TryHackMe Incident handling with Splunk Write-Up

Toumo · Follow
8 min read · Sep 12, 2023

Listen Share More

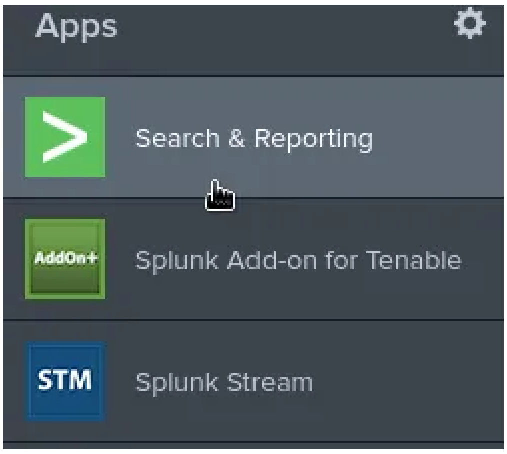
Image from tryhackme.com

I did the introductory Splunk room after a long break. I felt like the introductory room was pretty basic the second time around but it doesn't feel overwhelming as a beginner, so that's also good! Again, I will be doing all the Splunk room in the SOC Level 1 path again for more practice, and to write the corresponding write-up. Let's get started!

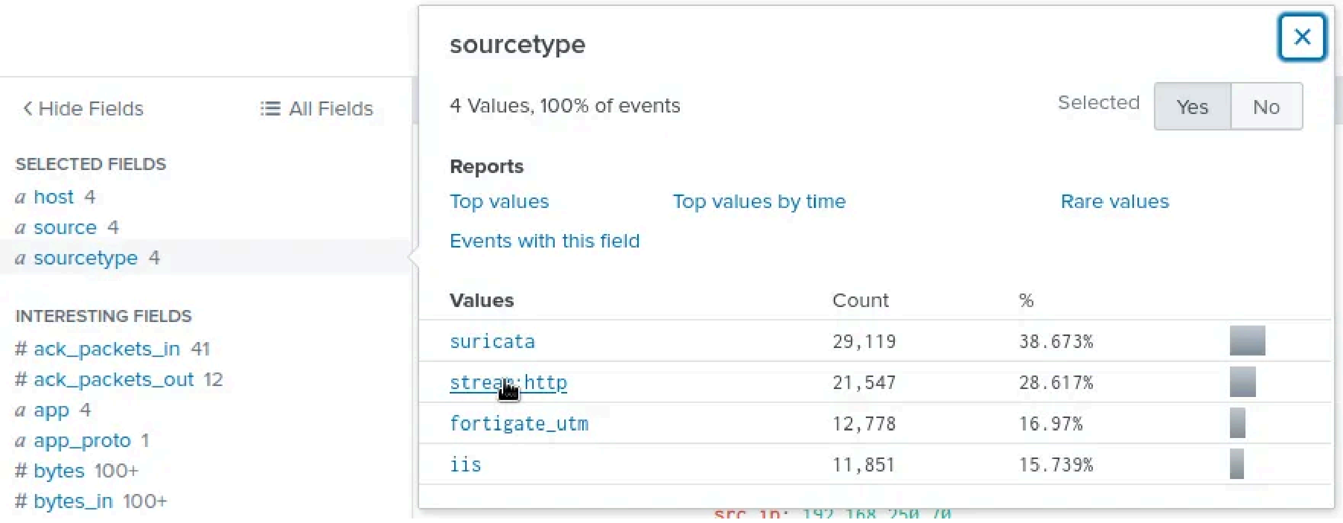
Task 4 Reconnaissance Phase

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

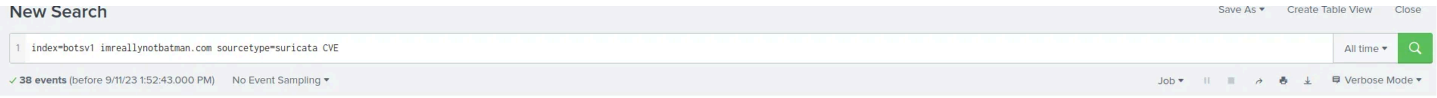
First, I used my Kali machine to do this lab. To connect to TryHackMe's network, follow this guide I wrote until step 6. Once you are connected, open a browser and connect to the IP that will be unique to you in task 3. It should show "Explore Splunk" in the middle. From there, go to the right and click on "Search & Reporting" so we can start our search queries.



I used the following query to find the answer `index=botsv1 imreallynotbatman.com sourcetype=suricata CVE` . `index=botsv1 imreallynotbatman.com` is given to us from the reading. I used `sourcetype=suricata` because we are looking for suricata alerts. You can look at the left side and click on suricata or you can type it in. I typed in `CVE` to narrow search results that mentions "CVE" in the results.



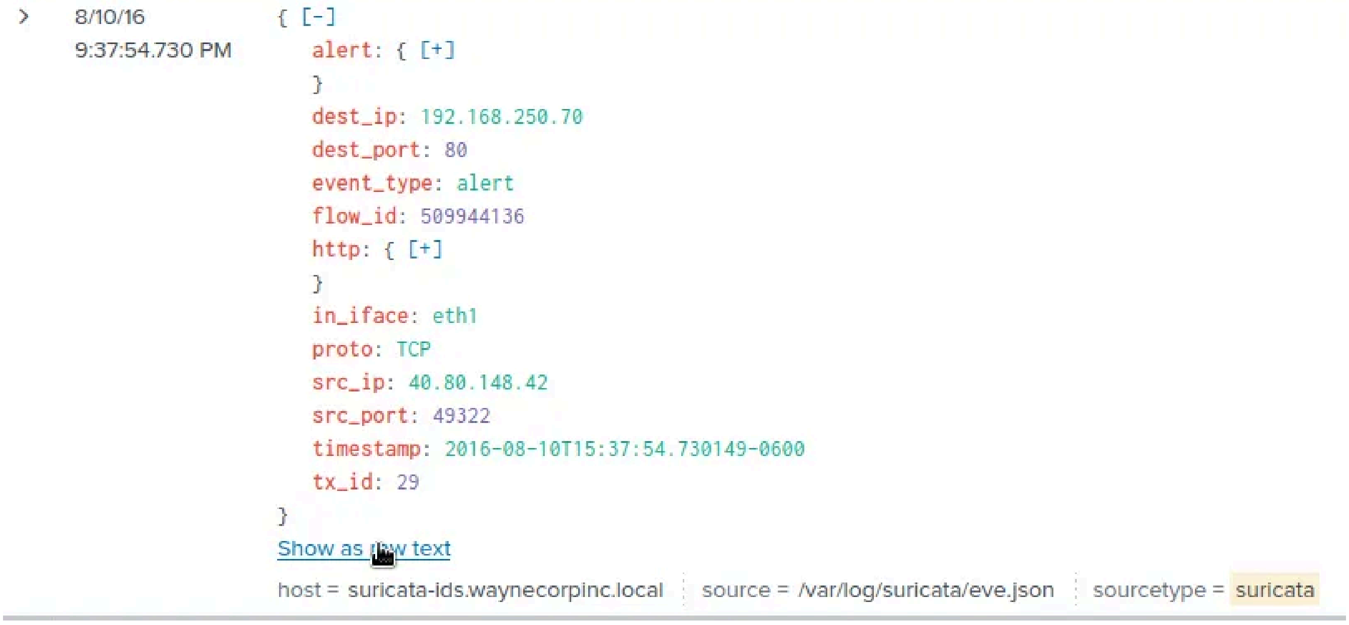
Values	Count	%
suricata	29,119	38.673%
stream:http	21,547	28.617%
fortigate_utm	12,778	16.97%
iis	11,851	15.739%



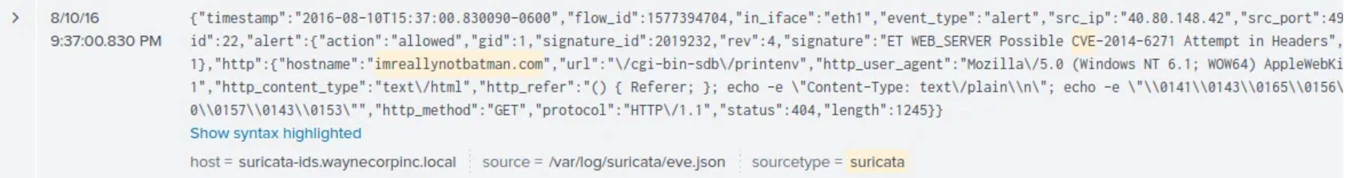
```
index=botsv1 imreallynotbatman.com sourcetype=suricata CVE
```

✓ 38 events (before 9/11/23 1:52:43.000 PM) No Event Sampling

Once the results populate, I clicked on "Show as raw text" to let me see the text. There's a few different results so keep looking through the other results.



```
> 8/10/16              { [-]
  9:37:54.730 PM          alert: { [+]
                          }
                          dest_ip: 192.168.250.70
                          dest_port: 80
                          event_type: alert
                          flow_id: 509944136
                          http: { [+]
                          }
                          in_iface: eth1
                          proto: TCP
                          src_ip: 40.80.148.42
                          src_port: 49322
                          timestamp: 2016-08-10T15:37:54.730149-0600
                          tx_id: 29
                       }
                       Show as raw text
                       host = suricata-ids.waynecorpinc.local   source = /var/log/suricata/eve.json   sourcetype = suricata
```

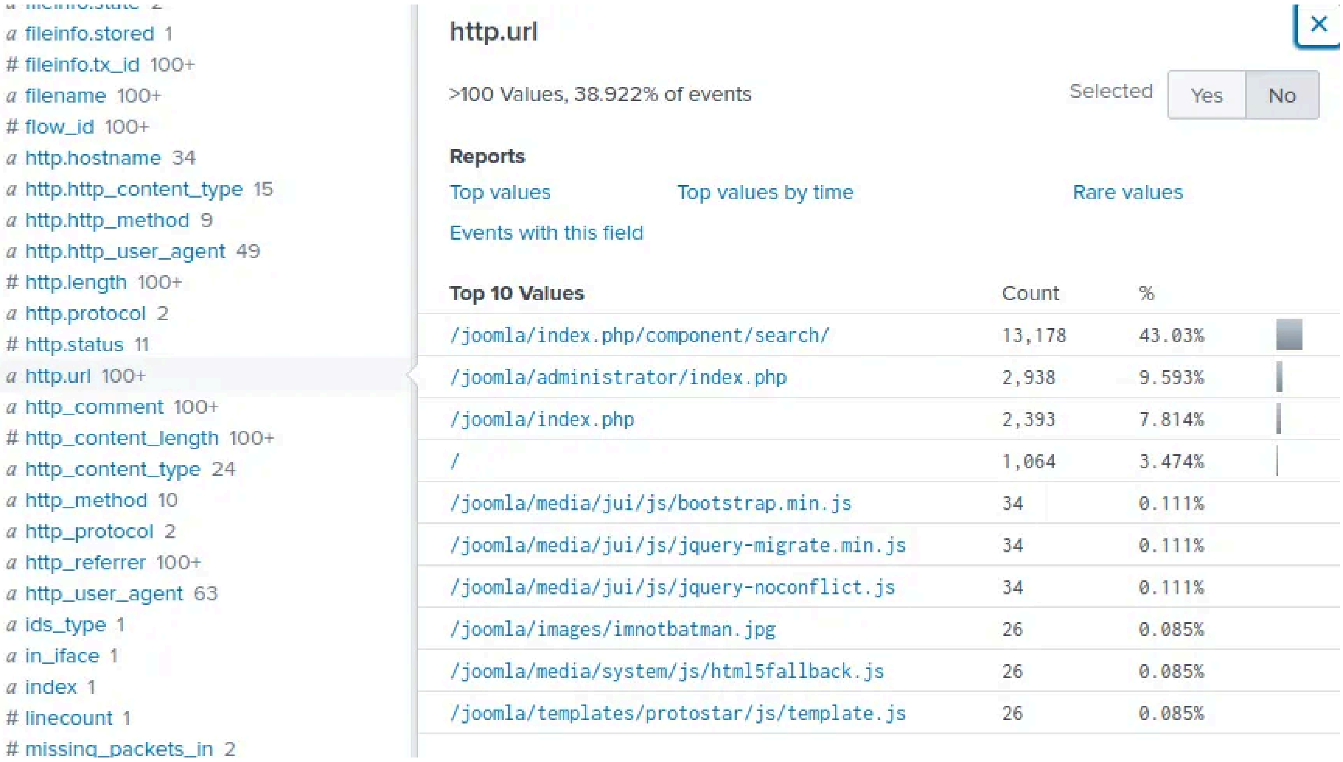


```
> 8/10/16         {"timestamp":"2016-08-10T15:37:00.830090-0600","flow_id":1577394704,"in_iface":"eth1","event_type":"alert","src_ip":"40.80.148.42","src_port":49
  9:37:00.830 PM  id":22,"alert":{"action":"allowed","gid":1,"signature_id":2019232,"rev":4,"signature":"ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers",
                  1},"http":{"hostname":"imreallynotbatman.com","url":"\/cgi-bin-sdb\/printenv","http_user_agent":"Mozilla\/5.0 (Windows NT 6.1; WOW64) AppleWebKi
                  1","http_content_type":"text\/html","http_refer":"() { Referer; }; echo -e \"Content-Type: text\/plain\\n\"; echo -e \"\\0141\\0143\\0165\\0156\
                  0\\0157\\0143\\0153\"","http_method":"GET","protocol":"HTTP\/1.1","status":404,"length":1245}}
                  Show syntax highlighted
                  host = suricata-ids.waynecorpinc.local   source = /var/log/suricata/eve.json   sourcetype = suricata
```

Answer: CVE-2014–6271

2: What is the CMS our web server is using?

I searched what CMS meant first since I had no idea. It stands for content management system. Since it helps us build websites, I looked at http.url fields. I clicked on it and saw lots of joomla. I also searched what it was, and it said that it's a CMS. Please note that I did change my search query back to `index=botsv1 imreallynotbatman.com` first. You may need to do that so you can see the http.url field at the left.


a fileinfo.state 2
a fileinfo.stored 1
# fileinfo.tx_id 100+
a filename 100+
# flow_id 100+
a http.hostname 34
a http.http_content_type 15
a http.http_method 9
a http.http_user_agent 49
# http.length 100+
a http.protocol 2
# http.status 11
a http.url 100+
a http_comment 100+
# http_content_length 100+
a http_content_type 24
a http_method 10
a http_protocol 2
a http_referrer 100+
a http_user_agent 63
a ids_type 1
a in_iface 1
a index 1
# linecount 1
# missing_packets_in 2

http.url

>100 Values, 38.922% of events

Reports

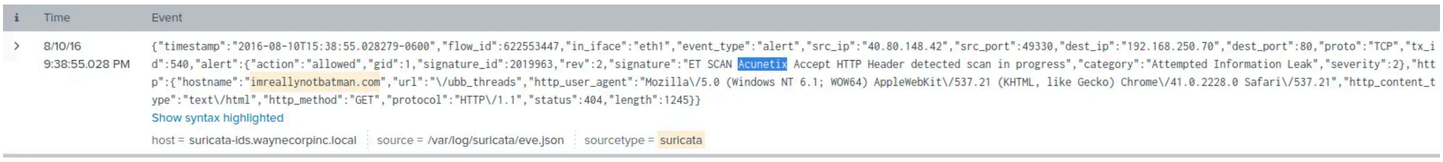
Top 10 Values	Count	%
/joomla/index.php/component/search/	13,178	43.03%
/joomla/administrator/index.php	2,938	9.593%
/joomla/index.php	2,393	7.814%
/	1,064	3.474%
/joomla/media/jui/js/bootstrap.min.js	34	0.111%
/joomla/media/jui/js/jquery-migrate.min.js	34	0.111%
/joomla/media/jui/js/jquery-noconflict.js	34	0.111%
/joomla/images/imnotbatman.jpg	26	0.085%
/joomla/media/system/js/html5fallback.js	26	0.085%
/joomla/templates/protostar/js/template.js	26	0.085%

Answer: joomla

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

I spent about 20 minutes on this, and solved question 4 while doing this. This was my search query `index=botsv1 imreallynotbatman.com sourcetype=suricata eventtype=suricata_eve_ids_attack dest=”imreallynotbatman.com” dest_ip=”192.168.250.70" status=404` . Some might not be needed. My thought process is that I wanted to limit my search results as much as possible. The eventtype filter is because we are under attack, which the IDS detected. The destination and destination IP is because we are being scanned. The status=404 filter is because if we are getting scanned, it should return some 404 results because web scanners check for subdirectories that may not exist for us.

I was able to find this from my search query. ET SCAN Acenetix seemed interesting, so I checked what what ET SCAN Acenetix was and found out Acenetix is a vulnerability scanner. That’s what we needed!



8/10/16
9:38:55.028 PM

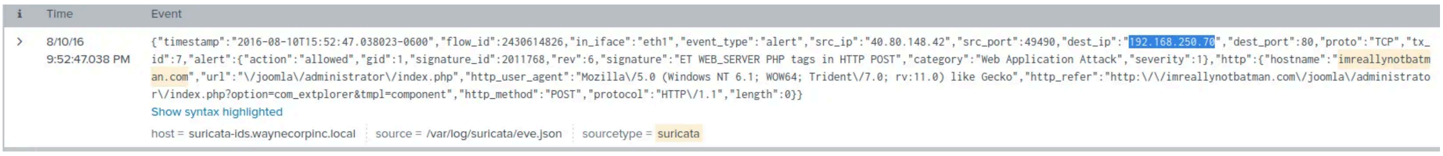
```
{"timestamp":"2016-08-10T15:38:55.028279-0600","flow_id":622553447,"in_iface":"eth1","event_type":"alert","src_ip":"40.80.148.42","src_port":49330,"dest_ip":"192.168.250.70","dest_port":80,"proto":"TCP","tx_id":540,"alert":{"action":"allowed","gid":1,"signature_id":2019963,"rev":2,"signature":"ET 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","protocol":"HTTP\/1.1","status":404,"length":1245}}
```

host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata

Answer: Acunetix

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

While attempting to do number 3, I did number 4. I know that we are getting attacked, so most likely we are the destination IP. I just grabbed one of the results from my search query `index=botsv1 imreallynotbatman.com sourcetype=suricata eventtype=suricata_eve_ids_attack` .



```
8/10/16
9:52:47.038 PM
{"timestamp":"2016-08-10T15:52:47.038023-0600","flow_id":2430614826,"in_iface":"eth1","event_type":"alert","src_ip":"40.80.148.42","src_port":49490,"dest_ip":"192.168.250.70","dest_port":80,"proto":"TCP","tx_id":7,"alert":{"action":"allowed","gid":1,"signature_id":2011768,"rev":6,"signature":"ET WEB_SERVER PHP tags in HTTP POST","category":"Web Application Attack","severity":1},"http":{"hostname":"imreallynotbatman.com","url":"\/joomla\/administrator\/index.php","http_user_agent":"Mozilla\/5.0 (Windows NT 6.1; WOW64; Trident\/7.0; rv:11.0) like Gecko","http_refer":"http:\/\/imreallynotbatman.com\/joomla\/administrator\/index.php?option=com_extplorer&tmpl=component","http_method":"POST","protocol":"HTTP\/1.1","length":0}}
host = suricata-ids.waynecorpinc.local   source = /var/log/suricata/eve.json   sourcetype = suricata
```

Answer: 192.168.250.70

Task 5 Exploitation Phase

1: What was the URI which got multiple brute force attempts?

This can be found in the text.

Answer: /joomla/administrator/index.php

2: Against which username was the brute force attempt made?

By following the text and trying the queries given, we will get the answer.

Answer: admin

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

By following the text and trying the queries given, we will get the answer.

Answer: batman

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

This can be found in the screenshot in the text.

Answer: 412

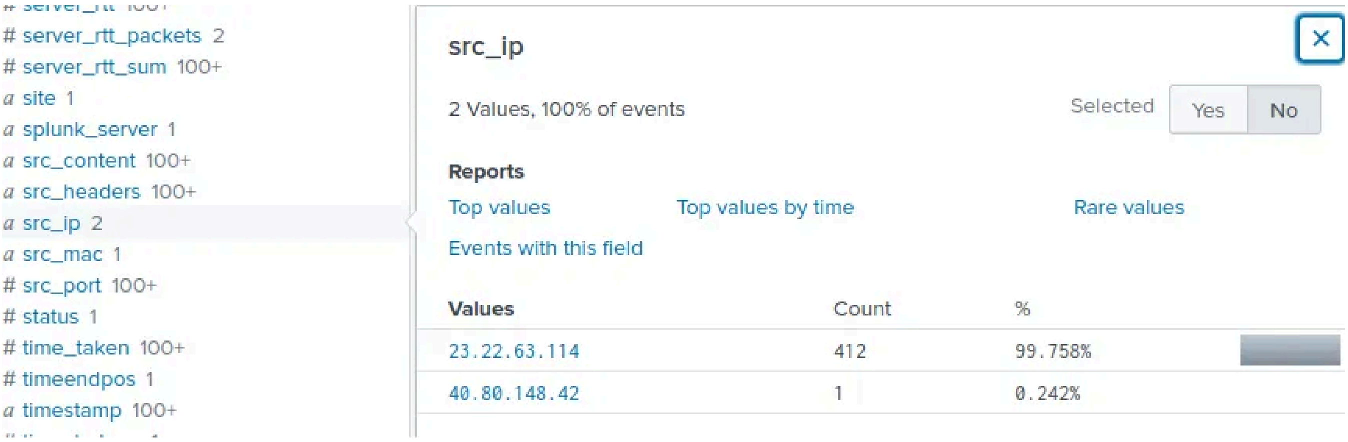
5: What IP address is likely attempting a brute force password attack against **imreallynotbatman.com**?

This can be found in the screenshot in the text. This is the query I used from the text `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 src_ip creds` . We will know which IP brute forced us since their IP will show up a lot.

Answer: 23.22.63.114

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

This can be found in the screenshot in the text. Using the same query, I navigated over to interesting fields and checked src_ip for different IPs. Only one different IP is shown which is probably what they used to log in.



server_rtt 100+
server_rtt_packets 2
server_rtt_sum 100+
a site 1
a splunk_server 1
a src_content 100+
a src_headers 100+
a src_ip 2
a src_mac 1
# src_port 100+
# status 1
# time_taken 100+
# timeendpos 1
a timestamp 100+

src_ip

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
23.22.63.114	412	99.758%
40.80.148.42	1	0.242%

Answer: 40.80.148.42

Task 6 Installation Phase

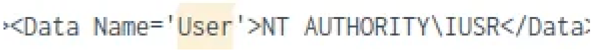
1: Sysmon also collects the Hash value of the processes being created. What is the MD5 HASH of the program 3791.exe?

I modified the query a bit that was given in the text. `index=botsv1 “3791.exe” sourcetype=”XmlWinEventLog” EventCode=1 MD5` I added “MD5” at the end so it will help highlight the text for me, helping me find the hash a lot easier. There were 5 results for me. I tried a few of them before finding out one result showed 3791.exe twice for me. I thought that could be it.

Answer: AAE3F5A29935E6ABCC2C2754D12A9AF0

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

This time, I used the same query, except I replaced “MD5" with “User” to help highlight the name for me.

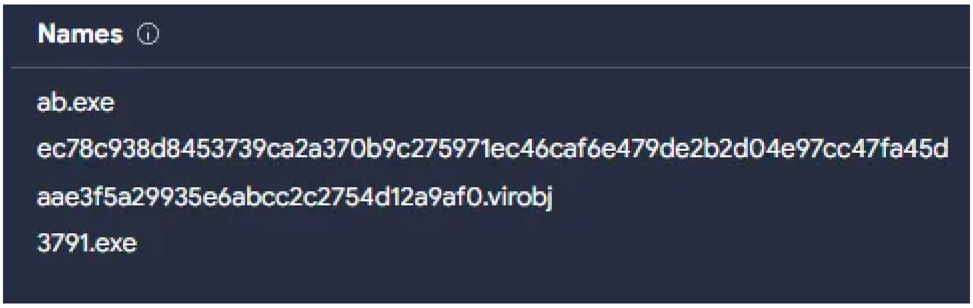


```
<Data Name='User'>NT AUTHORITY\IUSR</Data>
```

Answer: NT AUTHORITY\IUSR

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

I pasted the hash onto VirusTotal and went to the details tab. Scroll down a bit and you’ll find other names the program uses here.



Names

ab.exe
ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d
aae3f5a29935e6abcc2c2754d12a9af0.virobj
3791.exe

Answer: ab.exe

Task 7 Action on Objectives

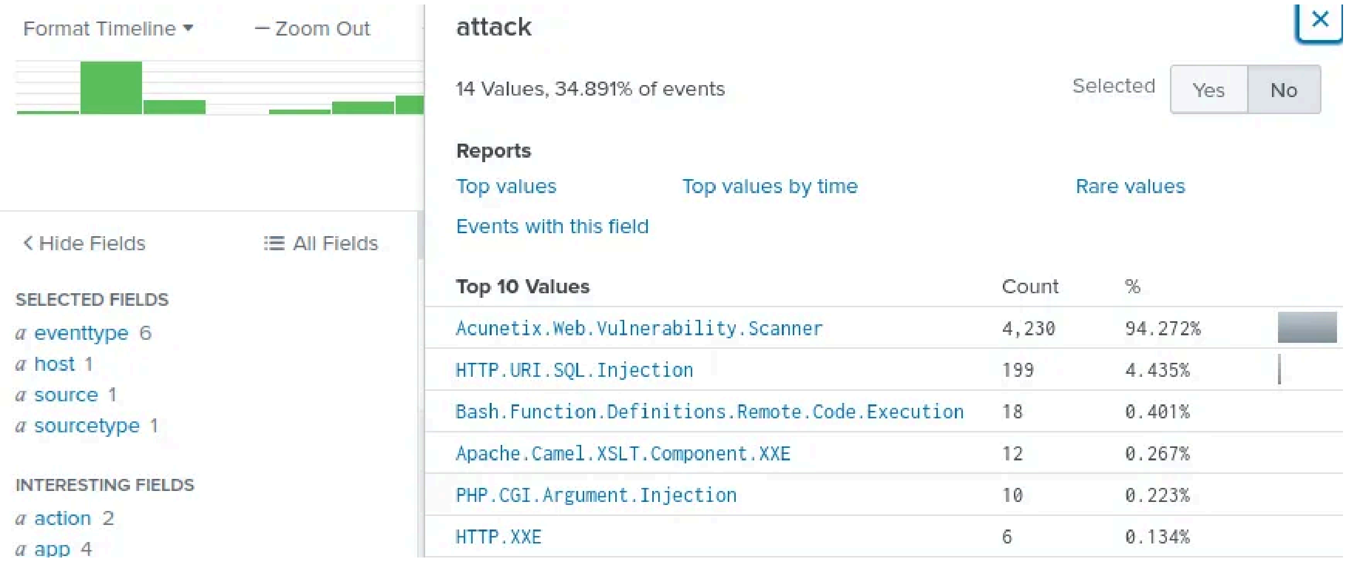
1: What is the name of the file that defaced the imreallynotbatman.com website ?

This can be found in the text and by following the example.

Answer: poisonivy-is-coming-for-you-batman.jpeg

2: 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?

This took me a little while. First, I changed the query into `index=botsv1 src=40.80.148.42 sourcetype=fortigate_utm` . We know we want to look at the data coming from fortigate_utm, and we also need to filter to make sure the source is from the attacker's IP. After that, I looked at the attack field on the left and looked at the results. We know it can't be the vulnerability scanner because the attacker has done the reconnaissance phase. SQL injection sounds right because they're attacking us now, besides the obvious that that the question tells us it's an SQL injection too.



attack

14 Values, 34.891% of events

Top 10 Values	Count	%
Acunetix.Web.Vulnerability.Scanner	4,230	94.272%
HTTP.URI.SQL.Injection	199	4.435%
Bash.Function.Definitions.Remote.Code.Execution	18	0.401%
Apache.Camel.XSLT.Component.XXE	12	0.267%
PHP.CGI.Argument.Injection	10	0.223%
HTTP.XXE	6	0.134%

Answer: HTTP.URI.SQL.Injection

Task 8 Command and Control Phase

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

This can be found in the screenshot in the text and by following the example query too.

Answer: prankglassinebracket.jumpingcrab.com

Task 9 Weaponization Phase

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

There were a lot of IPs throughout searching on VirusTotal and Robtex that I admittedly just looked at the answer format to see how many numbers were in each octet.

Answer: 23.22.63.114

2: 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?

I had to use the hint for this. I searched for about 5–10 minutes each on VirusTotal and Robtex and couldn't find anything. I used the site the hint gave and looked through the results.

Answer: lillian.rose@po1s0n1vy.com

Task 10 Delivery Phase

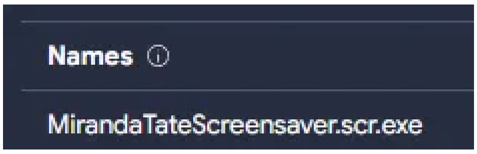
1: What is the HASH of the Malware associated with the APT group?

This can be found in the screenshot in the text.

Answer: c99131e0169171935c5ac32615ed6261

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

I simply just copied the hash and put it onto VirusTotal. I went to details tab and looked at the names at the bottom.



Names ⓘ

MirandaTateScreensaver.scr.exe

Answer: MirandaTateScreensaver.scr.exe

Thoughts:

Ah this was a good refresher! It walked you through a lot of stuff but also gave you a few questions where you had to figure out some queries yourself. I think I prefer this sort of training rather than those that doesn't give you anything. I usually struggle the most with where to start. Once I know how to start, I can start working my way to solving problems. That being said, I know in real-life scenarios, it will be different. That is one thing I want to improve on, knowing how to start. I know other training programs have Boss of the SOC that does minimal handholding. I hope to get better with Splunk before attempting those sorts of labs!

Cybersecurity Siem Splunk Incident Response

T

Follow

Written by Toumo

151 Followers · 1 Following

No responses yet

What are your thoughts?

Respond

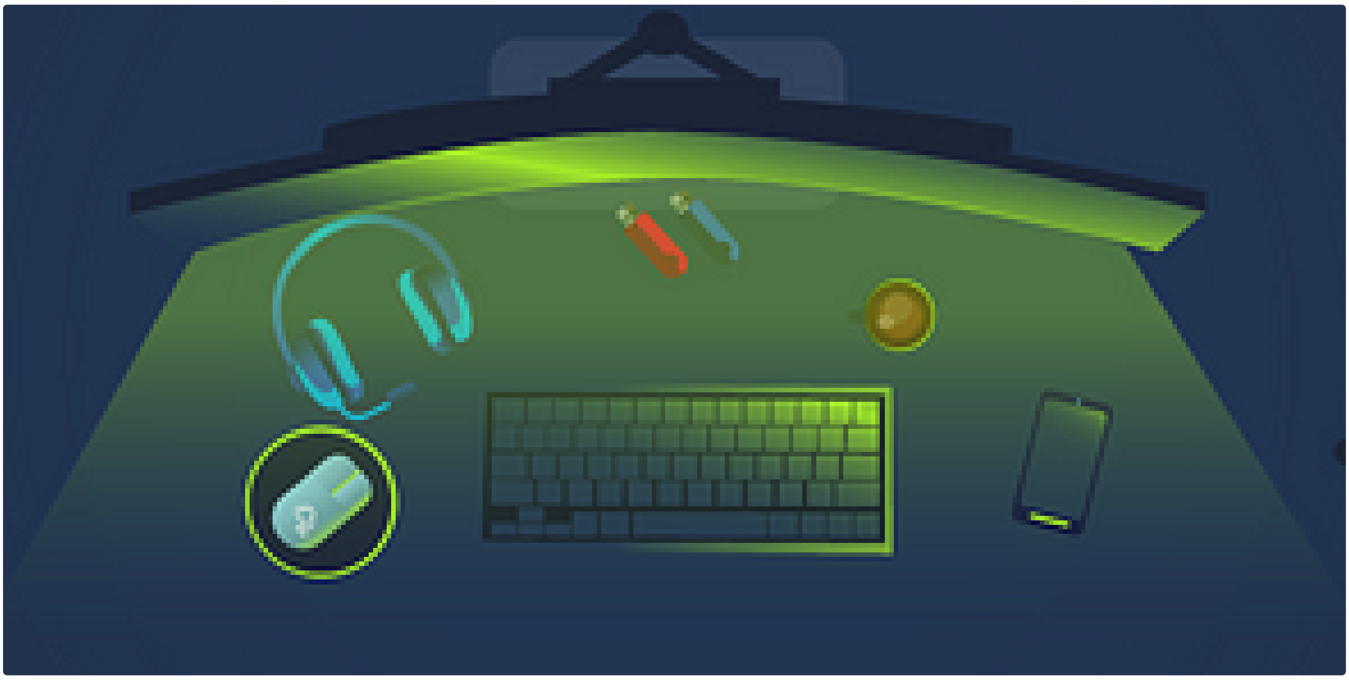
More from Toumo

T Toumo

TryHackMe Redline Write-Up

We just finished the Autopsy room and now we will be learning how to use Redline. I've never used it, nor have I heard of it before, so…

Aug 8, 2023 45 4

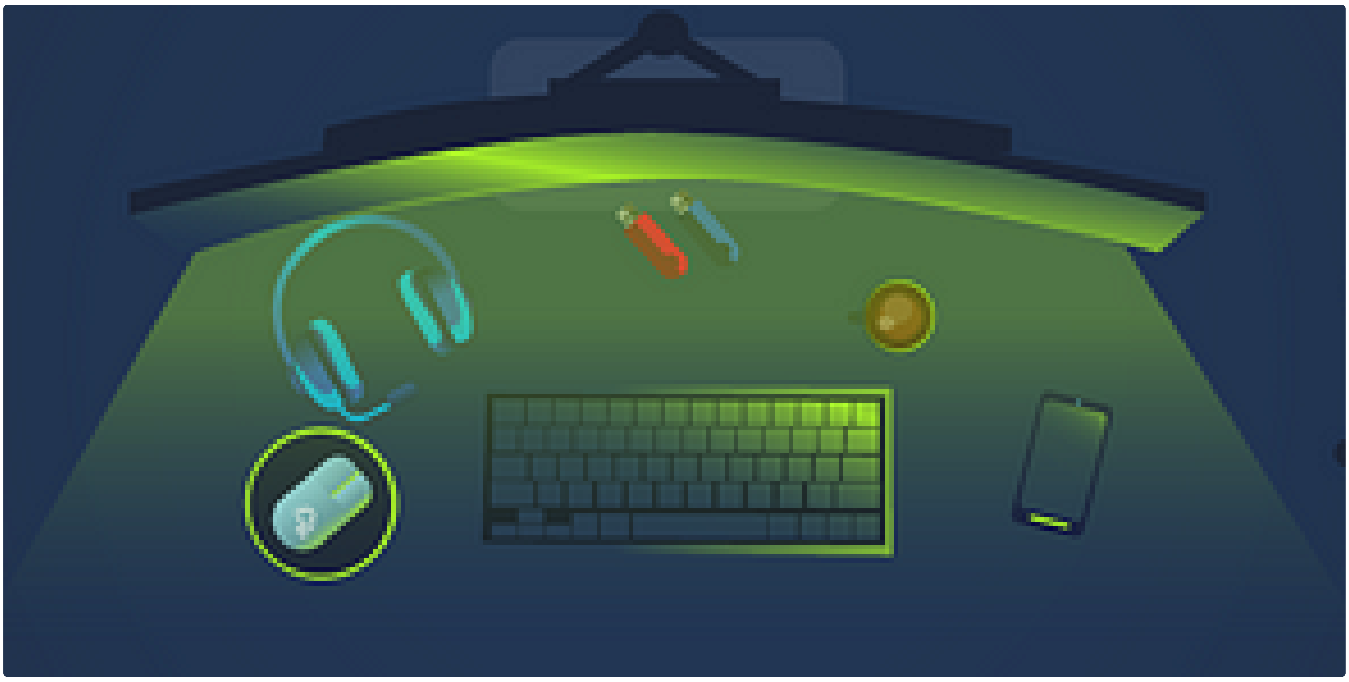


T Toumo

TryHackMe Windows Forensics 1 Write-Up

For me, it's the final stretch to completing the SOC Level 1 learning path. I have completed all the phishing rooms already early on before…

Aug 6, 2023 39 1

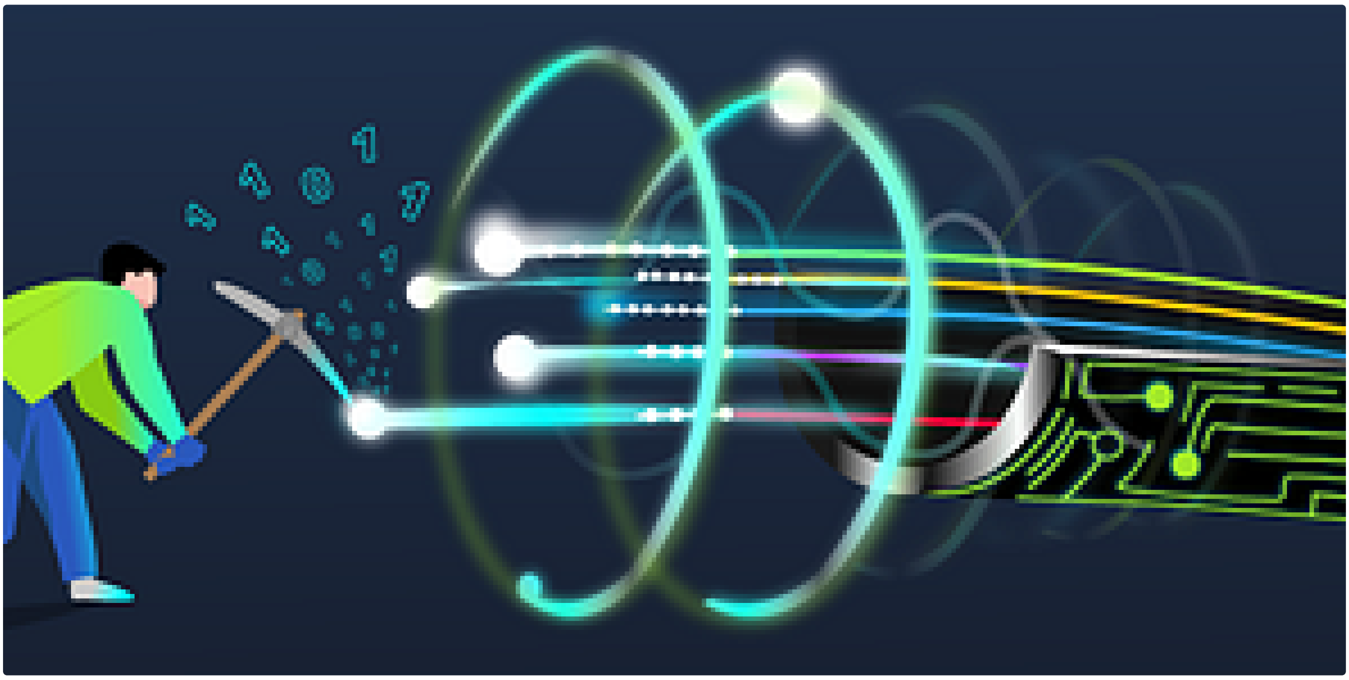


T Toumo

TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023 20 1



T Toumo

TryHackMe NetworkMiner Write-Up

This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what...

Jul 5, 2023 6 1

See all from Toumo

Recommended from Medium

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

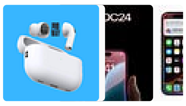
Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

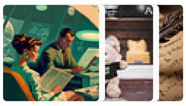
Sep 7, 2024 10

Lists



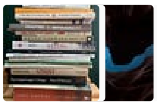
Tech & Tools

22 stories · 377 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4321 saves



Staff picks

793 stories · 1549 saves

Natural Language Processing

1883 stories · 1524 saves

Fritzadriano

Retracted — TryHackMe WriteUp

IInvestigate the case of the missing ransomware. After learning about Wazuh previously, today’s task is a bit different.

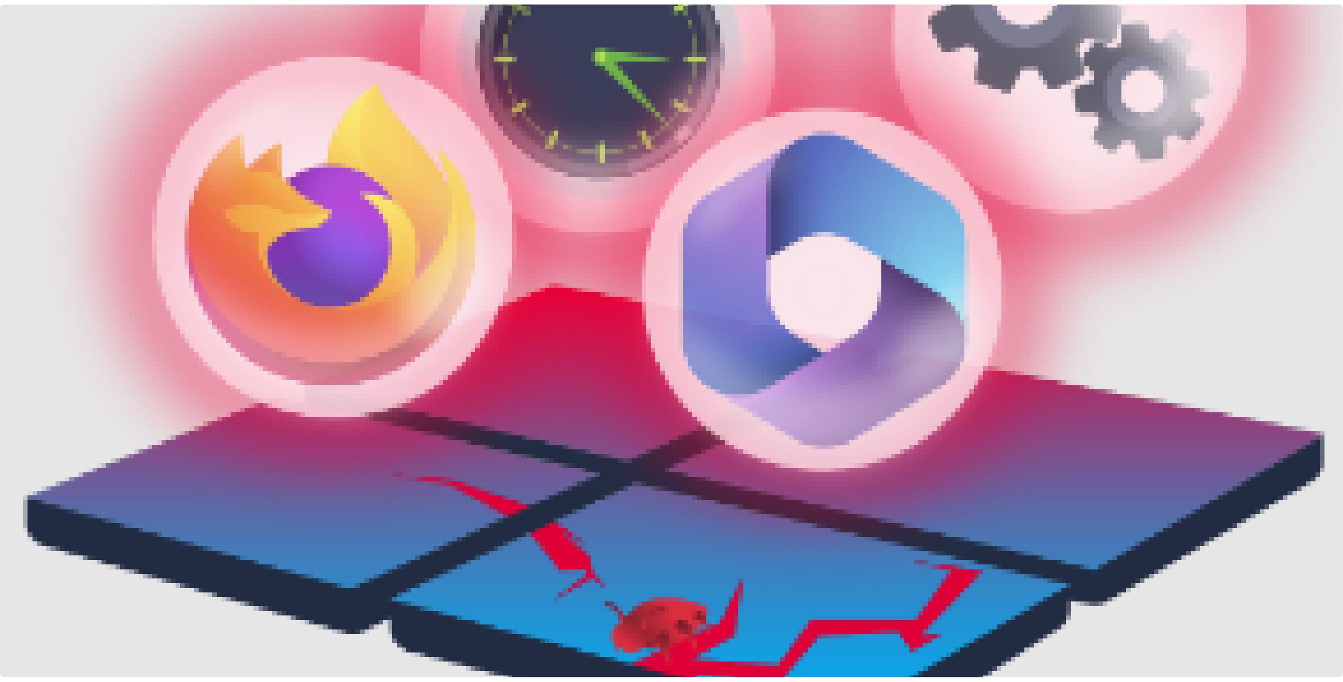
Sep 4, 2024 50

9purp0s3 | Steven

HackTheBox SOC Analyst Pathway Journey

HackTheBox SOC Analyst Pathway Journey

Jul 21, 2024 3

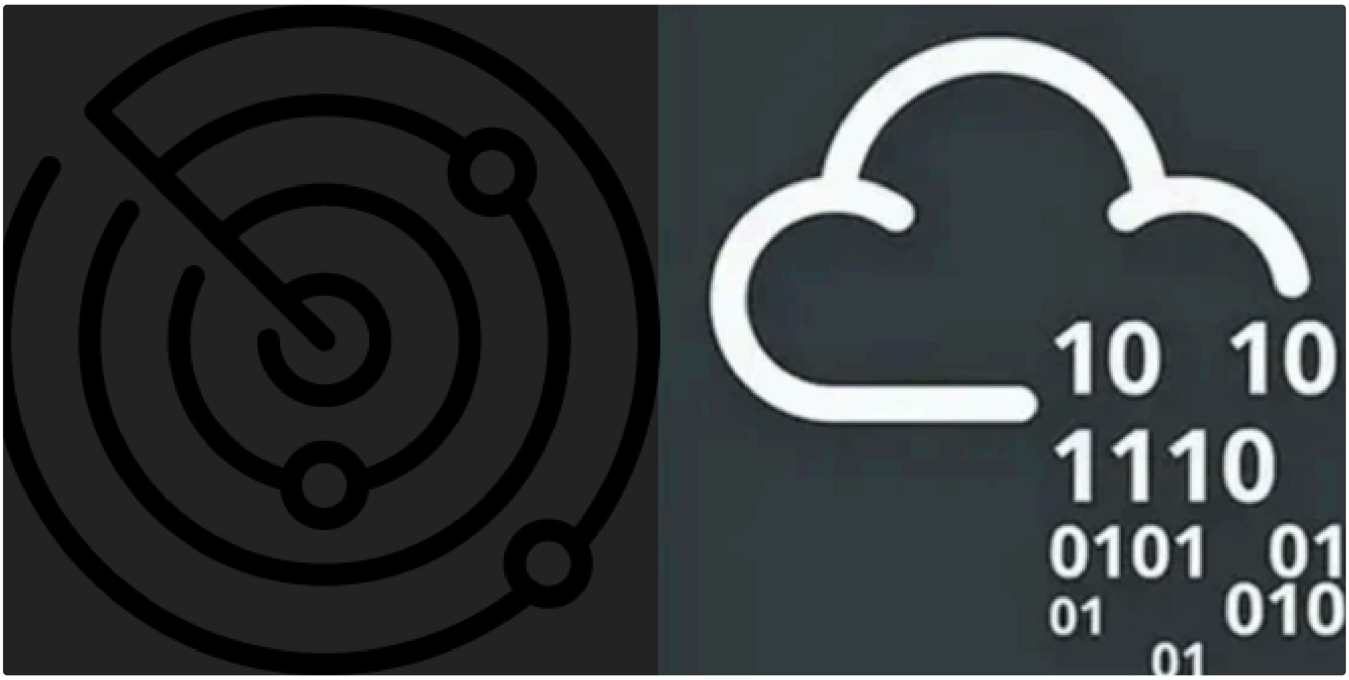


MAGESH

Windows Applications Forensics-Tryhackme Writeup

Perform a live analysis on Windows systems, focused on determining the outliers based on known behaviour of scheduled tasks, services, and...

Oct 20, 2024



IritT

Nmap—TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024

See more recommendations