Exploitation Phase

- attacker needs to exploit the vulnerability to gain access to the system/server

- we will look at the potential exploitation attempt from the attacker against our web server and see if the attacker got successful in exploiting or not

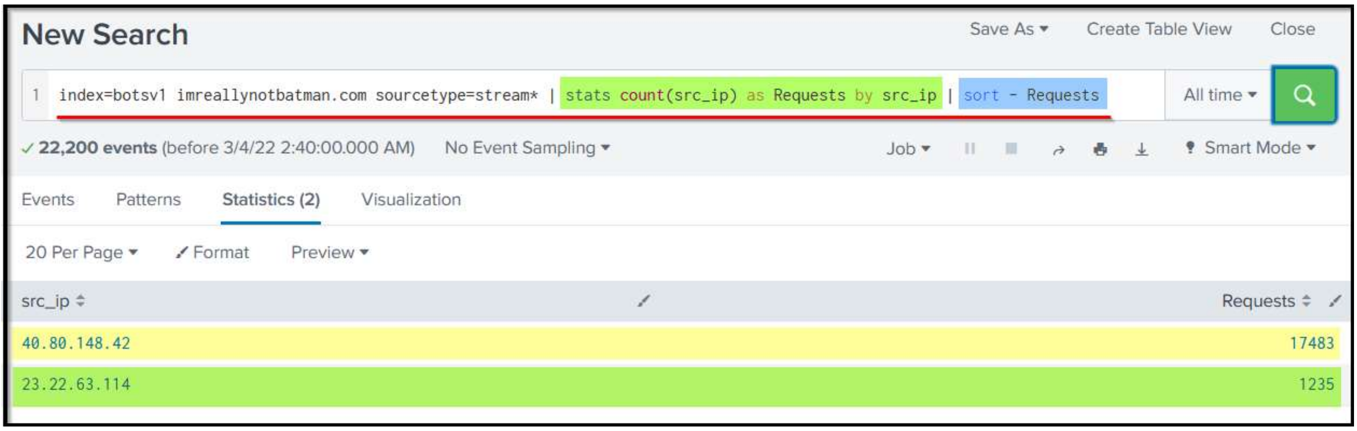
The information we have:
- found 2 IP addresses that are sending requests to our server
- 1 of the IPs 40.80.148.42 was seen attempting to scan the server with IP 192.168.250.70
- attacker was using the web scan Acunetix for the scanning attempt

Count
- use the following search query to see the number of counts by each IP against the web server

Search Query:

```
index=botsv1 imreallynotbatman.com sourcetype=stream* | stats count(src_ip) as Requests by src_ip | sort - Requests
```

Query explanation: this query uses the stats function to display the count of the IP addresses in the src_fied



New Search

```
1  index=botsv1 imreallynotbatman.com sourcetype=stream* | stats count(src_ip) as Requests by src_ip | sort - Requests
```

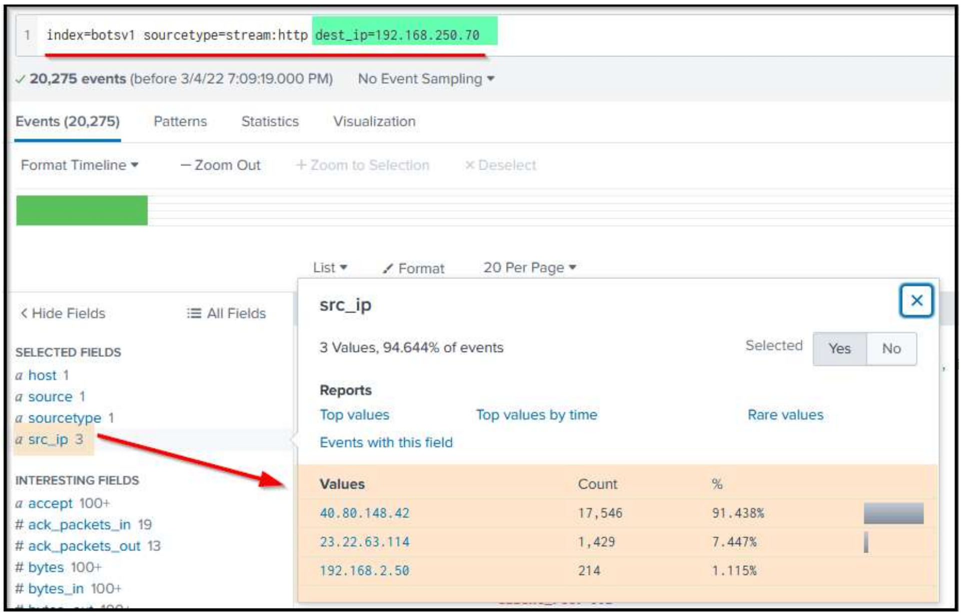
✓ 22,200 events (before 3/4/22 2:40:00.000 AM) No Event Sampling ▾

src_ip	Requests
40.80.148.42	17483
23.22.63.114	1235

- narrow down the result to show requests sent to our web server: 192.168.250.70

Search Query: index=botsv1 sourcetype=stream.http dest_ip="192.168.250.70"

Query Explanation: query will for all the inbound traffic towards 192.168.250.70 (webserver)



```
1  index=botsv1 sourcetype=stream:http dest_ip=192.168.250.70
```

✓ 20,275 events (before 3/4/22 7:09:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1
- a src_ip 3

INTERESTING FIELDS
- a accept 100+
- # ack_packets_in 19
- # ack_packets_out 13
- # bytes 100+
- # bytes_in 100+

src_ip

3 Values, 94.644% of events

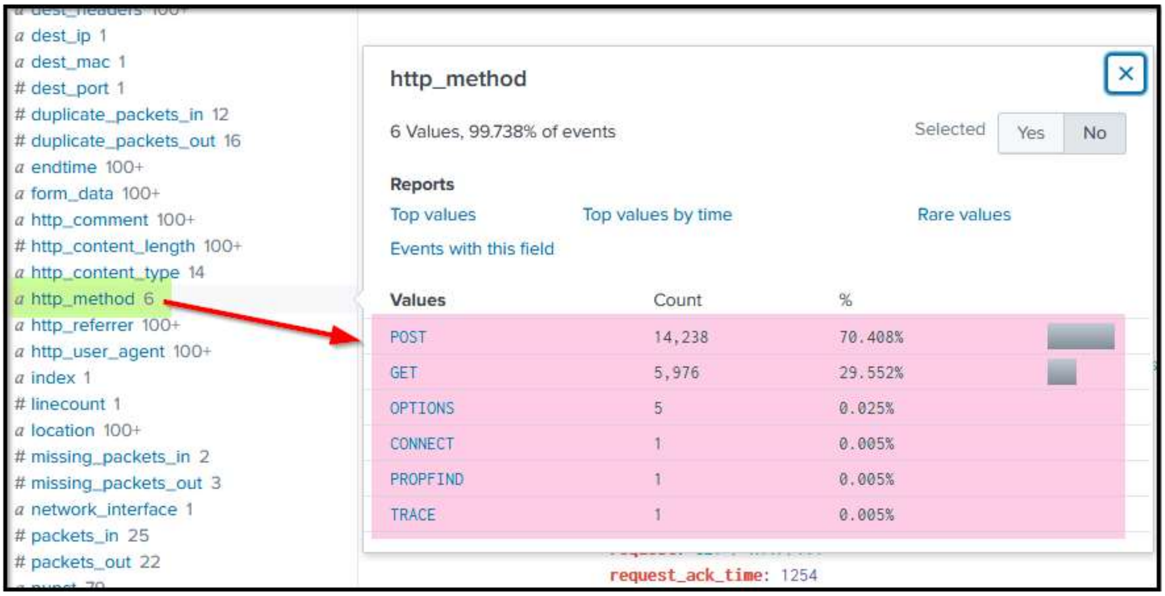
Selected: Yes [✓] No

Reports

Values	Count	%
40.80.148.42	17,546	91.438%
23.22.63.114	1,429	7.447%
192.168.2.50	214	1.115%

src_ip should 3 IP address (1 local and 2 remote IPs) that originated the HTTP traffic towards our web server:
- 40.80.148.42 [remote]
- 23.22.63.114 [remote]
- 192.168.2.50 [local]

http_method field will give us information about the HTTP Methods observed during these HTTP communications.
- observed most of the requests coming to our web server through the POST request



a dest_ip 1
a dest_mac 1
# dest_port 1
# duplicate_packets_in 12
# duplicate_packets_out 16
a endtime 100+
a form_data 100+
a http_comment 100+
# http_content_length 100+
a http_content_type 14
a http_method 6
a http_referrer 100+
a http_user_agent 100+
a index 1
# linecount 1
a location 100+
# missing_packets_in 2
# missing_packets_out 3
a network_interface 1
# packets_in 25
# packets_out 22

http_method

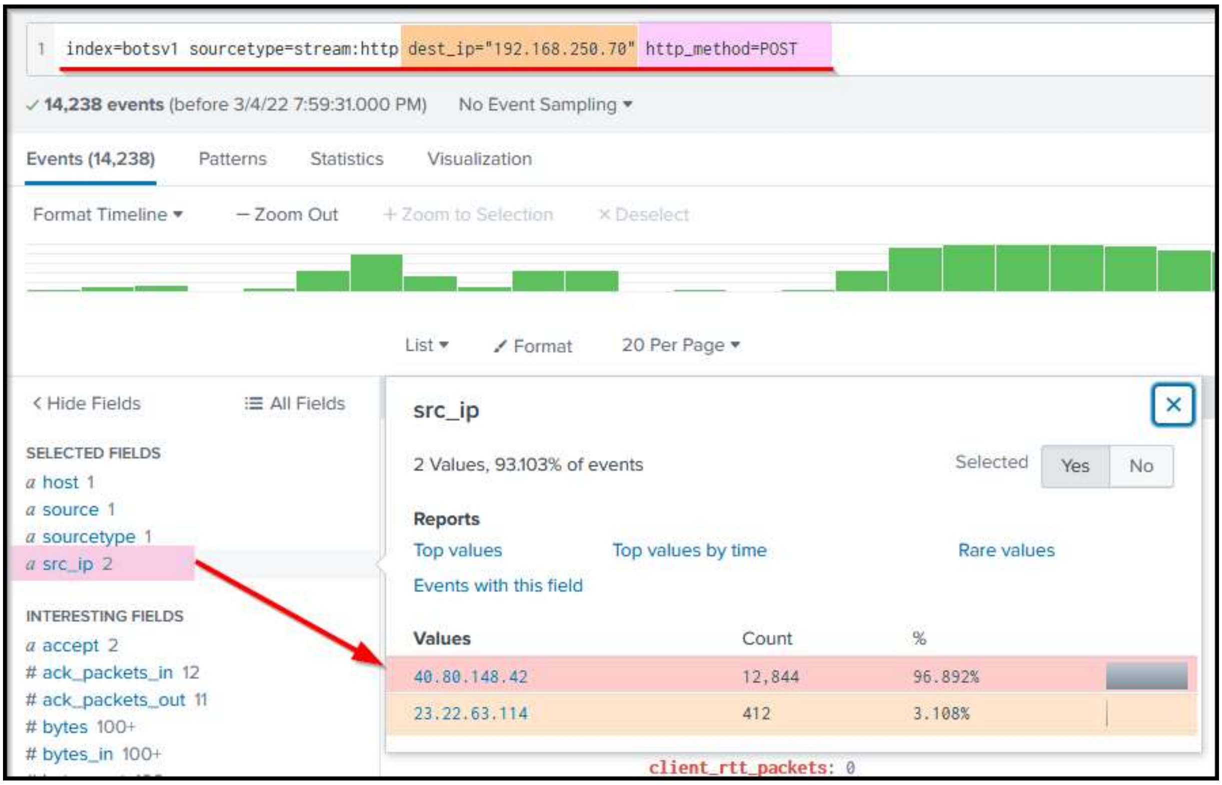
6 Values, 99.738% of events

Values	Count	%
POST	14,238	70.408%
GET	5,976	29.552%
OPTIONS	5	0.025%
CONNECT	1	0.005%
PROPFIND	1	0.005%
TRACE	1	0.005%

request_ack_time: 1254

http.method=POST > see the traffic coming through POST requests
Search Query:

```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" http_method=POST
```



```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" http_method=POST
```

✓ 14,238 events (before 3/4/22 7:59:31.000 PM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a src_ip 2

INTERESTING FIELDS
a accept 2
# ack_packets_in 12
# ack_packets_out 11
# bytes 100+
# bytes_in 100+

src_ip

2 Values, 93.103% of events

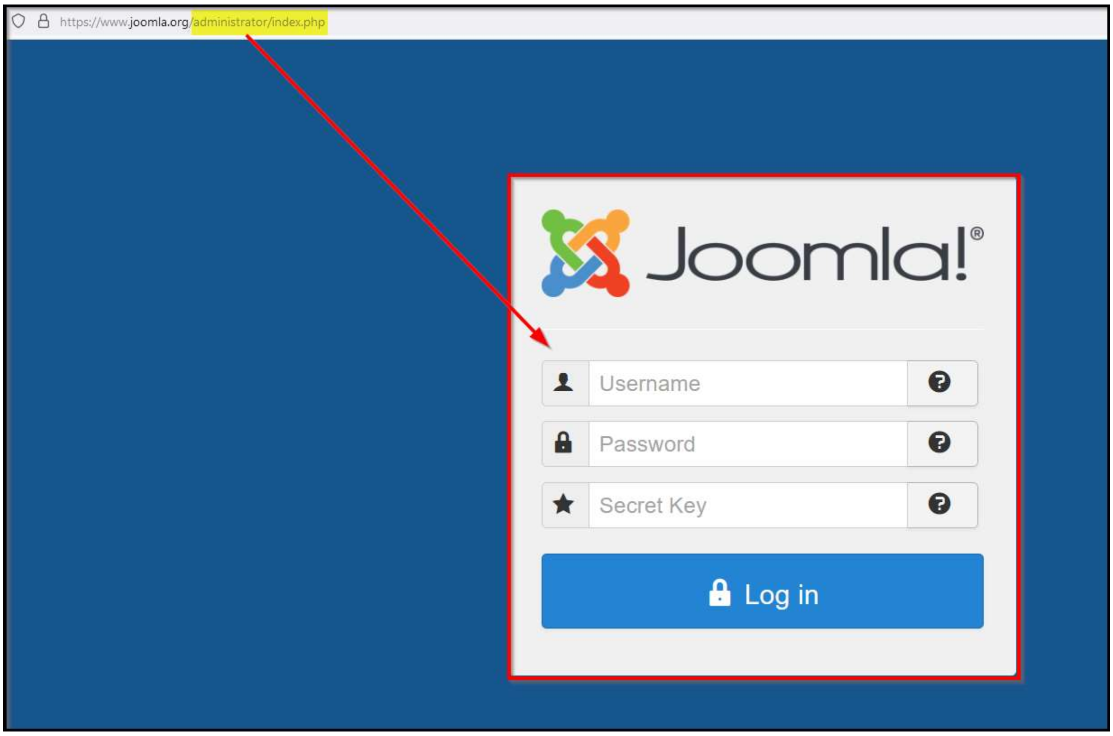
Values	Count	%
40.80.148.42	12,844	96.892%
23.22.63.114	412	3.108%

client_rtt_packets: 0

src_ip shows 2 IP addresses sending all the POST requests to our server.
Fields containing valuable information:
- src_ip
- form_data
- http_user_agent
- uri

The term Joomla is associated with the webserver found in a couple of fields (uri, uri_path, http_referrer)
- web server is using Joomla CMS (Content Management Service) in the backend

Admin login page for Joomla CMS > /joomla/administrator/index.php

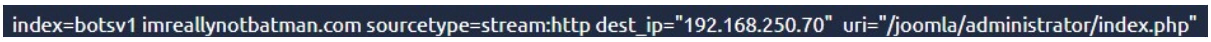


- URI contains the login page to access the web portal
- examine the traffic coming into this admin panel for a potential brute force attack

<u>Requests sent to login page</u>

Narrow down search to see the requests sent to the login page.

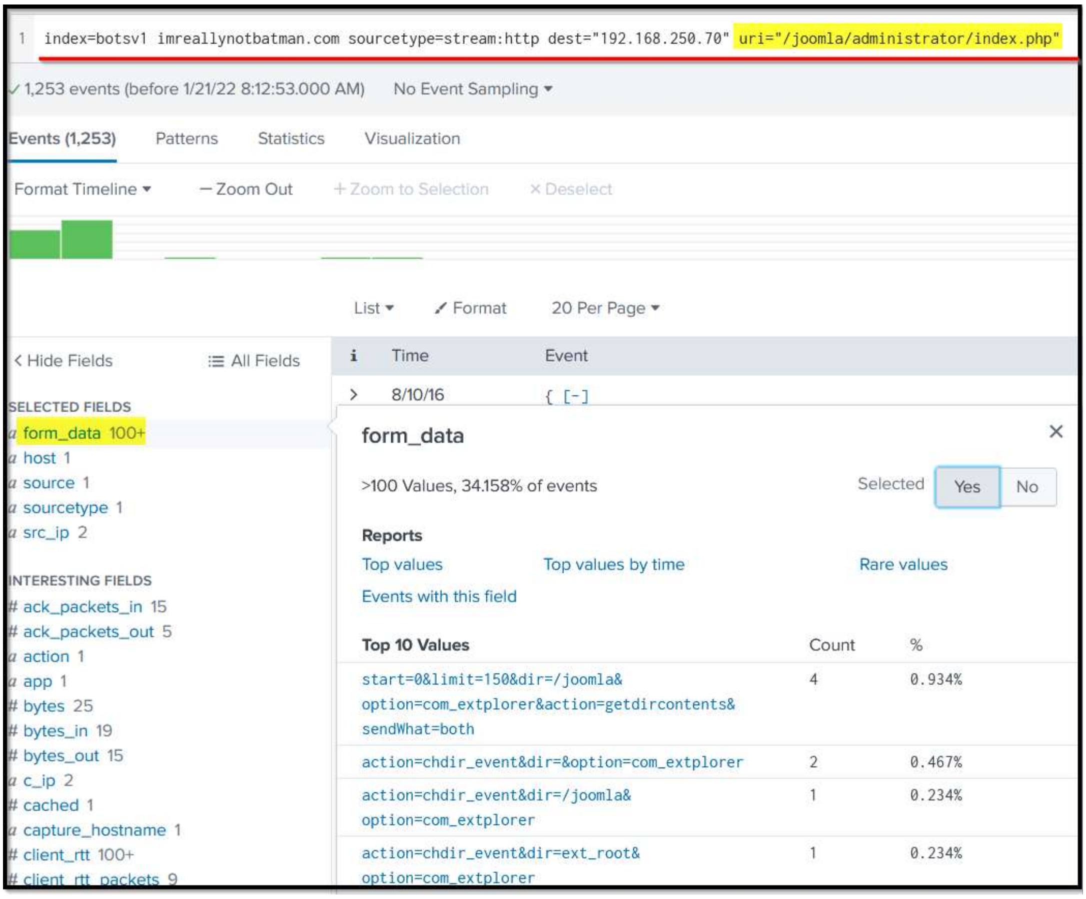
Search Query:



```
index=botsv1 imreallynotbatman.com sourcetype=stream:http dest_ip="192.168.250.70"  uri="/joomla/administrator/index.php"
```

Search Explanation:

- add uri="/joomla/administrator/index.php" to show traffic coming into this URI



```
index=botsv1 imreallynotbatman.com sourcetype=stream:http dest="192.168.250.70" uri="/joomla/administrator/index.php"
```

✓ 1,253 events (before 1/21/22 8:12:53.000 AM) No Event Sampling ▾

SELECTED FIELDS

a form_data	100+
a host	1
a source	1
a sourcetype	1
a src_ip	2

INTERESTING FIELDS

# ack_packets_in	15
# ack_packets_out	5
a action	1
a app	1
# bytes	25
# bytes_in	19
# bytes_out	15
a c_ip	2
# cached	1
a capture_hostname	1
# client_rtt	100+
# client_rtt_packets	9

i	Time	Event
>	8/10/16	{ [-]

form_data

>100 Values, 34.158% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

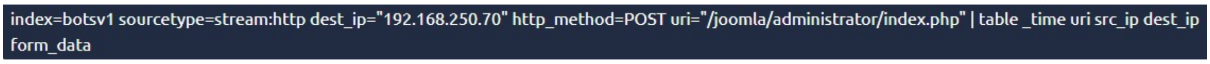
Top 10 Values	Count	%
start=0&limit=150&dir=/joomla&option=com_extplorer&action=getdircontents&sendWhat=both	4	0.934%
action=chdir_event&dir=&option=com_extplorer	2	0.467%
action=chdir_event&dir=/joomla&option=com_extplorer	1	0.234%
action=chdir_event&dir=ext_root&option=com_extplorer	1	0.234%

form_data

- field contains the requests sent through a form on the admin panel page
- suspect the attacker may have tried multiple credentials in an attempt to gain access to the admin panel

Dig deeper into the values contained within the form_data field.

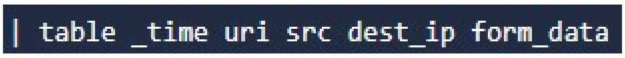
Search Query:



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

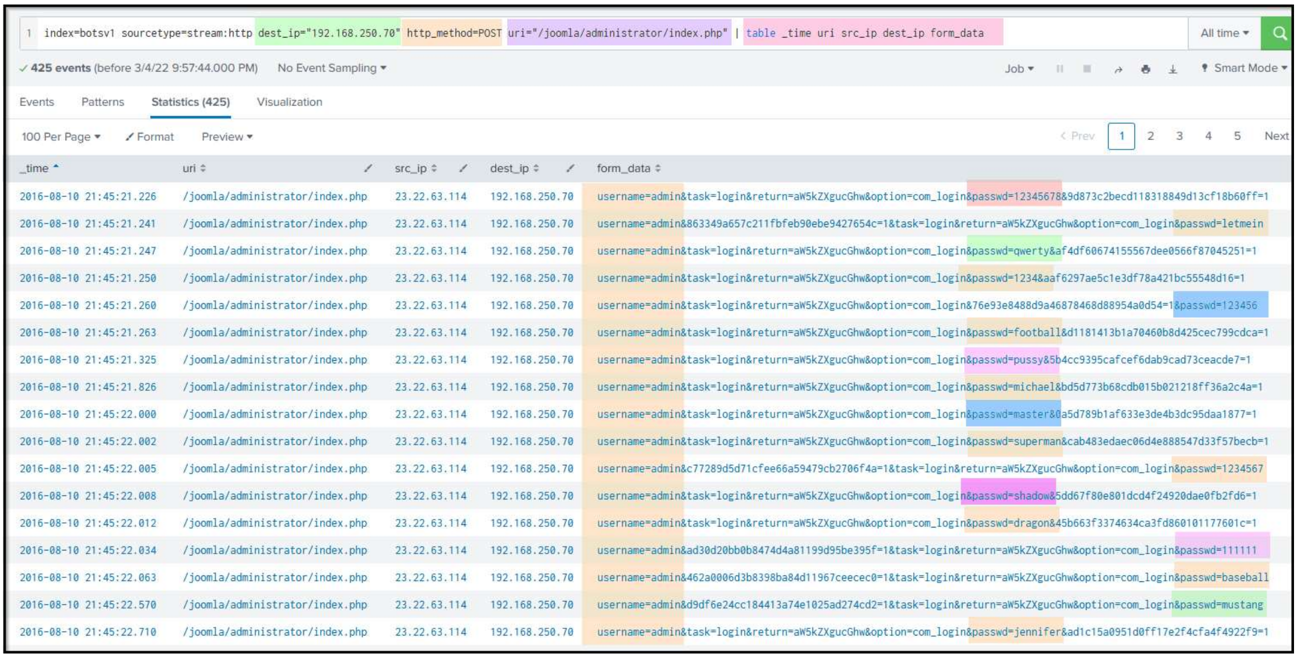
Query Explanation:

- we will add



```
| table _time uri src dest_ip form_data
```

- create a table containing important fields



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

✓ 425 events (before 3/4/22 9:57:44.000 PM) No Event Sampling ▾

_time	uri	src_ip	dest_ip	form_data
2016-08-10 21:45:21.226	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=12345678&9d873c2becd118318849d13cf18b60ff=1
2016-08-10 21:45:21.241	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&863349a657c211fbfeb90ebe9427654c=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=letmein
2016-08-10 21:45:21.247	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=qwerty&af4df60674155567dee0566f87045251=1
2016-08-10 21:45:21.250	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=1234&aaf6297ae5c1e3df78a421bc55548d16=1
2016-08-10 21:45:21.260	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&76e93e8488d9a46878468d88954a0d54=1&passwd=123456
2016-08-10 21:45:21.263	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=football&d1181413b1a70460b8d425cec799cdca=1
2016-08-10 21:45:21.325	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=pussy&5b4cc9395cafcef6dab9cad73ceacde7=1
2016-08-10 21:45:21.826	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=michael&bd5d773b68cdb015b021218ff36a2c4a=1
2016-08-10 21:45:22.000	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=master&0a5d789b1af633e3de4b3dc95daa1877=1
2016-08-10 21:45:22.002	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=superman&cab483edaec06d4e888547d33f57becb=1
2016-08-10 21:45:22.005	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&c77289d5d71cfee66a59479cb2706f4a=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=1234567
2016-08-10 21:45:22.008	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=shadow&5dd67f80e801dcd4f24920dae0fb2fd6=1
2016-08-10 21:45:22.012	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=dragon&45b663f3374634ca3fd860101177601c=1
2016-08-10 21:45:22.034	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&ad30d20bb0b8474d4a81199d95be395f=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=111111
2016-08-10 21:45:22.063	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&462a0006d3b8398ba84d11967ceecec0=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baseball
2016-08-10 21:45:22.570	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&d9df6e24cc184413a74e1025ad274cd2=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=mustang
2016-08-10 21:45:22.710	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=jennifer&ad1c15a0951d0ff17e2f4cfa4f4922f9=1

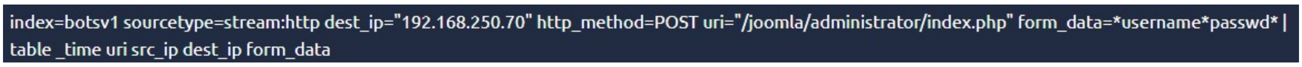
2 interesting fields ‘username’ that includes the single username ‘admin’ in all the events and another field ‘passwd’ that contains multiple passwords in it.

- attacker from IP 23.22.63.114 was trying to brute-force and attempted numerous passwords
- time elapsed between multiple events suggests that the attacker was using an automated tool

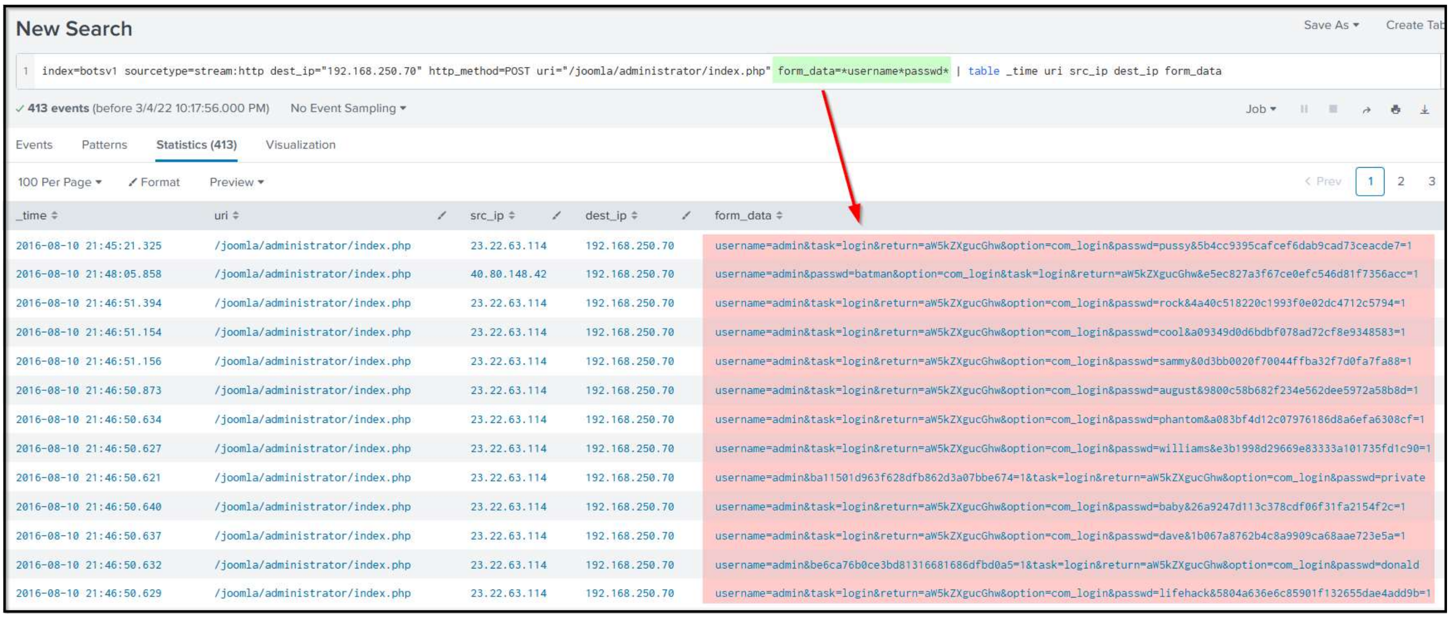
Extracting Username and Passwd fields using Regex

- use Regex in the search to extract only these 2 fields and their values from the logs and display them [username + passwd]
- display the logs that contain 'username' and 'passwd' values in the 'form_data' field by adding form_data=*username*passwd*

Search Query:



```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" http_method=POST uri="/joomla/administrator/index.php" form_data=*username*passwd* |
table _time uri src_ip dest_ip form_data
```

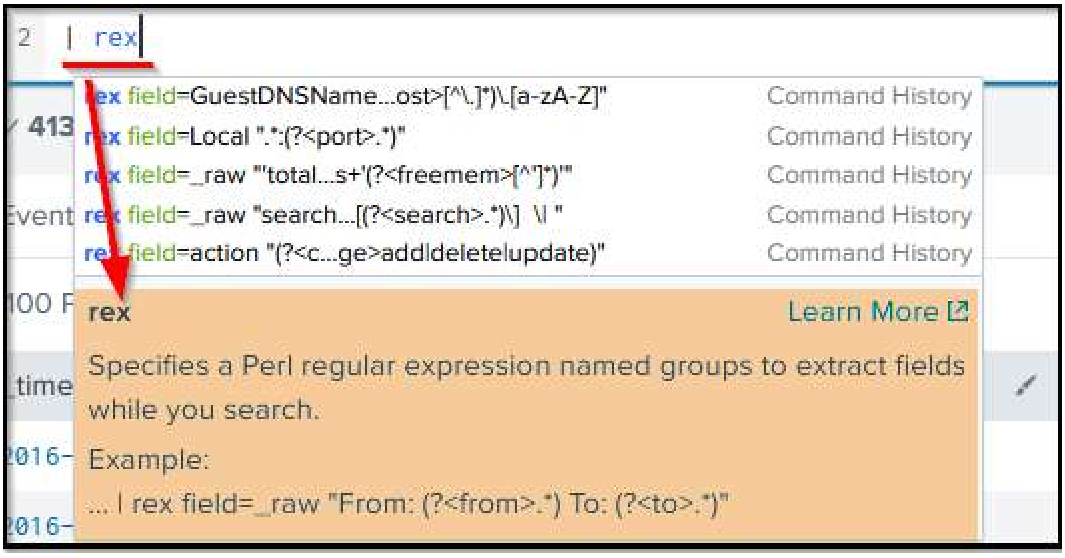


```
1  index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" http_method=POST uri="/joomla/administrator/index.php" form_data=*username*passwd* | table _time uri src_ip dest_ip form_data
```

✓ 413 events (before 3/4/22 10:17:56.000 PM)   No Event Sampling ▾

_time	uri	src_ip	dest_ip	form_data
2016-08-10 21:45:21.325	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=pussy&5b4cc9395cafcef6dab9cad73ceacde7=1
2016-08-10 21:48:05.858	/joomla/administrator/index.php	40.80.148.42	192.168.250.70	username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1
2016-08-10 21:46:51.394	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rock&4a40c518220c1993f0e02dc4712c5794=1
2016-08-10 21:46:51.154	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=cool&a09349d0d6bdbf078ad72cf8e9348583=1
2016-08-10 21:46:51.156	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=1
2016-08-10 21:46:50.873	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=august&9800c58b682f234e562dee5972a58b8d=1
2016-08-10 21:46:50.634	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=phantom&a083bf4d12c07976186d8a6efa6308cf=1
2016-08-10 21:46:50.627	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=williams&e3b1998d29669e83333a101735fd1c90=1
2016-08-10 21:46:50.621	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&ba11501d963f628dfb862d3a07bbe674=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=private
2016-08-10 21:46:50.640	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baby&26a9247d113c378cdf06f31fa2154f2c=1
2016-08-10 21:46:50.637	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=dave&1b067a8762b4c8a9909ca68aae723e5a=1
2016-08-10 21:46:50.632	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&be6ca76b0ce3bd81316681686dfbd0a5=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=donald
2016-08-10 21:46:50.629	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=lifehack&5804a636e6c85901f132655dae4add9b=1

Use Regex (Regular Expressions) to extract all password values found against the field passwd in the logs.



```
2  | rex
```

```
rex field=GuestDNSName...ost>[^\.]*)\.[a-zA-Z]"     Command History
rex field=Local ".*:(?<port>.*)"                    Command History
rex field=_raw "total...s+'(?<freemem>[^']*)'"      Command History
rex field=_raw "search...[(?<search>.*)\] \l "      Command History
rex field=action "(?<c...ge>add|delete|update)"     Command History
```

rex   Learn More

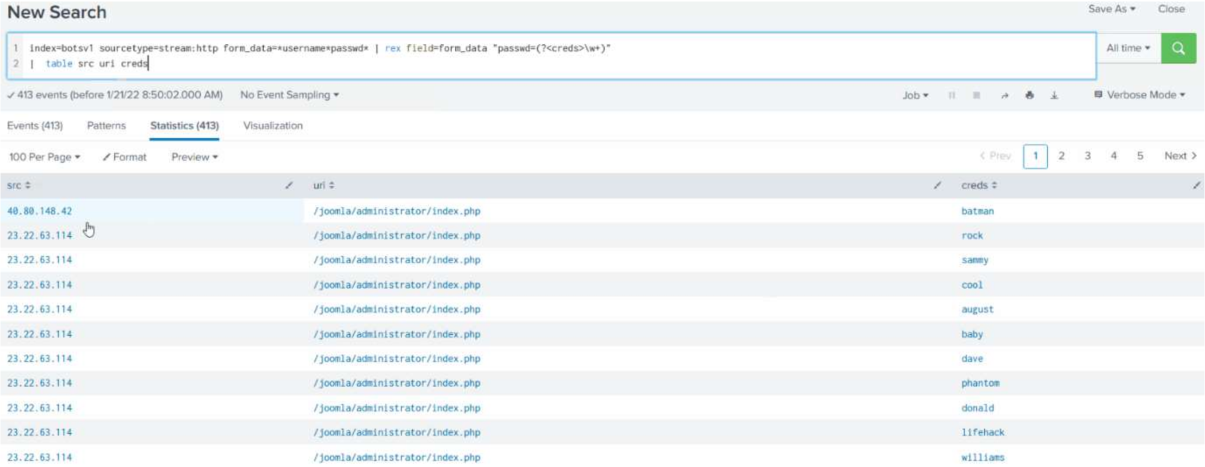
Specifies a Perl regular expression named groups to extract fields while you search.

Example:

... | rex field=_raw "From: (?<from>.*) To: (?<to>.*)"

rex field=form_data “passwd=(?<creds>\w+)”

- extract passwd values only
- this will pick the form_data field and extract all the values found with the field 'creds'



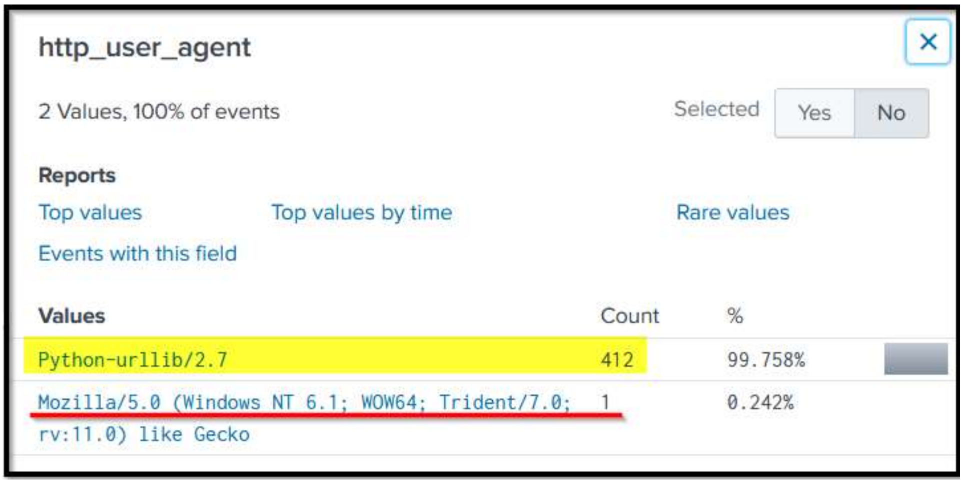
```
index=botsv1 sourcetype=stream:http form_data=*username*passwd* | rex field=form_data "passwd=(?<creds>\w+)"
| table src uri creds
```

✓ 413 events (before 1/21/22 8:50:02.000 AM) No Event Sampling

src	uri	creds
40.80.148.42	/joomla/administrator/index.php	batman
23.22.63.114	/joomla/administrator/index.php	rock
23.22.63.114	/joomla/administrator/index.php	sammy
23.22.63.114	/joomla/administrator/index.php	cool
23.22.63.114	/joomla/administrator/index.php	august
23.22.63.114	/joomla/administrator/index.php	baby
23.22.63.114	/joomla/administrator/index.php	dave
23.22.63.114	/joomla/administrator/index.php	phantom
23.22.63.114	/joomla/administrator/index.php	donald
23.22.63.114	/joomla/administrator/index.php	lifehack
23.22.63.114	/joomla/administrator/index.php	williams

We have extracted the passwords being used against the username admin on the admin panel of the web server.

- examine the fields in the logs, we will find 2 values against the field ‘http_user_agent’



http_user_agent

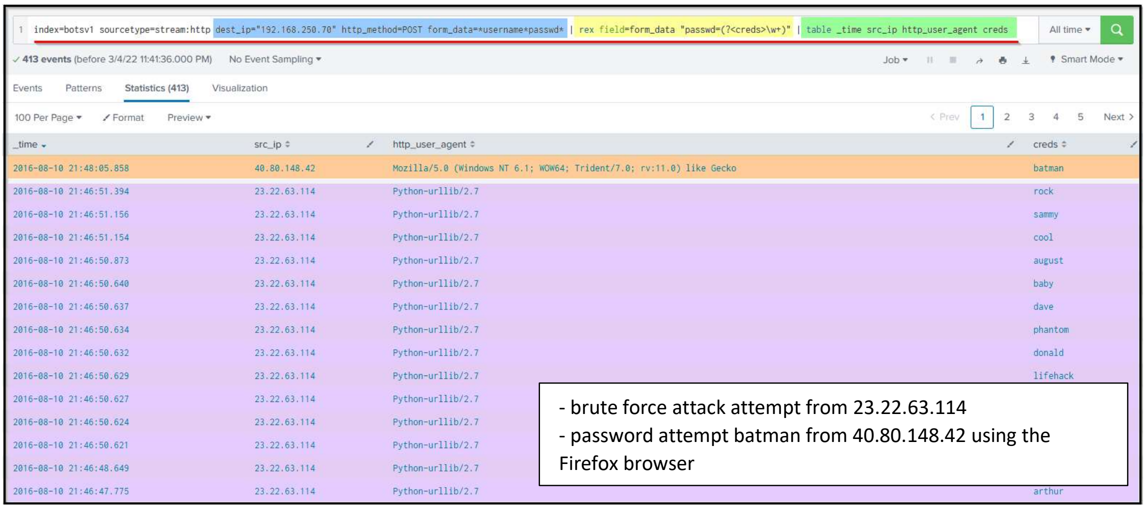
2 Values, 100% of events

Values	Count	%
Python-urllib/2.7	412	99.758%
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	1	0.242%

- Python script to automate the brute force attack against our server
- 1 request came from a Mozilla browser; change to the about search query and add http_user_agent to investigate

Search Query:

```
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
```



```
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 http_user_agent creds
```

✓ 413 events (before 3/4/22 11:41:36.000 PM) No Event Sampling

_time	src_ip	http_user_agent	creds
2016-08-10 21:48:05.858	40.80.148.42	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	Python-urllib/2.7	rock
2016-08-10 21:46:51.156	23.22.63.114	Python-urllib/2.7	sammy
2016-08-10 21:46:51.154	23.22.63.114	Python-urllib/2.7	cool
2016-08-10 21:46:50.873	23.22.63.114	Python-urllib/2.7	august
2016-08-10 21:46:50.640	23.22.63.114	Python-urllib/2.7	baby
2016-08-10 21:46:50.637	23.22.63.114	Python-urllib/2.7	dave
2016-08-10 21:46:50.634	23.22.63.114	Python-urllib/2.7	phantom
2016-08-10 21:46:50.632	23.22.63.114	Python-urllib/2.7	donald
2016-08-10 21:46:50.629	23.22.63.114	Python-urllib/2.7	lifehack
2016-08-10 21:46:50.627	23.22.63.114	Python-urllib/2.7	
2016-08-10 21:46:50.624	23.22.63.114	Python-urllib/2.7	
2016-08-10 21:46:50.621	23.22.63.114	Python-urllib/2.7	
2016-08-10 21:46:48.649	23.22.63.114	Python-urllib/2.7	
2016-08-10 21:46:47.775	23.22.63.114	Python-urllib/2.7	arthur

- brute force attack attempt from 23.22.63.114
- password attempt batman from 40.80.148.42 using the Firefox browser