

# Incident handling with splunk

## Task 4 Reconnaissance Phase

### Step 1:

Go to **Search & Reporting** in Splunk and run the following search:

```
index=botsv1s
```

This index is part of a Splunk dataset that contains **realistic data**, including **logs** and **security events**, commonly used for cybersecurity training and analysis.

The screenshot shows the Splunk 8.2.4 interface with a search bar containing the query "index=botsv1s". The results section displays 955,807 events from before June 11, 2025, at 2:27:12.000 PM. The "Events" tab is selected, showing a timeline from August 24, 2016, to August 24, 2016. The first event listed is a network log entry from host 192.168.250.1 at 6:27:44.000 PM, detailing a connection between 192.168.243.155.61 and 192.168.243.155.61 over port 6631. The second event listed is a SSL handshake log entry from host 192.168.250.1 at 6:27:43.273 PM.

Time	Event
Aug 24 12:27:44 192.168.250.1	date=2016-08-24 time=12:27:43 devname=gotham-fortigate devid=FGT6004614044725 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=188.243.155.61 dstip=71.39.18.122 dstport=23 dstintf="wan1" sessionid=4237667 proto=6 action=deny policyid=0 dstcountry="United States" srccountry="Russian Federation" trandisp=noop service="TELNET" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel=high host = 192.168.250.1   source = udp:514   sourcetype = fortigate_traffic
Aug 24 12:27:43 192.168.250.1	date=2016-08-24 time=12:27:43 devname=gotham-fortigate devid=FGT6004614044725 logid=0000000013 type=ssl subtype=handshake srcip=192.168.250.1 dstip=192.168.250.1 dstport=443 dstintf="wan1" sessionid=4237667 proto=6 app=ssl bytes: 5991 ack_packets_in: 12 ack_packets_out: 7 bytes_in: 2491 bytes_out: 5991

## Step 2:

Let's investigate the **source IP addresses**.

We can see that the IP address **40.80.148.42** has a **high number of events**, so we'll start our investigation with this one.

Search | Splunk 8.2.4 — Mozilla Firefox

10.10.38.138/en-US/app/search/search?q=search index%3Dbot

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

# response\_time 100+  
# server\_rtt 100+  
# server\_rtt\_packets 8  
# server\_rtt\_sum 100+  
a site 39  
a splunk\_server 1  
a src 3  
a src\_headers 100+  
a src\_ip 3  
a src\_mac 1  
# src\_port 100+  
# status 11  
a tag 7  
a tag:eventtype 7  
a time 100+  
# time\_taken 100+  
# timeendpos 3  
a timestamp 100+  
# timestamppos 3  
a transport 2  
a url 100+  
a url\_path 100+  
a url 100+  
a vendor 2  
  
154 more fields  
+ Extract New Fields

src\_ip

3 Values, 80.4% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	47,649	75.321%
192.168.250.70	11,493	18.168%
23.22.63.114	4,119	6.511%

searchword=&ordering=alpha&searchphrase=all&areas[0]="">here</a><br>dest\_headers: HTTP/1.1 303 See other  
Content-Type: text/html; charset=UTF-8  
Location: http://imreallynotbatman.com/joomla/index.php/component/search/?se...  
Server: Microsoft-IIS/8.5  
X-Powered-By: PHP/5.5.38  
Date: Wed, 10 Aug 2016 22:22:27 GMT  
Content-Length: 252

dest\_ip: 192.168.250.70  
dest\_mac: 00:0C:29:C4:02:7E  
dest\_port: 80  
duplicate\_packets\_in: 0  
duplicate\_packets\_out: 1  
endtime: 2016-08-10T22:22:27.612320Z  
form\_data: areas[]=""&ordering=alpha&searchphrase=all&searchword=&task=...  
http\_comment: HTTP/1.1 303 See other  
http\_content\_length: 252  
http\_content\_type: text/html; charset=UTF-8

The screenshot shows the Splunk 8.2.4 interface. A search bar at the top contains the query: `index=botsv1 imreallynotbatman.com src_ip="40.80.148.42" sourcetype=suricata`. Below the search bar, it says `15,290 events (8/10/16 9:00:00.000 PM to 8/10/16 10:00:00.000 PM)`. The main pane displays a table of event statistics under the heading "Events (15,290)". The table has columns for "Values", "Count", and "%". The top row of the table is highlighted in blue. A modal window titled "category" is overlaid on the page, showing a list of 9 values: "Web Application Attack", "A Network Trojan was detected", "Attempted Administrator Privilege Gain", "Generic Protocol Command Decode", "Attempted Information Leak", "access to a potentially vulnerable web application", "Information Leak", "Detection of a Network Scan", and "Potentially Bad Traffic". The "Selected" button for the first item is highlighted in blue.

Values	Count	%
Web Application Attack	248	52.431%
A Network Trojan was detected	99	20.93%
Attempted Administrator Privilege Gain	36	7.611%
Generic Protocol Command Decode	36	7.611%
Attempted Information Leak	32	6.765%
access to a potentially vulnerable web application	18	3.805%
Information Leak	2	0.423%
Detection of a Network Scan	1	0.211%
Potentially Bad Traffic	1	0.211%

as look in web application attack it was catgerise sql injection and lets look for the options 3

The screenshot shows a Splunk search interface with the URL `10.10.38.138/en-US/app/search/search?q=search%3Dbotsv1`. The search results table has three columns: 'All Fields' (with a dropdown for 'Hide Fields'), 'Time' (sorted by timestamp), and 'Event'. There is one event listed:

```
dest_port: 80
event_type: alert
flow_id: 1577394704
http: { [+]
}
in_iface: eth1
proto: TCP
src_ip: 40.80.148.42
src_port: 49214
timestamp: 2016-08-10T15:37:00.830090-0600
}

Show as raw text
action = allowed | category = Attempted Administrator Privilege Gain |
host = suricata-ids.waynecorpinc.local |
signature = ET WEB SERVER Possible CVE-2014-6271 Attempt |
source = /var/log/suricata/eve.json | sourcetype = suricata
```

One suricata alert highlighted the CVE value associated with the attack attempt.  
What is the CVE value?

Cve-2014-6271

Search | Splunk 8.2.4 — Mozilla Firefox

10.10.38.138/en-US/app/search/search?q=search index%3Dbotsv1

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

splunk>enterprise Apps 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

1 index=botsv1 imreallynotbatman.com src\_ip="40.80.148.42" sourcetype=sur New Search Date time range

7 events (8/10/16 9:00:00.000 PM to 8/10/16 10:00:00.000 PM) No Event Sampling Job II Smart Mode

Events (7) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields i Time Event

SELECTED FIELDS

- a action 1
- a category 2
- a host 1
- a signature 5
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a alert.action 1
- a alert.category 2
- # alert.gid 1
- # alert.rev 3
- # alert.severity 2
- a alert.signature 5
- # alert.signature\_id 5

8/10/16 9:38:55.028 PM

{ "timestamp": "2016-08-10T15:38:55.028279-0600", "flow\_id": 622553447, "in\_iface": "eth1", "event\_type": "alert", "src\_ip": "40.80.148.42", "src\_port": 49330, "dest\_ip": "192.168.250.70", "dest\_port": 80, "proto": "TCP", "tx\_id": 540, "alert": { "action": "allowed", "gid": 1, "signature\_id": 2019963, "rev": 2, "signature": "ET SCAN Acunetix Accept HTTP Header detected scan in progress", "category": "Attempted Information Leak", "severity": 2 }, "http": { "hostname": "imreallynotbatman.com", "url": "/ubb\_threads", "http\_user\_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21", "http\_content\_type": "text/html", "http\_method": "GET", "proto": "HTTP/1.1", "status": 404, "length": 1245 } }

Show syntax highlighted

action = allowed : category = Attempted Information Leak

host = suricata-ids.waynecorpinc.local

signature = ET SCAN Acunetix Accept HTTP Header detected scan in progress

source = /var/log/suricata/eve.json : sourcetype = suricata

like so show raw text

Selected Fields:

- a action 1
- a category 2
- a host 1
- a signature 5
- a source 1
- a sourcetype 1

Interesting Fields:

- a alert.action 1
- a alert.category 2
- # alert.gid 1
- # alert.rev 3
- # alert.severity 2
- a alert.signature 5
- # alert.signature\_id 5
- # alert\_gid 1
- # alert\_rev 3
- # bytes 4
- # date\_hour 1
- # date\_mday 1
- # date\_minute 3
- a date\_month 1
- # date\_second 5
- a date\_wday 1
- # date\_year 1
- # date\_zone 1
- a dest 1
- a dest\_ip 1
- # dest\_port 1
- a dvc 1
- a event\_type 1
- a eventtype 1

Event Log 1 (9:38:55.028 PM):

```
{
  "timestamp": "2016-08-10T15:38:55.028279-0600",
  "flow_id": 622553447,
  "in_iface": "eth1",
  "event_type": "alert",
  "src_ip": "40.80.148.42",
  "src_port": 49330,
  "dest_ip": "192.168.250.70",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 540,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2019963,
    "rev": 2,
    "signature": "ET SCAN Acunetix Accept HTTP Header detected scan in progress",
    "category": "Attempted Information Leak",
    "severity": 2
  },
  "http": {
    "url": "/ubb_threads",
    "http_user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21",
    "http_content_type": "text/html",
    "http_method": "GET",
    "proto": "HTTP/1.1"
  },
  "status": 404,
  "length": 1245
}
```

Event Log 2 (9:37:55.012 PM):

```
{
  "alert": [
    {
      "dest_ip": "192.168.250.70",
      "dest_port": 80,
      "event_type": "alert",
      "flow_id": 213384156,
      "http": [
        {
          "in_iface": "eth1",
          "proto": "TCP",
          "src_ip": "40.80.148.42",
          "src_port": 49326,
          "timestamp": "2016-08-10T15:37:55.012751-0600",
          "tx_id": 31
        }
      ]
    }
  ]
}
```

What is the web scanner, the attacker used to perform the scanning attempts?

acunetix

What is the IP address of the server imreallynotbatman.com?

192.168.250.70

## Task 5 Exploitation Phase

What was the URI which got multiple brute force attempts?

/joomla/administrator/index.php

The screenshot shows the Splunk 8.2.4 interface with a search query in the search bar:

```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" uri="/joomla/administrator/index.php" | table _time
```

The search results table displays 1,248 events from June 8, 2010, at 14:44:412. The table has columns for \_time, uri, src\_ip, dest\_ip, and form\_data. The data shows multiple login attempts from the same IP (23.22.63.114) to the Joomla administrator index page, with various password parameters in the form\_data field.

_time	uri	src_ip	dest_ip	form_data
6-08-10 14:44:854	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:842	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:540	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	
6-08-10 14:44:646	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:578	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	

use this query to create contain important file

two important field admin and password as we can see the mutiple password for the same ip 23.22.63.114 as it is a brute force attack

Against which username was the brute force attempt made?

admin

as u can see below ss the admin was the brute force attempt made

The screenshot shows the Splunk 8.2.4 interface with a search bar containing the query: `index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" uri="/joomla/administrator/index.php" | table _time uri src_ip dest_ip form_data`. The search results show 1,248 events from June 8, 2010, at 14:44:412, all originating from 23.22.63.114 to 192.168.250.70 with the URL /joomla/administrator/index.php and the form\_data "username=admin&task=login&return=aW5kZXgucGhw&option=com\_login&pass".

Time	URI	src_ip	dest_ip	form_data
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass
6-08-10 14:44:412	/joomla/ administrator/ index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&pass

What was the correct password for admin access to the content management system running **imreallynotbatman.com**?

batman

How many unique passwords were attempted in the brute force attempt?

412

The screenshot shows the Splunk 8.2.4 interface with a search bar containing the following query:

```
1 index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" http_method=POST form_data=*username*passwd* | rex field=form_data "passwd=(?<creds>\w+)" |table _time src_ip uri http_user_agent creds
```

The search results table displays 413 events. The columns are: \_time, src\_ip, url, http\_user\_agent, and creds. The data shows various IP addresses, URLs (mostly /joomla/administrator/index.php), user agents (Python-urllib/2.7, Mozilla/5.0, etc.), and credentials (pussy, batman, rock, cool, sammy, august, phantom, williams, private). The 'batman' credential appears twice.

_time	src_ip	url	http_user_agent	creds
2016-08-10 21:45:21.325	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	pussy
2016-08-10 21:48:05.858	40.80.148.42	/joomla/administrator/index.php	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	batman
2016-08-10 21:46:51.394	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	rock
2016-08-10 21:46:51.154	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	cool
2016-08-10 21:46:51.156	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	sammy
2016-08-10 21:46:50.873	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	august
2016-08-10 21:46:50.634	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	phantom
2016-08-10 21:46:50.627	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	williams
2016-08-10 21:46:50.621	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	private

as there were total 413 events and one was successful

What IP address is likely attempting a brute force password attack against **imreallynotbatman.com**?

23.22.63.114

After finding the correct password, which IP did the attacker use to log in to the admin panel?

40.80.148.42

#### Task 6 Installation phase

Sysmon also collects the Hash value of the processes being created. What is the MD5 HASH of the program 3791.exe?

AAE3F5A29935E6ABCC2C2754D12A9AF0

The screenshot shows the Splunk 8.2.4 interface with a search results table. The table has columns for Time, Event, and several other fields. One event is selected, showing detailed XML log data. A context menu is open over this event, with options like 'Add to search', 'Exclude from search', and 'New search'. The search bar at the bottom of the interface contains a specific search query.

```

host = we1149srv
source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = xmlwineventlog

```

Looking at the logs, which user executed the program 3791.exe on the server?

NT AUTHORITY\IUSR

The screenshot shows the Splunk 8.2.4 interface with a search result for a single event. The event details are as follows:

```

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.142461700Z' /><EventRecordID>428908</EventRecordID><Correlation/><Execution ProcessID='1296' ThreadID='1416' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149sr.v.waynecorpinc.local</Computer><Security UserID='S-1-5-18' /><System><Event Data><Data Name='UtcTime'>2016-08-10 21:56:18.142</Data><Data Name='ProcessGuid'>(E500B0EA-A302-57AB-0000-0010BD65C301)</Data><Data Name='ProcessId'>3880</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Name='CommandLine'>3791.exe</Data><Data Name='CurrentDirectory'>C:\inetpub\wwwroot\joomla\</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>(E500B0EA-219E-57AB-0000-0020E3030000)</Data><Data Name='LogonId'>0x3e3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=65DF73D77324D008C83C3E57845DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448</Data><Data Name='ParentProcessGuid'>(E500B0EA-A302-57AB-0000-002E63C301)</Data><Data Name='ParentProcessId'>2896</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /c "3791.exe 2&&1"</Data></EventData></Event>
host = we1149sr
source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = xmlwineventlog

```

Search hash on the virustotal. What other name is associated with this file 3791.exe?

ab.exe

Task 7 action on objectives

What is the name of the file that defaced the imreallynotbatman.com website ?

## poisonivy-is-coming-for-you-batman.jpeg

Splunk 8.2.4 search results for 'poisonivy-is-coming-for-you-batman.jpeg'.

Search Query:

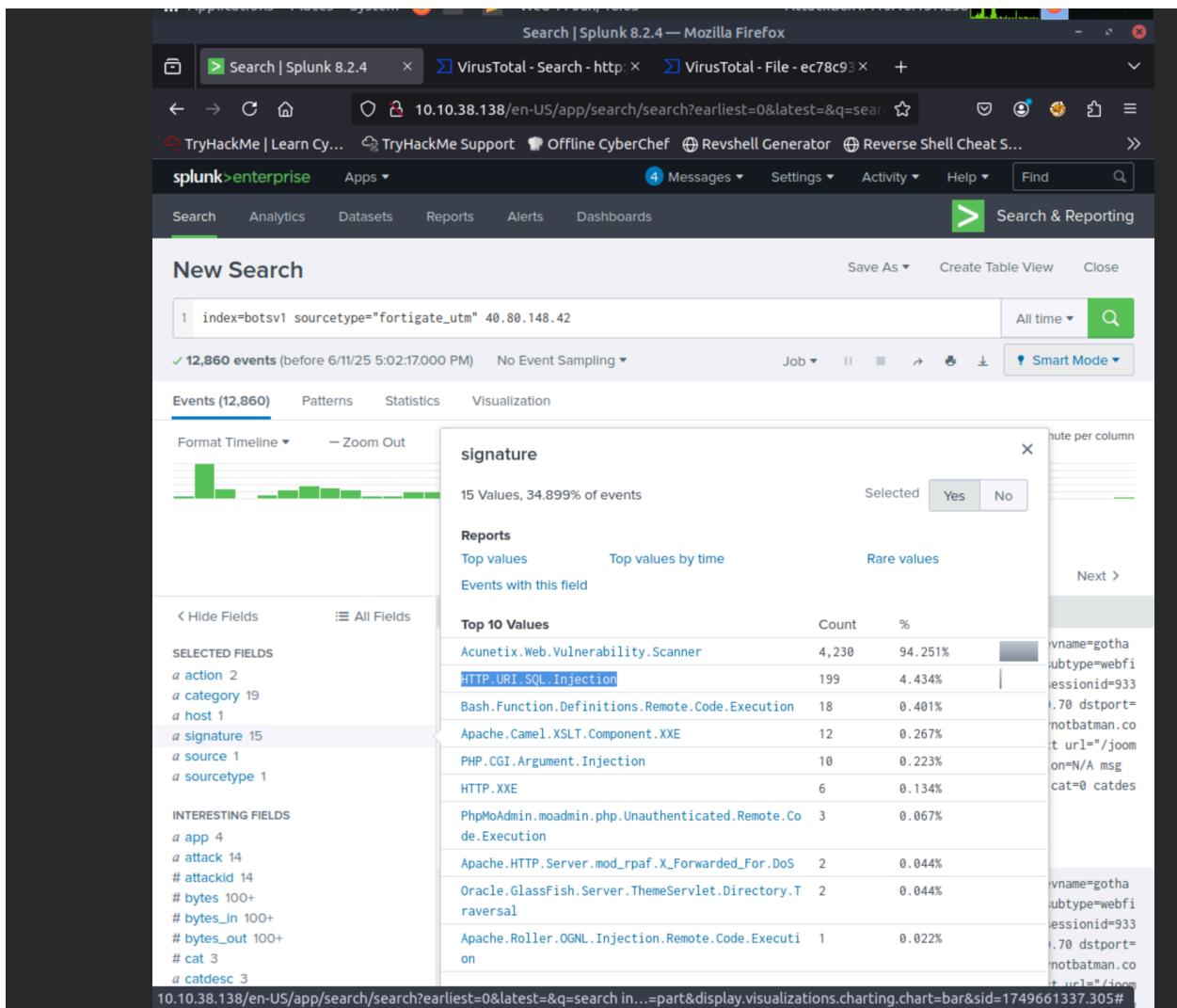
```
1 index=botsv1 url="/poisonivy-is-coming-for-you-batman.jpeg" dest_ip="192.168.250.70" | table _time src dest_ip http.hostname url
```

Results:

_time	src	dest_ip	http.hostname	url
2016-08-10 22:19:10.846	23.22.63.114	192.168.250.70	prankglassinebracket.jumpingcrab.com	/poisonivy-is-coming-for-you-batman.jpeg

Fortigate Firewall 'fortigate\_utm' detected SQL attempt from the attacker's IP 40.80.148.42. What is the name of the rule that was triggered during the SQL Injection attempt?

HTTP.URI.SQL.Injection



## Task 8 Command and Control Phase

This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

<http://prankglassinebracket.jumpingcrab.com/>

## Task 9 Weaponization Phase

What IP address has P01s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

23.22.63.114

Based on the data gathered from this attack and common open-source intelligence sources for domain names, what is the email address that is most likely associated with the P01s0n1vy APT group?

[lillian.rose@po1s0n1vy.com](mailto:lillian.rose@po1s0n1vy.com)

## Task 10 Delivery Phase

What is the HASH of the Malware associated with the APT group?

c99131e0169171935c5ac32615ed6261

What is the name of the Malware associated with the Poison Ivy Infrastructure?

MirandaTateScreensaver.scr.exe