Investigating Alerts in Cisco FMC

Presented by Isuru Tharanga Malawige

Threat Intel Events

IP LOOKUP

PASSIVE

- IP Lookup
  - https://ipinfo.io
  - https://shodan.io
  - https://greynoise.io
  - https://censys.io
  - https://onyphe.io
- ASN Lookup
  - https://spyse.com/tools/asn-lookup
- Reputation Lookup
  - https://talosintelligence.com/reputation_center
  - https://otx.alienvault.com
  - https://www.virustotal.com/gui/home/search
  - https://exchange.xforce.ibmcloud.com

ACTIVE

- Network Scanning
  - nmap -A $IP [**Noisy**]
    - Port Scanning (Common 1000 Ports)
    - Banner Grabbing
    - OS Fingerprinting
    - Script Scanning

LAST RESORT !!!

DOMAIN LOOKUP

- Reputation Lookup
  - https://talosintelligence.com/reputation_center
  - https://otx.alienvault.com
  - https://www.virustotal.com/gui/home/search
  - https://exchange.xforce.ibmcloud.com
  - https://app.threatconnect.com
  - https://pulsedive.com

Domain Info [**NOT Ideal**]

https://shodan.io
https://censys.io
https://greynoise.io

URL LOOKUP

- Reputation Lookup
  - https://talosintelligence.com/reputation_center
  - https://otx.alienvault.com
  - https://www.virustotal.com/gui/home/search
  - https://exchange.xforce.ibmcloud.com
  - https://urlscan.io
  - https://app.threatconnect.com
  - https://pulsedive.com

- Website Info
  - https://shodan.io
  - https://censys.io
  - https://greynoise.io
  - https://sitereport.netcraft.com
- Website History
  - https://web.archive.org
- Certificate Test
  - https://www.ssllabs.com/ssltest
- Web Technologies
  - Browser Extensions
    - Wappalyzer
    - WhatRuns
  - Websites
    - https://builtwith.com

This will be useful on IPS alerts on specific vulnerabilities of the organization's web applications

Malware Events

HASH LOOKUP

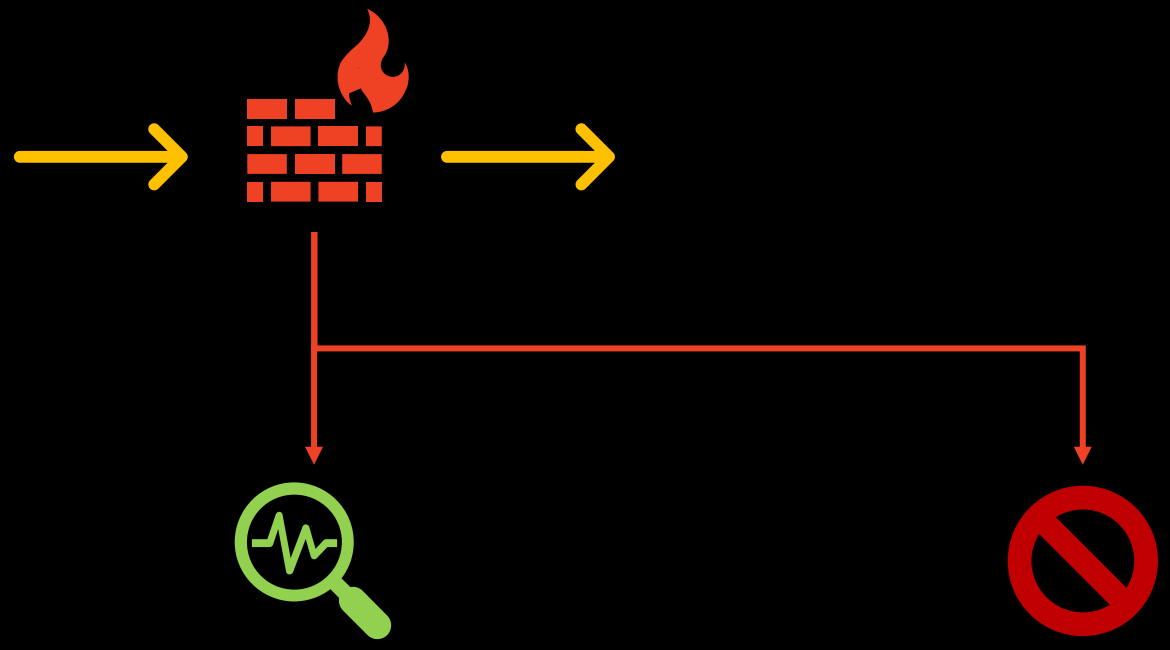
- Reputation Lookup
  - https://talosintelligence.com/talos_file_reputation
  - https://otx.alienvault.com
  - https://www.virustotal.com/gui/home/search
  - https://exchange.xforce.ibmcloud.com
  - https://www.hybrid-analysis.com
  - https://analyze.intezer.com
  - https://app.any.run/submissions
  - https://app.threatconnect.com
  - https://virusshare.com/search
- General Info
  - https://www.trendmicro.com/vinfo/us/threat-encyclopedia
  - https://www.fortiguard.com/encyclopedia
  - https://www.virusradar.com/en/threat_encyclopaedia/filter

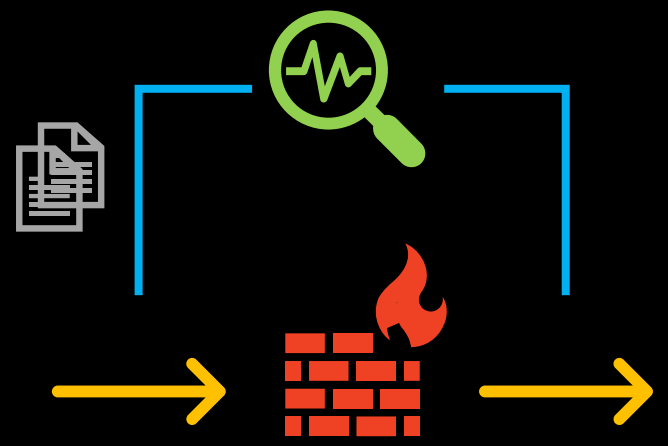
Intrusion Events

IPS MODES

PROMISCUOUS (Passive Inspection)

INLINE





PASSIVE INSPECTION

Detection/Monitor Mode

ACTIVE INSPECTION

Prevention Mode

PRIORITY

Priority	Severity
P1	CRITICAL
P2	HIGH
P3	MEDIUM
P4	LOW

Prevention Mode

Level	Event Type
P1	INTERNAL_NET -> INTERNAL_NET
P2	INTERNAL_NET -> EXTERNAL_NET
P3	EXTERNAL_NET -> INTERNAL_NET

Monitor Mode

Level	Event Type
P1	INTERNAL_NET -> INTERNAL_NET
P1	INTERNAL_NET -> EXTERNAL_NET
P1	EXTERNAL_NET -> INTERNAL_NET

SNORT Rules

RULE SAMPLE

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:
“BROWSER-IE Microsoft Internet Explorer CacheSize exploit
attempt”; flow: to_client,established; file_data;
content:"recordset"; offset:14; depth:9; content:".CacheSize";
distance:0; within:100; pcre:"/CacheSize\s*=\s*/";
byte_test:10,>,0x3ffffffe,0,relative,string; policy max-detect-
ips drop, service http; reference:cve,2016-8077; classtype:
attempted-user; sid:65535;rev:1;)
```

RULE HEADER BREAKDOWN

Rule Header

[action][protocol][sourceIP][sourceport] -> [destIP][destport] ([Rule options])

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg: ....)

->	Unidirectional
< >	Bidirectional
<-	Does NOT Exists

HEADER: ACTIONS

Action Type	Description
alert	Generate an alert using the selected alert method, and then log the packet
log	Log the packet
pass	Ignore the packet
drop	Block and log the packet
reject	Block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP
sdrop	Block the packet but do not log it
activate	Alert and then turn on another *dynamic* rule
dynamic	Remain idle until activated by an activate rule, then act as a log rule

RULE OPTIONS BREAKDOWN

Rule Option	Sample
Message	`msg: “BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt”;`
Flow	`flow: to_client,established;`

Detection	`file_data;`
	`content:"recordset"; offset:14; depth:9;`
	`content:".CacheSize"; distance:0; within:100;`
	`pcre:"/CacheSize\s*=\s*/";`
	`byte_test:10,>,0x3ffffffe,0,relative,string;`

Metadata	`policy max-detect-ips drop, service http;`
References	`reference: cve,2016-8077;`
Classification	`classtype: attempted-user;`
Signature ID	`sid:65535;rev:1;`

RULE OPTIONS BREAKDOWN

Rule Option	Sample	
Message	A meaningful message typically includes what the rule is detecting. The msg rule option tells Snort what to output when the rule matches. It is a simple text string.	
Flow	For the rule to fire, specifies which direction the network traffic is going. The flow keyword is used in conjunction with TCP stream reassembly. It allows rules to only apply to certain directions of the traffic flow.	
Detection	**content**	This important feature allows the user to set rules that search for specific content in the packet payload and trigger response based on that data. The option data can contain mixed text and binary data.
	distance/offset	These keywords allow the rule writer to specify where to start searching relative to the beginning of the payload or the beginning of a content match.
	within/depth	These keywords allow the rule write to specify how far forward to search relative to the end of a previous content match and, once that content match is found, how far to search for it.
	pcre	The pcre keyword allows rules to be written using perl compatible regular expressions which allows for more complex matches than simple content matches.
	byte_test	The byte_test options allows a rule to test a number of bytes against a specific value in binary.
Metadata	The metadata tag allows a rule writer to embed additional information about the rule, typically in a key-value format.	
References	The reference keyword allows rules to include references to external sources of information.	
Classification	The classtype keyword is how Snort shares what the effect of a successful attack would be.	
Signature ID	The snort id is a unique identifier for each rule. This information allows output plugins to identify rules easily and should be used with the rev (revision) keyword.	

RULE OPTIONS: FLOW

flow:

Option	Description
to_client	Trigger on server responses from A to B
to_server	Trigger on client requests from A to B
from_client	Trigger on client requests from A to B
from_server	Trigger on server responses from A to B
established	Trigger only on established TCP connections
not_established	Trigger only when no TCP connection is established
stateless	Trigger regardless of the state of the stream processor (useful for packets that are designed to cause machines to crash)
no_stream	Do not trigger on rebuilt stream packets (useful for dsize and stream5)
only_stream	Only trigger on rebuilt stream packets
no_frag	Do not trigger on rebuilt frag packets

RULE OPTIONS: DETECTION

content:

Hexadecimal	5c 00 50 00 49 00 50 00 45 00 5c								
Value	5c 00	P	00	I	00	P	00	E	00 5c
Breakdown	Hex	Text	Hex	Text	Hex	Text	Hex	Text	Hex

alert tcp any any -> any 139 (content:"|5c 00|P|00|I|00|P|00|E|00 5c|";)

alert tcp any any -> any 80 (content:!"GET";)

Hex Format: | |

Negate Option: !

RULE OPTIONS: DETECTION

content:

Content Modifiers		
nocase	within	http_raw_header
rawbytes	http_client_body	http_method
depth	http_cookie	http_uri
offset	http_raw_cookie	http_raw_uri
distance	http_header	http_stat_code
http_stat_msg	fast_pattern	

RULE OPTIONS: DETECTION

content:

alert tcp any 445 -> $HOME_NET any (content:"|FC|SMB"; depth:4; offset:4;)

```
0000   00 00 0c 9f f0 01 00 50 56 a8 e8 9d 81 00 00 9a   .......PV.......
0010   08 00 45 00 05 8c 3a ff 40 00 80 06 ff 69 0a 14   ..E...:.@....i..
0020   9a 7e 0a 64 0c 0d 01 bd db 10 e5 7b 80 a4 41 4b   .~.d.......{..AK
0030   be ad 50 10 1f fe c6 2c 00 00 ff 17 e3 43 fc 53   ..P....,.....C.S
0040   4d 42 00 00 00 00 00 00 00 00 34 57 e2 43 ea 60   MB........4W.C.`
0050   4c 42 00 00 00 00 00 00 00 00 17 96 e1 43 c8 7e   LB...........C.~
0060   4b 42 00 00 00 00 00 00 00 00 75 4d e1 43 98 2e   KB........uM.C..
0070   4b 42 00 00 00 00 00 00 00 00 54 10 e0 43 10 e6   KB........T..C..
```

RULE OPTIONS: DETECTION

content:

```
alert tcp any -> $HOME_NET 8009 (content:"|12 34|"; depth:2;
content:"|02|"; within:1; distance:2;)
```

```
0000   00 50 56 ba a9 d7 00 de fb 35 5a c3 81 00 07 da   .PV......5Z.....
0010   08 00 45 00 01 b6 02 ef 40 00 7f 06 f2 29 0a e3   ..E.....@....)..
0020   dd 24 0a e3 12 3f dd 47 1f 49 4b 80 23 6e d9 ae   .$...?.G.IK.#n..
0030   72 4f 50 18 20 14 f8 2b 00 00 12 34 01 8a 02 02   rOP. ..+...4....
0040   00 08 48 54 54 50 2f 31 2e 31 00 00 0f 2f 61 73   ..HTTP/1.1.../as
0050   64 66 2f 78 78 78 78 78 2e 6a 73 70 00 00 09 6c   df/xxxxx.jsp...l
0060   6f 63 61 6c 68 6f 73 74 00 ff ff 00 09 6c 6f 63   ocalhost.....loc
0070   61 6c 68 6f 73 74 00 00 50 00 00 09 a0 06 00 0a   alhost..P.......
```

RULE OPTIONS: CLASSIFICATION

classtype:

Priority	Classification Type	Description
HIGH	attempted-admin	Attempted Administrator Privilege Gain
	attempted-user	Attempted User Privilege Gain
	inappropriate-content	Inappropriate Content was Detected
	policy-violation	Potential Corporate Privacy Violation
	shellcode-detect	Executable code was detected
	successful-admin	Successful Administrator Privilege Gain
	successful-user	Successful User Privilege Gain
	trojan-activity	A Network Trojan was detected
	unsuccessful-user	Unsuccessful User Privilege Gain
	web-application-attack	Web Application Attack

RULE OPTIONS: CLASSIFICATION

classtype:

Priority	Classification Type	Description
MEDIUM	attempted-dos	Attempted Denial of Service
	attempted-recon	Attempted Information Leak
	bad-unknown	Potentially Bad Traffic
	default-login-attempt	Attempt to login by a default username and password
	denial-of-service	Detection of a Denial-of-Service Attack
	misc-attack	Misc Attack
	non-standard-protocol	Detection of a non-standard protocol or event
	rpc-portmap-decode	Decode of an RPC Query
	successful-dos	Denial of Service
	successful-recon-largescale	Large Scale Information Leak
	successful-recon-limited	Information Leak
	suspicious-filename-detect	A suspicious filename was detected
	suspicious-login	An attempted login using a suspicious username was detected
	system-call-detect	A system call was detected
	unusual-client-port-connection	A client was using an unusual port
	web-application-activity	Access to a potentially vulnerable web application

RULE OPTIONS: CLASSIFICATION

classtype:

Priority	Classification Type	Description
LOW	icmp-event	Generic ICMP event
	misc-activity	Miscellaneous activity
	network-scan	Detection of a Network Scan
	not-suspicious	Not Suspicious Traffic
	protocol-command-decode	Generic Protocol Command Decode
	string-detect	A suspicious string was detected
	unknown	Unknown Traffic
	tcp-connection	A TCP connection was detected

MORE INFO

- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html
- https://blog.joelesler.net/2010/03/offset-depth-distance-and-within.html
- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/DevNet-1693.pdf
- https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm

THANK YOU!