

Suricata Intrusion Detection System

Adli Wahid
Senior Internet Security Specialist

APNIC Tutorial

Trainer Introduction

- Let's Connect!
- LinkedIn – Adli Wahid
- Instagram/Twitter @adliwahid
- Email: adli@apnic.net

Tutorial Agenda

- Topics

- Setting up and installation (on Ubuntu VM)
 - Configuration
 - Rule-set management
- Suricata in action – some use cases
- Signature/Rule Writing
- Integration with other security tools (Elasticsearch)
- Hands-on:
 - Lab Sheet
 - Need to ssh to our backend
 - Wireshark is recommended for Lab 5,6,7
- Materials: <https://tinyurl.com/kxvbht85>
- Reference: <https://wiki.apnictraining.net/ids-20210428-online>

Objectives

- High level overview of Suricata
 - Functionality
 - Features
 - Setup
- Threats / Detection
 - Contextual
 - Rules / Signatures
- Deploy, try or play!

Suricata Intrusion Detection System

- Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.
 - Engine!
- It is open source and owned by a community-run non-profit foundation, the Open Information Security Foundation (OISF).
- Suricata is developed by the OISF
- The Suricata source code is licensed under version 2 of the GNU General Public License

Suricata - History

- Beta release – Dec 2009
- First standard release – July 2010
- Features
 - Multi-threading
 - Automatic protocol detection
 - JSON standard outputs
 - file matching, logging, extraction, md5 checksum
 - DNS logger
 - etc

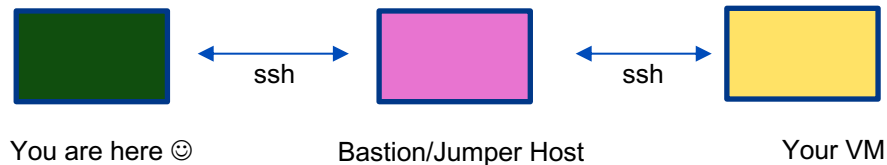
In a nutshell

- The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing
- Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats
- With standard input and output formats like YAML and JSON integrations with tools like existing SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other database become effortless

Accessing the Lab

Lab Overview – 1

- Suricata version 6.0.2
 - <https://suricata.readthedocs.io/en/suricata-6.0.2/>
- Virtual Machine
 - Ubuntu 20.04 LTS
 - 1 person per vm
 - Sign up
- Use native ssh client or Putty (for Windows)
 - Your network should let you ssh out (tcp/port 22)
 - Jump/Bastion host
 - Will use ssh tunneling, refer to relevant guide



Lab Overview - 2

- Sign up for your vm host
 - Put your name in there
 - Remember your IP 😊
 - Take note of your jump host IP address
- Check out steps to ssh in
 - Putty Users accessing_the_lab_putty.pdf
 - Native ssh client accessing_the_lab_ssh.pdf

Lab Overview – 3

- Credentials:
 - Username: apnic
 - Password: training
- Escalate privilege with *sudo*
 - Example:
 - `sudo systemctl status suricata`

Suricata Installation and Configuration

Installation

- We will install a couple of things
 - suricata
 - jq
 - evebox
- Refer to installation.pdf

System Check

- Suricata is already running as a service

`sudo systemctl status suricata`

`sudo systemctl stop suricata`

```
Terminal - analyst@nsm:~  
File Edit View Terminal Tabs Help  
analyst@nsm:~$ sudo systemctl status suricata  
[sudo] password for analyst:  
● suricata.service - LSB: Next Generation IDS/IPS  
   Loaded: loaded (/etc/init.d/suricata; generated)  
   Active: active (exited) since Wed 2020-06-10 08:05:35 AEST; 4min 29s ago  
     Docs: man:systemd-sysv-generator(8)  
  Process: 693 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)  
  
Jun 10 08:05:35 nsm systemd[1]: Starting LSB: Next Generation IDS/IPS...  
Jun 10 08:05:35 nsm suricata[693]: Starting suricata in IDS (af-packet) mode...  
Jun 10 08:05:35 nsm systemd[1]: Started LSB: Next Generation IDS/IPS.  
lines 1-9/9 (END)
```

Let's Play

- Download workshop.tar.gz in your vm
- `tar xzvf workshop.tar.gz`
- `cd workshop`

Lab1

- `cd ~/workshop/lab1`
- · Wannacry / Eternalblue
 - Credits to Malware Traffic Analysis
 - <https://www.malware-traffic-analysis.net/2017/05/18/index2.html>
 - 2017-05-18-WannaCry-ransomware-using-EnternalBlue-exploit.pcap
 - What is in the PCAP

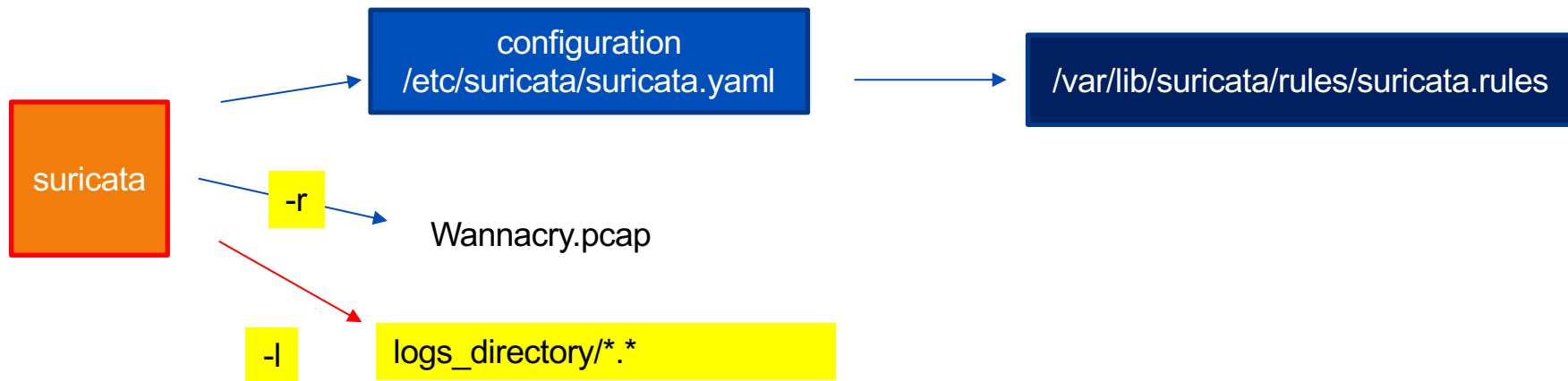
192.168.116.143 - a4:1f:72:20:54:01 - Windows 2012 R2 domain controller - TestDC1
192.168.116.150 - a4:1f:72:49:11:6d - Windows 2012 R2 server with a file share - WIN-2012-R2-1
192.168.116.138 - 00:19:bb:4f:4c:d8 - Windows 7 x64 - domain-joined workstation - DFIR_Win7_x64
192.168.116.149 - 00:25:b3:f5:fa:74 - Windows 7 x86 - domain-joined workstation - DFIR_Win7_x86 (wannacry launched here)
192.168.116.172 - 00:1c:c4:33:c6:dd - Windows 7 x86 - clone of DFIR_Win7_x86 - C-DFIR_Win7_x86

~/workshop/lab1\$

```
sudo suricata -r 2017-05-18-WannaCry-ransomware-using-  
InternalBlue-exploit.pcap -l logs -k none
```

- The directory “log” was already created
 - Else the logs will be in /var/log/suricata/
- -k none (no checksum checking)

Behind the 'scene'



If `-l` is not specified the logs will use configuration in `/etc/suricata/suricata.yaml` – normally `/var/log/suricata`
We can also specify which interface to monitor with `-i eth0` (example) or specifying it in `/etc/suricata/suricata.yaml`

Parsing the logs (the hard way 😊)

- cd logs

```
-rw-r--r-- 1 root  root   54K Jun  9 09:48 eve.json
```

```
-rw-r--r-- 1 root  root   3.3K Jun  9 09:48 fast.log
```

```
-rw-r--r-- 1 root  root   2.4K Jun  9 09:48 stats.log
```

```
-rw-r--r-- 1 root  root   1.6K Jun  9 09:48 suricata.log
```

- less fast.log

- (type Ctrl-C to get out of less 😊)

Parsing the logs (the hard way 😊) #2

- Inside ex1/logs
- `cat eve.json | jq . | less`
- `cat eve.json | jq 'select (.event_type == "alert")' | less`
- `cat eve.json | jq 'select (.event_type == "smb")' | less`

```
{
  "timestamp": "2017-05-18T18:06:21.120061+1000",
  "flow_id": 6188343065504,
  "pcap_cnt": 59,
  "event_type": "smb",
  "src_ip": "fe80:0000:0000:0000:ed6a:d848:6059:3c0e",
  "src_port": 49166,
  "dest_ip": "fe80:0000:0000:0000:6992:5661:9d0d:3f96",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 6,
    "dialect": "2.10",
    "command": "SMB2_COMMAND_TREE_CONNECT",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 114349209288709,
    "tree_id": 5,
    "share": "\\WIN-2012-R2-1\\Users",
    "share_type": "FILE"
  }
}
```


What's the story?

- Who is attacking who?
- Time
- Anything else?
- What was the vulnerability

Alerts & Signatures

- 05/18/2017-18:12:07.220702 [**] [1:2025649:3] **ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)** [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.116.149:49368 -> 192.168.116.138:445
- 05/18/2017-18:12:11.553081 [**] [1:2025650:3] **ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010** [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.116.172:445 -> 192.168.116.149:49444
- 05/18/2017-18:12:13.428436 [**] [1:2024217:3] **ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray** [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.116.149:49472 -> 192.168.116.138:445

cd /var/lib/suricata

- `grep -i "ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray" suricata.rules`
- `alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray"; flow:to_server,established; content:"|ff|SMB|33 00 00 00 00 18 07 c0 00 00 00 00 00 00 00 00 00 00 08 ff fe 00 08|"; offset:4; depth:30; fast_pattern:10,20; content:"|00 09 00 00 00 10|"; distance:1; within:6; content:"|00 00 00 00 00 00 10|"; within:8; content:"|00 00 00 10|"; distance:4; within:4; pcre:"/^[a-zA-Z0-9+/{1000,}/R"; threshold: type both, track by_src, count 3, seconds 30; metadata: former_category EXPLOIT; classtype:trojan-activity; sid:2024217; rev:3; metadata:attack_target SMB_Server, deployment Internal, signature_severity Critical, created_at 2017_04_17, updated_at 2017_05_13;)`

Lab 1 - Take Aways

- IDS provide context
 - What is the story
 - Known or unknown
 - Protocol aware
- Suricata must see traffic
 - Network interface
 - Feed it packets / Pcap
- What is the difference between Wireshark / Tcpdump vs Suricata

About rules – suricata-update

- Rulesets
 - Commercial and free rules
 - By default Open Emerging Threats rules included
- List of rulesets
 - `sudo suricata-update list-sources`
 - `sudo suricata-update list-enabled-sources`
- Update suricata-rules
 - `suricata-update`
- Automatic update
 - Use crontab to run `suricata-update` daily

Lab 2 – Dridex

~/workshop/lab2

- `cd ~/workshop/lab2`
- `sudo suricata -r 2019-07-09-password-protected-Word-doc-pushes-Dridex.pcap -l logs -k none`
 - Pcap from this files : <https://www.malware-traffic-analysis.net/2019/07/09/index.html>
- We'll use Evebox to parse the eve.json

```
· "timestamp": "2019-07-10T04:26:29.628847+1000",  
  "flow_id": 1226676421106482,  
  "pcap_cnt": 268,  
  "event_type": "alert",  
  "src_ip": "188.166.156.241",  
  "src_port": 443,  
  "dest_ip": "10.7.9.101",  
  "dest_port": 49205,  
  "proto": "TCP",  
  "alert": {  
    "action": "allowed",  
    "gid": 1,  
    "signature_id": 2023476,  
    "rev": 5,  
    "signature": "ET MALWARE ABUSE.CH SSL Blacklist Malicious  
SSL certificate detected (Dridex)",  
    "category": "A Network Trojan was detected",  
    "severity": 1,
```


What does the signature look like?

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL  
certificate detected (Dridex)"; flow:established,from_server; content:"|16|"; content:"|0b|"; within:8;  
byte_test:3,<,1200,0,relative; content:"|03 02 01 02 02 09 00|"; fast_pattern; content:"|30 09 06 03 55 04 06 13 02|";  
distance:0; pcre:"/^[A-Z]{2}/R"; content:"|55 04 07|"; distance:0; content:"|55 04 0a|"; distance:0; pcre:"/^{2}[A-Z][a-  
z]{3,}\s(?:[A-Z][a-z]{3,}\s)?(?:[A-Z](?:[A-Za-z]{0,4}?[A-Z])(?:\.?[A-Za-z]){1,3})|[A-Z]?[a-z]+|[a-z](?:\.?[A-Za-  
z]){1,3})\.?[01]/Rs"; content:"|55 04 03|"; distance:0; byte_test:1,>,13,1,relative; content:!"www."; distance:2; within:4;  
pcre:"/^{2}(?P<CN>(?:(?:\d?[A-Z]?[A-Z]?d?)(?:[a-z]{3,20}[a-z]{3,6}[0-9_][a-z]{3,6})\.){0,2}?(?:\d?[A-Z]?[A-Z]?d?)[a-  
z]{3,}(?:[0-9_][a-z]{3,})?\.(?!com|org|net|tv)[a-z]{2,9})[01].*?(?P=CN)[01]/Rs"; content:!"|2a 86 48 86 f7 0d 01 09 01|";  
content:!"GoDaddy"; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2023476; rev:5;  
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at  
2016_11_02, deployment Perimeter, performance_impact Low, signature_severity Major, tag SSL_Malicious_Cert,  
updated_at 2017_02_23;)
```

TLS / SSL client and server fingerprinting

- Encrypted communication
 - Suricata not able to perform full packet inspection / check application payload
 - Signature that goes into payload won't match
 - Some header information is still available
- Client and server TLS negotiation fingerprint
 - In a nutshell – TLS parameters combined -> md5
 - Both client and server
 - Confidence is in the manner response is in the same way
 - Multiple use-cases here
 - Client and server detection (malware, TOR, command and control, phishing sites etc)
- Ja3/ja3s developed by Salesforce
 - Integrated by Suricata
 - Abuse.ch has rulesets for TLS fingerprints
 - Ja3 = client , Ja3S = server
- Abuse.ch maintains an SSL blacklist repo
 - <https://sslbl.abuse.ch/blacklist/>
- Read more
 - <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967>
 - <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/inspecting-encrypted-network-traffic-with-ja3/>

<https://github.com/salesforce/ja3>

```
{
  "destination_ip": "188.166.156.241",
  "destination_port": 443,
  "ja3": "771,60-47-61-53-5-10-49191-49171-49172-49195-49187-49196-49188-49161-49162-64-50-106-56-19-4,65281-10-11-13,23-24,0",
  "ja3_digest": "74927e242d6c3feb8cb9cab10a7f889",
  "source_ip": "10.7.9.101",
  "source_port": 49205,
  "timestamp": 1562696789.50146
},
{
  "destination_ip": "188.166.156.241",
  "destination_port": 443,
  "ja3": "771,60-47-61-53-5-10-49191-49171-49172-49195-49187-49196-49188-49161-49162-64-50-106-56-19-4,65281-10-11-13,23-24,0",
  "ja3_digest": "74927e242d6c3feb8cb9cab10a7f889",
  "source_ip": "10.7.9.101",
  "source_port": 49206,
  "timestamp": 1562696791.350588
},
```

Optional, install ja3 &
run ja3 on the pcap
`$ja3 -a --json *pcap`

```
▼ Secure Sockets Layer
  ▼ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 131
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 127
      Version: TLS 1.0 (0x0301)
      ► Random
      Session ID Length: 0
      Cipher Suites Length: 24
      ▼ Cipher Suites (12 suites)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
        Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
        Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
```

```
{
  "destination_ip": "185.67.0.108",
  "destination_port": 443,
  "ja3": "769,49172-49171-53-47-49162-49161-56-50-10-19-5-4,0-5-10-11-65281,23-24-25,0",
  "ja3_digest":
  "1eede9d19dc45c2cb66d2f5c6849e843",
  "source_ip": "192.168.56.101",
  "source_port": 49161,
  "timestamp": 1527008276.377147
}
```

SSLVersion,Cipher,SSLExtension,EllipticCurve,EllipticCurvePointFormat -> string -> md5
echo -n “

Lab 2 - Take Aways

- Protocol analysis / Protocol aware
 - Do not have to specify the port
 - Web traffic not on port 80, ssh on 1337
 - Check out the supported protocols on Suricata documentation
- Signature
 - Contents of packets, headers not just plain text payload
 - TLS/ja3/ja3s
 - HASSH

Lab3 – Honeypots

Lab3

HOME_NET:

```
"[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12,45.76.116.172/32]"
```

- Our honeypot IP
 - 45.76.116.172
 - We should include this into our configuration file
\$HOME_NETWORK
 - Signature has direction, flow as criteria
- sudo suricata -r cowrie.pcap -l logs/ -k none
 - Verify logs in /logs
- Evebox
 - **evebox oneshot logs/eve.json**
 - Let's Explore
 - SSH
 - Alerts

Lab 3 - Take Aways

- IP/Domain Reputation
 - ET CINS Active Threat Intelligence Poor Reputation IP group 87
 - OSINT (open source intel)
 - Why is our hosts talking to a suspicious host, TOR exit node, malicious domain
 - VirusTotal, Dshield
 - <https://www.virustotal.com/gui/ip-address/92.118.160.57/reactions>
 - <https://www.dshield.org/ipinfo.html?ip=92.118.160.57>
- Suricata configuration
 - My network vs the world
- More Context
 - ALERT: ET MALWARE Possible Linux.Mirai Login Attempt (hi3518)
 - ET EXPLOIT HiSilicon DVR - Default Telnet Root Password Inbound

```
sudo less /var/lib/suricata/rules/suricata.rules | grep 2027973
```

- alert tcp \$EXTERNAL_NET any -> \$HOME_NET 23 (msg:"ET EXPLOIT HiSilicon DVR - Default Telnet Root Password Inbound"; flow:established,to_server; content:"xc3511"; fast_pattern; reference:url,github.com/tothi/pwn-hisilicon-dvr; classtype:default-login-attempt; sid:**2027973**; rev:2; metadata:affected_product DVR, attack_target IoT, created_at 2019_09_09, deployment Perimeter, former_category EXPLOIT, signature_severity Major, updated_at 2019_09_09;)

Lab 4 – File Extraction

Lab 4

- `cd ~/workshop/lab4`
- `sudo suricata -r 20202904.pcap -l logs -k none`
- *Evebox it* and explore
 - `evebox oneshot logs/eve.json`
- File extraction time!

File Extraction – Step 1

- Always read the docs!
 - <https://suricata.readthedocs.io/en/suricata-5.0.0/file-extraction/file-extraction.html>
 - Look for file-store in /etc/suricata/suricata.yaml
 - Use nano or vim to edit
 - Careful yaml files are sensitive

Default

```
- file-store:  
  version: 2  
  enabled: no
```

Change To

```
- file-store:  
  version: 2  
  enabled: yes
```

File Extraction Step 2

- Need to have as specific rule for this
- In ex4 folder create a file called extract.rule
- Copy the following rule:
 - alert http any any -> any any (msg:"FILE store all"; filestore; sid:1; rev:1;)
- Paste in extract.rule

File Extraction: Step 3

- Run Suricata with the extraction.rule

```
$sudo -r 20202904.pcap -l logs -S extract.rule -k none
```
- This should create a filestore directory inside logs
- Run the following to see the extracted files

```
$file */*
```
- See sample output in next slide

file */*

04/049431fab0d3461408345dd7ed70f9be994dc99dd56af2cd99f35a183cb9d859: **XZ compressed data**
06/067609f84812a154ef6c246e8b8cfbd4c7f6bba49450418227fa2acf523bba7b: **ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped**
1b/1bc56ca730194475721509e13c54a32005a6db2919f07eeacc46945c6e4b667f: **ASCII text**
20/206ad6aca45f12e07ede8032137b7536648b2b79302ed559df00d397e816432c: **Bourne-Again shell script, ASCII text executable**
34/34ed56e258232ea0be2d79f3eca3d09147f46880ce86c9da0c0473a1060669aa: **XZ compressed data**
36/366e3fbe8767805b2efb5b0df28d151b806c7e140ae53c57cacd390af2df11cf: **XZ compressed data**
4a/4a8389496b4f0fb164444fbd36ecd4cf38c3dd62c2bf190f20d937e605c3db73: **ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped**
69/690bd875ab5799394af7406f32f2e698c48e772ac367d520f74ec1095662da4d: **ASCII text**
97/97c42ab6f8c385658eed005846a9618d32fbaf4bcb5376ad863476ae21df8ffe: **XZ compressed data**
9e/9e3f14260ac0e015756468f191da390910c20117de8730e189613ca61429961a: **ASCII text**
cd/cd888ded56c3882397edf3c28376fee3134d45537826de9dc437cf57837d2c43: **Debian binary package (format 2.0)**
d0/d043d8bb305d66cf6b64b0e7ff48c84182c55697b91326f988eb9db0581eb831: **ASCII text**
da/da7d093bae12980e3e8b2e27318a6997831fbc5999d5d128942cb9b521aafcdf: **XZ compressed data**
e7/e7805f20300d402d030f1fef536b4267117f4d5bcc6c95664ff3adde93d88628: **Bourne-Again shell script, ASCII text executable**

Try

- less 20/206ad6aca45f12e07ede8032137b7536648b2b79302ed559df00d397e816432c
- Go to [virustotal.com](https://www.virustotal.com)
 - Search for **4a8389496b4f0fb164444fbd36ecd4cf38c3dd62c2bf190f20d937e605c3db73**

Take Aways

- File Extraction
 - Supported protocols http, smb, nfs, smtp, ftp
 - A few use cases – store all, certain md5sum, certain extension
 - Rule required to trigger extraction
- -S and -s
 - -S exclusively run this rule file ignore settings in suricata.yaml
 - -s run this rule file and the one mentioned in suricata.yaml
- Context
 - File reputation
 - Malware databases
 - Sites like virustotal.com and a few others can give context
 - Tools like TheHive allows to make query to multiple places

Wazuh

>	Dec 3, 2020 @ 07:14:44.721	/etc/hosts	modified	Integrity checksum change d.	7	550
>	Dec 3, 2020 @ 07:14:44.703	/etc/cups/subscriptions.conf.0	modified	Integrity checksum change d.	7	550
>	Dec 2, 2020 @ 23:06:53.279	/etc/test	modified	Integrity checksum change d.	7	550

```
f agent.id          001

f agent.ip          10.0.2.4

f agent.name        osboxes

f decoder.name      syscheck_integrity_changed

f full_log          ✓

File '/etc/hosts' modified
Mode: whodata
Changed attributes: size,mtime,inode,md5,sha1,sha256
Size changed from '300' to '289'
Old modification time was: '1606913905', now it is '1606943464'
Old inode was: '666413', now it is '666686'
Old md5sum was: '87e08d6373633640e86bc3245ae6b8ef'
New md5sum is : '469d03062b0040eeec2099cd186b629c'
Old sha1sum was: '95d575350dde6614dbed0cdc3f297270d125a745'
New sha1sum is : '2e51d84da6d581b88f574523bff580622097462b'
Old sha256sum was: '53a3753652e533711d9863645563eaa51dba77181fd1b404f9290980201ee070'
New sha256sum is : '9ddca8a95247329d1a652fe4b1932fb9493dfec5bbe89b520e57961b0e02d262'

f id                1606943684.83166639
```

```
f syscheck.changed_attributes  size, mtime, inode, md5, sha1, sha256

f syscheck.diff               4d3
                               < 7.7.7.7                vpn.my.home.xyz
                               6a6,7
                               > 5.5.5.5                test
                               >

f syscheck.event              modified

f syscheck.gid_after          0
```

Part 2 - Writing Suricata Signatures

Overview

- Suricata can dissect packets & is protocol aware
- Rules are applied against content of packets & protocol related information
 - do something (alert) if packet contains the word “ransom=“
 - do something (alert) if http traffic & http method is POST and content of packet has the word “ransom”
 - do something (alert) if there is dns request
 - do something (drop) if there is dns request and the record asked is ‘ransomware.com’

General Workflow

- Traffic
 - PCAP
 - Generate network activity on host
 - ping hostname.com
 - dig A apnic.net
 - wget <http://www.testmyids.com>
- Malware Analysis
 - Look for interesting strings & behavior
 - User agent, check-in command, file names, etc
 - Malware-traffic-analysis.net
- Get indicators of compromise from reports, advisories, threat sharing platform (i.e. MISP)
- Write signature
- Test signature
 - suricata -S rulefile -r file.pcap -l logdirectory -k none
 - suricata -S rulefile -i eth0 -l logdirectory -k none
 - -S load signature file exclusively
- Additional notes
 - Take note of the ip address to include in \$HOME_NET in /etc/suricata/suricata.yaml
 - Check pcap or interface

Signature writing use cases

- You know what you're looking for
 - Write specific rule
- Payload specific
 - Alert if packet contains xyz
 - Alert if packet contains IP address from known IOCs
 - Alert if there is telnet traffic to IP address in country XYZ
 - Alert if TLS fingerprint == XYZ
- Not payload specific
 - Alert if there is outbound ssh traffic
 - Alert if EXTERNAL_NET is a Tor Exit Node

Read the Docs

- Beware of out-of-date tutorials on the Internet

<https://suricata.readthedocs.io/en/suricata-6.0.2/file-extraction/file-extraction.html>

Rule Format

- There's 3 parts to it

Action **Header** (**Options**)

alert **tcp** **\$HOME_NET** **any** **->** **\$EXTERNAL_NET** **any** (**msg: "AW Suspicious Traffic "**; **sid:99999**; **rev:1**;

- Action – what happens when signature matches
- Header – defines protocol, IP address, ports and direction of the rule
- Rule Options – define the specifics of the rule. Can be specific to the protocol/action/payloads or metadata.
 - We won't be able to cover everything!

Hello World Rule

```
alert tcp any any -> any any (msg:"AW Hello World TCP"; sid:202010000; rev:1;)
```

```
sudo suricata -S myrule -i eth0 -k none -l logs
```

```
cat logs/fast.log
```

```
evebox one shot logs/eve.json
```

Hello World ICMP or UDP

alert any any -> any any (msg:"AW Hello World ICMP"; sid:202010001; rev:1;)

alert \$HOME_NETWORK any -> \$EXTERNAL_NETWORK any (msg:"AW Hello World UDP";
sid:202010002; rev:1;)

Lab 5 – Signature

cd ~/workshop/lab5

- Optional: open testmyidsPCAP in Wireshark
- Check content of http

Time	Source	Src Port	Destination	Dst Port	Host	Info
0.188443	10.16.1.11	54186	82.165.177.154	80	www.testmyids.com	GET / HTTP/1.1
0.376629	82.165.177.154	80	10.16.1.11	54186		HTTP/1.1 200 OK (text/html)

▶ Frame 6: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits)
 ▶ Ethernet II, Src: IntelCor_0d:06:f7 (00:15:17:0d:06:f7), Dst: Micro-St_ed:a1:46 (d8:cb:8a:ed:a1:46)
 ▶ Internet Protocol Version 4, Src: 82.165.177.154, Dst: 10.16.1.11
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54186, Seq: 1, Ack: 82, Len: 259
 ▼ **Hypertext Transfer Protocol**
 ▶ HTTP/1.1 200 OK\r\n
 Date: Wed, 13 Jul 2016 22:42:07 GMT\r\n
 Server: Apache\r\n
 Last-Modified: Mon, 15 Jan 2007 23:11:55 GMT\r\n
 ETag: "181c849a-27-4271c5f1ac4c0"\r\n
 Accept-Ranges: bytes\r\n
 Content-Length: 39\r\n
 Content-Type: text/html\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.188186000 seconds]
 [Request in frame: 4]
 [Request URI: http://www.testmyids.com/]
 File Data: 39 bytes
 ▼ Line-based text data: text/html (1 lines)
 uid=0(root) gid=0(root) groups=0(root)\n

```

0000 d8 cb 8a ed a1 46 00 15 17 0d 06 f7 08 00 45 00 .....F.....E
0010 01 2b 54 73 40 00 31 06 e4 ff 52 a5 b1 9a 0a 10 ..+Ts@1...R....
0020 01 0b 00 50 d3 aa 97 e6 d2 27 7a c8 a8 0f 50 18 ...P.....'z...P
0030 01 4b c0 0b 00 00 48 54 54 50 2f 31 2e 31 20 32 ...K...HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK..D ate: Wed
0050 2c 20 31 33 20 4a 75 6c 20 32 30 31 36 20 32 32 , 13 Jul 2016 22
0060 3a 34 32 3a 30 37 20 47 4d 54 0d 0a 53 65 72 76 :42:07 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 4c 61 73 74 er: Apac he..Last
0080 2d 4d 6f 64 69 66 69 65 64 3a 20 4d 6f 6e 2c 20 -Modifie d: Mon,
0090 31 35 20 4a 61 6e 20 32 30 30 37 20 32 33 3a 31 15 Jan 2 007 23:1
00a0 31 3a 35 35 20 47 4d 54 0d 0a 45 54 61 67 3a 20 1:55 GMT ..ETag:
00b0 22 31 38 31 63 38 34 39 61 2d 32 37 2d 34 32 37 "181c849 a-27-427
00c0 31 63 35 66 31 61 63 34 63 30 22 0d 0a 41 63 63 1c5f1ac4 c0"...Acc
00d0 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ept-Rang es: byte
00e0 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 s..Conte nt-Lengt
00f0 68 3a 20 33 39 0d 0a 43 6f 6e 74 65 6e 74 2d 54 h: 39..C ontent-T
0100 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a ype: tex t/html..
0110 0d 0a 75 69 64 3d 30 28 72 6f 6f 74 29 20 67 69 ..uid=0( root) gi
0120 64 3d 30 28 72 6f 6f 74 29 20 67 72 6f 75 70 73 d=0(root ) groups
0130 3d 30 28 72 6f 6f 74 29 0a =0(root) .
  
```

content: uid=0(root) gid=0(root) groups=0(root)

content: www.testmyids.com

(External) IP Address: 82.165.177.154

Basic Rule

```
alert http any any -> any any (msg:"AW - Suspicious Root  
Privilege"; content: "uid=0(root) gid=0(root) groups=0(root)";  
sid:202010004; rev:1;)
```


Take Aways

- Signature should be specific
 - Use parameters, pattern matching etc
 - Think of false positives
 - Alert fatigue, Counter productive
 - Validate the IOCs thoroughly
- Classification and priority
 - Classification
 - Classification.config
 - The classification.config file includes information for prioritizing rules
 - Any rule can override it

```
/var/lib/suricata/rules/classification.config
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
```

Lab 6 - Trickbot

Lab6

- Trickbot
 - <https://attack.mitre.org/software/S0266/>
 - <https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/>
 - Pcap 2020-02 from Malware-traffic-analysis.net - <https://www.malware-traffic-analysis.net/2020/02/25/index.html>
- Uses TLS/SSL to communicate with server on port 449 and 447

TLS activities over port 449 – Internet Wdigts Pty LTD

2020-02-25-Trickbot-gtag-red4-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl.handshake.type == 11

Expression... +

Time	Source	Src Port	Destination	Dst Port	Host	Info
2020-02-26 03:15:10.839499	45.138.72.155	443	10.22.33.145	49797		Server Hello, Certificate
2020-02-26 03:15:53.898396	45.138.72.155	443	10.22.33.145	49798		Server Hello, Certificate
2020-02-26 03:16:37.111706	45.138.72.155	443	10.22.33.145	49799		Server Hello, Certificate
2020-02-26 03:17:20.764853	45.138.72.155	443	10.22.33.145	49800		Server Hello, Certificate
2020-02-26 03:18:03.749892	45.138.72.155	443	10.22.33.145	49801		Server Hello, Certificate
2020-02-26 03:18:46.853258	45.138.72.155	443	10.22.33.145	49802		Server Hello, Certificate
2020-02-26 03:19:31.125313	45.138.72.155	443	10.22.33.145	49803		Server Hello, Certificate
2020-02-26 03:20:14.125783	45.138.72.155	443	10.22.33.145	49804		Server Hello, Certificate
2020-02-26 03:20:57.149743	45.138.72.155	443	10.22.33.145	49806		Server Hello, Certificate
2020-02-26 03:21:40.221805	45.138.72.155	443	10.22.33.145	49808		Server Hello, Certificate
2020-02-26 03:22:23.241726	45.138.72.155	443	10.22.33.145	49810		Server Hello, Certificate
2020-02-26 03:22:54.115286	190.214.13.2	449	10.22.33.145	49811		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 03:23:06.264716	45.138.72.155	443	10.22.33.145	49813		Server Hello, Certificate
2020-02-26 03:23:49.278387	45.138.72.155	443	10.22.33.145	49814		Server Hello, Certificate
2020-02-26 03:24:32.381877	45.138.72.155	443	10.22.33.145	49815		Server Hello, Certificate
2020-02-26 03:25:15.412384	45.138.72.155	443	10.22.33.145	49820		Server Hello, Certificate
2020-02-26 03:25:58.892705	45.138.72.155	443	10.22.33.145	49821		Server Hello, Certificate
2020-02-26 03:26:41.816539	45.138.72.155	443	10.22.33.145	49822		Server Hello, Certificate
2020-02-26 03:27:24.796997	45.138.72.155	443	10.22.33.145	49823		Server Hello, Certificate
2020-02-26 03:28:07.768397	45.138.72.155	443	10.22.33.145	49827		Server Hello, Certificate

signature (sha256WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)

issuer: rdnSequence (0)
rdnSequence: 3 items (id-at-organizationName=Internet Wdigts Pty Ltd,id-at-stateOrProvinceName=Some-State,id-at-county=Some-County)
 rdnSequence item: 1 item (id-at-countryName=AU)
 rdnSequence item: 1 item (id-at-stateOrProvinceName=Some-State)
 rdnSequence item: 1 item (id-at-organizationName=Internet Wdigts Pty Ltd)

validity
 notBefore: utcTime (0)
 notAfter: utcTime (0)

subject: rdnSequence (0)
rdnSequence: 3 items (id-at-organizationName=Internet Wdigts Pty Ltd,id-at-stateOrProvinceName=Some-State,id-at-county=Some-County)
 rdnSequence item: 1 item (id-at-countryName=AU)
 rdnSequence item: 1 item (id-at-stateOrProvinceName=Some-State)
 rdnSequence item: 1 item (id-at-organizationName=Internet Wdigts Pty Ltd)

subjectPublicKeyInfo
algorithm (rsaEncryption)
Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey: 3082010a028201010e14ae691039f5b836749c3136e0d19...
 modulus: 0x00e14ae691039f5b836749c3136e0d192cd2362e05a3488c...
 publicExponent: 65537

extensions: 2 items

00b0 05 00 30 45 31 b0 30 09 06 03 55 04 06 13 02 41 ... 00E1 0...U...A

00c0 55 31 13 30 11 06 03 55 04 08 0c 0a 53 6f 6d 65 ... 1 0...U...Some

00d0 20 53 74 61 74 65 31 21 30 1f 06 03 55 04 0a 0c ... -State1! 0...U...

00e0 18 49 6e 74 65 72 6e 65 74 20 57 69 64 67 69 74 ... -Interne t Wdgit

00f0 73 20 50 74 79 20 4c 74 64 30 1e 17 0d 31 39 31 ... s Pty Lt d0...191

0100 32 31 32 31 33 31 34 34 33 5a 17 0d 32 30 31 32 ... 21213144 3Z...2012

0110 31 31 31 33 31 34 34 33 5a 30 45 31 0b 30 09 06 ... 11131443 Z0E1-0...

0120 03 55 04 06 13 02 41 55 31 13 30 11 06 03 55 04 ... -U... AU 1-0...U-

0130 08 0c 0a 53 6f 6d 65 2d 53 74 61 74 65 31 21 30 ... -Some- State1!0

0140 1f 06 03 55 04 0a 0c 18 49 6e 74 65 72 6e 65 74 ... -U... Internet

0150 20 57 69 64 67 69 74 73 20 50 74 79 20 4c 74 64 ... Wdigts Pty Ltd

0160 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 ... 0...0... *H...

0170 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 ... 0...0...

0180 00 e1 4a e6 91 03 9f 5b 83 67 49 c3 13 6e 0d 19 ... -J...[gI...n...

0190 2c d2 36 2e 05 a3 48 8c 5f ca 33 e6 56 b4 6e 9b ... , 6...H...-3 V...n...

01a0 6f a7 94 46 fa f0 41 49 3b 01 5d 21 b1 e3 b6 d1 ... o...F...AI...;...!...

01b0 f8 59 cc d5 be a8 25 2e 91 38 28 df 2b 63 4f fb ... -6n...%, 8(+c0...

01c0 f6 a5 36 6e d4 b8 e6 ce 10 eb e1 bc ae 14 a8 17 ... -6n...%, 8(+c0...

01d0 26 5e 3e 6a af bc db db c2 8c 6f 8e 95 60 a2 82 ... &^>j...-o...n...

01e0 98 03 8e cf 71 89 b0 26 3c af 64 5f d8 45 45 28 ... -Y...q...&...<d...EE(

01f0 ab ee c4 17 b8 7a d1 89 08 99 71 63 18 b3 6d fa ... -Z...-qc...m...

0200 4d 2f 5e 04 1f dd 8a 85 3d b9 9c b0 1a 83 0d f8 ... M/A...=...

“Global Security” and “IT Department”

Time	Source	Src Port	Destination	Dst Port	Host	Info
2020-02-26 03:28:36.786937	5.2.77.18	447	10.22.33.145	49884		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 03:57:33.344929	5.2.77.18	447	10.22.33.145	49709		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 04:11:29.694310	5.2.77.18	447	10.22.33.145	49764		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 04:30:30.432909	66.85.173.20	447	10.22.33.145	50657		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 04:39:02.444681	66.85.173.20	447	10.22.33.145	50662		Server Hello, Certificate, Server Key Exchange, Server Hello Done

```

▶ issuer: rdnSequence (0)
▶ validity
▼ subject: rdnSequence (0)
  ▼ rdnSequence item: 1 item (id-at-commonName=example.com,id-at-organizationalUnitName=IT Department,id-at-organizationName=example.com)
    ▼ RDNSequence item: 1 item (id-at-countryName=GB)
      ▼ RelativeDistinguishedName item (id-at-countryName=GB)
        Id: 2.5.4.6 (id-at-countryName)
        CountryName: GB
      ▼ RDNSequence item: 1 item (id-at-stateOrProvinceName=London)
        ▼ RelativeDistinguishedName item (id-at-stateOrProvinceName=London)
          Id: 2.5.4.8 (id-at-stateOrProvinceName)
          ▼ DirectoryString: uTF8String (4)
            uTF8String: London
        ▼ RDNSequence item: 1 item (id-at-localityName=London)
          ▼ RelativeDistinguishedName item (id-at-localityName=London)
            Id: 2.5.4.7 (id-at-localityName)
            ▼ DirectoryString: uTF8String (4)
              uTF8String: London
          ▼ RDNSequence item: 1 item (id-at-organizationName=Global Security)
            ▼ RelativeDistinguishedName item (id-at-organizationName=Global Security)
              Id: 2.5.4.10 (id-at-organizationName)
              ▼ DirectoryString: uTF8String (4)
                uTF8String: Global Security
            ▼ RDNSequence item: 1 item (id-at-organizationalUnitName=IT Department)
              ▼ RelativeDistinguishedName item (id-at-organizationalUnitName=IT Department)
                Id: 2.5.4.11 (id-at-organizationalUnitName)
                ▼ DirectoryString: uTF8String (4)
                  uTF8String: IT Department
              ▼ RDNSequence item: 1 item (id-at-commonName=example.com)
                ▼ RelativeDistinguishedName item (id-at-commonName=example.com)
                  Id: 2.5.4.3 (id-at-commonName)
                  ▼ DirectoryString: uTF8String (4)
                    uTF8String: example.com
            ▶ subjectPublicKeyInfo
            ▶ extensions: 3 items
            ▶ algorithmIdentifier (sha256WithRSAEncryption)
              padding: 0
              encrypted: 683474e7cea5148cbccfffececc146146e8e9b7f43efaf...
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

```



Rules

· alert **tls** \$EXTERNAL_NET any -> \$HOME_NET any
(msg:"AW – Selfsigned TLS Certificate"; **tls.cert_issuer**;
content:"Internet Widgits Pty Ltd"; sid:10008; rev:1;)

alert **tls** \$EXTERNAL_NET any -> \$HOME_NET any
(msg:"AW - Trickbot CNC"; **tls.cert_issuer**; content:"Global
Security"; content:"IT Department"; sid:10009; rev:1;)

ja3 and ja3s

- Ja3 – method for profiling TLS/SSL clients
 - Clients - browser agents, malware, etc
 - Internal -> External
- Ja3s – method for profiling TLS/SSL servers
 - Command and Control, Services, Websites
- Fingerprints are based on configurations and details of TLS/SSL handshakes*
 - Not encrypted i.e ClientHello
 - SSLVersion,Cipher,SSLExtension,EllipticCurve,EllipticCurvePointFormat
 - 769,4-5-10-9-100-98-3-6-19-18-99,,,
 - 769,4-5-10-9-100-98-3-6-19-18-99,,, --> de350869b8c85de67a350c8d186f11e6
- <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967>

ssl

Expression...

Time	Source	Src Port	Destination	Dst Port	Host	Info
2020-02-26 03:22:23.243812	10.22.33.145	49810	45.138.72.155	443		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:22:23.462300	45.138.72.155	443	10.22.33.145	49810		New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:22:23.463375	10.22.33.145	49810	45.138.72.155	443		Application Data
2020-02-26 03:22:23.680809	45.138.72.155	443	10.22.33.145	49810		Application Data
2020-02-26 03:22:28.686738	10.22.33.145	49810	45.138.72.155	443		Encrypted Alert
2020-02-26 03:22:53.766771	10.22.33.145	49811	190.214.13.2	449		Client Hello
2020-02-26 03:22:54.155286	190.214.13.2	449	10.22.33.145	49811		Server Hello, Certificate, Server Key Exchange, Server Hello Done
2020-02-26 03:22:54.160734	10.22.33.145	49811	190.214.13.2	449		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:22:54.482966	190.214.13.2	449	10.22.33.145	49811		New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:22:54.510059	10.22.33.145	49811	190.214.13.2	449		Application Data, Application Data
2020-02-26 03:23:05.502485	190.214.13.2	449	10.22.33.145	49811		Application Data
2020-02-26 03:23:05.659806	10.22.33.145	49811	190.214.13.2	449		Application Data, Application Data
2020-02-26 03:23:06.034943	10.22.33.145	49813	45.138.72.155	443		Client Hello
2020-02-26 03:23:06.264716	45.138.72.155	443	10.22.33.145	49813		Server Hello, Certificate
2020-02-26 03:23:06.264747	45.138.72.155	443	10.22.33.145	49813		Server Key Exchange, Server Hello Done
2020-02-26 03:23:06.267028	10.22.33.145	49813	45.138.72.155	443		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:23:06.491577	45.138.72.155	443	10.22.33.145	49813		New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2020-02-26 03:23:06.492898	10.22.33.145	49813	45.138.72.155	443		Application Data
2020-02-26 03:23:06.720499	45.138.72.155	443	10.22.33.145	49813		Application Data
2020-02-26 03:23:11.726246	10.22.33.145	49813	45.138.72.155	443		Encrypted Alert

▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 147

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 143

Version: TLS 1.2 (0x0303)

Random: 5e5557eda787e849b31e6ac9be8d587f4e20ca7f430c87b5...

Session ID Length: 0

Cipher Suites Length: 38

Cipher Suites (19 suites)

Compression Methods Length: 1

Compression Methods (1 method)

Extensions Length: 64

Extension: status_request (len=5)

Extension: supported_groups (len=8)

Extension: ec_point_formats (len=2)

Extension: signature_algorithms (len=20)

Extension: SessionTicket TLS (len=0)

Extension: extended_master_secret (len=0)

Extension: renegotiation_info (len=1)

0000 20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00 ...G...E

0010 00 c0 f6 b9 40 00 80 06 0b ff 0a 16 21 91 be d6 ...@...!...

0020 0d 02 c2 93 01 c1 13 13 15 7f 02 2b 23 e4 50 18 ...+...P...

0030 fa f0 5f 9b 00 00 16 03 03 00 93 01 00 00 8f 93

0040 0e 5e 55 57 ed a7 87 e8 49 b3 1e 6a c9 be d8 58 ...AUN...I..j...X

0050 7f 4e 20 ca 7f 43 0c 87 b5 43 23 4d fa be de 38 ...N..C..C#M...-8...

0060 ab 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 ...&...+.../...\$...#

0070 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c ...(.

0080 00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 40 00 05 ...=<.5./...@...

0090 00 05 01 00 00 00 00 00 0a 00 08 00 06 00 1d 00

00a0 17 00 18 00 0b 00 02 01 00 00 0d 00 14 00 12 04

00b0 01 05 01 02 01 04 03 05 03 02 03 02 02 06 01 06

00c0 03 00 23 00 00 00 17 00 00 ff 01 00 01 00 ...#...

Maximum version supported by client (ssl.handshake.version), 2 bytes

Packets: 17227 · Displayed: 1953 (11.3%)

Profile: Default

APNIC


68

Ja3

Generate ja3 has with ja3 tool

- Check out ja3.json in your folder

Let's search for the client information on ja3er

- 3b5074b1b5d032e5620f69f9f700ff0e
- 72a589da586844d7f0818ce684948eea

Check out more information here: <https://ja3er.com/>

Rule

```
· alert tls $HOME_NET any -> $EXTERNAL_NET any  
(msg:"AW - Trickbot Infection"; ja3.hash;  
content:"72a589da586844d7f0818ce684948eea"; sid:10010;  
rev:1; )
```

Integration

Integration

- Reality on security monitoring & incident response
 - Lots of tools
 - Integrate data from various sources
 - Automation!
- We'll take a look at:
 - Sending Suricata logs to ElasticSearch
 - Generating Suricata Signatature from indicators with MISP

Lab 7 - ElasticSearch

Basic Idea

- Setup Elasticsearch instance
 - We'll use the free edition
 - <https://cloud.elastic.co/registration?fromURI=%2Fhome>
 - Create an instance, get username and password – log into instance
- Install filebeat (logshipper) on our vm
 - Configure ES settings
 - Configure path for reading logs
- We run this as a service, the logs get into Elasticsearch
- The Security section will have relevant screenshots

SIEM Take Aways

- SIEM
 - Visualisation
 - Searchability / Visibility
 - Forensics
 - Alerting
 - i.e. to Slack with elastAlert
 - Integrate with other data sources
 - Integrate data from other Suricata sensors
- Consideration
 - Architecture
 - Storage
 - Log retention policy etc

Also Check Out

- <https://www.stamus-networks.com/scirius-open-source>



What do you want to do with the Elastic Stack?

Let us know what your use case is and we'll help you get started with Elasticsearch, Kibana and the full Elastic Stack.

[Learn more](#)



General purpose

Not sure what you want? Choose this option, and there'll be help along the way.

Select



Enterprise Search

Add a search experience to your website, applications, or search the apps you use at work.

Select



Observability

Use logs, metrics, and APM data to monitor and react to events in your environment.

Select



Security

Prevent, detect, and respond to threats with SIEM, endpoint security, and threat hunting.

✓ Selected

BUILD MY OWN

START WITH A USE CASE

Settings

Choose the cloud provider, region, and Elastic Stack version.

[Collapse](#) ▾

Cloud provider

Pick a cloud and let us handle the rest. No additional accounts required.



Google Cloud



Azure



Amazon Web
Services

Region



New South Wales (australiaeast)



[announcement blog post](#).

Getting Started

macOS

DEB

RPM

Windows

1 Download and install Filebeat

First time using Filebeat? See the [Quick Start](#).

[Copy snippet](#)

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.12.1-amd64.deb
sudo dpkg -i filebeat-7.12.1-amd64.deb
```

Looking for the 32-bit packages? See the [Download page](#).

2 Edit the configuration

Modify `/etc/filebeat/filebeat.yml` to set the connection information for Elastic Cloud:

[Copy snippet](#)

```
cloud.id: "security-
deployment:YXVzdHJhbG1hZWZhdC5henVyZS5lbGFzdG1jLWNSb3VklmNvbSQ2ZWYwZWZiMjA5NWY0N2U3OTI3NzUyOWRiNzQ3OTc4M1QzNDYyMTQzMmVhNmE0OWQ3YjYwZTY0ZjNiODcx
cloud.auth: "elastic:<password>"
```

Integration with MISP

MISP Detection with Suricata

- MISP is a threat intel sharing platform
 - Check out my Jan Webinar on Practical Threat sharing
 - Allows community to share threats attributes (indicators)
 - APNIC runs a MISP instance
- Concept
 - From attributes/indicators -> generate Suricata rules automatically
- Export relevant indicators as Suricata Rules
 - Download rules formatted to work with Suricata IDS
 - Feed it to Suricata
 - Get alerts

Solarwinds Example – event from another MISP instance/feed

OSINT Threat Advisory: SolarWinds supply chain attack

Event ID	1358
UUID	e6d2f7c9-c183-43c9-bd3c-3dcfbb34665c
Creator org	CIRCL
Tags	type:OSINT osint:lifetime="perpetual" osint:certainty="50" ttp:white
Date	2020-12-15
Threat Level	High
Analysis	Completed
Distribution	All communities
Info	OSINT Threat Advisory: SolarWinds supply chain attack
Published	Yes (2021-01-13 01:23:05)
#Attributes	54 (10 Objects)
First recorded change	2020-12-15 08:16:20
Last change	2020-12-15 08:48:11
Modification map	
Extends	632aaf17-44db-4c3e-bf97-59820990491a
Sightings	0 (0) - restricted to own organisation only.

Related Events

 OSINT - UNC2452 / SUNBURST @vxunderground OSINT related findings	12
2020-12-14	

Solarwinds - Indicators (domain)

2020-12-15	Network activity	domain	databasegalore.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	incomeupdate.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	highdatabase.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	websitetheme.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	deftsecurity.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	virtualdataserver.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	thedoccloud.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	digitalcollege.org	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	globalnetworkissues.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	seobundlekit.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	virtualwebdata.com	  	☒	☒	Inherit	   (0/0/0)	 
2020-12-15	Network activity	domain	avsvmcloud.com	  	☒	☒	Inherit	   (0/0/0)	 

Export to Suricata rules

OSINT Threat Advisory: SolarWinds supply chain attack

Event ID 1358
UUID e6d2
Creator org CIRC
Tags MISP JSON (metadata + all attributes)
Date 2020 OpenIOC (all indicators marked to IDS)
Threat Level High CSV
Analysis Complete CSV with additional context
Distribution All contacts STIX XML (metadata + all attributes)
Info OSINT STIX JSON (metadata + all attributes)
Published Yes STIX2 (requires the STIX 2 library)
#Attributes 54 (1) RPZ Zone file
First recorded change 2020 Download Suricata rules
Last change 2020 Download Snort rules
Modification map Download Bro rules
Extends 632a Export all attribute values as a text file
Sightings 0 (0)

Choose the format that you wish to download the event in

MISP XML (metadata + all attributes)	Encode Attachments ☒
MISP JSON (metadata + all attributes)	Encode Attachments ☒
OpenIOC (all indicators marked to IDS)	
CSV	Include non-IDS marked attributes ☐
CSV with additional context	Include non-IDS marked attributes ☐
STIX XML (metadata + all attributes)	Encode Attachments ☐
STIX JSON (metadata + all attributes)	Encode Attachments ☐
STIX2 (requires the STIX 2 library)	Encode Attachments ☐
RPZ Zone file	
Download Suricata rules	
Download Snort rules	
Download Bro rules	
Export all attribute values as a text file	Include non-IDS marked attributes ☐

Cancel

Fetch Rules from the event

```
curl -X POST -k -H 'Accept: application/json' -H  
'Authorization: [API Key]' -H 'Content-Type:  
application/json' -o misp.suricata.rules  
'https://misp.honeynet.asia/attributes/restSearch' --data  
'{"eventid": "1358", "returnFormat": "suricata", "to_ids": "1"}'
```


Suricata Rules generated (snip)

```
alert dns any any -> any any (msg: "MISP e1358 [] Domain avsvmcloud.com";  
dns_query; content:"avsvmcloud.com"; nocase; pcre: "/(^|[^A-Za-z0-9-  
])avsvmcloud\.com$/i"; classtype:trojan-activity; sid:9823577; rev:1;  
priority:1; reference:url,https://misp.honeynet.asia/events/view/1358;)
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e1358 [] Outgoing HTTP  
Domain avsvmcloud.com"; flow:to_server,established; content: "Host|3a|"; nocase;  
http_header; content:"avsvmcloud.com"; fast_pattern; nocase; http_header; pcre:  
"/(^|[^A-Za-z0-9-])avsvmcloud\.com[^A-Za-z0-9-\.]\/Hi"; tag:session,600,seconds;  
classtype:trojan-activity; sid:9823578; rev:1; priority:1;  
reference:url,https://misp.honeynet.asia/events/view/1358;)
```

MISP – Take Aways

- MISP and Community Sharing is awesome 😊
- Integration Incident Response and Detection
- Allows automation
 - Distribute rules to a distributed sensors via api

Summary

- We've gone through some features but there are many other parts not covered
- Context is important to define usecase
 - What are we trying to detect or 'hunt'
 - False positives / False Negatives
 - Infrastructure is unique for everyone – so different hardware capacity and requirements
- Read the official docs!
 - Depecrated keywords
 - New syntax, features, keywords

Suricata Recap

- Check out the webinars
 - <https://suricata-ids.org/webinars/>
- Forum
 - <https://forum.suricata.io/>
- Twitter: https://twitter.com/Suricata_IDS
- Read the Docs - suricata.readthedocs.io/
- Women of Suricata Community Initiative
 - <https://forum.suricata.io/t/new-women-of-suricata-community-initiative/282>

Thank you

- Email: adli@apnic.net
- LinkedIn: Adli Wahid

