


## Hunting Windows Events and Logs » Brut3 Forc3

 Category: Digital Forensics

 Level: medium

 Points: 100

### Description

 Start Challenge

we suspect that one of our server at 192.168.250.70 was attacked by a web brute forcing attack, we need to identify:

- X: What is the attacker's IP address.
- Y: The Average password length (decimal number).

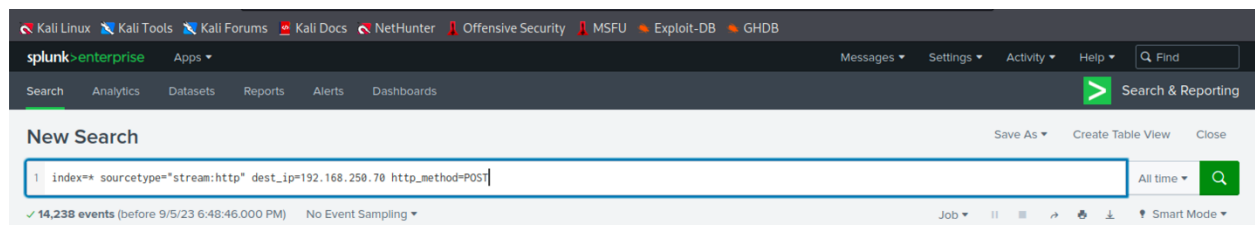
**Credentials:** cybertalents/cybertalents

**Flag format:** flag{X\_Y}

### Answer

From the description we know that:

- We will be looking for the source of the web brute force attack.
- Happened to our server 192.168.250.70 which is the destination.



I started off with this search :

- **Sourcetype="stream:http"** >> cuz in the description they mentioned the attack was by a web so will first focus on **http** traffic
- **dest\_ip=192.168.250.70** >> the attack happened in this server so we are looking for all the http traffic to this destination.
- **http\_method =POST** >> we are interested in POST requests since logins are usually performed through POST requests .

< Hide Fields

All Fields

List

Format

20 Per Page

src\_ip

2 Values, 93.103% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
40.80.148.42	12,844	96.892%
23.22.63.114	412	3.108%

No, we see here the result of the search.

- I scrolled down to the **src\_ip** field we see that there are two ip addresses but witch one of them is the attacker's?

We will check both to know.

54.193.247.148/en-US/app/search/search?earliest=0&latest=&q=search index%3D\* sourcetype%3D"stream%3A"

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

New Search

1 index=\* sourcetype="stream:http" dest\_ip=192.168.250.70 http\_method=POST src\_ip="40.80.148.42"

All time

12,844 events (before 9/5/23 6:51:20.000 PM) No Event Sampling

Job

Smart Mode

- I started with **src\_ip** 40.80.148.42

Events (12,844)

Patterns

Statistics

Format Timeline

Zoom Out

< Hide Fields

All Fields

SELECTED FIELDS

a form\_data 100+

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a accept 2

# ack\_packets\_in 11

# ack\_packets\_out 6

# bytes 100+

# bytes\_in 100+

# bytes\_out 100+

a c\_ip 1

# cached 1

a capture\_hostname 1

# client\_rtt 100+

form\_data

>100 Values, 69.807% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%
84a70de902dda7c3513582cceb46b40f=1&from=1&layout=default&link=d1cd50917e6d732a5e05c314550120fa5278b7dd&mailto=sample@email.tst&option=com_mailto&sender=sample@email.tst&subject=1&task=send&tmpl=component	17	0.19%
<?php echo(md5(acunetix-php-cgi-rce)); ?>	9	0.1%
areas[]=categories&ordering=category&searchphrase=all&searchword=the&task=search	7	0.078%
areas[]=categories&ordering=newest&searchphrase=all&searchword=e&task=search	6	0.067%
&ordering=newest&searchphrase=all&searchword=&task=search	5	0.056%
&ordering=newest&searchphrase=all&searchword=the&task=search	5	0.056%

- We checked the **form\_data** > “The **form\_data** field contains information that we want to check when dealing with POST requests.”
- We see here nothing indicates that there was a bruteforce attack so .. we will check the other IP address.

splunk>enterprise Apps Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

1 index=\* sourcetype="stream:http" dest\_ip=192.168.250.70 http\_method=POST src\_ip="23.22.63.114" All time

✓ 412 events (before 9/5/23 6:52:56.000 PM) No Event Sampling Job

Events (412) Patterns Statistics

Format Timeline Zoom Out

Hide Fields All Fields

SELECTED FIELDS

a form\_data 100+

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

# ack\_packets\_in 2

# ack\_packets\_out 3

# bytes 6

# bytes\_in 6

# bytes\_out 2

a c\_ip 1

# cached 1

a capture\_hostname 1

# client\_rtt 100+

username=admin&0960d493674eb04861bd64da9b662118=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=arthur	1	0.243%
username=admin&0edae02d7478dfb41641700ef384807a=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=bigdaddy	1	0.243%
username=admin&115c3aa6072f4b02b4354909431510f6=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=blazer	1	0.243%
username=admin&12c709bcc2e14d5a015f054d18d36537=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=fire	1	0.243%
username=admin&2a2ddf97716c1d1e9da21cdaf82b231e=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=777777	1	0.243%
username=admin&2c340c4e46444ba249ff7e599e6dfa52=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=flower	1	0.243%
username=admin&32c15329bc3f78039869bb3bf17c28a6=1&task=login&	1	0.243%

- So, it seems **23.22.63.114** performed brute force attack.

- But we need to make sure by :

```
index=botsv1 sourcetype=stream:http dest_ip=192.168.250.70  
http_method=POST form_data=*username*passwd* | stats count by src
```

The screenshot shows the Splunk Enterprise Search interface. The search bar contains the query: `index=* sourcetype=stream:http dest_ip=192.168.250.70 http_method=POST form_data=*username*passwd* | stats count by src_ip`. The results are displayed in a table with two columns: `src_ip` and `count`. The first row shows `23.22.63.114` with a count of `412`. The second row shows `40.80.148.42` with a count of `1`.

src_ip	count
23.22.63.114	412
40.80.148.42	1

- We can see the count for the **23.22.63.114** is way higher than the other IP address cool so indeed did a brute force attack on the server.

**X:23.22.63.114**

- 
- Now we need to know if the brute force was successful by :

```
index=botsv1 sourcetype=stream:http form_data=*username*passwd*  
dest_ip=192.168.250.70 | rex field=form_data  
"passwd=(?<userpassword>\w+)" | stats count by userpassword | sort -  
count
```

splunk>enterprise Apps Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

```
1 index=* sourcetype=stream:http form_data=*username*passwd* dest_ip=192.168.250.70 | rex field=form_data "passwd=(?<userpasswd>\w+)" | stats count by userpasswd | sort -
```

413 events (before 9/5/23 7:02:27.000 PM) No Event Sampling Job II III IV V VI VII VIII ... Smart Mode

Events Patterns **Statistics (412)** Visualization

20 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 ... Next >

userpasswd	count
batman	2
000000	1
1111	1
111111	1
11111111	1
112233	1
1212	1

- “The search above extracts every user password and counts the times it has been seen/used. If a password is seen more than one time, this probably means that attackers got a hit and used the password again to log in. This is why we are sorting on count.”
- We see here that the password used for the login is **batman**

The password average Length is: 6  
So I tried it in the flag and it was correct

**Y:6**  
**Flag{X\_Y}**

Brut3 Forc3	flag{23.22.63.114_6} ✓	Correct	100
-------------	------------------------	---------	-----

Disclaimer: I solved this challenge by going through the BOTSv1 Lab.

Written by: Safana H.