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

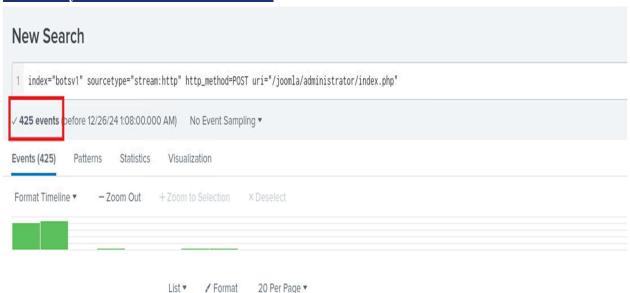
## **Splunk Investigation 1 PROMPT:**

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.

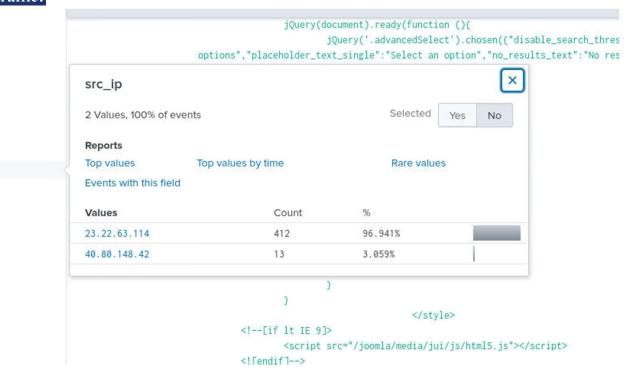
This investigation isn't as simple as looking at one type of event sourcetype. You will need to use your analysis skills to investigate and compare different log types to work out exactly what has happened. As a starting point, we know the administrator URL is

http://imreallynotbatman.com/joomla/administrator/index.phpand 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?



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 i	index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php" src_ip="23.22.63.114"			
√ 412	2 events (before 12/26/24 1:11:37.000 AM) No Event Sampling ▼			
Event	ts (412) Patterns Statistics Visualization			
Form	mat Timeline ▼ — Zoom Out + Zoom to Selection × Deselect			

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

After adding "imreallynotbatman.com" to the search



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 '&')

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
```

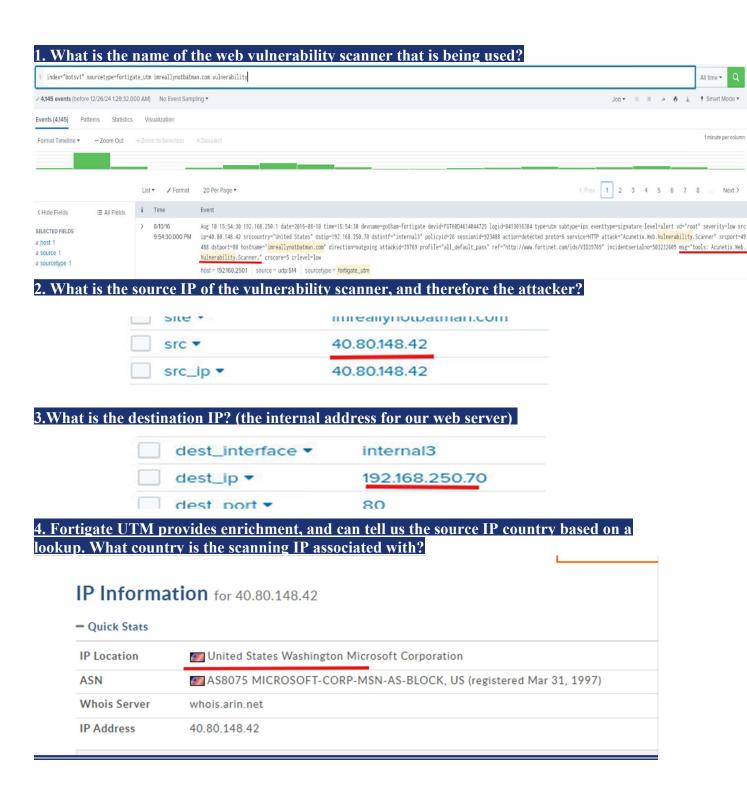
7. We can better visualize the form\_data values using the table functionality. Remove the details about timestamps from your search query and add the following | table timestamp,form\_data. Once this has loaded click the timestamp column heading to sort by the oldest event first (arrow pointing up).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



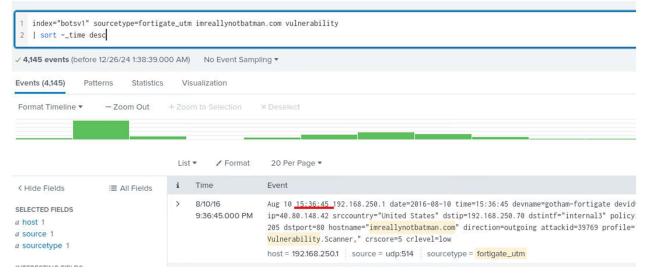
## **Splunk Investigation 2 PROMPT:**

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.



## 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!)



## **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 Vindows\SysWoW64" allowing interaction with 32-bit apps. It is [Some online articles and forum posts equate or confuse them.) It creen. 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?

N	New Search					
1	1 index="botsv1" sourcetype=xmlwineventlog osk.exe					
14	19,608 events (pefore 12/26/24 2:22:45.000 PM)	No Event Sampling ▼				

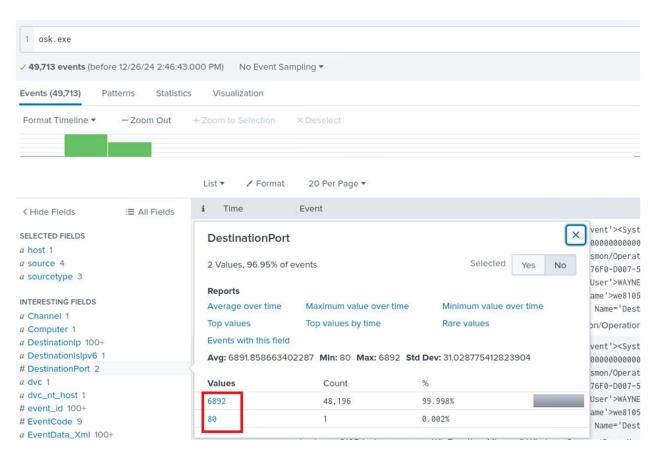
4. What is the full file path of the suspicious executable?

	Hostname'>we8105desk.waynecorpinc.local <data name="SourcePort">49457<data name="SourcePortName"><data name="DestinationIp">85.93.63.255 Name='DestinationIp'&gt;85.93.63.255 Data Name='DestinationIp'&gt;6892 Data Name='DestinationPort'&gt;6892 Data Name='DestinationPort'&gt;6892 Data Name='DestinationPort'&gt;6892</data></data></data>
EventID ▼	3
EventRecordID ▼	427058
Guid ▼	'(5770385F-C22A-43E0-BF4C-06F5698FFBD9)'
☐ Image ▼	C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\(35ACA89F-933F-6A5D-2776-A3589FB99832\)\tosk.exe
Initiated ▼	true
Keywords ▼	0x80000000000000
100000000000000000000000000000000000000	0x800000000000000000000000000000000000
Keywords ▼	
Keywords ▼	4

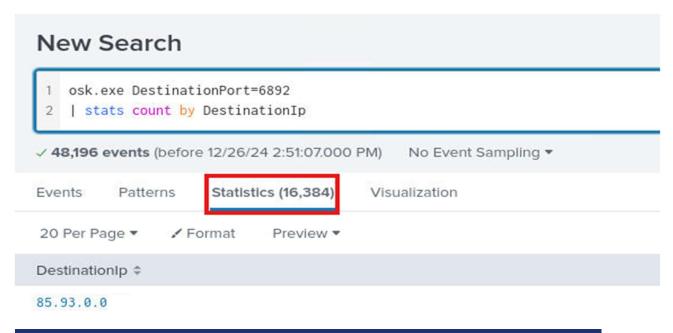
5. What computer is the suspicious file running on, what is the internal IP address, and which user account is running it?

EventRecordID ▼	42/055			
Guid ▼	'[5770385F-C22A-43E0-BF4C-06F5698FFBD9]'			
☐ Image ▼	C:\Users\bob.smith.\UAYNECORPINC\AppData\Roaming\(35ACA89F-933F-6A5D-2776-A3589FB99832)\osk.exe			
Initiated ▼	true			
Keywords ▼	0x80000000000000			
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			
Sourcelp ▼	192.168.250.100			

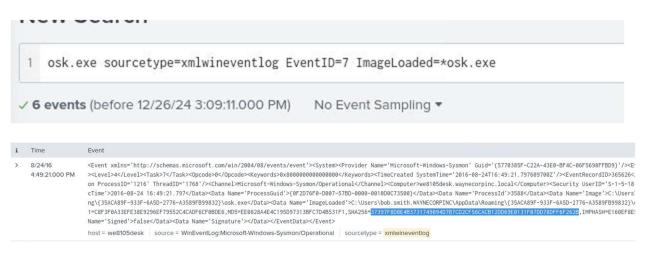
6. To scope our next searches only on this executable, find an appropriate field + value pair to add to your search query. Next it's a good idea to see if there are any network connections - what destination ports is this file connecting to?



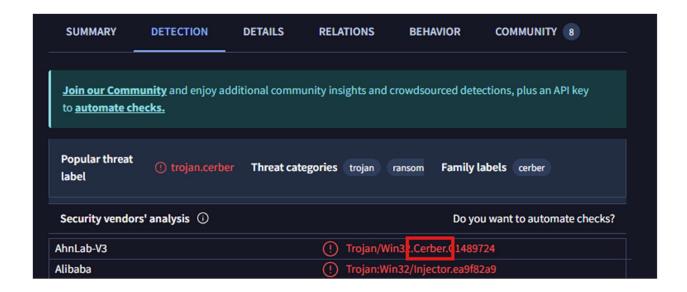
7. Adding the destination port with the highest activity to your query, use 'stats count' functionality to identify the number of unique destination IP addresses this file is connecting to



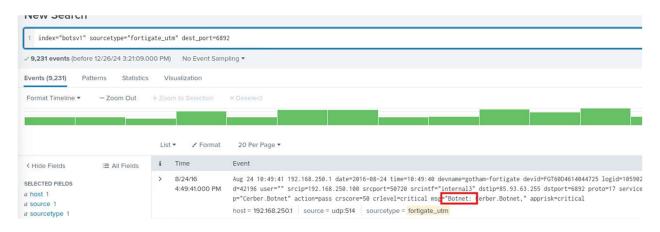
8. Sysmon EventID 7 logs contain the hash values of files (ImageLoaded field) that are executed. Use this to find the SHA256 hash of the suspicious osk.exe and submit it



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?



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?



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

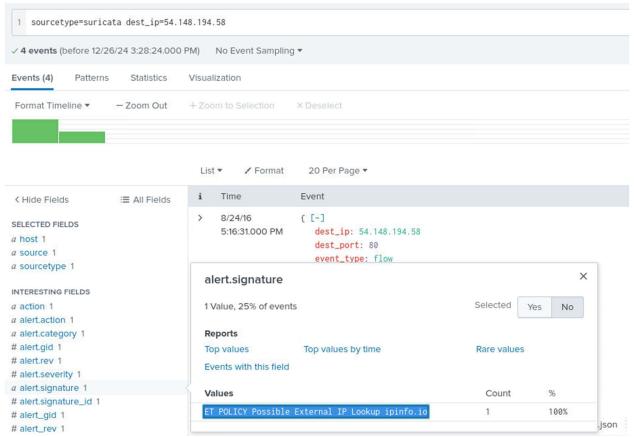
INEW Search			
1 index="botsv1"	sourcetype="forti	gate_utm" dest_port=689	12
✓ <b>9,231 events</b> (befo	re 12/26/24 3:21:09.0	000 PM) No Event Sam	pling ▼
Events (9,231)	atterns Statistics	Visualization	
Format Timeline ▼	- Zoom Out	+ Zoom to Selection	× Deselect
		List ▼ / Format	20 Per Page ▼
< Hide Fields	:≣ All Fields	i Time	Event
selected FIELDS a host 1 a source 1 a sourcetype 1		> 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" dstio=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 = fortgate_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)

Cerbe ransomware s 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



### **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?

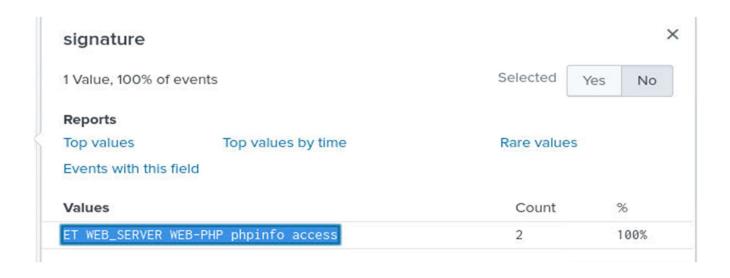
# New Search | index=\* sourcetype=suricata event\_type=alert alert.category!=""| stats count as Total | 617 events (before 12/26/24 3:58:19.000 PM) | No Event Sampling \*

## 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?

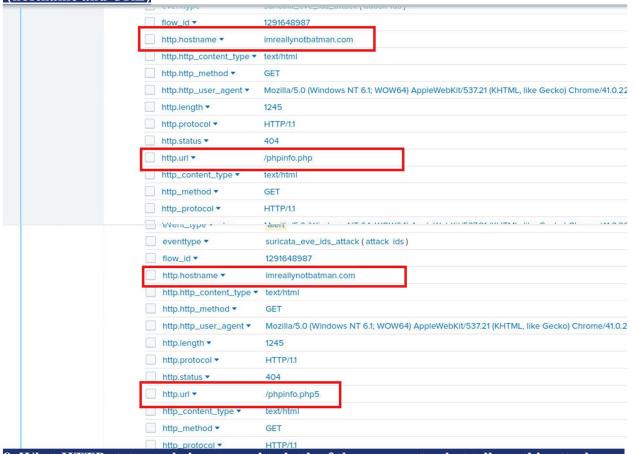
5. What action did Suricata take after observing these events?



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?



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)



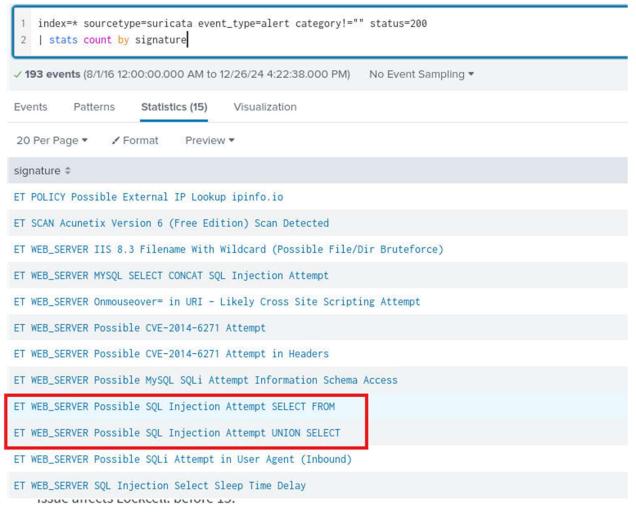
8. What HTTP status code is returned to both of these requests, that tells us this attack was not successful?



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?

<pre>index=* sourcetype=suricata event_type=alert category!="" category="A Network Trojan was detected"   stats count by signature</pre>					
√ 104 e	vents (8/1/16 12	2:00:00.000 AM to	12/26/24 4:19:52.000 PM)	No Event Sampling ▼	
Events	Patterns	Statistics (12)	Visualization		

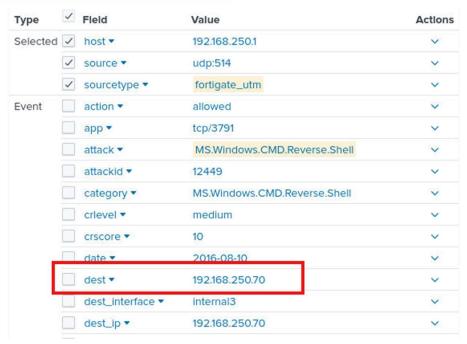
### CVE identifier. Search this CVE on the National Vulnerability Database.- what is the CVSS Version 3 Score?





### 11. On the Fortigate Security Alerts dashboard table click on

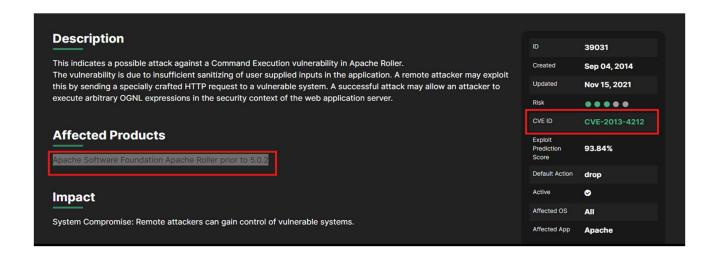
'MS.Windows.CMD.Reverse.Shell'. Identify the internal IP within this event, and use your SIEM skills to identify the name of this system.



### 

### 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?



# 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

