Incident handling with splunk

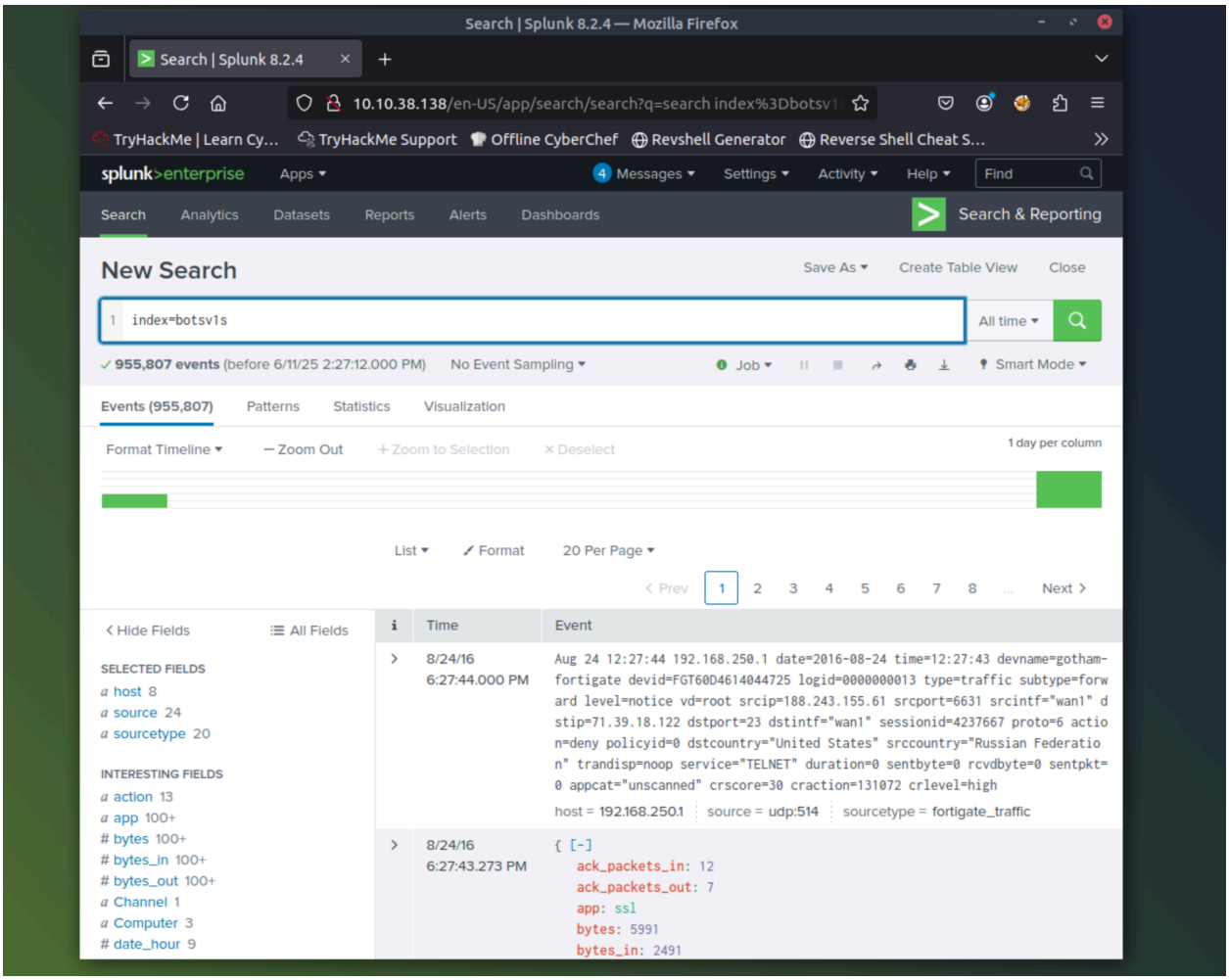
Task 4 **Reconnaissance Phase**

Step 1:

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

```
index=botsv1s
```

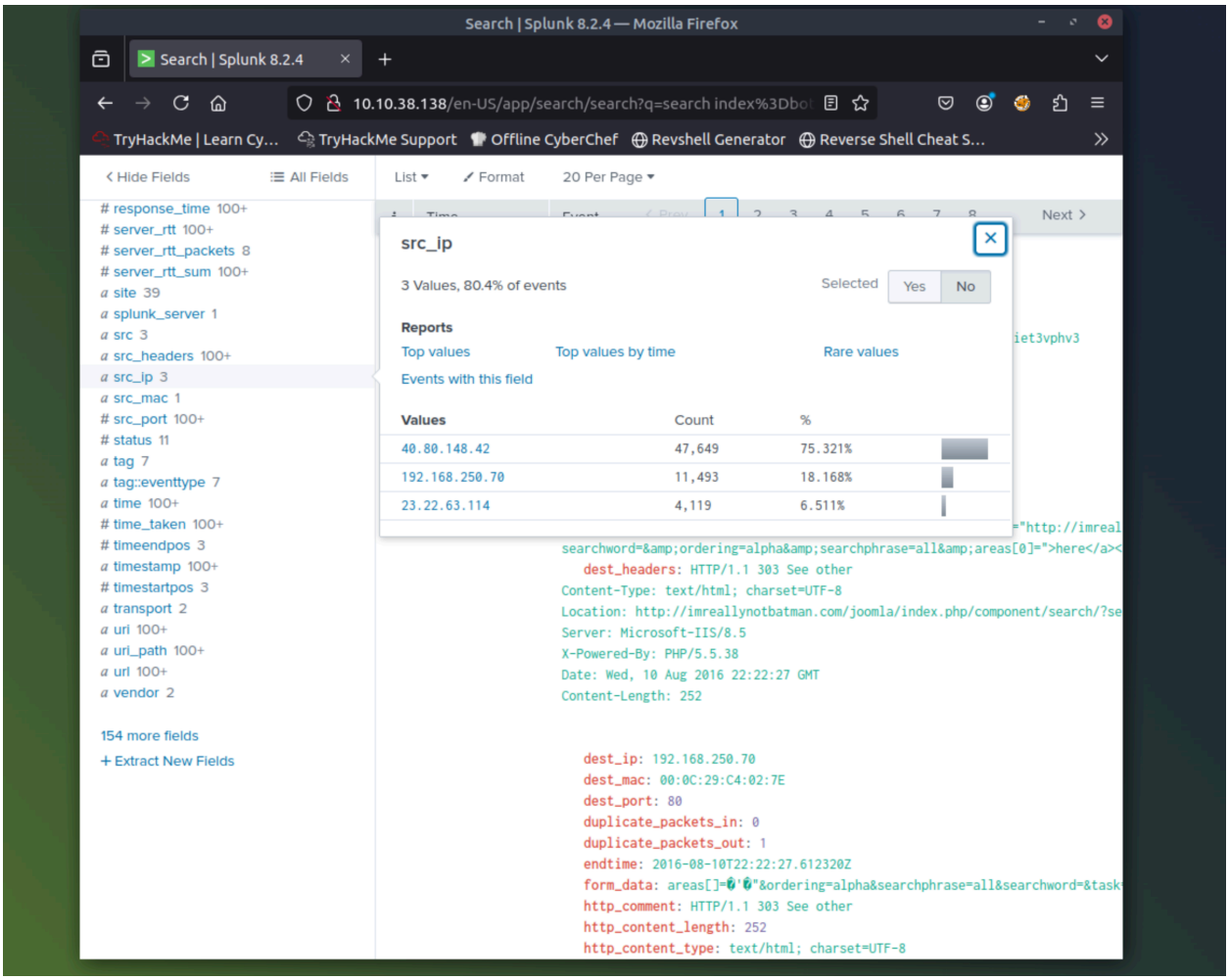
This index is part of a Splunk dataset that contains **realistic data**, including **logs** and **security events**, commonly used for cybersecurity training and analysis.

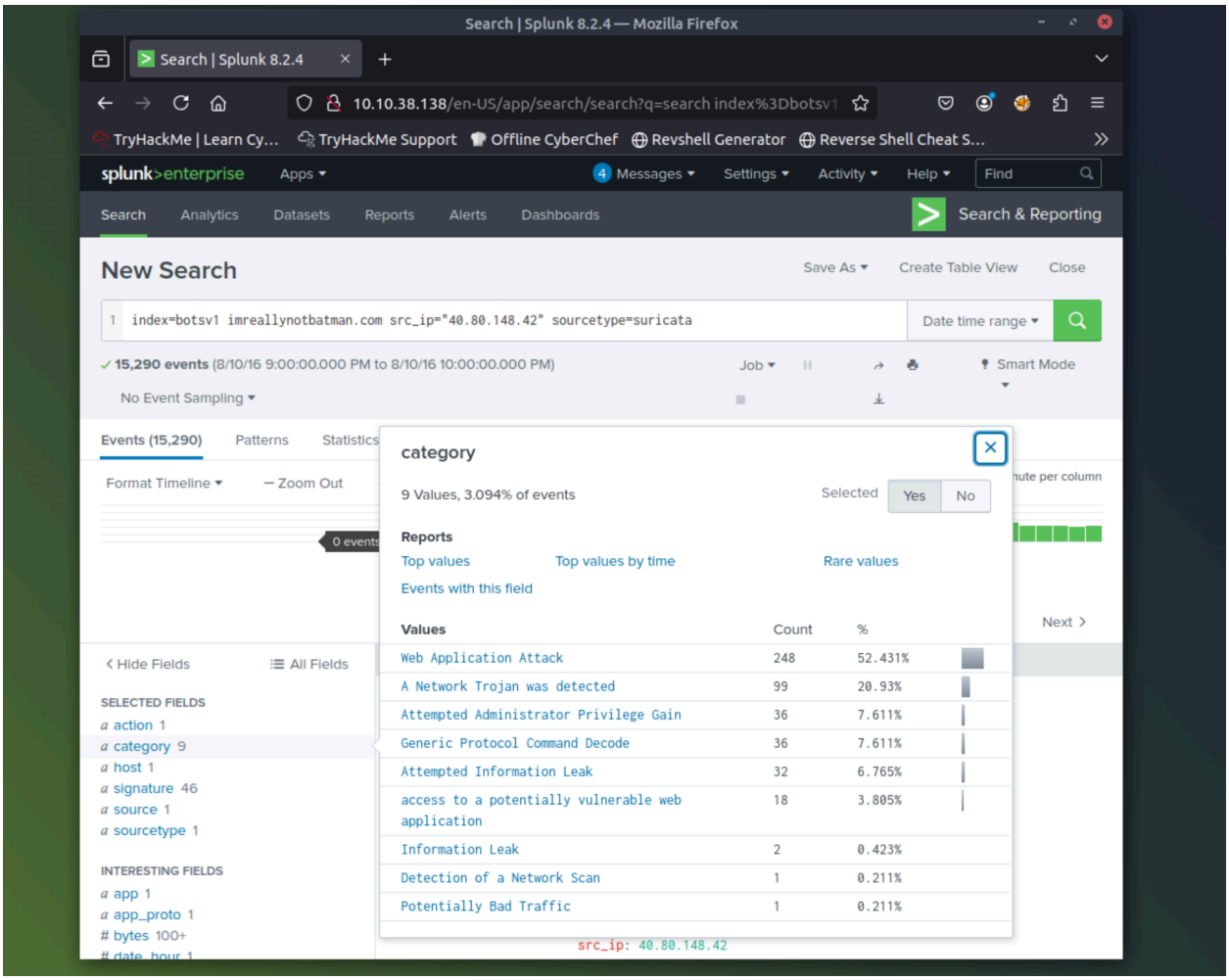


Step 2:

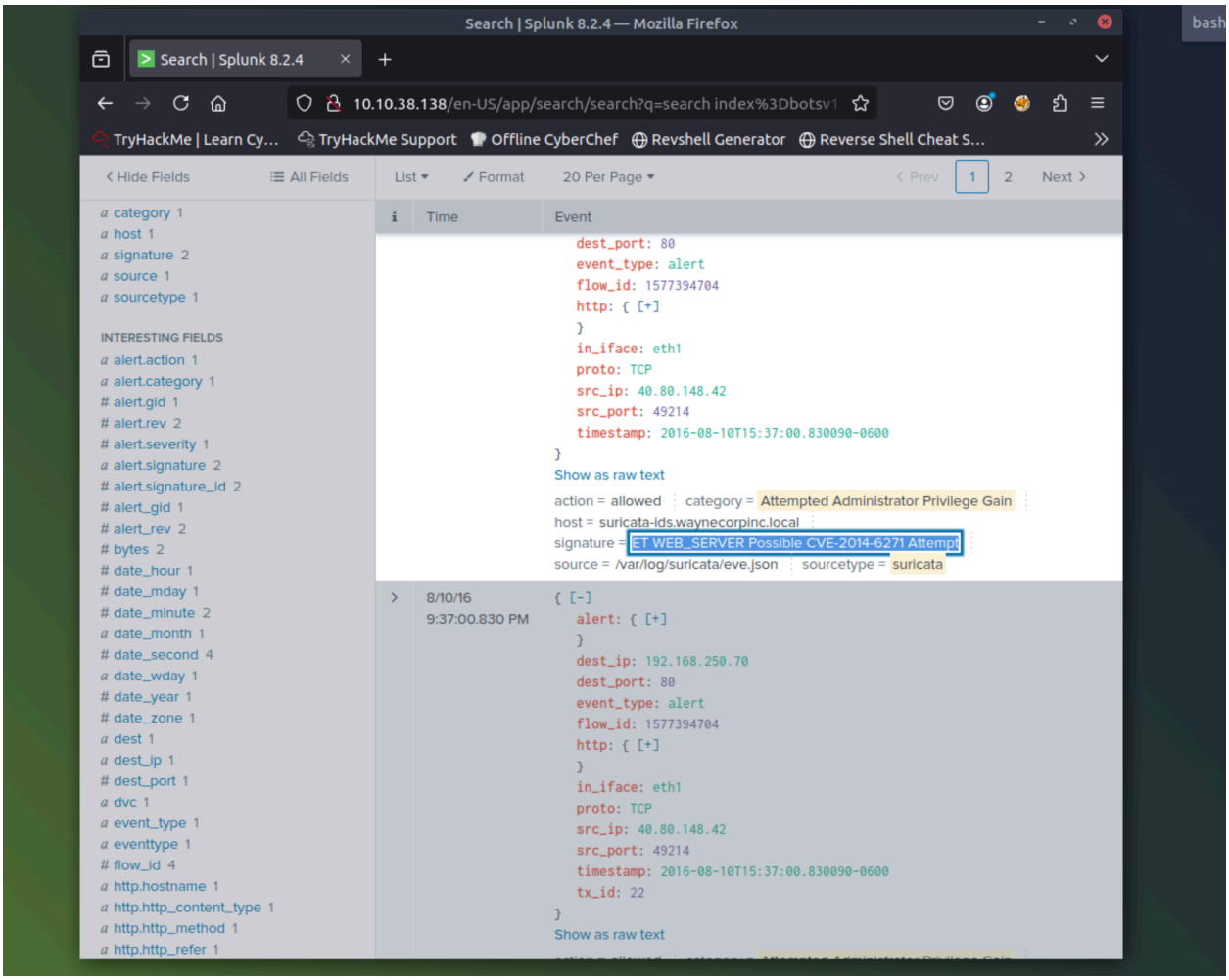
Let's investigate the **source IP addresses**.

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
Search | Splunk 8.2.4
10.10.38.138/en-US/app/search/search?q=search index%3Dbo
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
Hide Fields
All Fields
List
Format
20 Per Page
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+
timestartpos 3
a transport 2
a uri 100+
a uri_path 100+
a url 100+
a vendor 2
154 more fields
+ Extract New Fields
Next
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<
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

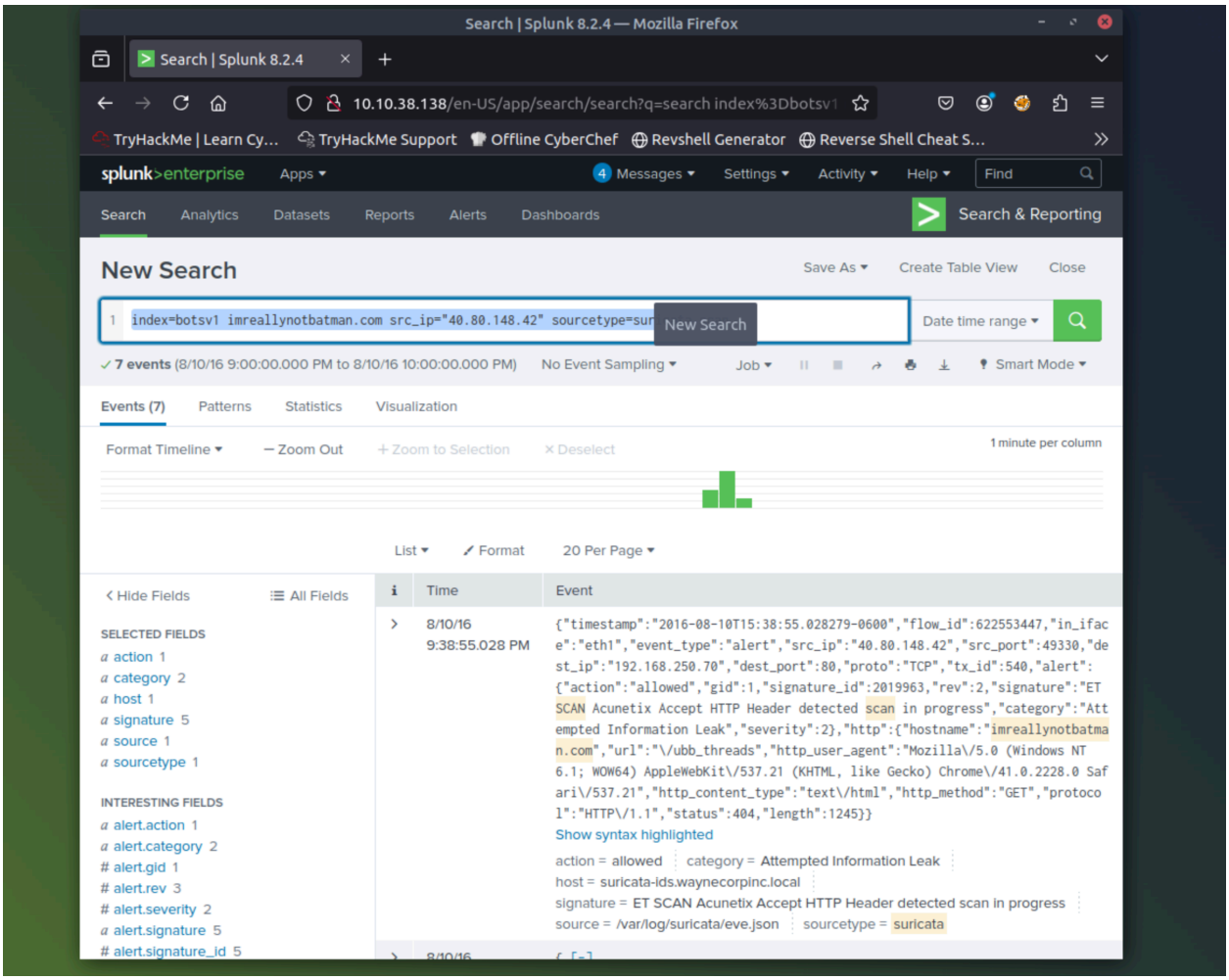


as look in web application attack it was catgerise sql injection and lets look for the options 3

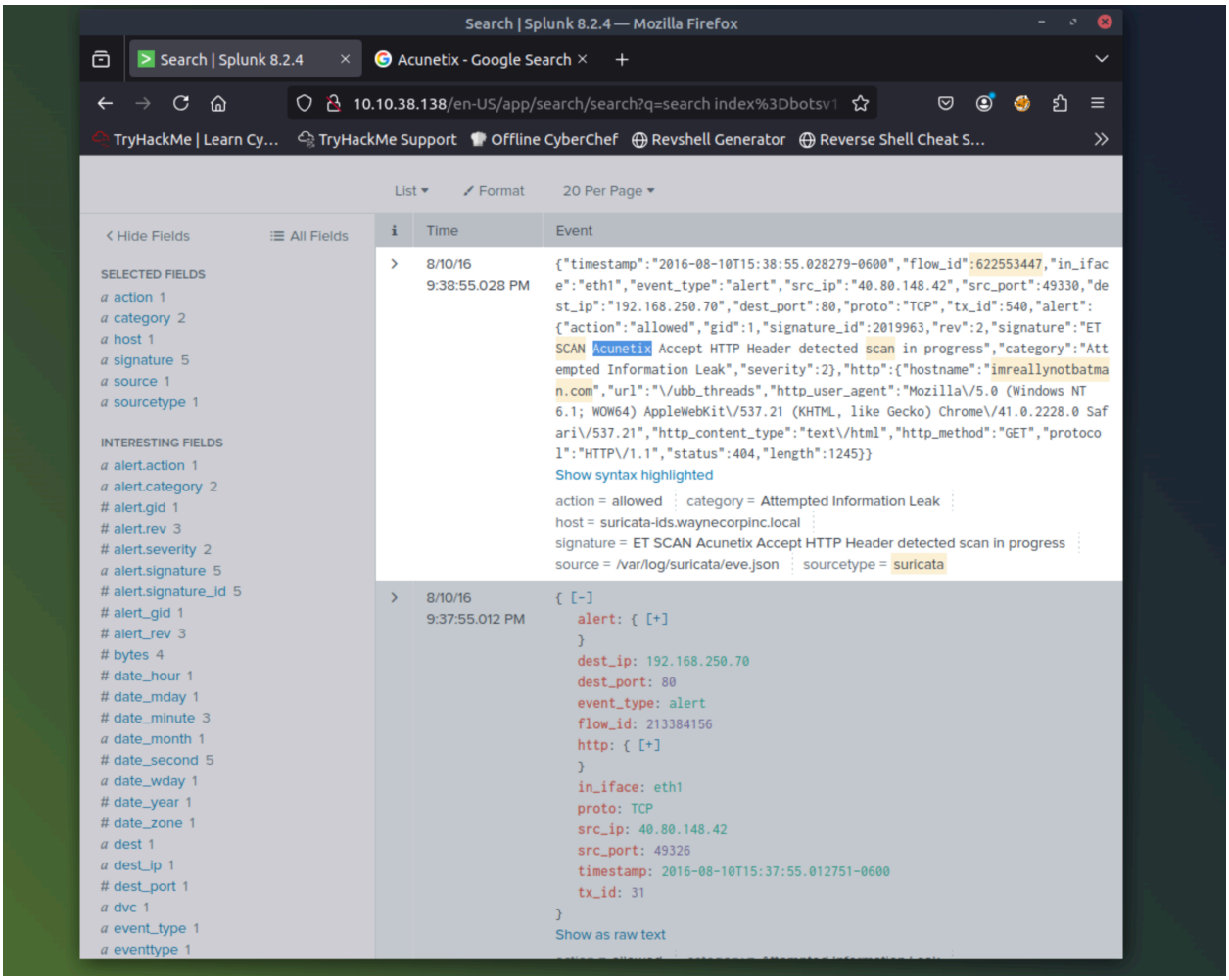


One suricata alert highlighted the CVE value associated with the attack attempt. What is the CVE value?

Cve-2014-6271



like so show raw text



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

acunetix

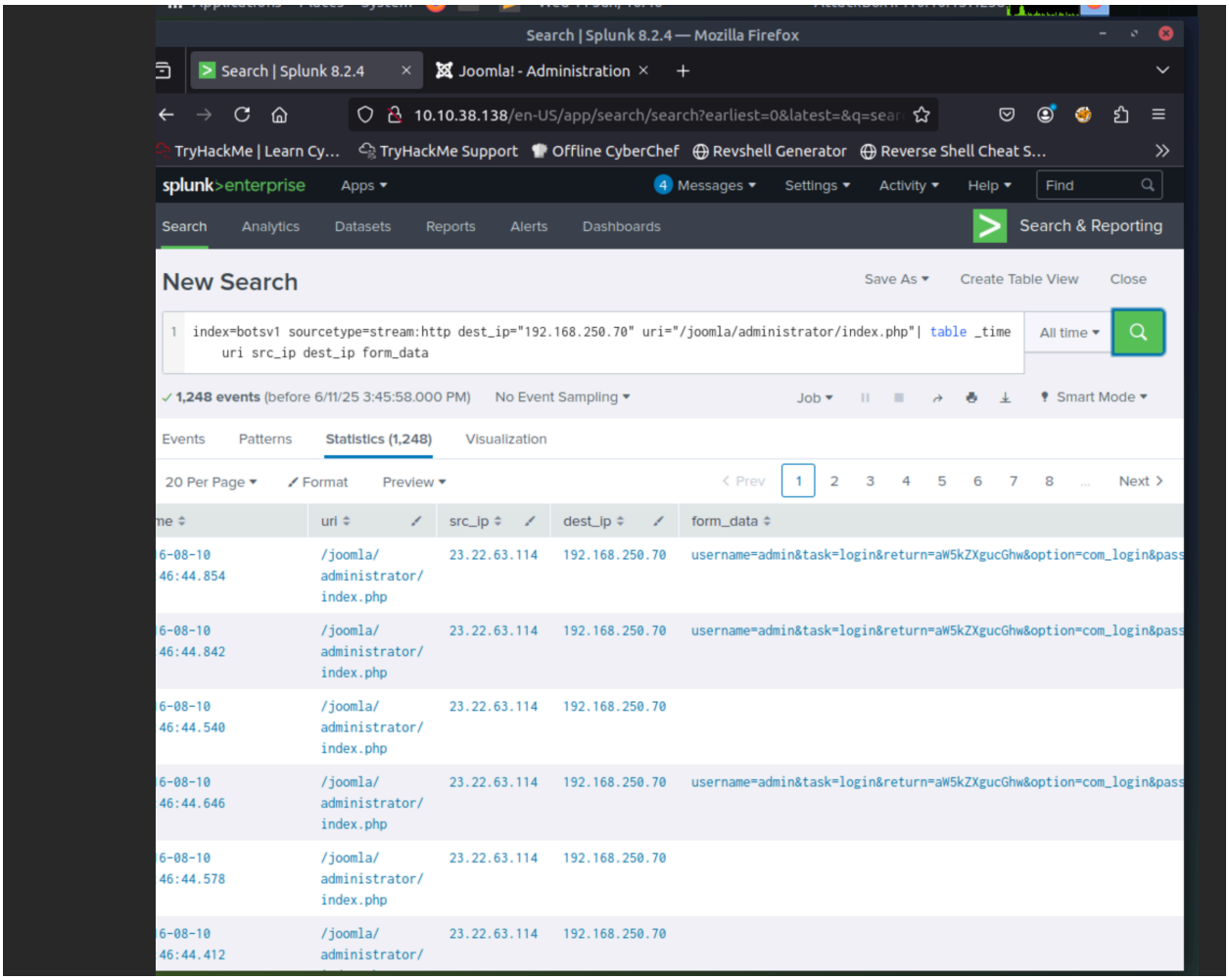
What is the IP address of the server imreallynotbatman.com?

192.168.250.70

Task 5 Exploitation Phase

What was the URI which got multiple brute force attempts?

/joomla/administrator/index.php



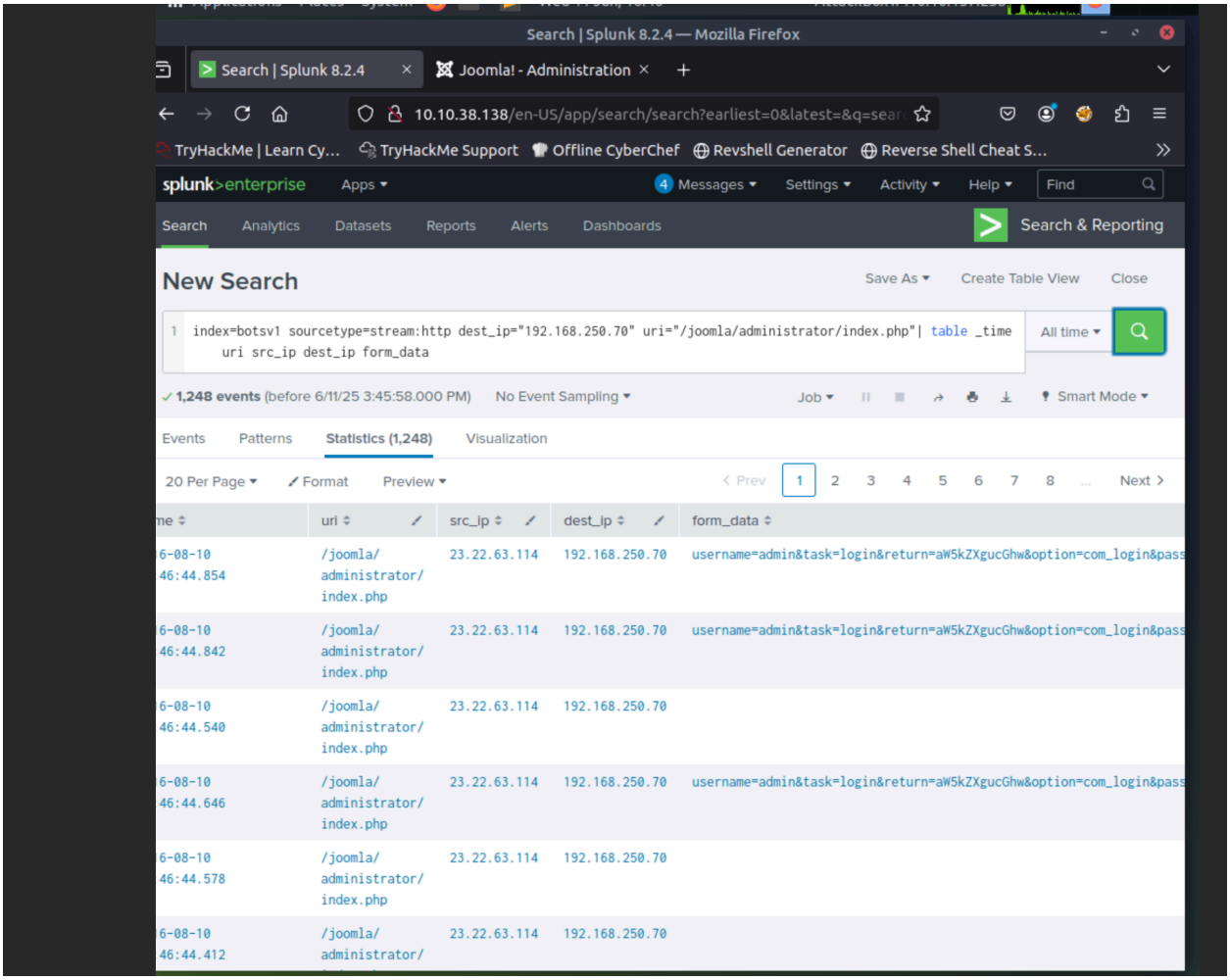
use this query to create contain important file

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

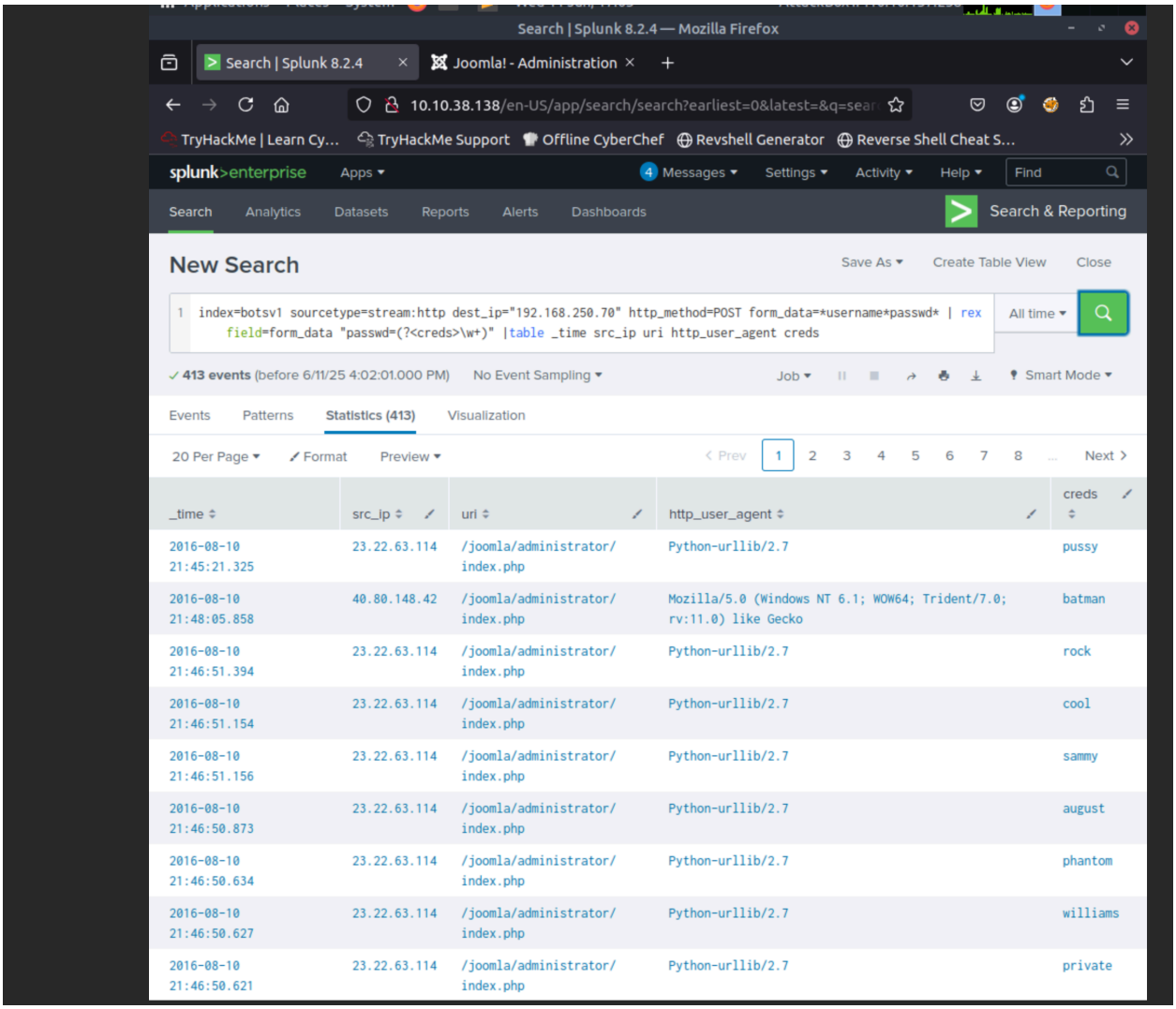


What was the correct password for admin access to the content management system running **imreallynotbatman.com**?

batman

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

412



as there were total 413 events and one was succesful

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

23.22.63.114

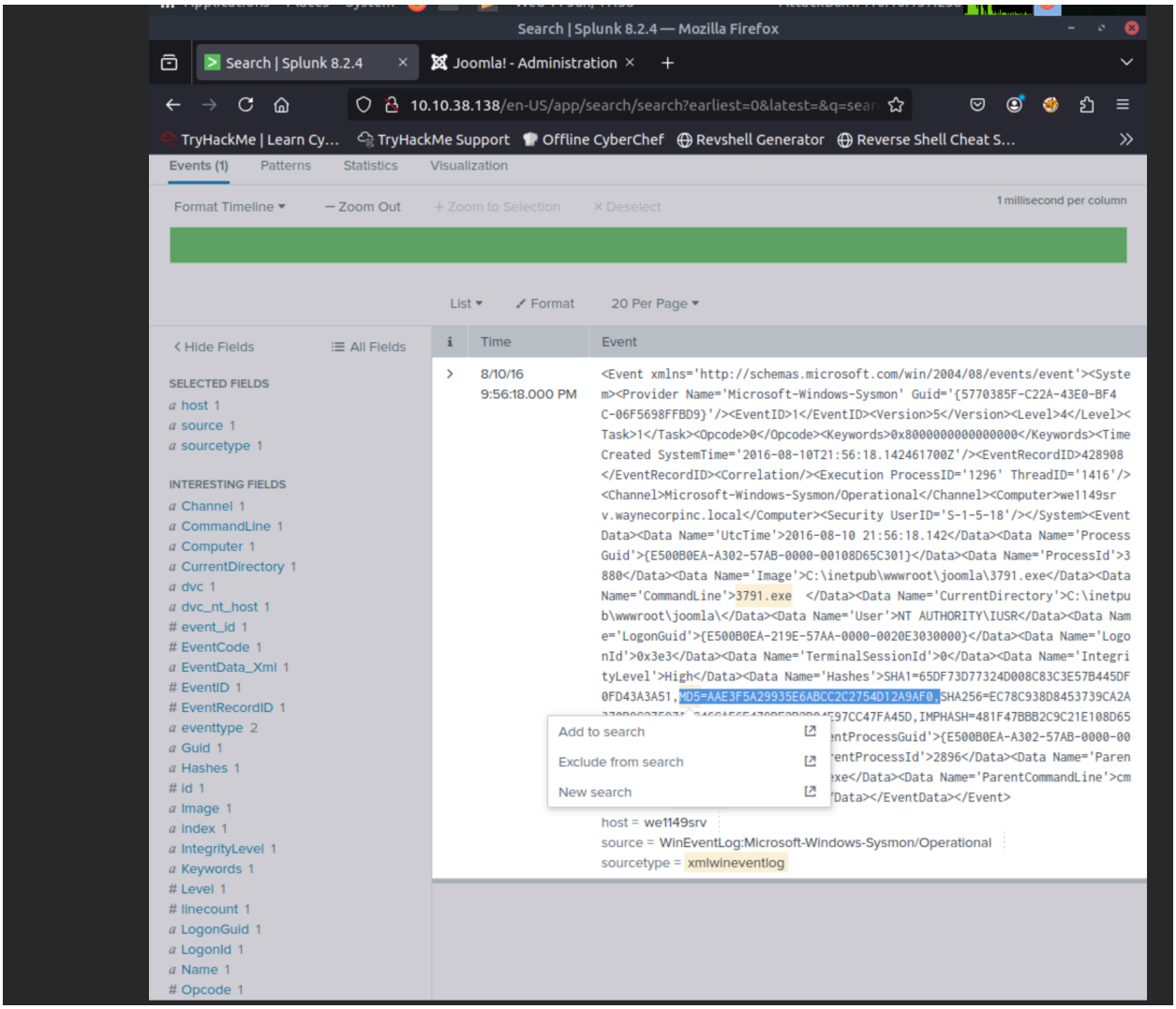
After finding the correct password, which IP did the attacker use to log in to the admin panel?

40.80.148.42

Task 6 Installation phase

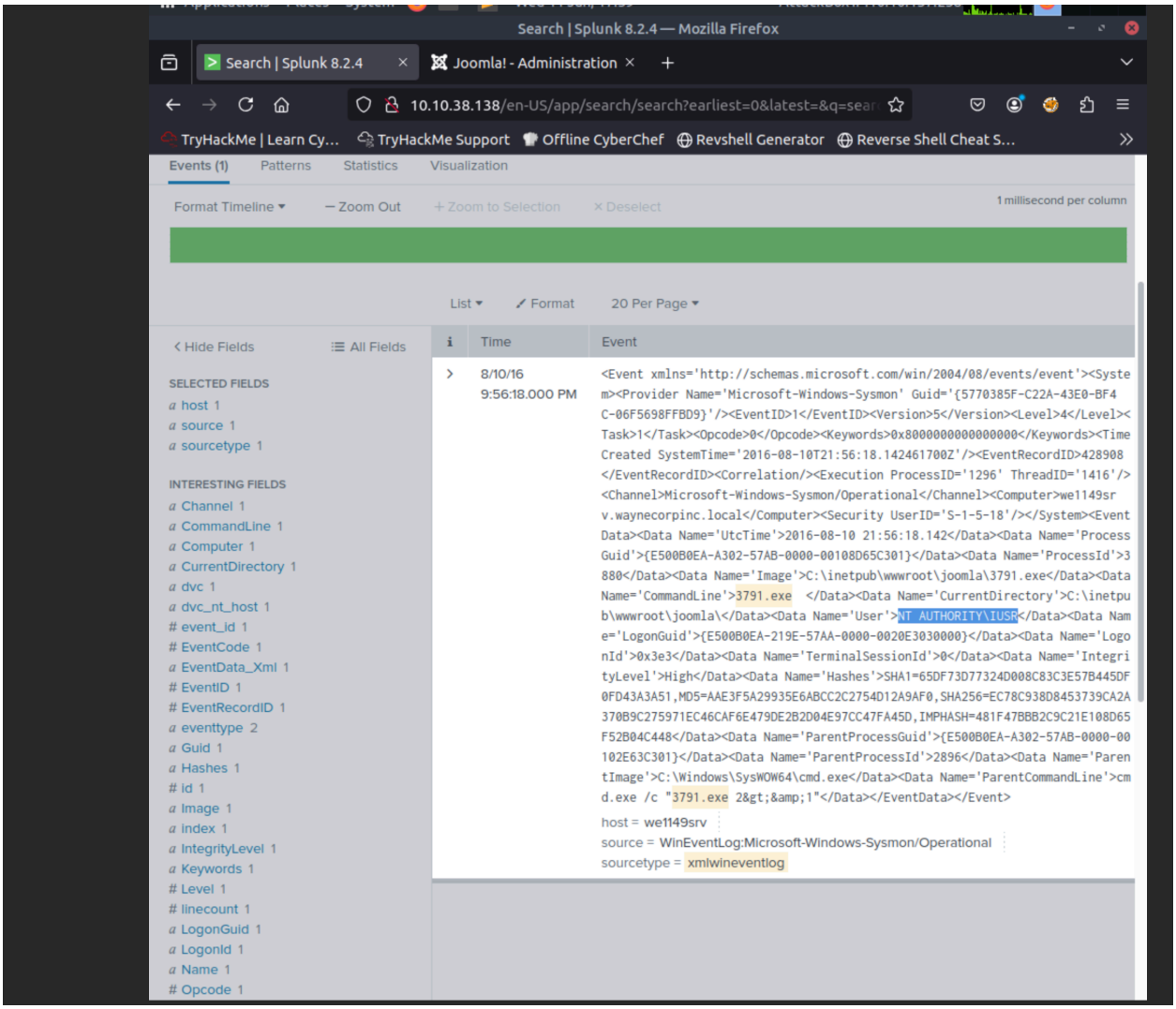
Sysmon also collects the Hash value of the processes being created. What is the MD5 HASH of the program 3791.exe?

AAE3F5A29935E6ABCC2C2754D12A9AF0



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

NT AUTHORITY\IUSR



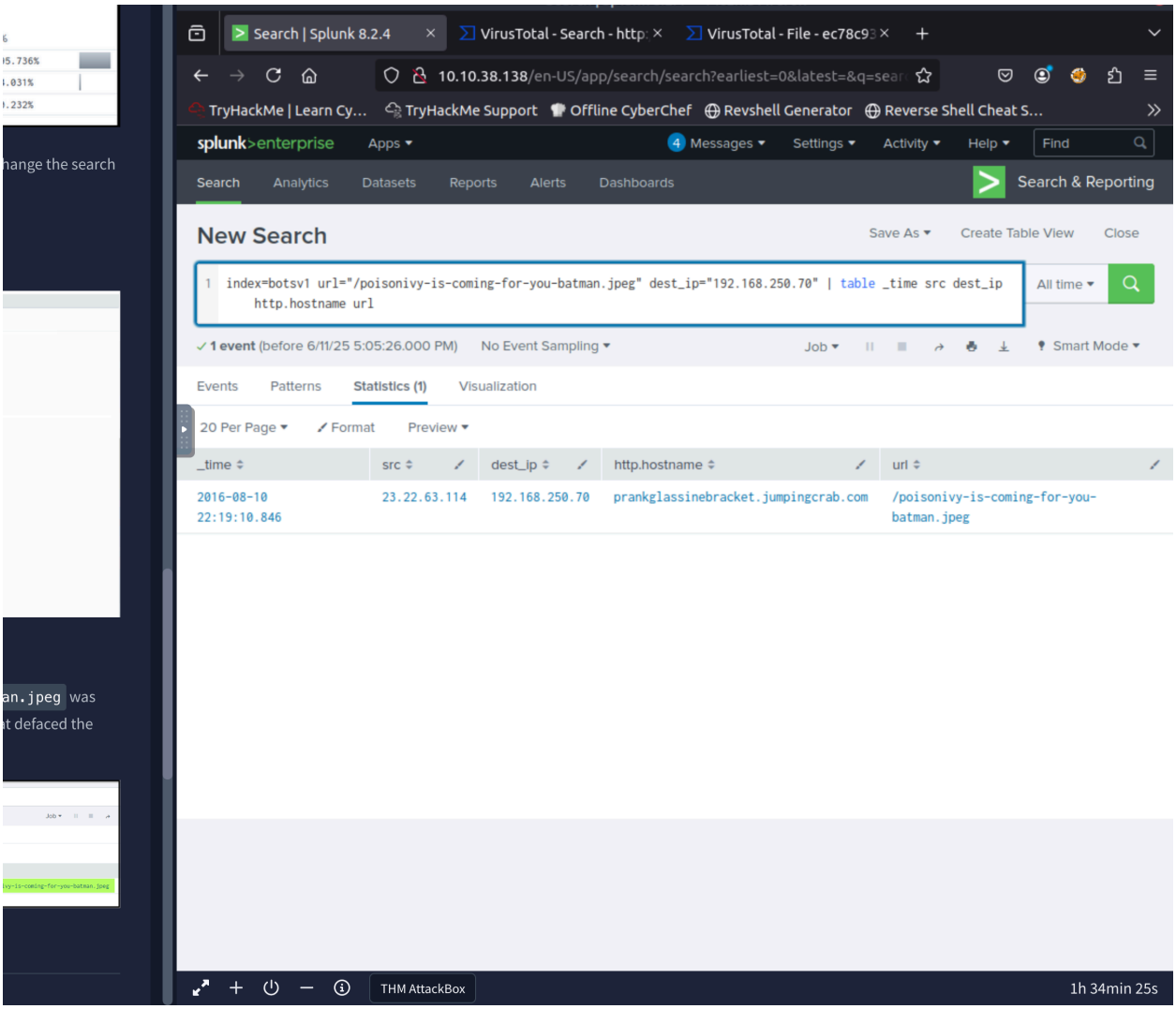
Search hash on the virustotal. What other name is associated with this file 3791.exe?

ab.exe

Task 7 action on objectives

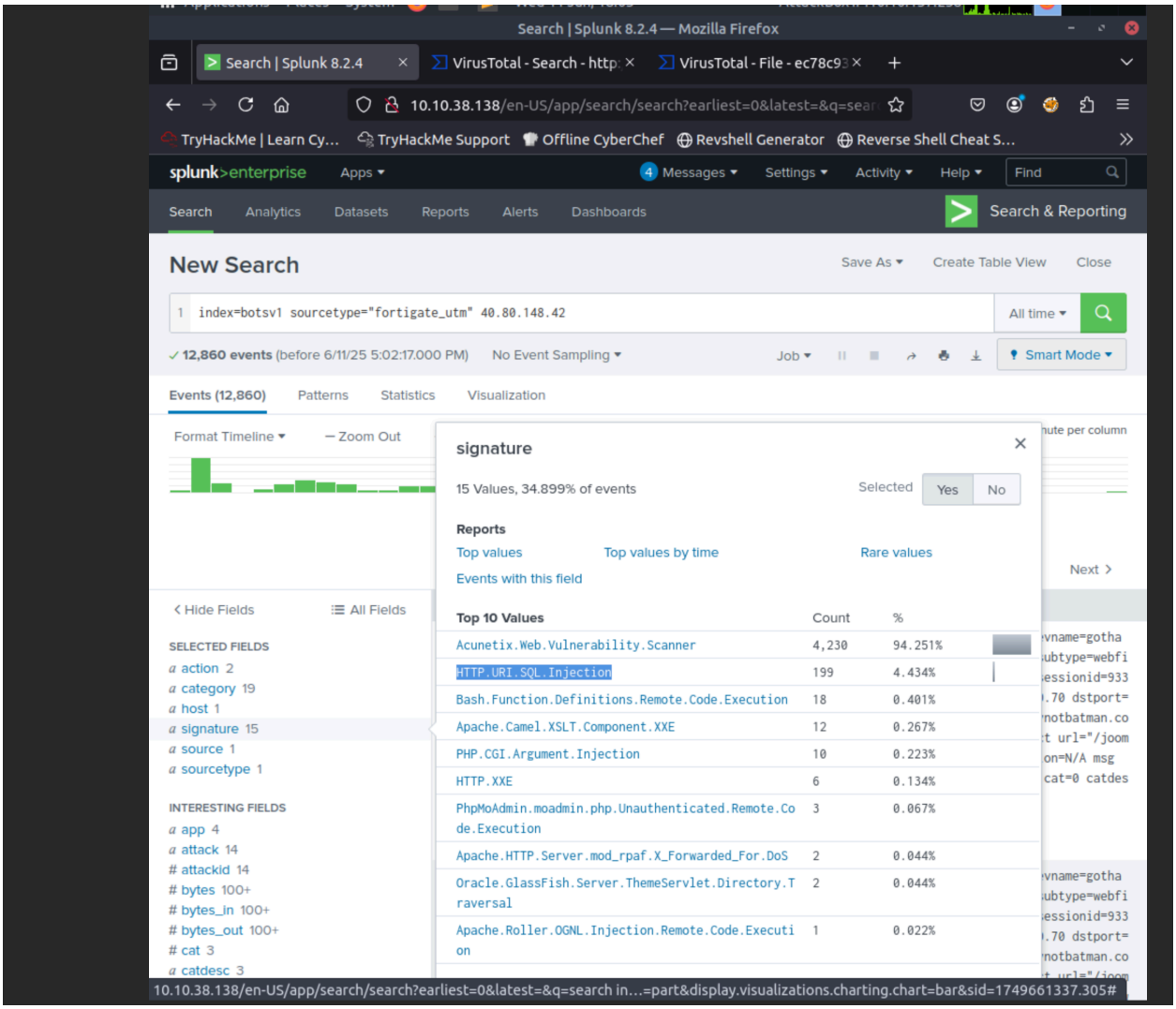
What is the name of the file that defaced the imreallynotbatman.com website ?

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



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

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