

Security Information and Event Monitoring (Splunk)(Done 2 times) ✓

Overview

In this lab you act as the on-call responder for an active web-facing incident. Across four coordinated Splunk investigations you will: identify and quantify credential brute-force attempts against a Joomla admin endpoint; track a high-volume vulnerability scanner (and its tools and origin) via Fortigate UTM logs; investigate a suspicious executable discovered in the Windows registry using Sysmon, OSINT, and reputation services; and validate / extend an operational security dashboard using Suricata and Fortigate alerts. The scenario emphasizes rapid triage, event correlation across multiple sourcetypes, enrichment with external intelligence, and turning log findings into containment- and remediation-focused actions.

Tools, log sources & techniques used

- **Splunk** — complex searches, spath, table, stats, sorting, saved dashboards, and event sampling controls.
 - **Web/application logs** — stream:http sourcetype, POST body inspection (form_data), HTTP status analysis.
 - **Firewall / UTM** — fortigate_utm sourcetype for scanner identification, source geolocation, destination IPs, and enrichment fields.
 - **Network IDS/IPS** — Suricata alerts for signature-based detection (Information Leak, Trojan, CVE-linked signatures).
 - **Endpoint telemetry** — Sysmon (xmlwineventlog) for process creation, ImageLoaded hashes, network connections, and EventID correlation.
 - **OSINT & reputation services** — Google (osk.exe research), VirusTotal (SHA256 lookup), and NVD for CVE/CVSS lookups.
 - **Investigation workflow** — pivoting from events to fields (e.g., src_ip, destination ports), narrowing queries with spath / field filters, exporting evidence, and using stats / table to find counts, uniques, and timelines.
-

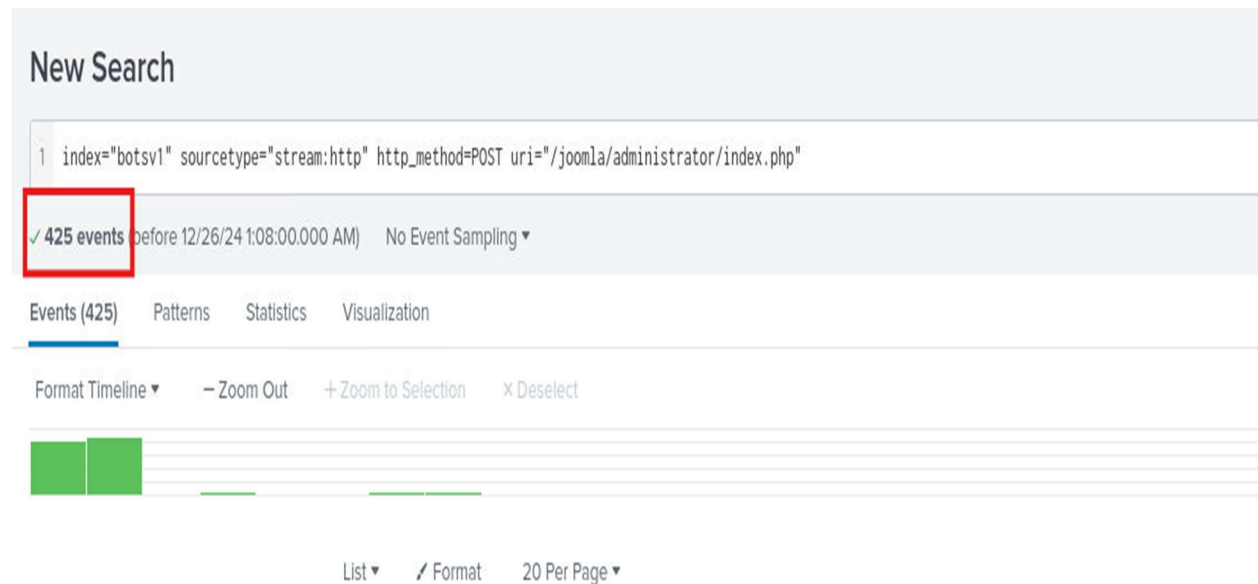
Splunk Investigation 1

PROMPT:

Alongside the vulnerability scan our security tools have alerted us to a malicious actor that is brute forcing accounts for the website. We need you to investigate, find out where the attack is coming from, if they were successful, and if they were, what did they do with their access. This is an extremely time-sensitive investigation, every second is potentially more time the attacker has control over systems on the server.

This investigation isn't as simple as looking at one type of event sourcetype. You will need to use your analysis skills to investigate and compare different log types to work out exactly what has happened. As a starting point, we know the administrator URL is `http://imreallynotbatman.com/joomla/administrator/index.php` and that usernames and passwords will be submitted in an HTTP POST request (`http_method=POST`). Ensure that event sampling is set to 'No Event Sampling' so we can see every single event. Let's investigate!

1. Use the following search query to identify the malicious activity `index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php"`. How many events have been identified?



2. Under the 'Interesting Fields' on the left scroll down to 'src_ip'. Click on it to view the count of events per source IP. Which IP address is the source IP for the majority of the traffic?

src_ip

2 Values, 100% of events

Selected

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
23.22.63.114	412	96.941%
40.80.148.42	13	3.059%

3. Left-click the IP address with the highest % of events to add it to our search query. How many events are there in total now?

New Search

1 index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php" src_ip="23.22.63.114"

✓ 412 events (before 12/26/24 1:11:37.000 AM) No Event Sampling ▼

Events (412) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

Bar chart visualization showing event distribution over time.

4. What is the destination IP? (IP address of our web server hosting imreallynotbatman.com)

After adding "imreallynotbatman.com" to the search

Connection: close

dest_ip

1 Value, 100% of events

Selected

Reports

[Top values](#)
[Top values by time](#)
[Rare values](#)

[Events with this field](#)

Values	Count	%
192.168.250.70	412	100%

http_content_type: text/html; charset=UTF-8

5. Let's take a look at one of these requests to see exactly what's going on. Add the following to the end of your current search query | spath timestamp | search timestamp="2016-08-10T21:46:44.453730Z". Identify the form_data value in the event. What is the username the attacker is trying to use? (only include the string before the '&')

```
dest_ip: 192.168.250.70
dest_mac: 00:0C:29:C4:02:7E
dest_port: 80
duplicate_packets_in: 1
duplicate_packets_out: 1
endtime: 2016-08-10T21:46:50.640101Z
form_data: username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baby&26a9247d113c37
http_comment: HTTP/1.1 303 See other
http_content_length: 182
http_content_type: text/html; charset=UTF-8
http_method: POST
http_user_agent: Python-urllib/2.7
location: http://imreallynotbatman.com/joomla/administrator/index.php
missing_packets_in: 0
missing_packets_out: 0
```

6. What is the password that is being entered in the form_data value? (only include the string before the '&')

```

dest_ip: 192.168.250.70
dest_mac: 00:0C:29:C4:02:7E
dest_port: 80
duplicate_packets_in: 1
duplicate_packets_out: 1
endtime: 2016-08-10T21:46:50.640101Z
form_data: username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baby&26a9247d113c378cdf06f311
http_comment: HTTP/1.1 303 See other
http_content_length: 182
http_content_type: text/html; charset=UTF-8
http_method: POST
http_user_agent: Python-urllib/2.7
location: http://imreallynotbatman.com/joomla/administrator/index.php
missing_packets_in: 0
missing_packets_out: 0
network_interface: eth1
packets_in: 7

```

7. We can better visualize the form_data values using the table functionality. Remove the details about timestamps from your search query and add the following | table timestamp,form_data. Once this has loaded click the timestamp column heading to sort by the oldest event first (arrow pointing up). What was the first password in the brute-force attack? (only include the string before the '&')

New Search	
<pre>1 index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php" src_ip="23.22.63.114" imreallynotbatman.com</pre> <pre>2 table timestamp,form_data</pre>	
✓ 412 events (before 12/26/24 1:21:15.000 AM) No Event Sampling ▼	
Events	Patterns
Statistics (412)	Visualization
20 Per Page ▼	Format Preview ▼
timestamp ▲	form_data ↕
2016-08-10T21:45:10.253339Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=123456789d873c2becd118318849d13cf18b60ff=1
2016-08-10T21:45:10.253584Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=football&d1181413b1a70460b8d425cec799cdca=1
2016-08-10T21:45:10.389519Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&76e93e8488d9a46878468d88954a0d54=1&passwd=123456
2016-08-10T21:45:10.389526Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=1234aaf6297ae5c1e3df78a421bc55548d16=1
2016-08-10T21:45:10.396756Z	username=admin&863349a657c211fbfeb90ebe9427654c=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=letmein
2016-08-10T21:45:10.525435Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=qwerty&af4df60674155567dee0566f87045251=1

Splunk Investigation 2

PROMPT:

Our website has shown signs of high resource usage, but it doesn't look like a distributed denial-of-service attack, because the requests are coming from one single IP address. They seem to be performing a port scan and trying to access different resources on the website - it could be a vulnerability scanner. We need you to investigate and gather information about this activity, including where it's coming from, what tools they are using, and the resources they have accessed. We run routine checks, but if they find something we haven't seen before, this could get bad really quick.

Instead of looking through thousands of web logs we can look at logs from the Fortigate firewall, specifically the Unified Threat Management solution, so make sure to set your sourcetype as fortigate_utm. You should search for our domain name as a string, "imreallynotbatman.com" and the string "vulnerability" to find events related to this activity.

1. What is the name of the web vulnerability scanner that is being used?

The screenshot shows the FortiGate UTM event log interface. The search bar contains the query: `index="botsv1" sourcetype=fortigate_utm imreallynotbatman.com vulnerability`. The results show 4,145 events. The selected event is from August 10, 2016, at 15:54:30. The event details are as follows:

Time	Event
8/10/16 9:54:30.000 PM	Aug 10 15:54:30 192.168.250.1 date=2016-08-10 time=15:54:30 devname=gotham-fortigate devid=FGT60D4614844725 logid=0419016384 type=utm subtype=ips eventtype=signature level=alert vd=root severity=low src ip=40.80.148.42 srccountry="United States" dstip=192.168.250.70 dstintf="internal3" policyid=26 sessionid=923488 action=detected proto=6 service=HTTP attack="Acunetix.Web.Vulnerability.Scanner" srcport=45488 dstport=80 hostname="imreallynotbatman.com" direction=outgoing attackid=39769 profile="all_default_pass" ref="http://www.fortinet.com/ids/VID39769" incidentserialno=503232608 msg="tools: Acunetix.Web.Vulnerability.Scanner," crscore=5 crlevel=low host = 192.168.250.1 source = udp:514 sourcetype = fortigate_utm

2. What is the source IP of the vulnerability scanner, and therefore the attacker?

<input type="checkbox"/> site	imreallynotbatman.com
<input type="checkbox"/> src	40.80.148.42
<input type="checkbox"/> src_ip	40.80.148.42

3. What is the destination IP? (the internal address for our web server)

<input type="checkbox"/> dest_interface	internal3
<input type="checkbox"/> dest_ip	192.168.250.70
<input type="checkbox"/> dest_port	80

4. Fortigate UTM provides enrichment, and can tell us the source IP country based on a lookup. What country is the scanning IP associated with?

IP Information for 40.80.148.42	
Quick Stats	
IP Location	United States Washington Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Whois Server	whois.arin.net
IP Address	40.80.148.42

5. What is the log 'time' field value for the first Fortigate UTM log referencing the vulnerability scan, on 8/10/16, in the format HH:MM:SS? (Use Sort!)

```
1 index="botsv1" sourcetype=fortigate_utm imreallynotbatman.com vulnerability
2 | sort -_time desc
```

✓ 4,145 events (before 12/26/24 1:38:39.000 AM) No Event Sampling ▼

Events (4,145) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	8/10/16	Aug 10 15:36:45 192.168.250.1 date=2016-08-10 time=15:36:45 devname=gotham-fortigate devid
a host 1			9:36:45.000 PM	ip=40.80.148.42 srccountry="United States" dstip=192.168.250.70 dstintf="internal3" policy
a source 1				205 dstport=80 hostname="imreallynotbatman.com" direction=outgoing attackid=39769 profile=
a sourcetype 1				Vulnerability.Scanner," crscore=5 crlevel=low
				host = 192.168.250.1 source = udp:514 sourcetype = fortigate_utm

Splunk Investigation 3

PROMPT:

One of our IT technicians has reported an unexpected file in the registry of an employee they were assisting. You have been tasked with investigating using various log sources and OSINT to understand if the file is legitimate or malicious, and what it is doing.

1. OSINT can be extremely useful in almost every investigation. Perform a Google search for `osk.exe` - what is the full name of the Windows feature associated with `osk.exe`?

What is `osk.exe`?

The genuine `osk.exe` file is a software component of *Microsoft Windows Operating System* by *Microsoft Corporation*. "OSK.exe" is Microsoft's [On-Screen Keyboard](#), part of its Ease of Use options for users with disabilities. Introduced in Windows 7, it remains available in Windows 8.1 and 10, although each version has changed how to turn it on. It resides in "C:\Windows\System32". On 64-bit systems there are two versions with the same name, with the one in "C:\Windows\SysWoW64" allowing interaction with 32-bit apps. It is not the same as the Touch Keyboard in "TabTip.exe" and "TabTip32.exe". (Some online articles and forum posts equate or confuse them.) It presents a virtual keyboard layout in an actual resizable window on the screen. It allows hovering, scanning, or clicking with a mouse or game joystick to select and activate keys, but not touch. It offers features the Touch Keyboard lacks, including 101-key, 102-key, and 106-key layouts. It is convenient for users but developers trying to make code interact with it often report problems.

2. Continue with your OSINT research. What is the expected file path for `osk.exe`? (Path to the folder, or full file paths are accepted)

perating System by Microsoft Corporation.

ons for users with disabilities. Introduced in Windows 7, it remains
/ to turn it on. It resides in "C:\Windows\System32". On 64-bit
Windows\SysWoW64" allowing interaction with 32-bit apps. It is
(Some online articles and forum posts equate or confuse them.) It
screen. It allows hovering, scanning, or clicking with a mouse or
the Touch Keyboard lacks, including 101-key, 102-key, and 106-
interact with it often report problems.

3. Filter on Sysmon events (sourcetype=xmlwineventlog) and search for the suspicious executable name. How many events are returned based on this query?

New Search

1 index="botsv1" sourcetype=xmlwineventlog osk.exe

✓ 49,608 events (before 12/26/24 2:22:45.000 PM) No Event Sampling ▼

4. What is the full file path of the suspicious executable?

ata><Data Name="Protocol">udp</Data><Data Name="Initiated">true</Data><Data Name="SourceIpsv6">>false</Data><Data Name="SourceIp">192.168.2	
Hostname">we8105desk.waynecorpinc.local</Data><Data Name="SourcePort">49457</Data><Data Name="SourcePortName"></Data><Data Name="De	
Name="DestinationIp">85.93.63.255</Data><Data Name="DestinationHostname"></Data><Data Name="DestinationPort">6892</Data><Data Name="De	
<input type="checkbox"/> EventID ▼	3
<input type="checkbox"/> EventRecordID ▼	427058
<input type="checkbox"/> Guid ▼	{5770385F-C22A-43E0-BF4C-06F5698FFBD9}
<input type="checkbox"/> Image ▼	C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\{35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe
<input type="checkbox"/> Initiated ▼	true
<input type="checkbox"/> Keywords ▼	0x8000000000000000
<input type="checkbox"/> Level ▼	4
<input type="checkbox"/> Name ▼	'Microsoft-Windows-Sysmon'
<input type="checkbox"/> Opcode ▼	0
<input type="checkbox"/> ProcessGuid ▼	{0F2D76F0-D007-57BD-0000-0010D0C73500}

5. What computer is the suspicious file running on, what is the internal IP address, and which user account is running it?

EventRecordID	427055
Guid	{5770385F-C22A-43E0-BF4C-06F5698FFBD9}
Image	C:\Users\Bob.Smith\WAYNECORPINC\AppData\Roaming\{35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe
Initiated	true
Keywords	0x8000000000000000
Level	4
Name	'Microsoft-Windows-Sysmon'
Opcode	0
ProcessGuid	{0F2D76F0-D007-57BD-0000-0010D0C73500}
ProcessID	'1216'
ProcessId	3588
Protocol	udp
RecordNumber	427055
SourceHostname	we8105desk.waynecorpinc.local
SourceIp	192.168.250.100

6. To scope our next searches only on this executable, find an appropriate field + value pair to add to your search query. Next it's a good idea to see if there are any network connections - what destination ports is this file connecting to?

1 osk.exe

✓ 49,713 events (before 12/26/24 2:46:43.000 PM) No Event Sampling

Events (49,713)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

List

Format

20 Per Page

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 4

a sourcetype 3

INTERESTING FIELDS

a Channel 1

a Computer 1

a DestinationIp 100+

a DestinationIpV6 1

DestinationPort 2

a dvc 1

a dvc_nt_host 1

event_id 100+

EventCode 9

a EventData_Xml 100+

Time

Event

DestinationPort

2 Values, 96.95% of events

Selected Yes No

Reports

Average over time

Maximum value over time

Minimum value over time

Top values

Top values by time

Rare values

Events with this field

Avg: 6891.858663402287 Min: 80 Max: 6892 Std Dev: 31.028775412823904

Values	Count	%
6892	48,196	99.998%
80	1	0.002%

7. Adding the destination port with the highest activity to your query, use 'stats count' functionality to identify the number of unique destination IP addresses this file is connecting to

New Search

```
1 osk.exe DestinationPort=6892
2 | stats count by DestinationIp
```

✓ 48,196 events (before 12/26/24 2:51:07.000 PM) No Event Sampling ▼

Events Patterns **Statistics (16,384)** Visualization

20 Per Page ▼ Format Preview ▼

DestinationIp ⇅

85.93.0.0

8. Sysmon EventID 7 logs contain the hash values of files (ImageLoaded field) that are executed. Use this to find the SHA256 hash of the suspicious osk.exe and submit it

```
1 osk.exe sourcetype=xmlwineventlog EventID=7 ImageLoaded=*osk.exe
```

✓ 6 events (before 12/26/24 3:09:11.000 PM) No Event Sampling ▼

i	Time	Event
>	8/24/16 4:49:21.000 PM	<pre><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /><EventLevel>4</EventLevel><Task>7</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:49:21.797609700Z' /><EventRecordID>365626</EventRecordID><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18' /><ProcessID>'1216' ThreadID='1768' /><Data><Data Name='ProcessGuid'>{0F2076F0-D007-57BD-0000-001000C73500}</Data><Data Name='ProcessId'>3588</Data><Data Name='Image'>C:\Users\ng\35ACA89F-933F-6A5D-2776-A3589FB99832\osk.exe</Data><Data Name='ImageLoaded'>C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\35ACA89F-933F-6A5D-2776-A3589FB99832\1=C8F3F0A33EFE38E9296EF79552C4CADF6CF0BDE6,MD5=EE0828A4E4C195D97313BF7D4B531F1,SHA256=37397F808E4B3731749694D767CD2CF56CACB120069E0131F070D78DFF6F262B,IMPHASH=E160EF8E1</Data></Event></pre> <p>host = we8105desk source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog</p>

9. Outside of the lab, submit the SHA256 hash to VirusTotal. Based on the results on the Detection page, what is the potential name of this malware?

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 8

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label 🚫 trojan.cerber Threat categories trojan ransom Family labels cerber

Security vendors' analysis ⓘ Do you want to automate checks?

AhnLab-V3	🚫 Trojan:Win32.Cerber.01489724
Alibaba	🚫 Trojan:Win32/Injector.ea9f82a9

10. Sysmon was useful, but let's investigate the network traffic coming from the suspicious file out to thousands of IP addresses. To do this we'll look at the Fortigate Unified Threat Management logs. Find something all (but one) of the osk.exe sysmon logs have in common regarding network traffic and use this in your search query. What is the category of malware dedicated by Fortigate?

New Search

1 index="botsv1" sourcetype="fortigate_utm" dest_port=6892

✓ 9,231 events (before 12/26/24 3:21:09.000 PM) No Event Sampling ▼

Events (9,231) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

i	Time	Event
>	8/24/16 4:49:41.000 PM	Aug 24 10:49:41 192.168.250.1 date=2016-08-24 time=10:49:40 devname=gotham-fortigate devid=FGT60D4614044725 logid=105902 d=42196 user="" srcip=192.168.250.100 srcport=50720 srcintf="internal3" dstip=85.93.63.255 dstport=6892 proto=17 service=p="Cerber.Botnet" action=pass crscore=50 crlevel=critical msg="Botnet: cerber.Botnet," apprisk=critical host = 192.168.250.1 source = udp:514 sourcetype = fortigate_utm

11. What is the name given to this specific malware by Fortigate?

NEW SEARCH

1 index="botsv1" sourcetype="fortigate_utm" dest_port=6892

✓ 9,231 events (before 12/26/24 3:21:09.000 PM) No Event Sampling ▼

Events (9,231) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ ✓ Format 20 Per Page ▼

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

i	Time	Event
>	8/24/16 4:49:41.000 PM	Aug 24 10:49:41 192.168.250.1 date=2016-08-24 time=10:49:40 devname=gotham-fortigate devid=FGT6004614044725 logid=105902 d=42196 user="" srcip=192.168.250.100 srcport=50720 srcintf="internal3" dstip=85.93.63.255 dstport=6892 proto=17 service p="Cerber.Botnet" action=pass crscore=50 crlevel=critical msg="Botnet: Cerber Botnet," apprisk=critical host = 192.168.250.1 source = udp:514 sourcetype = fortigate_utm

12. Conduct another OSINT search for the name of the malware. What is the primary function of this malware? (Submit the malware category, different from Q10)

Cerber **ransomware** is a ransomware-as-a-service (RaaS) application that attacks your files by encrypting your important documents and database files. Learn how to protect your files from and keep your data safe.

**13. Finally, let's investigate the single connection from osk.exe to a remote IP address on destination port 80 HTTP. Find the IP from the Sysmon logs and use it to search in the suricata logs - these logs have different event types, and we're interested in 'alert'. If Suricata has alerted on this activity, what is the alert.signature value?
Destination IP: 54.148.194.58**

1 sourcetype=suricata dest_ip=54.148.194.58

✓ 4 events (before 12/26/24 3:28:24.000 PM) No Event Sampling ▼

Events (4) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a action 1
- a alert.action 1
- a alert.category 1
- # alert.gid 1
- # alert.rev 1
- # alert.severity 1
- a alert.signature 1
- # alert.signature_id 1
- # alert_gid 1
- # alert_rev 1

Time Event

8/24/16 5:16:31.000 PM { [-]

dest_ip: 54.148.194.58

dest_port: 80

event_type: flow

alert.signature

1 Value, 25% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values Count %

ET POLICY Possible External IP Lookup ipinfo.io 1 100%

json

Splunk Investigation 4

PROMPT:

The security team has begun to create an operational dashboard within their SIEM instance to highlight important events. You've been tasked with trying it out to investigate some suspicious activity, and also add some new panels to the dashboard!

1. Click on Dashboards and go to Splunk Investigation 4. How many Suricata alerts are there, and how many Fortigate alerts are there



2. Edit the dashboard and look at the search query for the Fortigate Alerts counter. What is the full query used to generate this number?

1 index=* sourcetype=fortigate_utm level=alert | stats count as Total

3. What is the full query used to generate the Suricata Alerts counter?

New Search

1 `index=* sourcetype=suricata event_type=alert alert.category!=""| stats count as Total`

✓ 617 events (before 12/26/24 3:58:19.000 PM) No Event Sampling ▾

4. Click on the Suricata alert titled 'Information Leak' to see the associated events. What is the source IP address, and what is the destination IP address?

i	Time	Event
>	8/10/16 9:37:42.414 PM	<pre>{ [-] alert: { [+] } dest_ip: 192.168.250.70 dest_port: 80 event_type: alert flow_id: 1291648987 http: { [+] } in_iface: eth1 proto: TCP src_ip: 40.80.148.42 src_port: 49291 timestamp: 2016-08-10T15:37:42.414781-0600 tx_id: 75 }</pre> <p>Show as raw text</p> <p>host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata</p>

5. What action did Suricata take after observing these events?

action		
1 Value, 100% of events		Selected <input type="button" value="Yes"/> <input type="button" value="No"/>
Reports		
Top values	Top values by time	Rare values
Events with this field		
Values	Count	%
allowed	2	100%

6. We know the alert category is 'Information Leak', however the specific signature can provide us with more information about this activity. What is the signature shared by both events?

signature

1 Value, 100% of events

Selected

YesNo

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
ET WEB_SERVER WEB-PHP phpinfo access	2	100%

7. Based on the logs, combine two fields to understand the full website addresses being accessed by the attacker (Remember, in some logs a "/" character must be escaped by putting a "\" in front of it. You should not reference the "\") (hostname and URL)

eventtype	suricata_eve_ids_attack (attack ids)
flow_id	1291648987
http.hostname	imreallynotbatman.com
http.http_content_type	text/html
http.http_method	GET
http.http_user_agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.22
http.length	1245
http.protocol	HTTP/1.1
http.status	404
http.uri	/phpinfo.php
http_content_type	text/html
http_method	GET
http_protocol	HTTP/1.1
eventtype	suricata_eve_ids_attack (attack ids)
eventtype	suricata_eve_ids_attack (attack ids)
flow_id	1291648987
http.hostname	imreallynotbatman.com
http.http_content_type	text/html
http.http_method	GET
http.http_user_agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2
http.length	1245
http.protocol	HTTP/1.1
http.status	404
http.uri	/phpinfo.php5
http_content_type	text/html
http_method	GET
http_protocol	HTTP/1.1

8. What HTTP status code is returned to both of these requests, that tells us this attack was not successful?

<input type="checkbox"/>	http.protocol ▾	HTTP/1.1
<input type="checkbox"/>	http.status ▾	404
<input type="checkbox"/>	http.url ▾	/phpinfo.php5

9. Return to the Dashboard and click on the Suricata alert titled 'A Network Trojan was detected' to load this search. Modify the search query to show count of every signature field within this alert category. How many unique suricata signatures are present?

New Search

```

1 index=* sourcetype=suricata event_type=alert category!=" category="A Network Trojan was detected"
2 | stats count by signature

```

✓ 104 events (8/1/16 12:00:00.000 AM to 12/26/24 4:19:52.000 PM) No Event Sampling ▾

Events Patterns **Statistics (12)** Visualization


10. Search manually through Suricata logs where the HTTP status code is 200, then perform a count of each signature field to find two signatures that reference a vulnerability

CVE identifier. Search this CVE on the National Vulnerability Database.- what is the CVSS Version 3 Score?

```
1 index=* sourcetype=suricata event_type=alert category!=" " status=200
2 | stats count by signature
```

✓ **193 events** (8/1/16 12:00:00.000 AM to 12/26/24 4:22:38.000 PM) No Event Sampling ▾

Events Patterns **Statistics (15)** Visualization

20 Per Page ▾  Format Preview ▾

signature ⇅

ET POLICY Possible External IP Lookup ipinfo.io

ET SCAN Acunetix Version 6 (Free Edition) Scan Detected

ET WEB_SERVER IIS 8.3 Filename With Wildcard (Possible File/Dir Bruteforce)

ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt

ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt

ET WEB_SERVER Possible CVE-2014-6271 Attempt

ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers

ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access

ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM

ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT

ET WEB_SERVER Possible SQLi Attempt in User Agent (Inbound)

ET WEB_SERVER SQL Injection Select Sleep Time Delay


ISSUE DIRECTLY LOCKDOWN BEFORE IS.

Metrics

CVSS Version 4.0 **CVSS Version 3.x** CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information c

CVSS 3.x Severity and Vector Strings:

 **CNA:** Computer
Emergency Response
Team of the Republic
of Turkey

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N

11. On the Fortigate Security Alerts dashboard table click on 'MS.Windows.CMD.Reverse.Shell'. Identify the internal IP within this event, and use your SIEM skills to identify the name of this system.

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	host ▾	192.168.250.1	▾
	<input checked="" type="checkbox"/>	source ▾	udp:514	▾
	<input checked="" type="checkbox"/>	sourcetype ▾	fortigate_utm	▾
Event	<input type="checkbox"/>	action ▾	allowed	▾
	<input type="checkbox"/>	app ▾	tcp/3791	▾
	<input type="checkbox"/>	attack ▾	MS.Windows.CMD.Reverse.Shell	▾
	<input type="checkbox"/>	attackid ▾	12449	▾
	<input type="checkbox"/>	category ▾	MS.Windows.CMD.Reverse.Shell	▾
	<input type="checkbox"/>	crlevel ▾	medium	▾
	<input type="checkbox"/>	crscore ▾	10	▾
	<input type="checkbox"/>	date ▾	2016-08-10	▾
	<input type="checkbox"/>	dest ▾	192.168.250.70	▾
	<input type="checkbox"/>	dest_interface ▾	internal3	▾
	<input type="checkbox"/>	dest_ip ▾	192.168.250.70	▾

New Search

1 index=* sourcetype=xmlwineventlog 192.168.250.70

✓ 88,129 events (8/1/16 12:00:00.000 AM to 12/26/24 4:56:54.000 PM) No Event Sampling ▾

Event	<input type="checkbox"/>	Channel ▾	Microsoft-Windows-Sysmon/Operational
	<input type="checkbox"/>	Computer ▾	we5201srv.waynecorpinc.local
	<input type="checkbox"/>	DestinationHostname ▾	we5201srv.waynecorpinc.local
	<input type="checkbox"/>	DestinationIp ▾	192.168.250.70

12. Go back to the Fortigate Security Events table and click on 'Apache.Roller.OGNL.Injection.Remote.Code.Execution'. Find the reference field in the log and open the URL on your host machine. What is the Affected Products text, and the CVE identifier?

Description

This indicates a possible attack against a Command Execution vulnerability in Apache Roller. The vulnerability is due to insufficient sanitizing of user supplied inputs in the application. A remote attacker may exploit this by sending a specially crafted HTTP request to a vulnerable system. A successful attack may allow an attacker to execute arbitrary OGNL expressions in the security context of the web application server.

Affected Products

Apache Software Foundation Apache Roller prior to 5.0.2

Impact

System Compromise: Remote attackers can gain control of vulnerable systems.

ID	39031
Created	Sep 04, 2014
Updated	Nov 15, 2021
Risk	<div><div></div><div></div><div></div><div></div><div></div></div>
CVE ID	CVE-2013-4212
Exploit Prediction Score	93.84%
Default Action	drop
Active	<input checked="" type="checkbox"/>
Affected OS	All
Affected App	Apache

13. On the dashboard consider the Fortigate category with the highest number of events. Try to find the version of the scanning tool being used, looking at Fortigate logs then Suricata logs. Had to go to Suricata and search Acunetix

<input type="checkbox"/> in_iface ▾	eth1	▾
<input type="checkbox"/> product ▾	Suricata	▾
<input type="checkbox"/> proto ▾	TCP	▾
<input type="checkbox"/> severity ▾	medium	▾
<input type="checkbox"/> severity_id ▾	2	▾
<input type="checkbox"/> signature ▾	ET SCAN Acunetix Version 6 (Free Edition) Scan Detected	▾
<input type="checkbox"/> src ▾	40.80.148.42	▾
<input type="checkbox"/> src_ip ▾	40.80.148.42	▾
<input type="checkbox"/> src_port ▾	49468	▾