Network Security Practices

CY5150

Lab 4 - Suricata IDS Lab

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

Lab Steps:

- **What is the IPv4 address and subnet mask?**
  IPv4 Address: 10.0.0.35
  Subnet Mask: 255.255.255.0

```
cy5150@lab:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.35  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 2601:197:780:9d60::fea5  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::20c:29ff:fecb:639e  prefixlen 64  scopeid 0x20<link>
        inet6 2601:197:780:9d60:20c:29ff:fecb:639e  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:cb:63:9e  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 4439 (4.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 5745 (5.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 768  bytes 54624 (54.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 768  bytes 54624 (54.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **What is the OS version running on VM?**

  The OS version running on VM is **Ubuntu 18.04.4 LTS**.

```
cy5150@lab:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic
cy5150@lab:~$
```

- **What is the version of suricata-update?**

  The version of suricata-update is **5.0.2.**

```
cy5150@lab:~$ sudo suricata-update check-versions
31/3/2020 -- 23:52:02 - <Info> -- Using data-directory /var/lib/suricata.
31/3/2020 -- 23:52:02 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/3/2020 -- 23:52:02 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/3/2020 -- 23:52:02 - <Info> -- Found Suricata version 5.0.2 at /usr/bin/suricata.
31/3/2020 -- 23:52:02 - <Info> -- Suricata version 5.0.2 is up to date
cy5150@lab:~$
```

- **List the enabled sources list for rules in suricata-update.**

```
cy5150@lab:~$ sudo suricata-update list-enabled-sources
[sudo] password for cy5150:
1/4/2020 -- 19:24:01 - <Info> -- Using data-directory /var/lib/suricata.
1/4/2020 -- 19:24:01 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
1/4/2020 -- 19:24:01 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
1/4/2020 -- 19:24:01 - <Info> -- Found Suricata version 5.0.2 at /usr/bin/suricata.
Enabled sources:
  - et/open
  - oisf/trafficid
cy5150@lab:~$ _
```

Rules:

- **Write a rule to Detect Ping to 8.8.8.8.**

  The rule to detect ping to 8.8.8.8:
  alert icmp $HOME_NET any -> 8.8.8.8 any (msg:“8.8.8.8 ping”;flow:to_server; sid:1000002;)

```
cy5150@lab:~$ sudo tail /var/log/suricata/fast.log
03/31/2020-15:27:37.575598  [**] [1:2013028:4] ET POLICY curl User-Agent Outbound [**] [Classificati
on: Attempted Information Leak] [Priority: 2] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.575598  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.575922  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.599356  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:29:53.757013  [**] [1:2200024:2] SURICATA ICMPv4 unknown type [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 1.0.0.10:9 -> 224.0.0.1:0
03/31/2020-15:41:02.107623  [**] [1:1000003:0] facebook.com accessed [**] [Classification: (null)] [
Priority: 3] {TCP} 10.0.0.35:49940 -> 31.13.71.36:443
03/31/2020-15:41:52.065329  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:53.068052  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:54.069946  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:55.072291  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
```

- **Write a rule to alert on facebook access from home_net to external.**

  alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:“facebook.com accessed”; flow:to_server;content:“www.facebook.com”;sid:1000003;)

```
03/31/2020-15:27:37.575922  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.599356  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:29:53.757013  [**] [1:2200024:2] SURICATA ICMPv4 unknown type [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 1.0.0.10:9 -> 224.0.0.1:0
03/31/2020-15:41:02.107623  [**] [1:1000003:0] facebook.com accessed [**] [Classification: (null)] [
Priority: 3] {TCP} 10.0.0.35:49940 -> 31.13.71.36:443
cy5150@lab:~$ _
```

Screenshots of rules and alert generated:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Port 80 connection!";flow:to_server,established;si
d:1000001;)
alert icmp $HOME_NET any -> 8.8.8.8 any (msg:"8.8.8.8 ping";flow:to_server;sid:1000002;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"facebook.com accessed";flow:to_server;content:"ww
w.facebook.com";sid:1000003;)
~
~
```

```
cy5150@lab:~$ sudo tail /var/log/suricata/fast.log
03/31/2020-15:27:37.575598  [**] [1:2013028:4] ET POLICY curl User-Agent Outbound [**] [Classificati
on: Attempted Information Leak] [Priority: 2] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.575598  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.575922  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:27:37.599356  [**] [1:1000001:0] Port 80 connection! [**] [Classification: (null)] [Pr
iority: 3] {TCP} 10.0.0.35:55410 -> 31.13.71.36:80
03/31/2020-15:29:53.757013  [**] [1:2200024:2] SURICATA ICMPv4 unknown type [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 1.0.0.10:9 -> 224.0.0.1:0
03/31/2020-15:41:02.107623  [**] [1:1000003:0] facebook.com accessed [**] [Classification: (null)] [
Priority: 3] {TCP} 10.0.0.35:49940 -> 31.13.71.36:443
03/31/2020-15:41:52.065829  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:53.068052  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:54.069946  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
03/31/2020-15:41:55.072291  [**] [1:1000002:0] 8.8.8.8 ping [**] [Classification: (null)] [Priority:
 3] {ICMP} 10.0.0.35:8 -> 8.8.8.8:0
cy5150@lab:~$
```

Script:

Screenshot of rules used (test.rules):

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Well! What do you  know? H4x0r here!";flow:to_ser
ver;content:"HTTP/1.1";reference:url,www.google.com;reference:url,www.khoury.northeastern.edu;refere
nce:url,www.youtube.com;reference:url,blackboard.northeastern.edu;sid:1000001;)
```

Screenshot of alerts (fast.log):

```
03/31/2020-22:51:46.958878  [**] [1:1000001:0] Well! What do you  know? H4x0r here! [**] [Classifica
tion: (null)] [Priority: 3] {TCP} 10.0.0.35:60450 -> 172.217.12.196:80
03/31/2020-22:51:47.160129  [**] [1:1000001:0] Well! What do you  know? H4x0r here! [**] [Classifica
tion: (null)] [Priority: 3] {TCP} 10.0.0.35:47910 -> 52.70.229.197:80
03/31/2020-22:51:47.505215  [**] [1:1000001:0] Well! What do you  know? H4x0r here! [**] [Classifica
tion: (null)] [Priority: 3] {TCP} 10.0.0.35:48760 -> 172.217.9.238:80
03/31/2020-22:51:47.686899  [**] [1:1000001:0] Well! What do you  know? H4x0r here! [**] [Classifica
tion: (null)] [Priority: 3] {TCP} 10.0.0.35:41634 -> 34.226.166.216:80
cy5150@lab:~$ _
```

Suricata-Update:

- **What are the available sources in suricata-update?**

```
cy5150@lab:~$ sudo suricata-update list-sources | head -35
31/3/2020 -- 23:36:37 - <Info> -- Using data-directory /var/lib/suricata.
31/3/2020 -- 23:36:37 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/3/2020 -- 23:36:37 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/3/2020 -- 23:36:37 - <Info> -- Found Suricata version 5.0.2 at /usr/bin/suricata.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: ptresearch/attackdetection
  Vendor: Positive Technologies
  Summary: Positive Technologies Attack Detection Team ruleset
  License: Custom
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
cy5150@lab:~$
```

```
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/security
  Vendor: Secureworks
  Summary: Secureworks suricata-security ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: sslbl/ssl-fp-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: Non-Commercial
Name: sslbl/ja3-fingerprints
  Vendor: Abuse.ch
  Summary: Abuse.ch Suricata JA3 Fingerprint Ruleset
  License: Non-Commercial
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
  Summary: Etnetera aggressive IP blacklist
  License: MIT
Name: tgreen/hunting
  Vendor: tgreen
  Summary: Threat hunting rules
  License: GPLv3
cy5150@lab:~$ _
```

- **Screenshot of the list of enabled sources:**

```
31/3/2020 -- 23:45:05 - <Info> -- Dropped 0 rules.
31/3/2020 -- 23:45:05 - <Info> -- Enabled 149 rules for flowbit dependencies.
31/3/2020 -- 23:45:05 - <Info> -- Backing up current rules.
31/3/2020 -- 23:45:06 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 27
155; enabled: 20379; added: 0; removed 0; modified: 0
31/3/2020 -- 23:45:06 - <Info> -- No changes detected, exiting.
cy5150@lab:~$ sudo suricata-update list-enabled-sources
31/3/2020 -- 23:51:18 - <Info> -- Using data-directory /var/lib/suricata.
31/3/2020 -- 23:51:18 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/3/2020 -- 23:51:18 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/3/2020 -- 23:51:18 - <Info> -- Found Suricata version 5.0.2 at /usr/bin/suricata.
Enabled sources:
  - et/open
  - ptresearch/attackdetection
  - oisf/trafficid
cy5150@lab:~$ _
```

- **What is the name of the malware?**

  Name of the Malware: **ET malware Tinba Checkin**

```
04/01/2020-01:10:20.692252  [**] [1:2200078:2] SURICATA ICMPv4 invalid checksum [**] [Classification
: Generic Protocol Command Decode] [Priority: 3] {ICMP} 10.0.2.2:11 -> 10.0.2.15:0
04/01/2020-01:10:20.693801  [**] [1:2020568:5] ET MALWARE Tinba Checkin 3 [**] [Classification: Malw
are Command and Control Activity Detected] [Priority: 1] {TCP} 10.0.2.15:1611 -> 82.165.37.127:80
04/01/2020-01:10:20.694003  [**] [1:2020568:5] ET MALWARE Tinba Checkin 3 [**] [Classification: Malw
are Command and Control Activity Detected] [Priority: 1] {TCP} 10.0.2.15:1612 -> 82.165.37.127:80
cy5150@lab:~$
```

File Extraction:

Screenshot of the JSON file info created for the test.gif file:

```
cy5150@lab:/var/log/suricata$ sudo ls filestore/
00  0b  16  21  2c  37  42  4d  58  63  6e  79  84  8f  9a  a5  b0  bb  c6  d1  dc  e7  f2  fd
01  0c  17  22  2d  38  43  4e  59  64  6f  7a  85  90  9b  a6  b1  bc  c7  d2  dd  e8  f3  fe
02  0d  18  23  2e  39  44  4f  5a  65  70  7b  86  91  9c  a7  b2  bd  c8  d3  de  e9  f4  ff
03  0e  19  24  2f  3a  45  50  5b  66  71  7c  87  92  9d  a8  b3  be  c9  d4  df  ea  f5  tmp
04  0f  1a  25  30  3b  46  51  5c  67  72  7d  88  93  9e  a9  b4  bf  ca  d5  e0  eb  f6
05  10  1b  26  31  3c  47  52  5d  68  73  7e  89  94  9f  aa  b5  c0  cb  d6  e1  ec  f7
06  11  1c  27  32  3d  48  53  5e  69  74  7f  8a  95  a0  ab  b6  c1  cc  d7  e2  ed  f8
07  12  1d  28  33  3e  49  54  5f  6a  75  80  8b  96  a1  ac  b7  c2  cd  d8  e3  ee  f9
08  13  1e  29  34  3f  4a  55  60  6b  76  81  8c  97  a2  ad  b8  c3  ce  d9  e4  ef  fa
09  14  1f  2a  35  40  4b  56  61  6c  77  82  8d  98  a3  ae  b9  c4  cf  da  e5  f0  fb
0a  15  20  2b  36  41  4c  57  62  6d  78  83  8e  99  a4  af  ba  c5  d0  db  e6  f1  fc
cy5150@lab:/var/log/suricata$ sudo ls filestore/fe
cy5150@lab:/var/log/suricata$ cd
cy5150@lab:~$ sha256sum test.gif
b443dfe69fafed3e07f91f194a068fa678bc2afdc79d4bb571f6f836470e585f  test.gif
cy5150@lab:~$ cd /var/log/suricata/
cy5150@lab:/var/log/suricata$ sudo ls filestore/b4
b443dfe69fafed3e07f91f194a068fa678bc2afdc79d4bb571f6f836470e585f
b443dfe69fafed3e07f91f194a068fa678bc2afdc79d4bb571f6f836470e585f.1585719790.1.json
cy5150@lab:/var/log/suricata$ _
```

```
cy5150@lab:/var/log/suricata$ sudo cat filestore/b4/b443dfe69fafed3e07f91f194a068fa678bc2afdc79d4bb5
71f6f836470e585f.1585719790.1.json
{"timestamp": "2020-04-01T01:43:10.711557-0400", "flow_id": 1744858973590 31, "in_iface": "ens33", "e
vent_type": "fileinfo", "src_ip": "52.216.224.91", "src_port": 80, "dest_ip": "10.0.0.35", "dest_por
t": 51818, "proto": "TCP", "http": {"hostname": "s3.amazonaws.com", "url": "/edu.neu.cy5150/4b626c32
-7685-4a3b-8226-b6deb23b3a15/test.gif", "http_user_agent": "Wget/1.19.4 (linux-gnu)", "http_content_
type": "image/gif", "http_method": "GET", "protocol": "HTTP/1.1", "status": 200, "length": 19}, "app
_proto": "http", "fileinfo": {"filename": "/edu.neu.cy5150/4b626c32-7685-4a3b-8226-b6deb23b3a15/test
.gif", "sid": [100123], "gaps": false, "state": "CLOSED", "sha256": "b443dfe69fafed3e07f91f194a068fa
678bc2afdc79d4bb571f6f836470e585f", "stored": true, "size": 19, "tx_id": 0}}cy5150@lab:/var/log/suri
cata$ _
```

Screenshot of the rule to trigger when an .exe file is downloaded:

```
alert http any any -> any any (msg:"EXE Downloaded";fileext:"exe";filemagic:"PE32 executable";filest
ore;sid:100123;)
```

Screenshot of “fast.log”:

The alert highlighted in blue is generated by default for test1.exe and the alert highlighted in red is the alert configured in test.rules for the download of the actual exe file (which did not get triggered for the download of test1.exe).

```
cy5150@lab:~$ wget -q http://s3.amazonaws.com/edu.neu.cy5150/4b626c32-7685-4a3b-8226-b6deb23b3a15/ac
tual.exe
cy5150@lab:~$ sudo tail /var/log/suricata/fast.log
04/01/2020-13:36:26.678000  [**] [1:2027076:3] ET INFO Wget Request for Executable [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {TCP} 10.0.0.35:46788 -> 52.216.100.117:80
04/01/2020-13:36:26.678443  [**] [1:100123:0] EXE Downloaded [**] [Classification: (null)] [Priority
: 3] {TCP} 52.216.100.117:80 -> 10.0.0.35:46788
04/01/2020-13:36:26.678697  [**] [1:2013414:10] ET POLICY Executable served from Amazon S3 [**] [Cla
ssification: Potentially Bad Traffic] [Priority: 2] {TCP} 52.216.100.117:80 -> 10.0.0.35:46788
04/01/2020-13:36:26.734800  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [*
*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 52.216.100.117:80 ->
10.0.0.35:46788
04/01/2020-13:38:56.347239  [**] [1:2027076:3] ET INFO Wget Request for Executable [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {TCP} 10.0.0.35:48650 -> 52.217.32.22:80
04/01/2020-13:39:10.969679  [**] [1:2200024:2] SURICATA ICMPv4 unknown type [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 1.0.0.10:9 -> 224.0.0.1:0
04/01/2020-13:39:27.231563  [**] [1:2027076:3] ET INFO Wget Request for Executable [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {TCP} 10.0.0.35:60026 -> 52.216.138.221:80
04/01/2020-13:39:27.231862  [**] [1:100123:0] EXE Downloaded [**] [Classification: (null)] [Priority
: 3] {TCP} 52.216.138.221:80 -> 10.0.0.35:60026
04/01/2020-13:39:27.231926  [**] [1:2013414:10] ET POLICY Executable served from Amazon S3 [**] [Cla
ssification: Potentially Bad Traffic] [Priority: 2] {TCP} 52.216.138.221:80 -> 10.0.0.35:60026
04/01/2020-13:39:27.279218  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [*
*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 52.216.138.221:80 ->
10.0.0.35:60026
cy5150@lab:~$ _
```

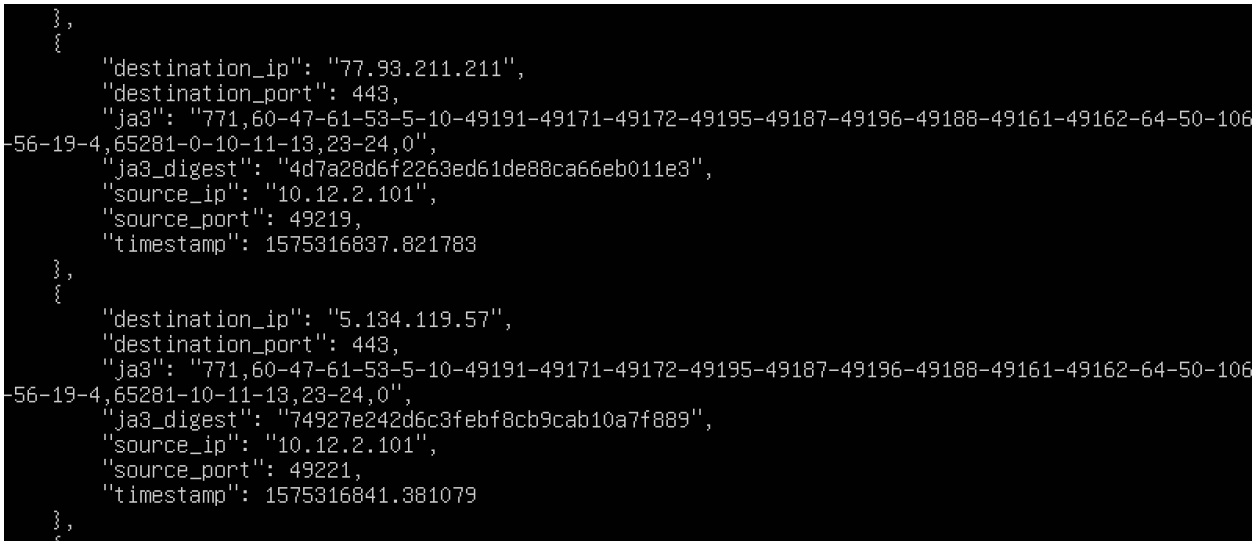
Screenshot of JSON file for actual.exe

```
cy5150@lab:~$ sha256sum actual.exe
cc3a2524d59445a5ae4e0f39bce25acfb94569c2d3d7b54f2e1eb803b71924e4  actual.exe
cy5150@lab:~$ cd /var/log/suricata/
cy5150@lab:/var/log/suricata$ sudo ls filestore/cc
cc3a2524d59445a5ae4e0f39bce25acfb94569c2d3d7b54f2e1eb803b71924e4
cc3a2524d59445a5ae4e0f39bce25acfb94569c2d3d7b54f2e1eb803b71924e4.1585761574.1.json
cy5150@lab:/var/log/suricata$ sudo cat filestore/cc/cc3a2524d59445a5ae4e0f39bce25acfb94569c2d3d7b54f
2e1eb803b71924e4.1585761574.1.json
{"timestamp": "2020-04-01T13:19:34.593907-0400", "flow_id": 1904357581153944, "in_iface": "ens33", "
event_type": "fileinfo", "src_ip": "52.216.19.19", "src_port": 80, "dest_ip": "10.0.0.35", "dest_por
t": 52400, "proto": "TCP", "http": {"hostname": "s3.amazonaws.com", "url": "/edu.neu.cy5150/4b626c32
-7685-4a3b-8226-b6deb23b3a15/actual.exe", "http_user_agent": "Wget/1.19.4 (linux-gnu)", "http_conten
t_type": "application/x-msdownload", "http_method": "GET", "protocol": "HTTP/1.1", "status": 200, "l
ength": 989744}, "app_proto": "http", "fileinfo": {"filename": "/edu.neu.cy5150/4b626c32-7685-4a3b-8
226-b6deb23b3a15/actual.exe", "sid": [100123], "magic": "PE32 executable (GUI) Intel 80386, for MS W
indows", "gaps": false, "state": "CLOSED", "sha256": "cc3a2524d59445a5ae4e0f39bce25acfb94569c2d3d7b5
4f2e1eb803b71924e4", "stored": true, "size": 989744, "tx_id": 0}}cy5150@lab:/var/log/suricata$
```

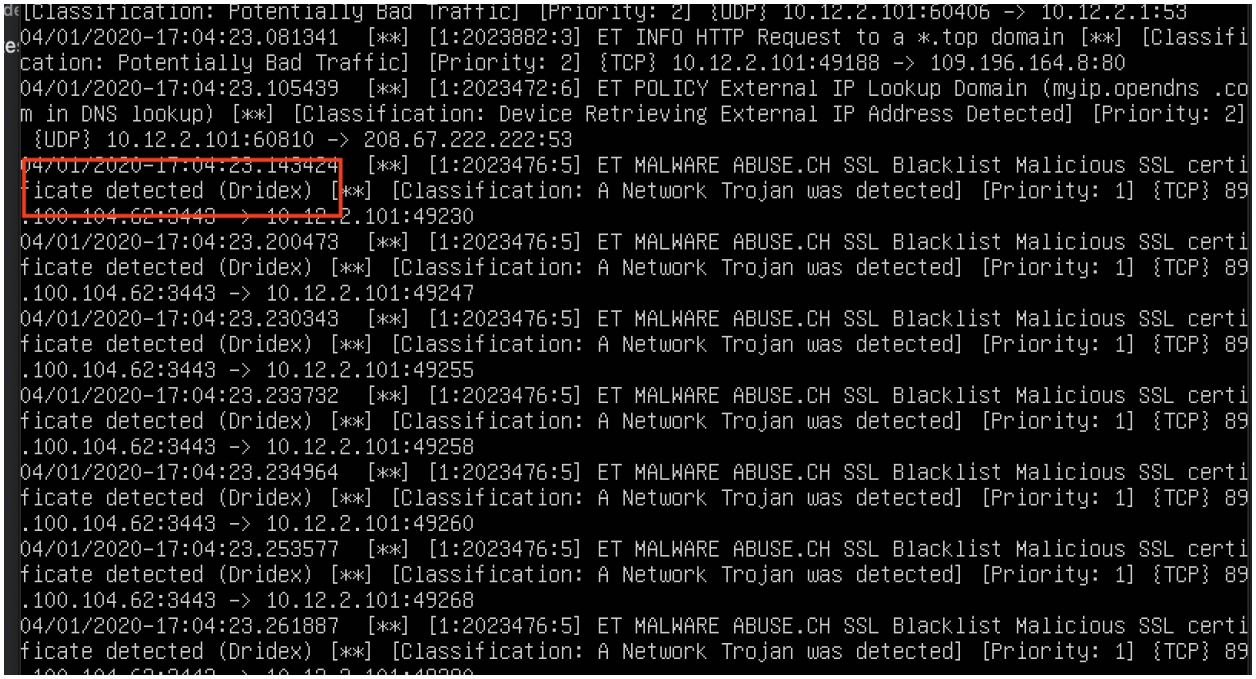
Bonus:

Rule to detect the malware:

For writing the rule, at first JA3 hash had to be determined. So, I gave test2.pcap as an input to JA3, which gave the hashes in the pcap file:



Running tcpreplay without any rule gave the first malware, i.e. **Dridex:**



After getting the JA3 hashes, following rule gave the other Malware:

```
alert tls any any -> any any (msg:"Look Look! I'm Here";ja3_hash;content:"4d7a28d6f2263ed61de88ca66e
b011e3";sid:2;)
#alert http any any -> any any (msg:"EXE Downloaded";fileext:"exe";filemagic:"PE32 executable";files
tore;sid:100123;)
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Activity";flow:to_server;content:"this looks fis
```

This rule gave the following alerts:

```
04/01/2020-19:02:45.646922  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49283 -> 194.61.1.178:443
04/01/2020-19:02:45.647445  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49284 -> 194.61.1.178:443
04/01/2020-19:02:45.647894  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49286 -> 194.61.1.178:443
04/01/2020-19:02:45.648558  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49287 -> 194.61.1.178:443
04/01/2020-19:02:45.649217  [**] [1:2023476:5] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certi
ficate detected (Dridex) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 85
.100.104.62:3443 -> 10.12.2.101:49289
04/01/2020-19:02:45.649507  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49290 -> 194.61.1.178:443
04/01/2020-19:02:45.650070  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49292 -> 194.61.1.178:443
04/01/2020-19:02:45.654613  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49293 -> 194.61.1.178:443
04/01/2020-19:02:45.655860  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49295 -> 194.61.1.178:443
04/01/2020-19:02:45.656637  [**] [1:2023476:5] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certi
ficate detected (Dridex) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 85
.100.104.62:3443 -> 10.12.2.101:49297
04/01/2020-19:02:45.657019  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49298 -> 194.61.1.178:443
04/01/2020-19:02:45.657306  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49299 -> 194.61.1.178:443
04/01/2020-19:02:45.658151  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49301 -> 194.61.1.178:443
04/01/2020-19:02:45.658428  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49302 -> 194.61.1.178:443
04/01/2020-19:02:45.661234  [**] [1:2:0] Look Look! I'm Here [**] [Classification: (null)] [Priority
: 3] {TCP} 10.12.2.101:49303 -> 194.61.1.178:443
04/01/2020-19:02:45.661865  [**] [1:2023476:5] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certi
ficate detected (Dridex) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 85
.100.104.62:3443 -> 10.12.2.101:49305
```

Since the hash gave an alert, hash was compared against the list of hashes given in the lab pdf and found out to be **Tofsee malware:**

2018-11-14 12:08:22	46efd49abcca8ea9baa932da68fdb529	Adware	359
2018-11-14 12:07:05	4d7a28d6f2263ed61de88ca66eb011e3	Tofsee	224
2018-11-14 12:06:56	b2b61db7b9490a60d270ccb20b462826	Adware	289
2018-11-14 12:02:57	92579701f145605e9edc0b01a901c6d5	Adware	296
2018-11-14 12:02:08	7691297bcb20a41233fd0a0baa0a3628	Adware	636

References:

[1] https://github.com/salesforce/ja3/tree/master/python
[2] https://sslbl.abuse.ch/ja3-fingerprints/
[3] https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967
[4] https://suricata.readthedocs.io/en/suricata-4.1.0/rules/ja3-keywords.html