTTP/1.1 ..User-A
67 65 6E 74 3A 20 4D 6F  7A 69 6C 6C 61 2F 34 2E  gent: Mo zilla/4.
30 20 28 63 6F 6D 70 61  74 69 62 6C 65 3B 20 4D  0 (compa tible; M
53 49 45 20 38 2E 30 3B  20 57 69 6E 64 6F 77 73  SIE 8.0;  Windows
20 4E 54 20 36 2E 31 29  0D 0A 48 6F 73 74 3A 20   NT 6.1) ..Host:
62 6C 75 65 77 61 74 65  72 73 74 6F 6E 65 2E 72  bluewate rstone.r
75 0D 0A 43 6F 6E 6E 65  63 74 69 6F 6E 3A 20 4B  u..Conne ction: K
65 65 70 2D 41 6C 69 76  65 0D 0A 43 61 63 68 65  eep-Aliv e..Cache
2D 43 6F 6E 74 72 6F 6C  3A 20 6E 6F 2D 63 61 63  -Control : no-cac
68 65 0D 0A 0D 0A                                 he....
```

```
-- [0] /home/htb-student/pcaps/ursnif.pcap
--------------------------------------------------
Packet Statistics
--------------------------------------------------
daq
                    pcaps: 1
                 received: 49
                 analyzed: 49
                    allow: 49
                 rx_bytes: 5925
--------------------------------------------------
codec
                    total: 49          (100.000%)
                      eth: 49          (100.000%)
                     ipv4: 49          (100.000%)
                      tcp: 16          ( 32.653%)
                      udp: 33          ( 67.347%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
appid
                  packets: 49
        processed_packets: 49
           total_sessions: 15
       service_cache_adds: 5
             bytes_in_use: 760
             items_in_use: 5
--------------------------------------------------
back_orifice
                  packets: 33
--------------------------------------------------
binder
                new_flows: 12
          service_changes: 2
                 inspects: 12
--------------------------------------------------
detection
                 analyzed: 49
              raw_searches: 2
          cooked_searches: 1
             pkt_searches: 3
            file_searches: 1
                   alerts: 1
             total_alerts: 1
                   logged: 1
--------------------------------------------------
dns
                  packets: 19
                 requests: 12
                responses: 7
--------------------------------------------------
file_id
              total_files: 1
          total_file_data: 304
     max_concurrent_files: 1
--------------------------------------------------
http_inspect
                    flows: 2
                    scans: 9
               reassembles: 9
               inspections: 9
                  requests: 2
                 responses: 2
             get_requests: 1
            post_requests: 1
           request_bodies: 1
  max_concurrent_sessions: 2
              total_bytes: 1603
--------------------------------------------------
port_scan
                  packets: 49
                 trackers: 7
--------------------------------------------------
search_engine
                max_queued: 1
            total_flushed: 2
            total_inserts: 2
             total_unique: 2
     non_qualified_events: 1
         qualified_events: 1
           searched_bytes: 2192
--------------------------------------------------
stream
```

```
                    flows: 12
               total_prunes: 7
  idle_prunes_proto_timeout: 7
-------------------------------------------------
stream_tcp
                  sessions: 2
                       max: 2
                   created: 2
                  released: 2
               instantiated: 2
                     setups: 2
                  restarts: 2
               syn_trackers: 2
                segs_queued: 4
              segs_released: 4
                  segs_used: 4
            rebuilt_packets: 9
              rebuilt_bytes: 1627
                       syns: 2
                   syn_acks: 2
                     resets: 2
                   max_segs: 1
                  max_bytes: 981
-------------------------------------------------
stream_udp
                  sessions: 10
                       max: 10
                   created: 13
                  released: 13
                  timeouts: 3
               total_bytes: 1964
-------------------------------------------------
wizard
                 tcp_scans: 2
                  tcp_hits: 2
                 udp_scans: 3
                udp_misses: 3
-------------------------------------------------
Appid Statistics
-------------------------------------------------
detected apps and services
               Application: Services   Clients    Users      Payloads   Misc       Referred
                   unknown: 11         9          0          2          0          0
-------------------------------------------------
Summary Statistics
-------------------------------------------------
timing
                   runtime: 00:00:00
                   seconds: 0.039200
                  pkts/sec: 1250
                  Mbits/sec: 1
o")~   Snort exiting
```

Invest some time in scrutinizing both the `ursnif.pcap` file using `Wireshark` and this rule to comprehend how it works.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/ursnif.pcap .
```

Snort Rule Development Example 2: Detecting Cerber

Snort Rule Development

```
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible Cerber Check-in"; dsize:9; content:"hi"
```

The Snort rule above is designed to detect certain variations of Cerber malware. Let's break down the important parts of this rule to understand its workings.

- `$HOME_NET any -> $EXTERNAL_NET any` signifies the rule applies to any `UDP` traffic going from any port in the home network to any port on external networks.
- `dsize:9;`: This is a condition that restricts the rule to UDP datagrams that have a payload

data size of exactly 9 bytes.

- content:"hi", depth 2, fast_pattern;: This checks the payload's first 2 bytes for the string hi. The fast_pattern modifier makes the pattern matcher search for this pattern before any others in the rule, optimizing the rule's performance.
- pcre:"/^[af0-9]{7}$/R";: This stands for Perl Compatible Regular Expressions. The rule is looking for seven hexadecimal characters (from the set a-f and 0-9) starting at the beginning of the payload (after the hi), and this should be the complete payload (signified by the $ end anchor).
- detection_filter:track by_src, count 1, seconds 60;: The detection_filter keyword in Snort rule language is used to suppress alerts unless a certain threshold of matched events occurs within a specified time frame. In this rule, the filter is set to track by source IP (by_src), with a count of 1 and within a time frame of 60 seconds. This means that the rule will trigger an alert only if it matches more than one event (specifically, more than count events which is 1 here) from the same source IP address within 60 seconds.

The above rule is already incorporated in the `local.rules` file found in the `/home/htb-student` directory of this section's target. To test it, first, you need to uncomment the rule. Then, execute Snort on the `cerber.pcap` file, which is located in the `/home/htb-student/pcaps` directory.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ sudo snort -c /root/snorty/etc/snort/snort.lua --daq-dir /usr/local/lib/daq
--------------------------------------------------
o")~   Snort++ 3.1.64.0
--------------------------------------------------
Loading /root/snorty/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        output
---SNIP---
        trace
Finished /root/snorty/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Loading rule args:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Finished rule args:
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     210       2     210    /root/snorty/etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 210
          duplicate rules: 2
              text rules: 210
            option chains: 210
            chain headers: 5
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       0       1       1       0
   total       0       1       1       0
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      208     208
                    total:      208     208
--------------------------------------------------
fast pattern groups
                     any: 2
               to_server: 1
               to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 3
                 patterns: 417
            pattern chars: 2511
               num states: 1781
```

```
         num match states: 371
             memory scale: KB
             total memory: 69.8359
           pattern memory: 18.7383
        match list memory: 27.3828
        transition memory: 23.3398
appid: MaxRss diff: 3024
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to read-file.
Commencing packet processing
++ [0] /home/htb-student/pcaps/cerber.pcap
07/22-02:17:56.486663 [**] [1:2816763:4] "Possible Cerber Check-in" [**] [Priority: 0] {UDP} 10.0.2
08:00:27:A9:8C:97 -> 52:54:00:12:35:02 type:0x800 len:0x3C
10.0.2.15:1046 -> 31.184.234.1:6892 UDP TTL:128 TOS:0x0 ID:83 IpLen:20 DgmLen:37
Len: 9

snort.raw[9]:
- - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - - -
68 69 30 30 37 32 38 39  35                      hi007289 5
- - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - - -

07/22-02:17:56.486795 [**] [1:2816763:4] "Possible Cerber Check-in" [**] [Priority: 0] {UDP} 10.0.2
08:00:27:A9:8C:97 -> 52:54:00:12:35:02 type:0x800 len:0x3C
10.0.2.15:1046 -> 31.184.234.2:6892 UDP TTL:128 TOS:0x0 ID:84 IpLen:20 DgmLen:37
Len: 9

snort.raw[9]:
- - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - - -
68 69 30 30 37 32 38 39  35                      hi007289 5
---SNIP---
-- [0] /home/htb-student/pcaps/cerber.pcap
--------------------------------------------------
Packet Statistics
--------------------------------------------------
daq
                    pcaps: 1
                 received: 1035
                 analyzed: 1035
                    allow: 1035
                 rx_bytes: 65672
--------------------------------------------------
codec
                    total: 1035        (100.000%)
                      eth: 1035        (100.000%)
                     ipv4: 1035        (100.000%)
                      tcp: 9           (  0.870%)
                      udp: 1026        ( 99.130%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
appid
                  packets: 1035
         processed_packets: 1035
            total_sessions: 1026
        service_cache_adds: 514
              bytes_in_use: 78128
              items_in_use: 514
--------------------------------------------------
back_orifice
                  packets: 514
--------------------------------------------------
binder
                new_flows: 1026
           service_changes: 1
                  inspects: 1026
--------------------------------------------------
detection
                  analyzed: 1035
              raw_searches: 1026
              pkt_searches: 1026
             file_searches: 1
                    alerts: 511
              total_alerts: 511
                    logged: 511
--------------------------------------------------
dns
                  packets: 2
                 requests: 1
                responses: 1
--------------------------------------------------
file_id
               total_files: 1
          total_file_data: 164
```

```
     max_concurrent_files: 1
-------------------------------------------------
http_inspect
                   flows: 1
                   scans: 5
             reassembles: 5
             inspections: 5
                requests: 1
               responses: 1
            get_requests: 1
  max_concurrent_sessions: 1
             total_bytes: 462
-------------------------------------------------
pcre
              pcre_rules: 2
             pcre_native: 2
-------------------------------------------------
port_scan
                 packets: 1035
                trackers: 516
-------------------------------------------------
search_engine
              max_queued: 1
            total_flushed: 512
            total_inserts: 512
             total_unique: 512
     non_qualified_events: 1
         qualified_events: 511
           searched_bytes: 17146
-------------------------------------------------
stream
                   flows: 1026
-------------------------------------------------
stream_tcp
                sessions: 1
                     max: 1
                 created: 1
                released: 1
            instantiated: 1
                  setups: 1
                restarts: 1
            syn_trackers: 1
             segs_queued: 2
            segs_released: 2
                segs_used: 2
          rebuilt_packets: 5
            rebuilt_bytes: 474
                     syns: 1
                syn_acks: 1
                    fins: 1
                max_segs: 1
               max_bytes: 435
-------------------------------------------------
stream_udp
                sessions: 1025
                     max: 1025
                 created: 1025
                released: 1025
             total_bytes: 16982
-------------------------------------------------
wizard
               tcp_scans: 1
                tcp_hits: 1
               udp_scans: 1024
              udp_misses: 1024
-------------------------------------------------
Appid Statistics
-------------------------------------------------
detected apps and services
             Application: Services   Clients    Users      Payloads   Misc       Referred
                 unknown: 2          1          0          1          0          0
-------------------------------------------------
Summary Statistics
-------------------------------------------------
timing
                runtime: 00:01:11
                seconds: 71.153373
               pkts/sec: 15
o")~   Snort exiting
```

Invest some time in scrutinizing both the `cerber.pcap` file using `Wireshark` and this rule to comprehend how it works.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/cerber.pcap .
```

Snort Rule Development Example 3: Detecting Patchwork

Snort Rule Development

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"OISF TROJAN Targeted AutoIt FileStealer/Downloa
```

The Snort rule above is designed to detect certain variations of malware used by the Patchwork APT. Please notice the use of HTTP sticky buffers in this rule. Let's break down the important parts of this rule to understand its workings.

- `flow:established,to_server;`: This keyword is used to specify the direction of the traffic we are interested in. In this case, we're looking at established connections where the traffic is going from the client to the server.
- `http_method; content:"POST";`: We are looking for HTTP traffic where the method used is `POST`.
- `http_uri; content:".php?profile=";`: This specifies that we're looking for HTTP URIs that contain the string `.php?profile=`.
- `http_client_body; content:"ddager=", depth 7;`: We're examining the body of the HTTP request. Specifically, we're looking for the string `ddager=` within the first `7` bytes of the body.
- `http_client_body; content:"&r1=", distance 0;`: We're still examining the body of the HTTP request, but now we're looking for the string `&r1=` immediately following the previous content match.
- `http_header; content:!"Accept"; http_header; content:!"Referer|3a|";`: These conditions are looking for the absence of the `Accept` and `Referer` HTTP headers. The `!` before the content means `not`, so we're looking for situations where these headers are not present.

The above rule is already incorporated in the `local.rules` file found in the `/home/htb-student` directory of this section's target. To test it, first, you need to uncomment the rule. Then, execute Snort on the `patchwork.pcap` file, which is located in the `/home/htb-student/pcaps` directory.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ sudo snort -c /root/snorty/etc/snort/snort.lua --daq-dir /usr/local/lib/daq
--------------------------------------------------
o")~   Snort++ 3.1.64.0
--------------------------------------------------
Loading /root/snorty/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        output
---SNIP---
        trace
Finished /root/snorty/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Loading rule args:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Finished rule args:
--------------------------------------------------
ips policies rule stats
               id  loaded  shared enabled    file
                0     210       2     210    /root/snorty/etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 210
          duplicate rules: 2
               text rules: 210
```

```
            option chains: 210
            chain headers: 5
-------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
   total       0       0       1       0
-------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      208     208
                     http:        1       0
                    http2:        1       0
                    http3:        1       0
                    total:      211     208
-------------------------------------------------
fast pattern groups
                to_server: 4
                to_client: 1
-------------------------------------------------
search engine (ac_bnfa)
                instances: 5
                 patterns: 419
            pattern chars: 2550
               num states: 1820
         num match states: 373
             memory scale: KB
             total memory: 73.0088
           pattern memory: 18.8525
        match list memory: 27.75
        transition memory: 25.7812
appid: MaxRss diff: 2964
appid: patterns loaded: 300
-------------------------------------------------
pcap DAQ configured to read-file.
Commencing packet processing
++ [0] /home/htb-student/pcaps/patchwork.pcap
06/01-19:24:43.339294 [**] [1:10000006:1] "OISF TROJAN Targeted AutoIt FileStealer/Downloader CnC B
0

http_inspect.http_method[4]:
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
50 4F 53 54                                           POST
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -

http_inspect.http_version[8]:
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
48 54 54 50 2F 31 2E 31                               HTTP/1.1
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -

http_inspect.http_uri[37]:
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
2F 64 72 6F 70 70 65 72  2E 70 68 70 3F 70 72 6F  /dropper .php?pro
66 69 6C 65 3D 63 6D 56  6B 63 30 42 43 55 45 46  file=cmV kc0BCUEF
4A 54 67 3D 3D                                    JTg==
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -

http_inspect.http_header[167]:
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
43 6F 6E 6E 65 63 74 69  6F 6E 3A 20 4B 65 65 70  Connecti on: Keep
2D 41 6C 69 76 65 0D 0A  43 6F 6E 74 65 6E 74 2D  -Alive.. Content-
54 79 70 65 3A 20 61 70  70 6C 69 63 61 74 69 6F  Type: ap plicatio
6E 2F 78 2D 77 77 77 2D  66 6F 72 6D 2D 75 72 6C  n/x-www- form-url
65 6E 63 6F 64 65 64 0D  0A 55 73 65 72 2D 41 67  encoded. .User-Ag
65 6E 74 3A 20 4D 6F 7A  69 6C 6C 61 2F 35 2E 30  ent: Moz illa/5.0
20 46 69 72 65 66 6F 78  20 28 4C 69 6B 65 20 53   Firefox  (Like S
61 66 61 72 69 2F 57 65  62 6B 69 74 29 0D 0A 43  afari/We bkit)..C
6F 6E 74 65 6E 74 2D 4C  65 6E 67 74 68 3A 20 36  ontent-L ength: 6
34 0D 0A 48 6F 73 74 3A  20 32 31 32 2E 31 32 39  4..Host:  212.129
2E 31 33 2E 31 31 30                              .13.110
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -

http_inspect.http_client_body[64]:
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -
64 64 61 67 65 72 3D 30  26 72 31 3D 56 30 6C 4F  ddager=0 &r1=V0lO
58 7A 63 3D 26 72 32 3D  57 44 59 30 26 72 33 3D  Xzc=&r2= WDY0&r3=
4D 53 34 78 26 72 34 3D  4D 41 3D 3D 26 72 35 3D  MS4x&r4= MA==&r5=
49 43 41 3D 26 72 36 3D  56 48 4A 31 5A 51 3D 3D  ICA=&r6= VHJ1ZQ==
- - - - - - - - - - - - -  - - - - - - - - - - - - - -  - - - - - - - - - -

06/01-19:25:09.059391 [**] [1:10000006:1] "OISF TROJAN Targeted AutoIt FileStealer/Downloader CnC B
0
---SNIP---
-- [0] /home/htb-student/pcaps/patchwork.pcap
-------------------------------------------------
Packet Statistics
```

```
Packet Statistics
-------------------------------------------------
daq
                   pcaps: 1
                received: 4868
                analyzed: 4868
                   allow: 4155
               whitelist: 713
                rx_bytes: 3561155
-------------------------------------------------
codec
                   total: 4868         (100.000%)
                discards: 1            (  0.021%)
                     eth: 4868         (100.000%)
                    ipv4: 4868         (100.000%)
                     tcp: 4834         ( 99.302%)
                     udp: 33           (  0.678%)
-------------------------------------------------
Module Statistics
-------------------------------------------------
appid
                 packets: 4867
       processed_packets: 4867
          total_sessions: 11
       service_cache_adds: 6
            bytes_in_use: 912
            items_in_use: 6
-------------------------------------------------
back_orifice
                 packets: 33
-------------------------------------------------
binder
             raw_packets: 1
               new_flows: 10
         service_changes: 7
                inspects: 11
-------------------------------------------------
dce_smb
                sessions: 1
                 packets: 17
           ignored_bytes: 287
 max_outstanding_requests: 1
  max_concurrent_sessions: 1
     total_smb1_sessions: 1
-------------------------------------------------
detection
                analyzed: 4868
            pdu_searches: 257
           file_searches: 514
                  alerts: 257
            total_alerts: 257
                  logged: 257
-------------------------------------------------
file_id
             total_files: 514
          total_file_data: 390466
     max_concurrent_files: 1
-------------------------------------------------
http_inspect
                   flows: 4
                   scans: 2822
              reassembles: 2822
              inspections: 1542
                requests: 257
               responses: 257
            post_requests: 257
          request_bodies: 257
  max_concurrent_sessions: 1
             total_bytes: 2081981
-------------------------------------------------
normalizer
        test_tcp_trim_win: 8
-------------------------------------------------
port_scan
                 packets: 4867
                trackers: 8
-------------------------------------------------
search_engine
              max_queued: 1
           total_flushed: 513
           total_inserts: 513
            total_unique: 513
     non_qualified_events: 256
         qualified_events: 257
           searched_bytes: 399719
```

```
-------------------------------------------------
ssl
                packets: 71
                decoded: 71
            client_hello: 2
            server_hello: 2
             certificate: 2
             server_done: 6
      client_key_exchange: 2
           change_cipher: 4
       client_application: 3
       server_application: 56
                   alert: 1
     unrecognized_records: 6
     handshakes_completed: 1
         sessions_ignored: 1
  max_concurrent_sessions: 1
-------------------------------------------------
stream
                  flows: 10
            total_prunes: 3
idle_prunes_proto_timeout: 3
-------------------------------------------------
stream_tcp
                sessions: 7
                     max: 7
                 created: 7
                released: 7
            instantiated: 7
                  setups: 7
                restarts: 7
          invalid_seq_num: 8
             syn_trackers: 7
              segs_queued: 2735
            segs_released: 2735
                segs_used: 2734
          rebuilt_packets: 1631
            rebuilt_bytes: 2981239
                     gaps: 6
                     syns: 8
                 syn_acks: 7
                   resets: 1
                     fins: 10
                max_segs: 15
               max_bytes: 20520
-------------------------------------------------
stream_udp
                sessions: 3
                     max: 3
                 created: 4
                released: 4
                timeouts: 1
             total_bytes: 2359
-------------------------------------------------
wizard
               tcp_scans: 9
                tcp_hits: 7
               udp_scans: 3
             udp_misses: 3
-------------------------------------------------
Appid Statistics
-------------------------------------------------
detected apps and services
             Application: Services   Clients    Users      Payloads   Misc       Referred
                 unknown: 9          4          0          6          0          0
-------------------------------------------------
Summary Statistics
-------------------------------------------------
timing
                runtime: 00:01:21
                seconds: 81.152785
               pkts/sec: 60
o")~   Snort exiting
```

Invest some time in scrutinizing both the `patchwork.pcap` file using `Wireshark` and this rule to comprehend how it works.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/patchwork.pcap .
```

Snort Rule Development Example 4: Detecting Patchwork (SSL)

Snort Rule Development

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Patchwork SSL Cert Detected"; flow:established,f
```

The Snort rule above is designed to detect certain variations of malware used by the Patchwork APT. Let's break down the important parts of this rule to understand its workings.

- `flow:established,from_server;`: This keyword pair signifies that we're interested in observing `established` flows of traffic originating from the server.
- `content:"|55 04 03|";`: This rule is looking for the specific hex values `55 04 03` within the payload of the packet. These hex values represent the ASN.1 (Abstract Syntax Notation One) tag for the "common name" field in an X.509 certificate, which is often used in SSL/TLS certificates to denote the domain name that the certificate applies to.
- `content:"|08|toigetgf", distance 1, within 9;`: Following the common name field, this rule looks for the string `toigetgf`. The distance `1` means that Snort should start looking for the string `toigetgf` `1` byte after the end of the previous content match. The within `9` sets an upper limit on how far into the packet's payload Snort should search, starting from the beginning of this content field.

The above rule is already incorporated in the `local.rules` file found in the `/home/htb-student` directory of this section's target. To test it, first, you need to uncomment the rule. Then, execute Snort on the `patchwork.pcap` file, which is located in the `/home/htb-student/pcaps` directory.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ sudo snort -c /root/snorty/etc/snort/snort.lua --daq-dir /usr/local/lib/daq

--------------------------------------------------
o")~   Snort++ 3.1.64.0
--------------------------------------------------
Loading /root/snorty/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        ips
--SNIP---
        trace
        active
Finished /root/snorty/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Loading rule args:
Loading /home/htb-student/local.rules:
Finished /home/htb-student/local.rules:
Finished rule args:
--------------------------------------------------
ips policies rule stats
               id  loaded  shared enabled    file
                0     210       2     210    /root/snorty/etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 210
          duplicate rules: 2
               text rules: 210
             option chains: 210
             chain headers: 5
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       1       0       1       0
   total       1       0       1       0
```

```
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      208     208
                    total:      208     208
--------------------------------------------------
fast pattern groups
                      any: 2
                to_server: 1
                to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 3
                 patterns: 417
            pattern chars: 2518
               num states: 1788
          num match states: 371
              memory scale: KB
              total memory: 69.9795
            pattern memory: 18.7451
         match list memory: 27.4375
         transition memory: 23.4219
appid: MaxRss diff: 3084
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to read-file.
Commencing packet processing
++ [0] /home/htb-student/pcaps/patchwork.pcap
06/01-19:25:29.876240 [**] [1:10000008:1] "Patchwork SSL Cert Detected" [**] [Classification: A Net

ssl.stream_tcp[807]:
- - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
16 03 03 00 51 02 00 00  4D 03 03 74 19 1E 0B 50  ....Q... M..t...P
F2 80 7F 3F 81 1C 07 CF  58 0B A0 48 B0 F7 A7 D4  ...?.... X..H....
8B 08 53 2D 10 62 F9 23  F0 CD 76 20 A3 17 4D A2  ..S-.b.# ..v ..M.
35 58 EC 8B 4A F2 74 6D  72 7F CC 80 45 E8 1E 73  5X..J.tm r...E..s
2E 22 18 99 75 FB D1 FF  0E 97 C8 04 00 3C 00 00  ."..u... .....<..
05 FF 01 00 01 00 16 03  03 02 C3 0B 00 02 BF 00  ........ ........
02 BC 00 02 B9 30 82 02  B5 30 82 01 9D A0 03 02  .....0.. .0......
01 02 02 08 44 0E 87 29  65 41 6D 2A 30 0D 06 09  ....D..) eAm*0...
2A 86 48 86 F7 0D 01 01  0B 05 00 30 13 31 11 30  *.H..... ...0.1.0
0F 06 03 55 04 03 0C 08  74 6F 69 67 65 74 67 66  ...U.... toigetgf
30 1E 17 0D 31 34 31 31  31 38 30 36 30 38 33 38  0...1411 18060838
5A 17 0D 32 34 31 31 31  35 30 36 30 38 33 38 5A  Z..24111 5060838Z
30 13 31 11 30 0F 06 03  55 04 03 0C 08 74 6F 69  0.1.0... U....toi
67 65 74 67 66 30 82 01  22 30 0D 06 09 2A 86 48  getgf0.. "0...*.H
86 F7 0D 01 01 01 05 00  03 82 01 0F 00 30 82 01  ........ .....0..
0A 02 82 01 01 00 C6 B9  1B 97 5C 6E DA 23 4C 02  ........ ..\n.#L.
EC A6 A8 09 56 FA 85 5E  35 75 A8 BB 63 B5 81 30  ....V..^ 5u..c..0
90 91 45 D7 19 36 0B 20  DF 70 37 0E 91 05 FB 86  ..E..6.  .p7.....
22 E8 56 3D A5 89 BA 13  01 60 DF 43 A6 F0 05 7B  ".V=.... .`.C...{
5A 04 7F 53 14 80 C1 64  EA 9C 09 98 A2 B8 99 EA  Z..S...d ........
91 26 52 81 62 D3 BB CE  A2 4E E7 BB 97 C9 19 D2  .&R.b... .N......
EF 61 8A A5 50 9A D7 6B  9F 9D 54 7B AE E2 6F 53  .a..P..k ..T{..oS
BB 7A B4 D2 93 06 73 96  CD 04 19 55 D3 7A DA 34  .z....s. ...U.z.4
8F 05 2D 2E 98 7F 6C 9E  0B C8 41 A2 49 BA FB CC  ..-...l. ..A.I...
A4 20 BD 8A E5 18 27 88  BB 87 F9 F6 F3 56 8F 73  . ....'. .....V.s
D6 BA 92 29 F9 F0 A6 AB  F5 FD 5F E0 92 C6 96 2D  ...)....  .._....-
41 80 FA 0B 4C C9 9B AE  2D 69 F7 9D B5 4B 14 81  A...L... -i...K..
AD F8 71 6F 2B A8 59 66  6E FD B5 8B 3B 14 09 F7  ..qo+.Yf n...;...
B8 FC 20 EF 7D A0 D5 40  D6 66 BB 65 B6 FC 92 3A  .. .}..@ .f.e...:
71 F5 BA 5B F1 07 A5 FD  E3 11 F2 A9 51 6C 16 8F  q..[.... ....Ql..
C8 72 B7 A0 D7 26 43 3A  18 7B F8 7B 38 72 01 37  .r...&C: .{.{8r.7
4F 42 28 42 2F 01 02 03  01 00 01 A3 0D 30 0B 30  OB(B/... .....0.0
09 06 03 55 1D 13 04 02  30 00 30 0D 06 09 2A 86  ...U.... 0.0...*.
48 86 F7 0D 01 01 0B 05  00 03 82 01 01 00 2D 0E  H.......  ......-.
CC D5 50 AB DF 20 37 BB  71 10 31 C5 1F 17 EC F9  ..P.. 7. q.1.....
D7 20 1A 19 39 F4 DE D8  BA C1 A3 F5 57 E0 E0 6B  . ..9... ....W..k
DC 6F E1 1F 6B 07 98 FB  38 1A 0A 77 BD B4 0A 94  .o..k... 8..w....
01 45 95 0C 09 F1 43 D5  7D 57 E7 D6 E7 74 98 6C  .E....C. }W...t.l
4F D0 46 81 F2 9D 5A 29  1E BD 7F 03 5B 64 B3 98  O.F...Z) ....[d..
D4 52 B0 E1 CE 11 62 68  31 1D CC 0F DD B6 AA 5C  .R....bh 1......\
44 D0 44 18 9E 3D AE 30  C7 10 C6 97 F6 C1 C9 D7  D.D..=.0 ........
11 13 44 AA B4 C9 2D 0C  AC 2B AD 9A CB 7B 5D 51  ..D...-. .+...{]Q
3F 45 C6 2E 99 CF 71 F6  66 9A 09 28 44 28 34 3B  ?E....q. f..(D(4;
EC 0B A6 F4 E3 5F FE 7E  30 59 DC 3D 4E 33 22 11  ....._.~ 0Y.=N3".
BA CA 8A 4B 41 5D 97 3E  CD BB 3C DD 28 37 12 47  ...KA].> ..<.(7.G
E0 BE AC 3B 13 EC 59 A0  E3 1A CE 28 B2 11 5D 3B  ...;..Y. ...(..];
AC AD CF 32 F5 EA CB B2  92 20 BC 5C 3C 4C B9 43  ...2.... . .\<L.C
5A BC 1B 2F E3 F3 DF DC  04 DB 24 6A 73 13 EA E5  Z../.... ..$js...
32 45 6A F6 D9 CC 66 9C  80 99 3D EC D9 2D 13 9A  2Ej...f. ..=..-..
9A 6F 90 69 47 95 B6 46  D8 F2 E8 EF CC CA 16 03  .o.iG..F ........
03 00 04 0E 00 00 00                              .......
- - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
```

```
06/01-19:25:44.259156 [**] [1:10000008:1] "Patchwork SSL Cert Detected" [**] [Classification: A Net

ssl.stream_tcp[807]:
- - - - - - - - - - - - -  - - - - - - - - - - - - -  - - - - - - - - - -
16 03 01 00 51 02 00 00  4D 03 01 BA 21 1C 95 C6  ....Q... M...!...
8A 83 F3 C8 31 16 EF 25  32 C4 63 7E 82 B0 7D D0  ....1..% 2.c~..}.
01 EF 6C 7B DC A3 CD 53  97 18 62 20 C6 FE 9D B0  ..l{...S ..b ....
B0 F4 9B 9A 6E 1D 6B 74  64 4D E4 CC 30 2E 05 B8  ....n.kt dM..0...
30 1A 34 D0 30 94 5B FA  AB 64 27 09 00 2F 00 00  0.4.0.[. .d'../..
05 FF 01 00 01 00 16 03  01 02 C3 0B 00 02 BF 00  ........ ........
02 BC 00 02 B9 30 82 02  B5 30 82 01 9D A0 03 02  .....0.. .0......
01 02 02 08 44 0E 87 29  65 41 6D 2A 30 0D 06 09  ....D..) eAm*0...
2A 86 48 86 F7 0D 01 01  0B 05 00 30 13 31 11 30  *.H..... ...0.1.0
0F 06 03 55 04 03 0C 08  74 6F 69 67 65 74 67 66  ...U.... toigetgf
30 1E 17 0D 31 34 31 31  31 38 30 36 30 38 33 38  0...1411 18060838
5A 17 0D 32 34 31 31 31  35 30 36 30 38 33 38 5A  Z..24111 5060838Z
30 13 31 11 30 0F 06 03  55 04 03 0C 08 74 6F 69  0.1.0... U....toi
67 65 74 67 66 30 82 01  22 30 0D 06 09 2A 86 48  getgf0.. "0...*.H
86 F7 0D 01 01 01 05 00  03 82 01 0F 00 30 82 01  ........ .....0..
0A 02 82 01 01 00 C6 B9  1B 97 5C 6E DA 23 4C 02  ........ ..\n.#L.
EC A6 A8 09 56 FA 85 5E  35 75 A8 BB 63 B5 81 30  ....V..^ 5u..c..0
90 91 45 D7 19 36 0B 20  DF 70 37 0E 91 05 FB 86  ..E..6.  .p7.....
22 E8 56 3D A5 89 BA 13  01 60 DF 43 A6 F0 05 7B  ".V=.... .`.C...{
5A 04 7F 53 14 80 C1 64  EA 9C 09 98 A2 B8 99 EA  Z..S...d ........
91 26 52 81 62 D3 BB CE  A2 4E E7 BB 97 C9 19 D2  .&R.b... .N......
EF 61 8A A5 50 9A D7 6B  9F 9D 54 7B AE E2 6F 53  .a..P..k ..T{..oS
BB 7A B4 D2 93 06 73 96  CD 04 19 55 D3 7A DA 34  .z....s. ...U.z.4
8F 05 2D 2E 98 7F 6C 9E  0B C8 41 A2 49 BA FB CC  ..-...l. ..A.I...
A4 20 BD 8A E5 18 27 88  BB 87 F9 F6 F3 56 8F 73  . ....'. .....V.s
D6 BA 92 29 F9 F0 A6 AB  F5 FD 5F E0 92 C6 96 2D  ...)....  .._....-
41 80 FA 0B 4C C9 9B AE  2D 69 F7 9D B5 4B 14 81  A...L... -i...K..
AD F8 71 6F 2B A8 59 66  6E FD B5 8B 3B 14 09 F7  ..qo+.Yf n...;...
B8 FC 20 EF 7D A0 D5 40  D6 66 BB 65 B6 FC 92 3A  .. .}..@ .f.e...:
71 F5 BA 5B F1 07 A5 FD  E3 11 F2 A9 51 6C 16 8F  q..[.... ....Ql..
C8 72 B7 A0 D7 26 43 3A  18 7B F8 7B 38 72 01 37  .r...&C: .{.{8r.7
4F 42 28 42 2F 01 02 03  01 00 01 A3 0D 30 0B 30  OB(B/... .....0.0
09 06 03 55 1D 13 04 02  30 00 30 0D 06 09 2A 86  ...U.... 0.0...*.
48 86 F7 0D 01 01 0B 05  00 03 82 01 01 00 2D 0E  H.......  ......-.
CC D5 50 AB DF 20 37 BB  71 10 31 C5 1F 17 EC F9  ..P.. 7. q.1.....
D7 20 1A 19 39 F4 DE D8  BA C1 A3 F5 57 E0 E0 6B  . ..9... ....W..k
DC 6F E1 1F 6B 07 98 FB  38 1A 0A 77 BD B4 0A 94  .o..k... 8..w....
01 45 95 0C 09 F1 43 D5  7D 57 E7 D6 E7 74 98 6C  .E....C. }W...t.l
4F D0 46 81 F2 9D 5A 29  1E BD 7F 03 5B 64 B3 98  O.F...Z) ....[d..
D4 52 B0 E1 CE 11 62 68  31 1D CC 0F DD B6 AA 5C  .R....bh 1......\
44 D0 44 18 9E 3D AE 30  C7 10 C6 97 F6 C1 C9 D7  D.D..=.0 ........
11 13 44 AA B4 C9 2D 0C  AC 2B AD 9A CB 7B 5D 51  ..D...-. .+...{]Q
3F 45 C6 2E 99 CF 71 F6  66 9A 09 28 44 28 34 3B  ?E....q. f..(D(4;
EC 0B A6 F4 E3 5F FE 7E  30 59 DC 3D 4E 33 22 11  ....._.~ 0Y.=N3".
BA CA 8A 4B 41 5D 97 3E  CD BB 3C DD 28 37 12 47  ...KA].> ..<.(7.G
E0 BE AC 3B 13 EC 59 A0  E3 1A CE 28 B2 11 5D 3B  ...;..Y. ...(..];
AC AD CF 32 F5 EA CB B2  92 20 BC 5C 3C 4C B9 43  ...2.... . .\<L.C
5A BC 1B 2F E3 F3 DF DC  04 DB 24 6A 73 13 EA E5  Z../.... ..$js...
32 45 6A F6 D9 CC 66 9C  80 99 3D EC D9 2D 13 9A  2Ej...f. ..=..-..
9A 6F 90 69 47 95 B6 46  D8 F2 E8 EF CC CA 16 03  .o.iG..F ........
01 00 04 0E 00 00 00                              .......
- - - - - - - - - - - - -  - - - - - - - - - - - - -  - - - - - - - - - -

-- [0] /home/htb-student/pcaps/patchwork.pcap
------------------------------------------------
Packet Statistics
------------------------------------------------
daq
                    pcaps: 1
                 received: 4868
                 analyzed: 4868
                    allow: 4155
                whitelist: 713
                 rx_bytes: 3561155
------------------------------------------------
codec
                    total: 4868         (100.000%)
                  discards: 1           (  0.021%)
                       eth: 4868         (100.000%)
                      ipv4: 4868         (100.000%)
                       tcp: 4834         ( 99.302%)
                       udp: 33           (  0.678%)
------------------------------------------------
Module Statistics
------------------------------------------------
appid
                  packets: 4867
          processed_packets: 4867
             total_sessions: 11
         service_cache_adds: 6
```

```
            bytes_in_use: 912
            items_in_use: 6
-------------------------------------------------
back_orifice
                 packets: 33
-------------------------------------------------
binder
             raw_packets: 1
               new_flows: 10
         service_changes: 7
                inspects: 11
-------------------------------------------------
dce_smb
                sessions: 1
                 packets: 17
           ignored_bytes: 287
 max_outstanding_requests: 1
  max_concurrent_sessions: 1
     total_smb1_sessions: 1
-------------------------------------------------
detection
                analyzed: 4868
            raw_searches: 21
         cooked_searches: 619
            pkt_searches: 640
           file_searches: 514
                  alerts: 2
            total_alerts: 2
                  logged: 2
-------------------------------------------------
file_id
             total_files: 514
          total_file_data: 390466
     max_concurrent_files: 1
-------------------------------------------------
http_inspect
                   flows: 4
                   scans: 2822
             reassembles: 2822
             inspections: 1542
                requests: 257
               responses: 257
           post_requests: 257
          request_bodies: 257
  max_concurrent_sessions: 1
             total_bytes: 2081981
-------------------------------------------------
normalizer
        test_tcp_trim_win: 8
-------------------------------------------------
port_scan
                 packets: 4867
                trackers: 8
-------------------------------------------------
search_engine
              max_queued: 1
            total_flushed: 258
            total_inserts: 258
             total_unique: 258
     non_qualified_events: 256
         qualified_events: 2
           searched_bytes: 3260955
-------------------------------------------------
ssl
                 packets: 71
                 decoded: 71
             client_hello: 2
             server_hello: 2
              certificate: 2
              server_done: 6
      client_key_exchange: 2
            change_cipher: 4
       client_application: 3
       server_application: 56
                   alert: 1
     unrecognized_records: 6
     handshakes_completed: 1
         sessions_ignored: 1
  max_concurrent_sessions: 1
-------------------------------------------------
stream
                   flows: 10
             total_prunes: 3
idle_prunes_proto_timeout: 3
-------------------------------------------------
```

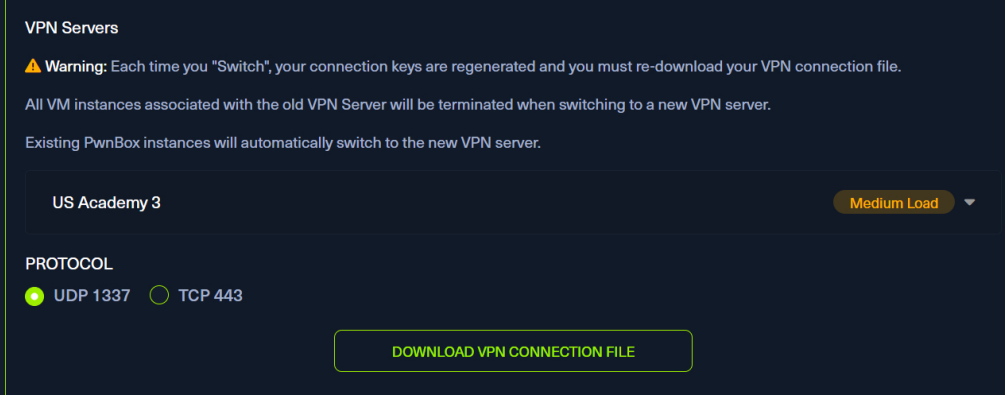
```
stream_tcp
                 sessions: 7
                      max: 7
                  created: 7
                 released: 7
             instantiated: 7
                   setups: 7
                 restarts: 7
           invalid_seq_num: 8
              syn_trackers: 7
               segs_queued: 2735
             segs_released: 2735
                 segs_used: 2734
           rebuilt_packets: 1631
             rebuilt_bytes: 2981239
                      gaps: 6
                      syns: 8
                  syn_acks: 7
                    resets: 1
                      fins: 10
                 max_segs: 15
                max_bytes: 20520
-------------------------------------------------
stream_udp
                 sessions: 3
                      max: 3
                  created: 4
                 released: 4
                 timeouts: 1
              total_bytes: 2359
-------------------------------------------------
wizard
                tcp_scans: 9
                 tcp_hits: 7
                udp_scans: 3
               udp_misses: 3
-------------------------------------------------
Appid Statistics
-------------------------------------------------
detected apps and services
             Application: Services   Clients    Users      Payloads   Misc       Referred
                 unknown: 9          4          0          6          0          0
-------------------------------------------------
Summary Statistics
-------------------------------------------------
timing
                  runtime: 00:00:00
                  seconds: 0.078293
                pkts/sec: 62177
               Mbits/sec: 347
o")~   Snort exiting
```

Invest some time in scrutinizing both the `patchwork.pcap` file using `Wireshark` and this rule to comprehend how it works.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Snort Rule Development

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/patchwork.pcap .
```



Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 138ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 2 There is a file named log4shell.pcap in the /home/htb-student/pcaps directory, which contains network traffic related to log4shell exploitation attempts, where the payload is embedded within the user agent. Enter the keyword that should be specified right before the content keyword of the rule with sid 10000098 within the local.rules file so that an alert is triggered as your answer. Answer format: [keyword];

http_header;

Submit

Previous Next

Mark Complete & Next