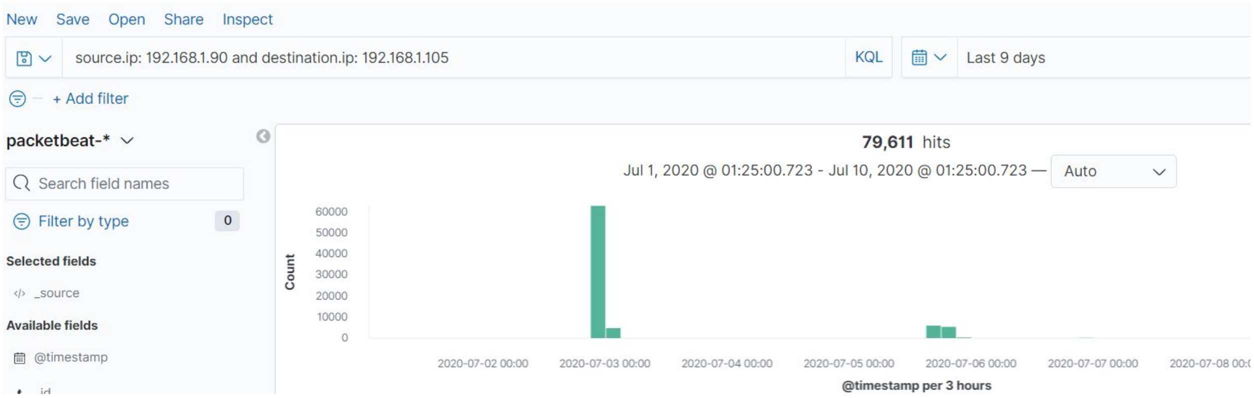
After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.

    ○ Identify the traffic between your machine and the web machine:
        ■ When did the interaction occur?

Answer: The interactions occurred between 7/2 at 22:45 and 7/6 at 22:00. Instances of significance were as follows:

- 9012 instances on 7/2 22:50
- 5060 instances on 7/2 at 23:25
- 48847 instances on 7/2 at 23:30
- 4020 instances on 7/3 at 1:55
- 6000 instances on 7/5 at 17:00
- 4348 instances on 7/5 at 19:00



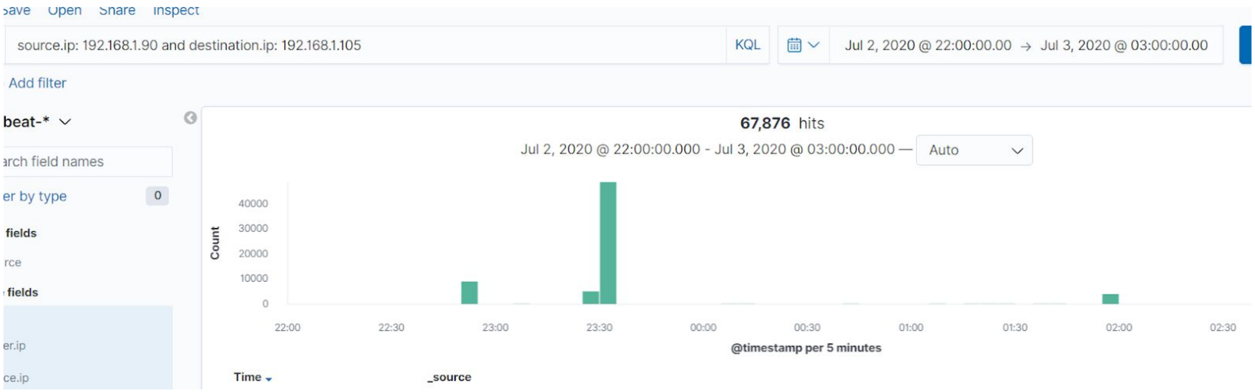
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

Last 9 days

packetbeat-*

79,611 hits

Jul 1, 2020 @ 01:25:00.723 - Jul 10, 2020 @ 01:25:00.723 — Auto



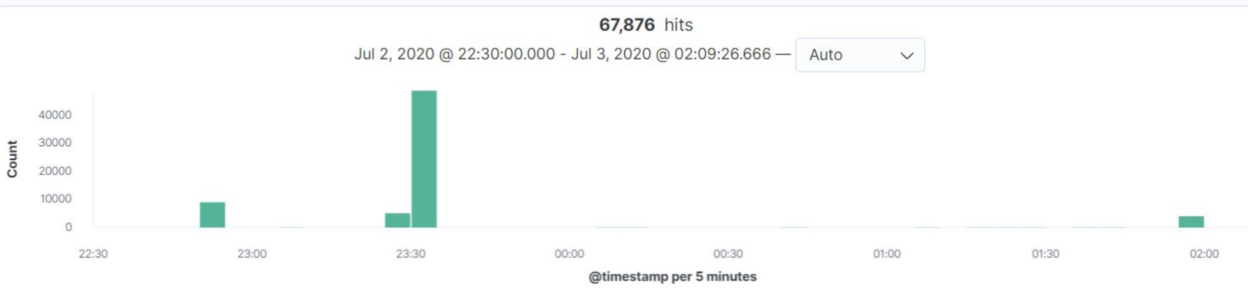
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

Jul 2, 2020 @ 22:00:00.00 → Jul 3, 2020 @ 03:00:00.00

beat-*

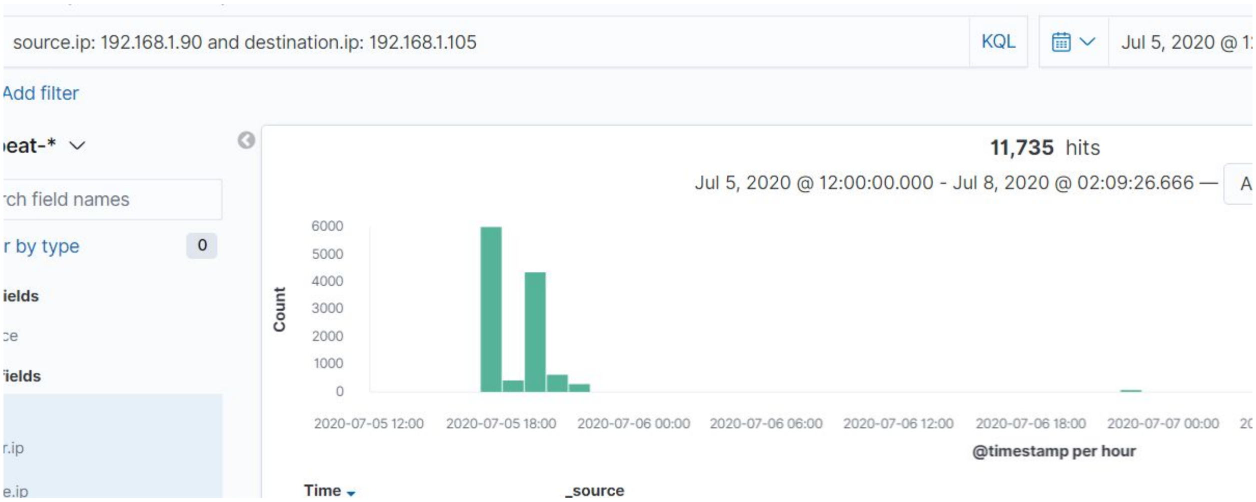
67,876 hits

Jul 2, 2020 @ 22:00:00.000 - Jul 3, 2020 @ 03:00:00.000 — Auto



67,876 hits

Jul 2, 2020 @ 22:30:00.000 - Jul 3, 2020 @ 02:09:26.666 — Auto



source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

KQL

Jul 5, 2020 @ 1

Add filter

eat-*

ch field names

r by type 0

ields

ce

ields

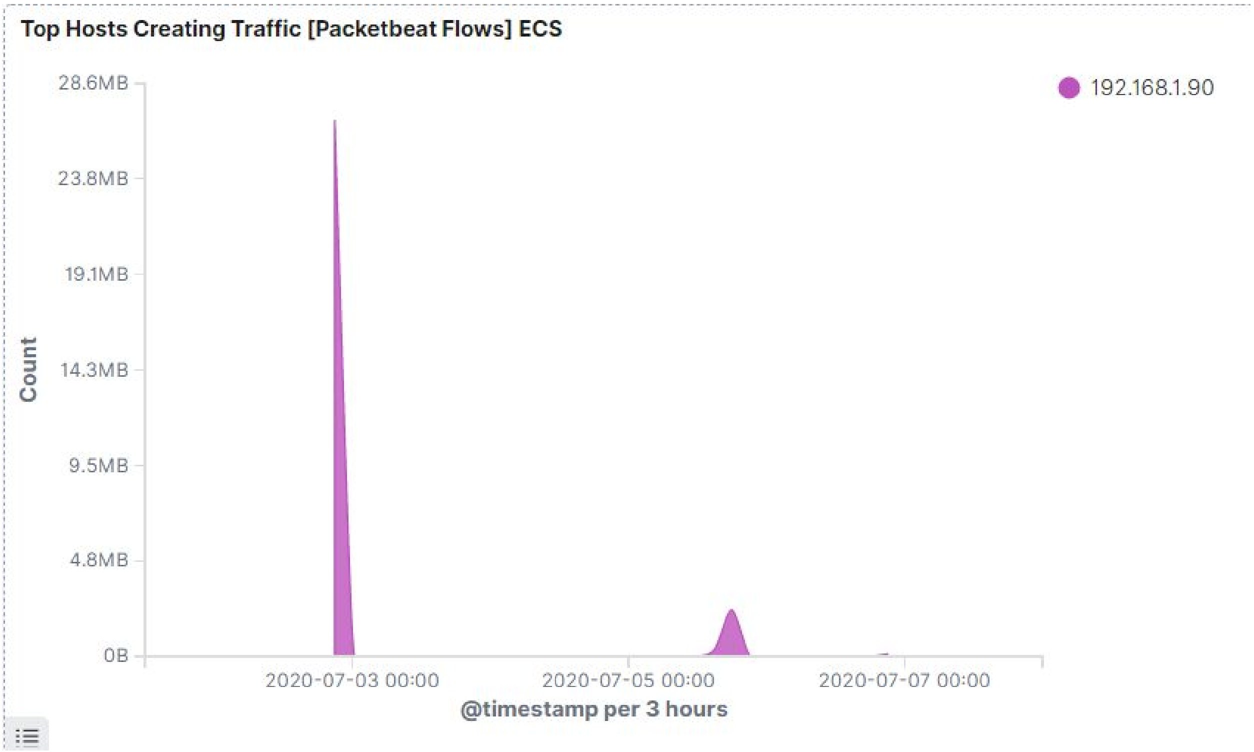
r.ip

e.ip

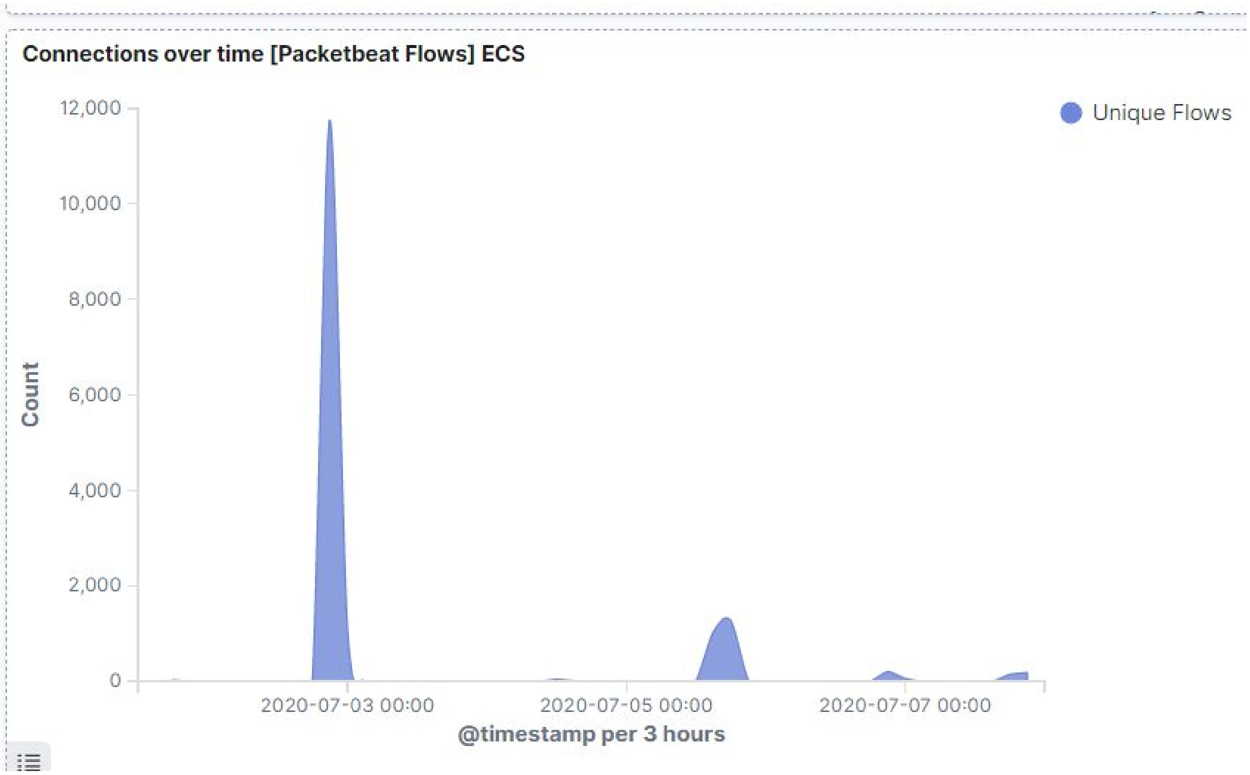
11,735 hits

Jul 5, 2020 @ 12:00:00.000 - Jul 8, 2020 @ 02:09:26.666 — A

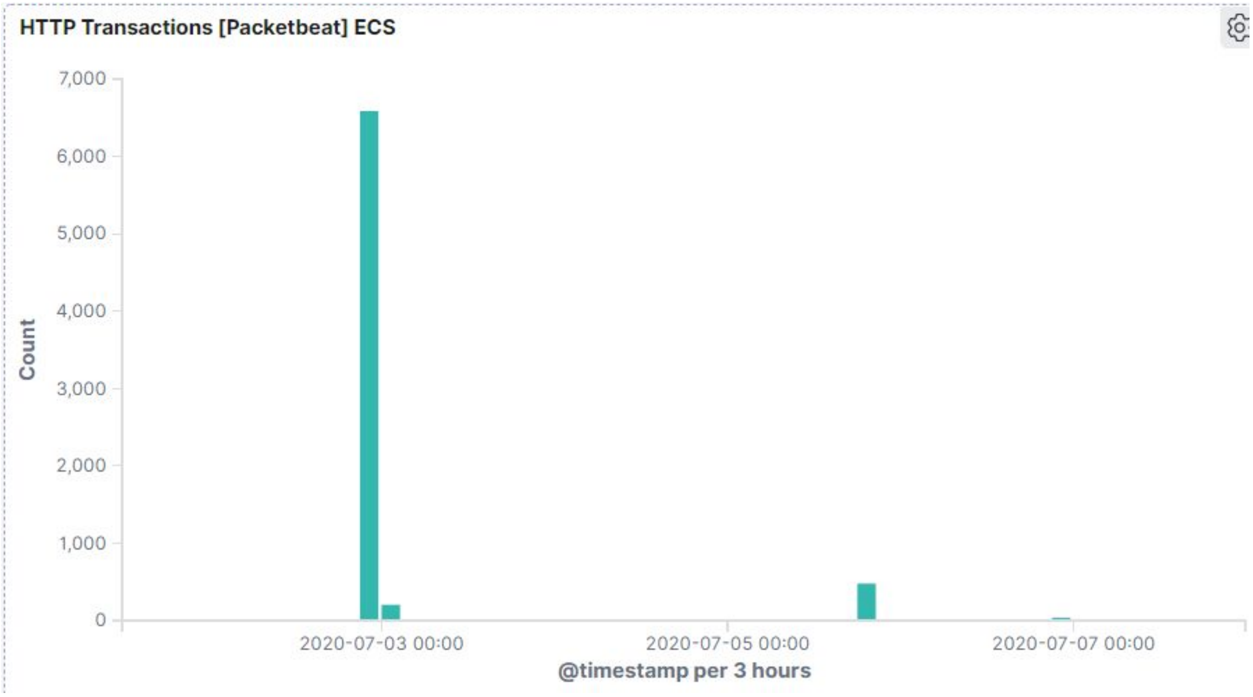
Time _source



Top Hosts Creating Traffic [Packetbeat Flows] ECS



Connections over time [Packetbeat Flows] ECS

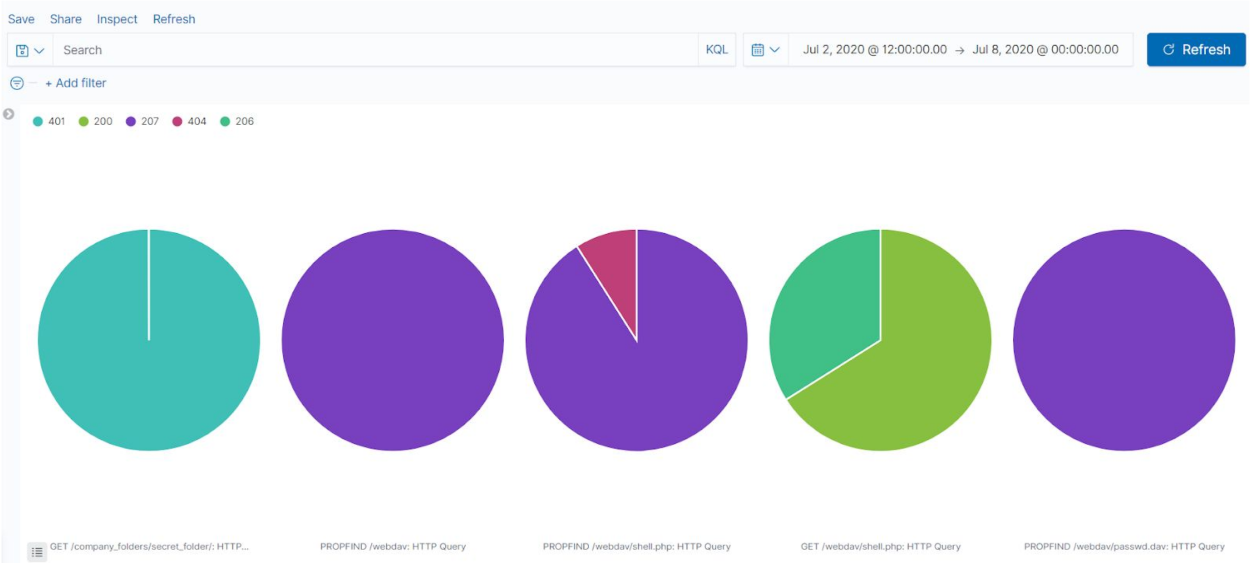


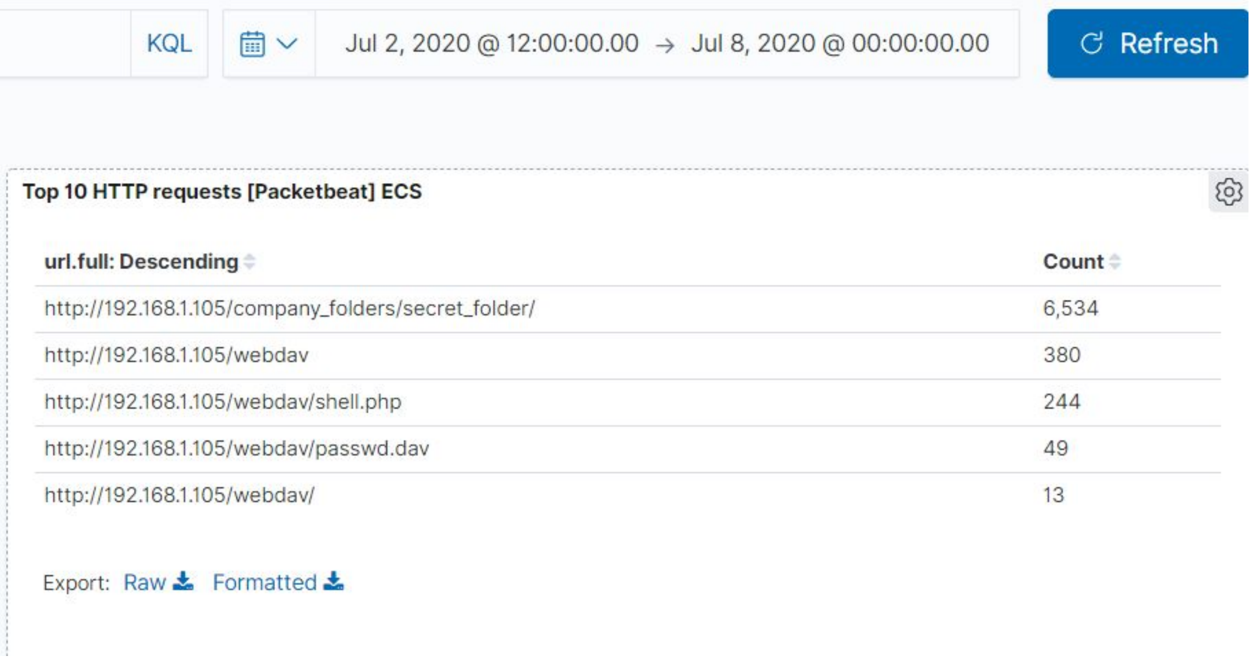
HTTP Transactions [Packetbeat] ECS

- What responses did the victim send back?

Answer:

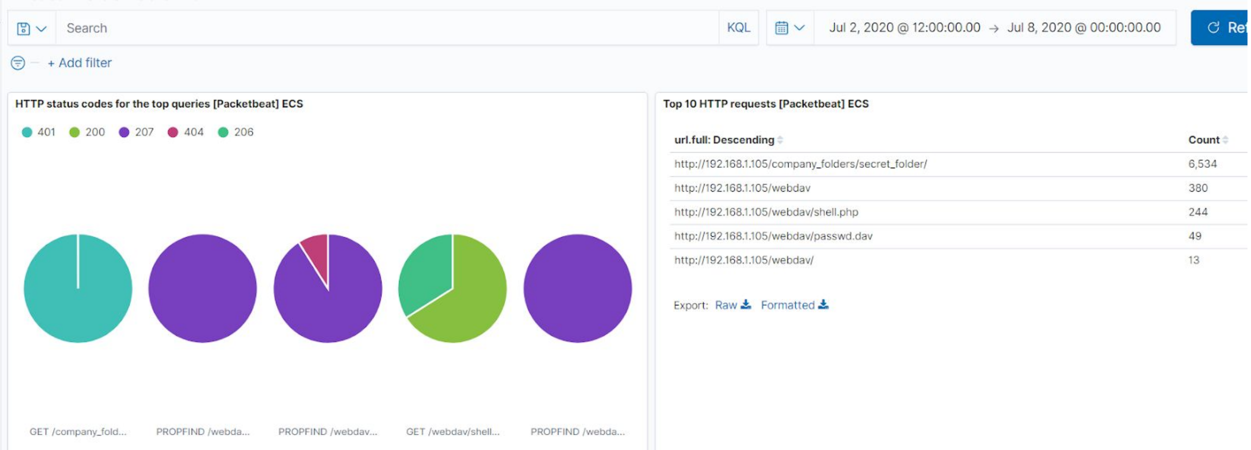
- The victim sent back a 401 (Unauthorized) response code 6531 times (99.98%) for GET request queries on /company_folders/secret_folder/ location path, and a 200 (OK) response 2 times (0.02%) on this same directory.
- The victim sent back a 200 (OK) response code 35 times (66%) for GET request queries on the webdav/shell.php file, and a 206 response code 18 times (34%) on this same file.
- The victim sent back a 207 () response code 360 times (100%) for all PROPFIND queries on the webdav file path, and 49 times (100%) for all PROPFIND queries on the webdav/passwd.dav file.
- The victim sent back a 207 () response code 162 times (91%) for PROPFIND queries on the webdav/shell.php file, and a 404 response code 16 times (9%) on this same file.


Save
Share
Inspect
Refresh
Search
KQL
Jul 2, 2020 @ 12:00:00.00 → Jul 8, 2020 @ 00:00:00.00
Refresh
+ Add filter
● 401
● 200
● 207
● 404
● 206
GET /company_folders/secret_folder/: HTTP...
PROPFIND /webdav: HTTP Query
PROPFIND /webdav/shell.php: HTTP Query
GET /webdav/shell.php: HTTP Query
PROPFIND /webdav/passwd.dav: HTTP Query



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,534
http://192.168.1.105/webdav	380
http://192.168.1.105/webdav/shell.php	244
http://192.168.1.105/webdav/passwd.dav	49
http://192.168.1.105/webdav/	13



HTTP status codes for the top queries [Packetbeat] ECS

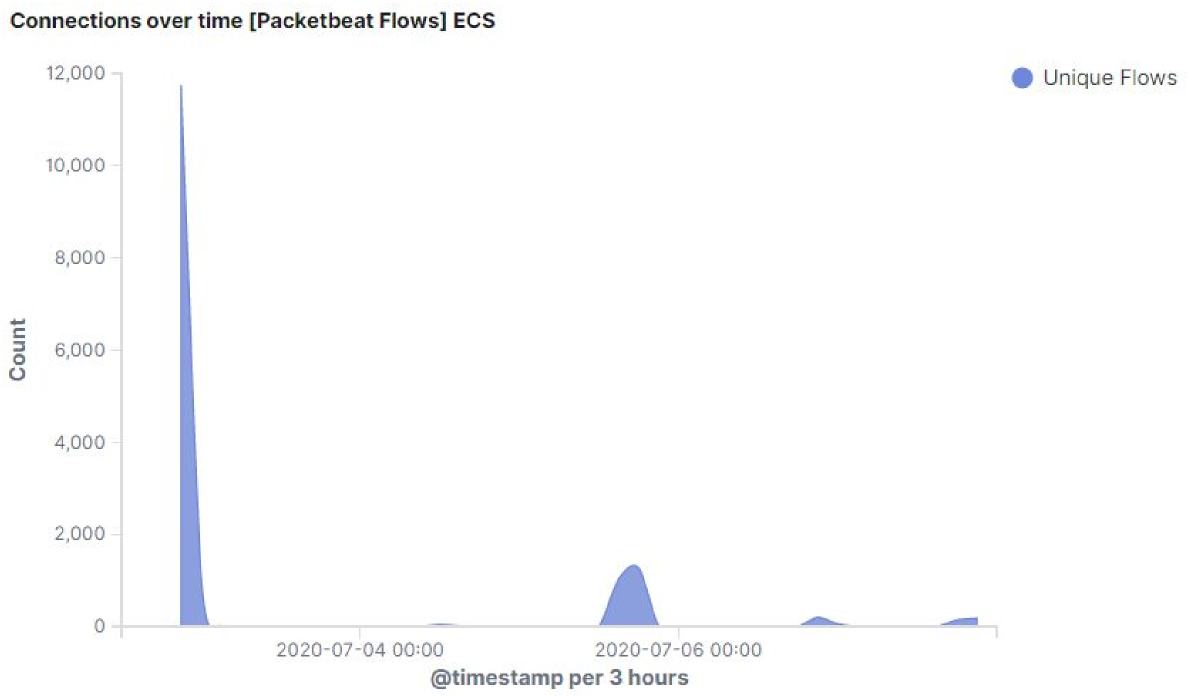
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,534
http://192.168.1.105/webdav	380
http://192.168.1.105/webdav/shell.php	244
http://192.168.1.105/webdav/passwd.dav	49
http://192.168.1.105/webdav/	13

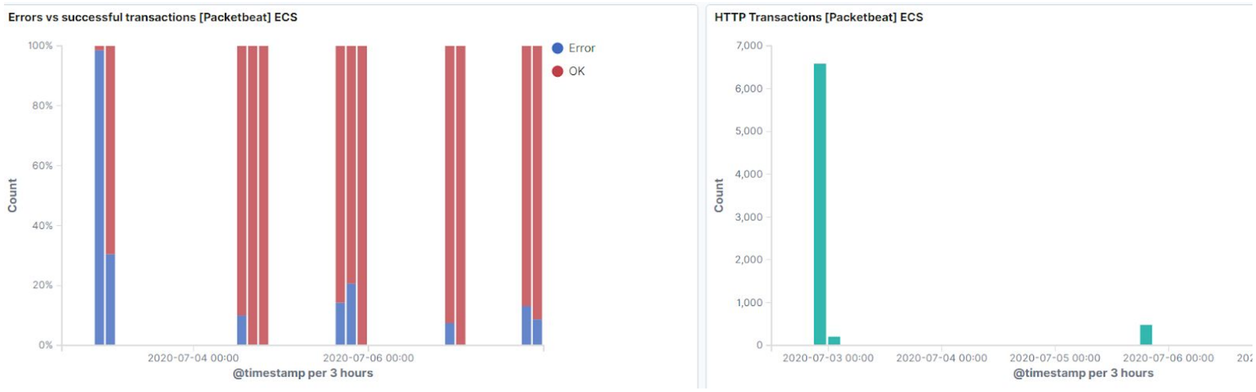
■ What data is concerning from the Blue Team perspective?

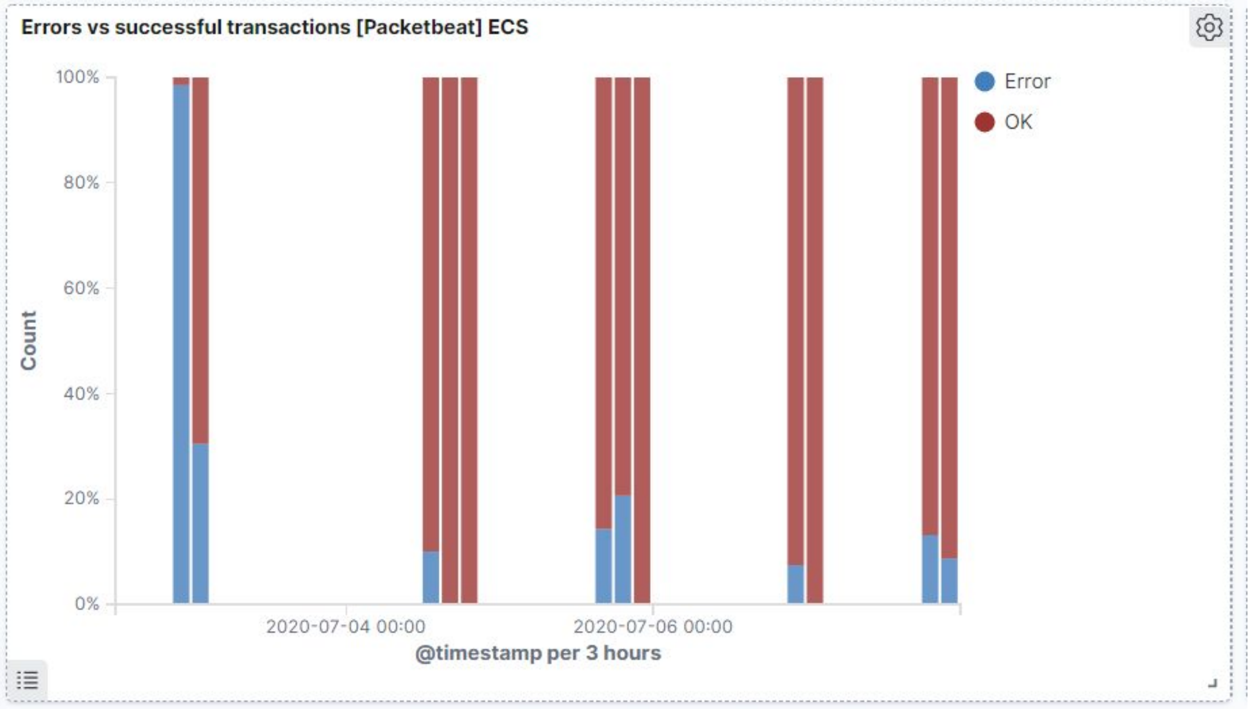
Answer:

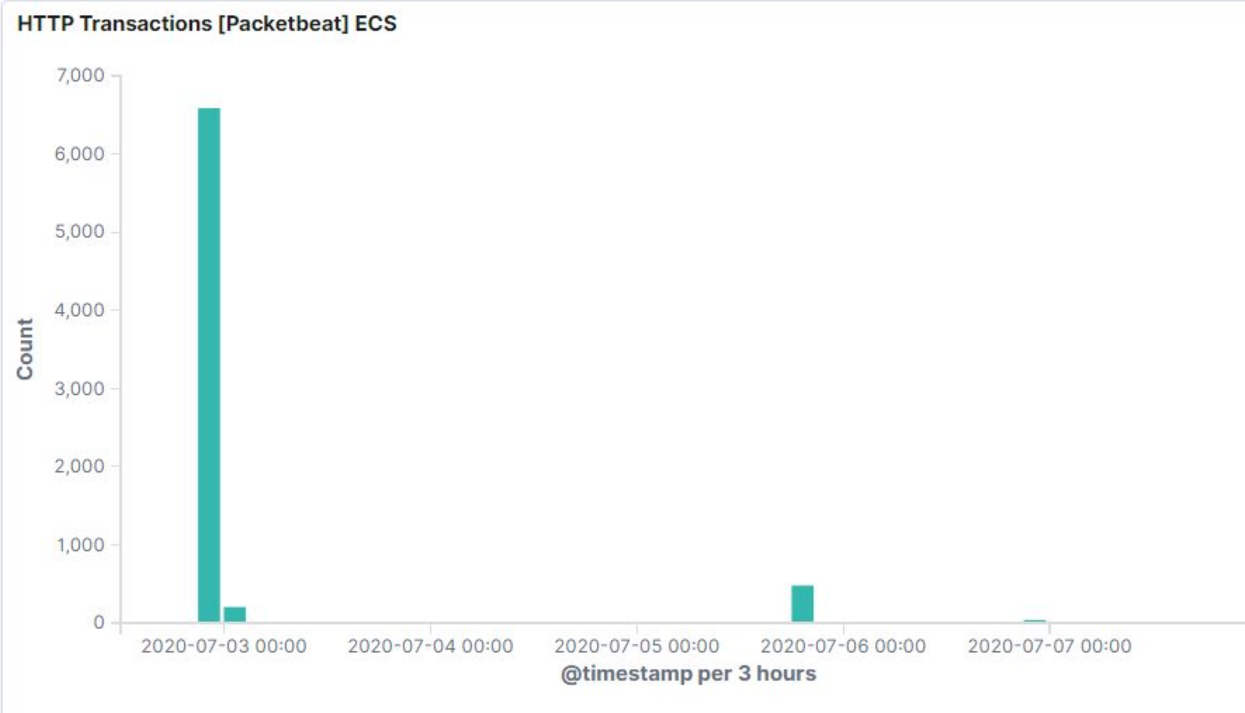
- A massive spike in connections (11,751) on 7/2 around 22:00, and a smaller but significant spike (1273) on 7/5 around 18:00.



- The 98.5% error rate on transactions around 7/2 at 21:00, followed by a 30.4% error rate on 7/3 at 00:00. Over 6586 HTTP transactions on 7/2 at 21:00, and 240 transactions on 7/3 at 00:00.
-




Errors vs successful transactions [Packetbeat] ECS

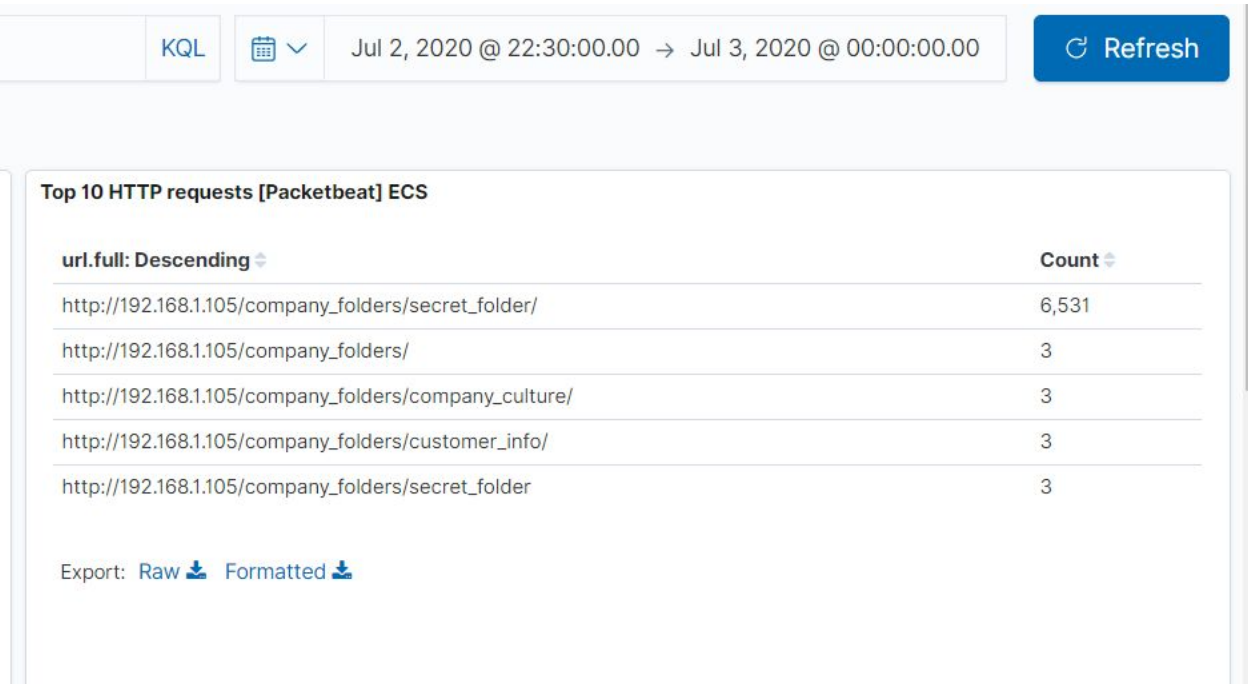

HTTP Transactions [Packetbeat] ECS

2. Find the request for the hidden directory.

    - In your attack, you found a secret folder. Let's look at that interaction between these two machines.
        - How many requests were made to this directory? At what time and from which IP address(es)?

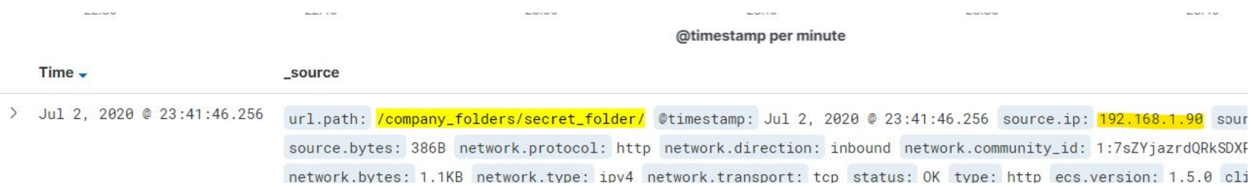
          Answer:

          The company_folders/secret_folder/ directory was requested 6534 times total from 7/2-7/7, but 6531 times within the one-hour attack time frame on 7/2. The source IP address for all 6531 requests was 198.168.1.90.

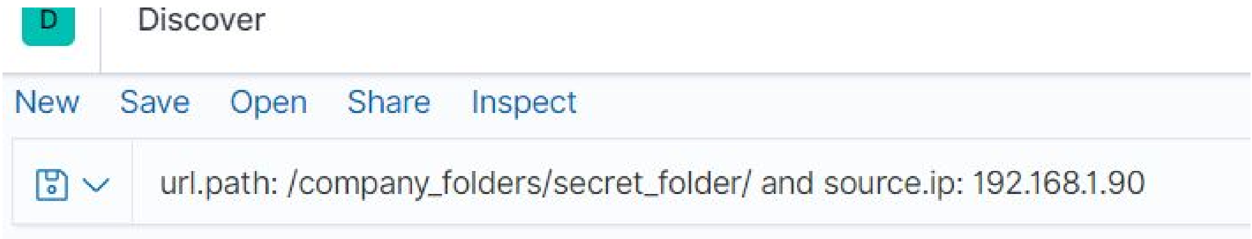


Top 10 HTTP requests [Packetbeat] ECS

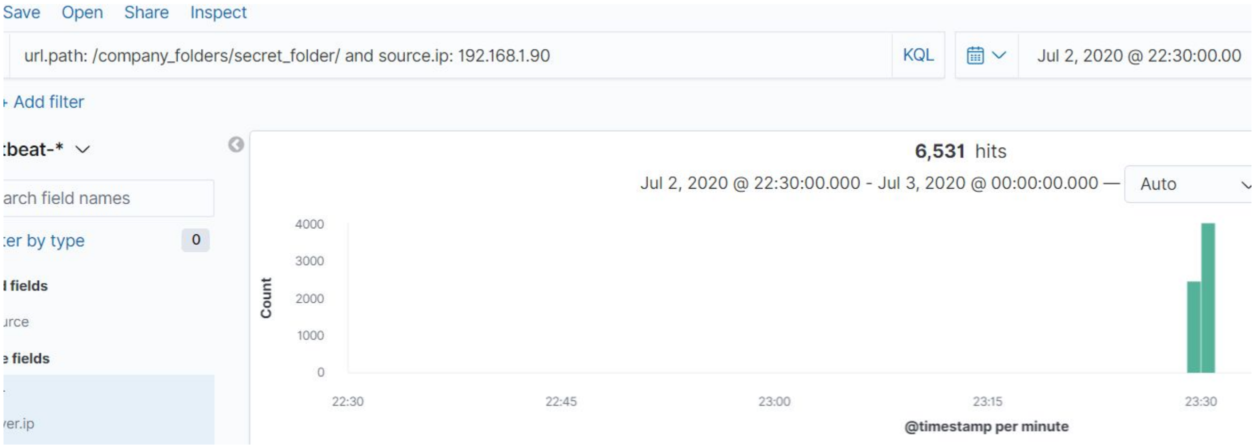
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,531
http://192.168.1.105/company_folders/	3
http://192.168.1.105/company_folders/company_culture/	3
http://192.168.1.105/company_folders/customer_info/	3
http://192.168.1.105/company_folders/secret_folder	3



```
Time     _source
Jul 2, 2020 @ 23:41:46.256   url.path: /company_folders/secret_folder/ @timestamp: Jul 2, 2020 @ 23:41:46.256 source.ip: 192.168.1.90 sour
source.bytes: 386B network.protocol: http network.direction: inbound network.community_id: 1:7sZYjazrdQRkSDXF
network.bytes: 1.1KB network.type: ipv4 network.transport: tcp status: OK type: http ecs.version: 1.5.0 cli
```



url.path: /company_folders/secret_folder/ and source.ip: 192.168.1.90

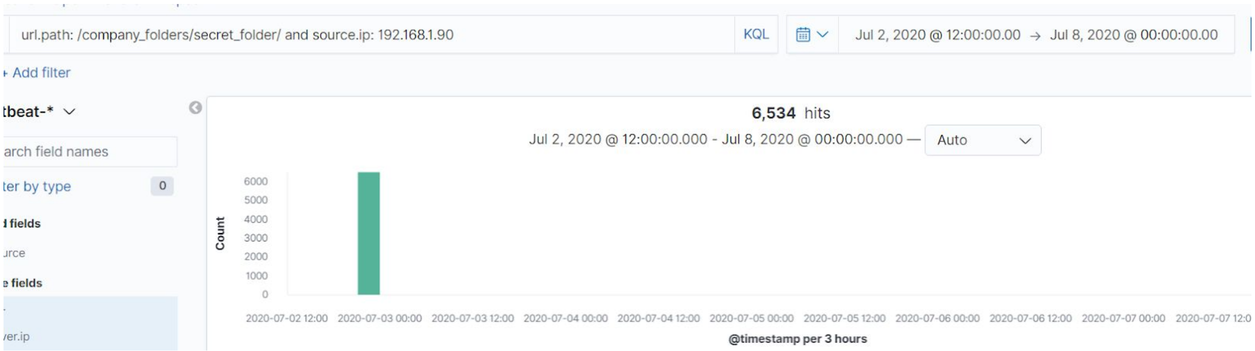


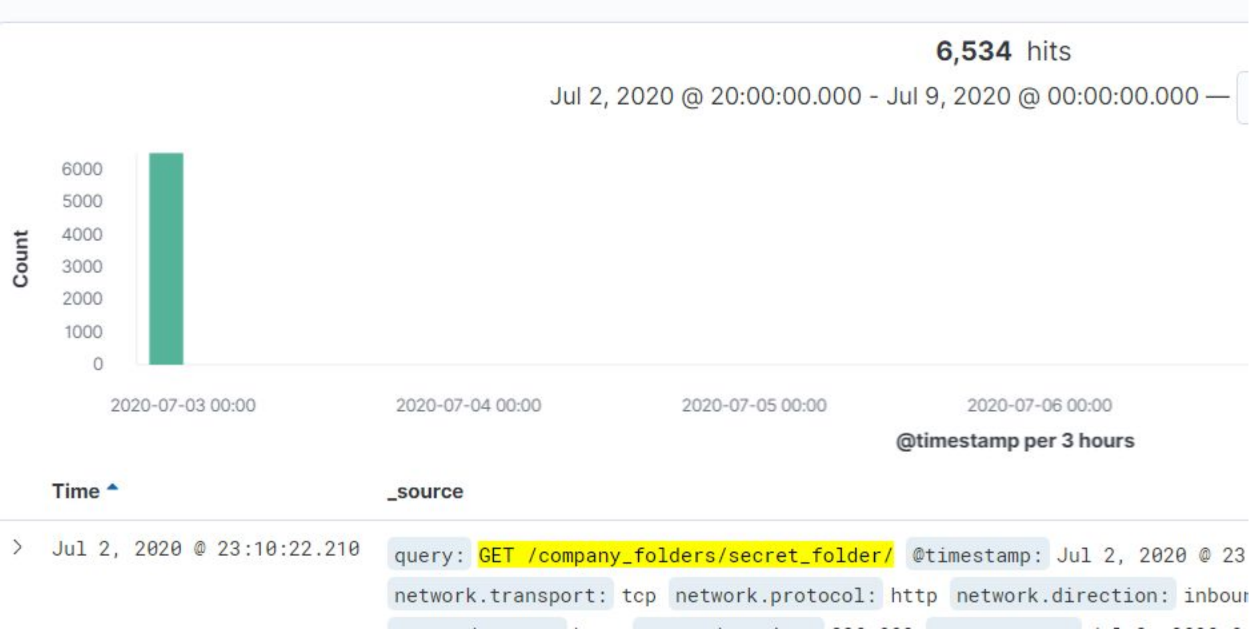
url.path: /company_folders/secret_folder/ and source.ip: 192.168.1.90

Jul 2, 2020 @ 22:30:00.00

6,531 hits

Jul 2, 2020 @ 22:30:00.000 - Jul 3, 2020 @ 00:00:00.000 —





```
> Jul 2, 2020 @ 23:10:22.210   query: GET /company_folders/secret_folder/  @timestamp: Jul 2, 2020 @ 23
                               network.transport: tcp  network.protocol: http  network.direction: inbour
```

- Which files were requested? What information did they contain?

  The file http://192.168.1.105/company_folders/secret_folder/ was requested. This file contains instructions on how to logon and access the company's internal, WebDav server.

- What kind of alarm would you set to detect this behavior in the future?

  Since only 1-2 people in the company should have access to this file, an alert to flag a user's machine trying to access this file should help.

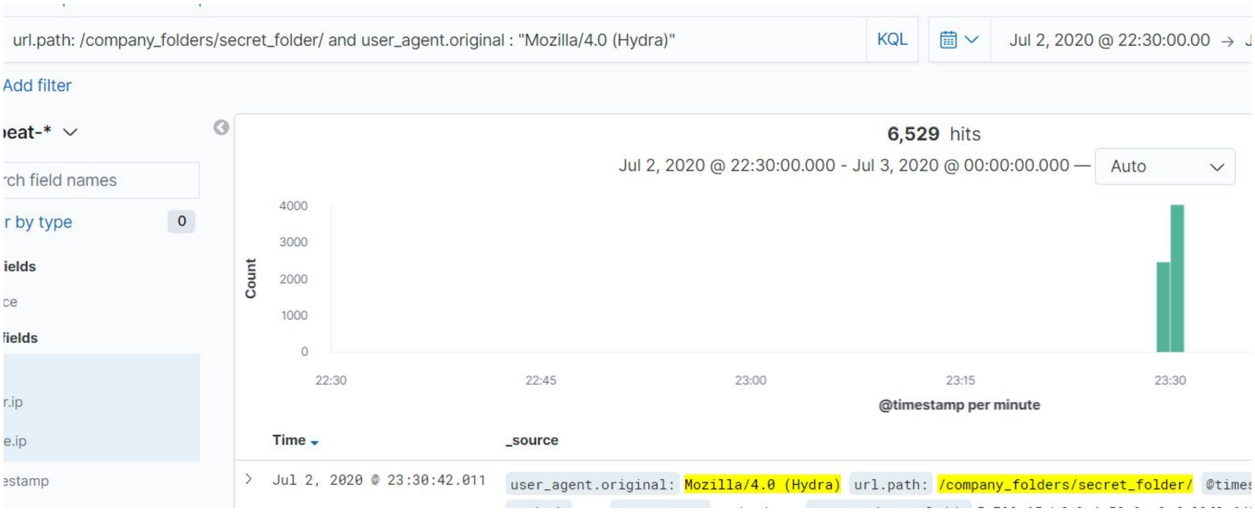
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.

The directory and file should either be moved to a different location or removed altogether. Also, mentions to this file from other file paths and directories should be removed.

3. Identify the brute force attack.

   - After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
     - Can you identify packets specifically from Hydra?

       Yes, when searching for the field “Mozilla/4.0 (Hydra)”, 6529 out of the 6534 packet requests contain this Hydra reference.



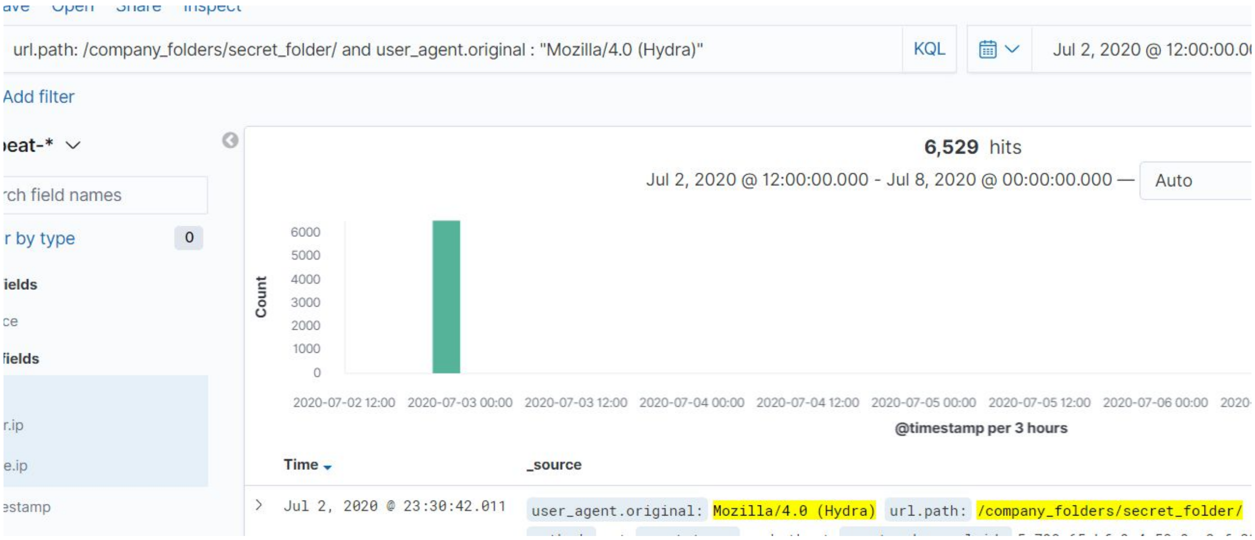
url.path: /company_folders/secret_folder/ and user_agent.original : "Mozilla/4.0 (Hydra)"

Jul 2, 2020 @ 22:30:00.00 → J

6,529 hits

Jul 2, 2020 @ 22:30:00.000 - Jul 3, 2020 @ 00:00:00.000 — Auto

```
Jul 2, 2020 @ 23:30:42.011   user_agent.original: Mozilla/4.0 (Hydra)  url.path: /company_folders/secret_folder/  @times
```



url.path: /company_folders/secret_folder/ and user_agent.original : "Mozilla/4.0 (Hydra)"

Jul 2, 2020 @ 12:00:00.0

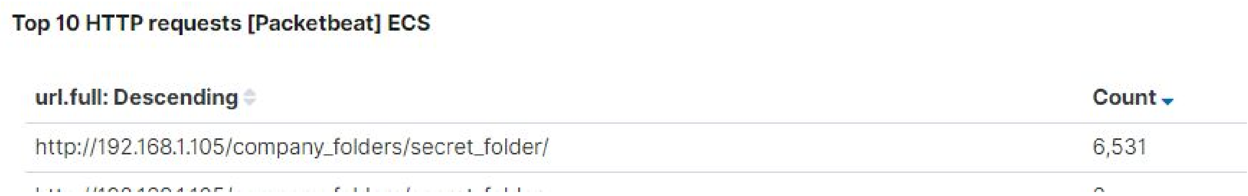
6,529 hits

Jul 2, 2020 @ 12:00:00.000 - Jul 8, 2020 @ 00:00:00.000 — Auto

```
Jul 2, 2020 @ 23:30:42.011   user_agent.original: Mozilla/4.0 (Hydra)  url.path: /company_folders/secret_folder/
```

- How many requests were made in the brute-force attack?

  6531 requests were made during the brute-force attack.

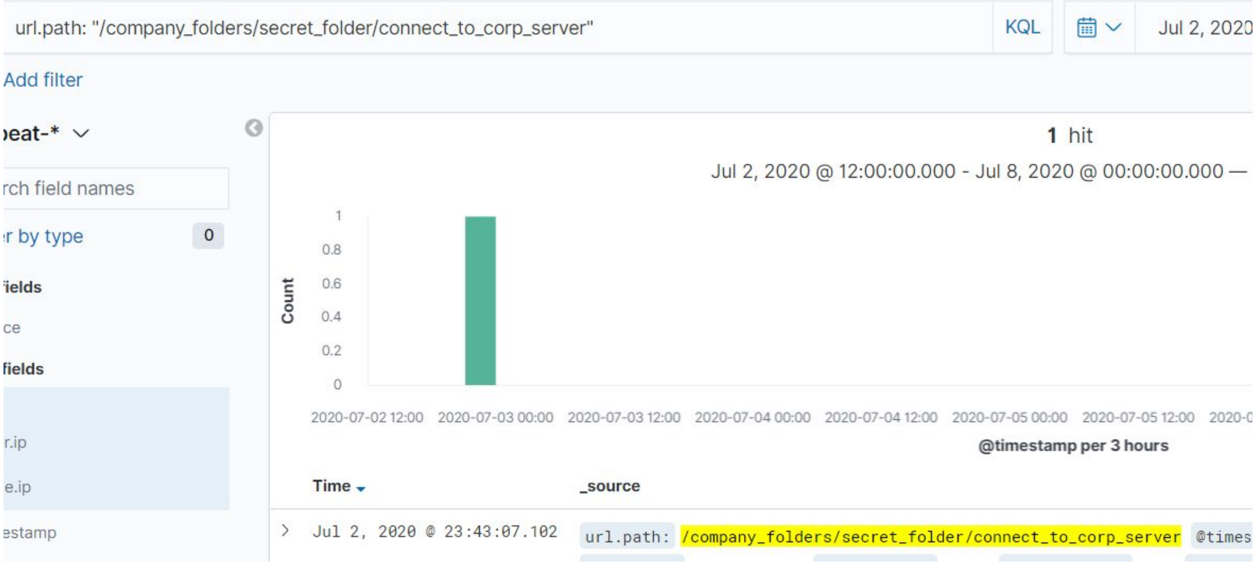


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,531

- How many requests had the attacker made before discovering the correct password in this one?

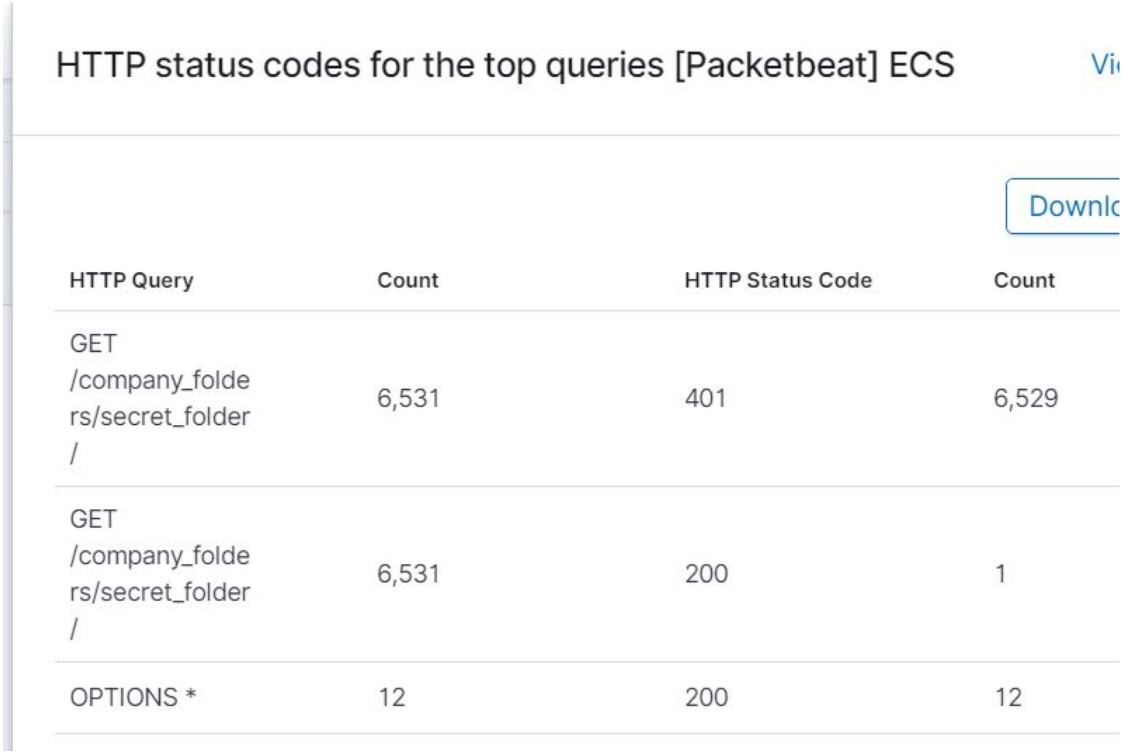
  6529 attempts until he/she was successful one time at 23:47 on 7/2.



url.path: "/company_folders/secret_folder/connect_to_corp_server"

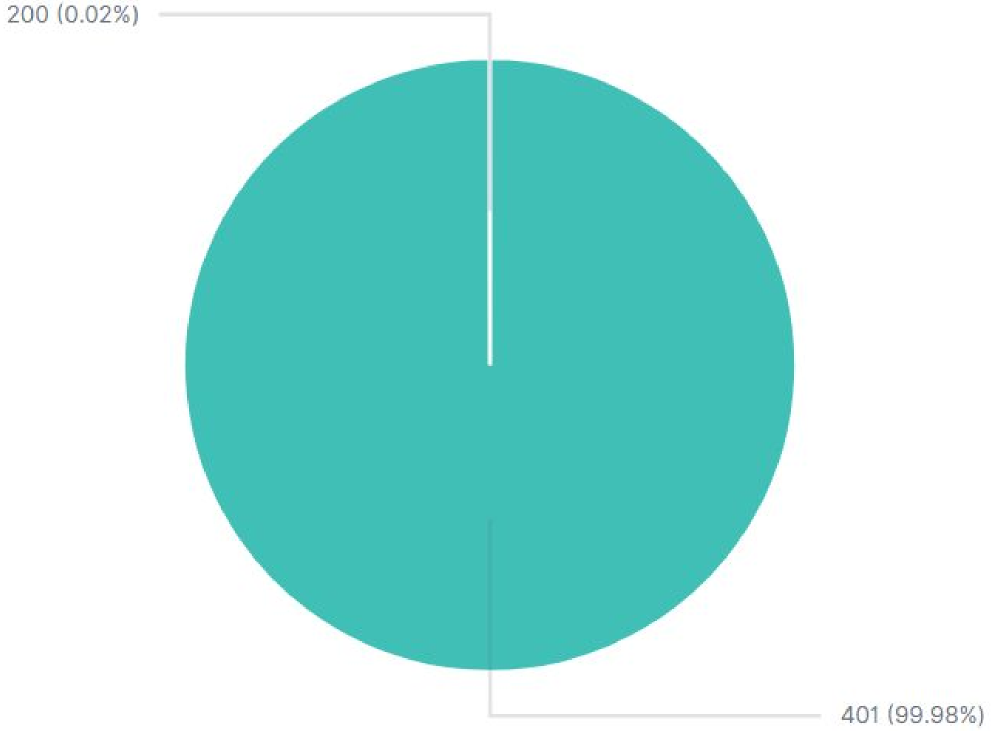
```
Jul 2, 2020 @ 23:43:07.102    url.path: /company_folders/secret_folder/connect_to_corp_server @times
```

Additionally, the host/victim returned the 401 Unauthorized status code for 6529 requests, then a 200 OK status for the one successful authentication hack.



HTTP status codes for the top queries [Packetbeat] ECS

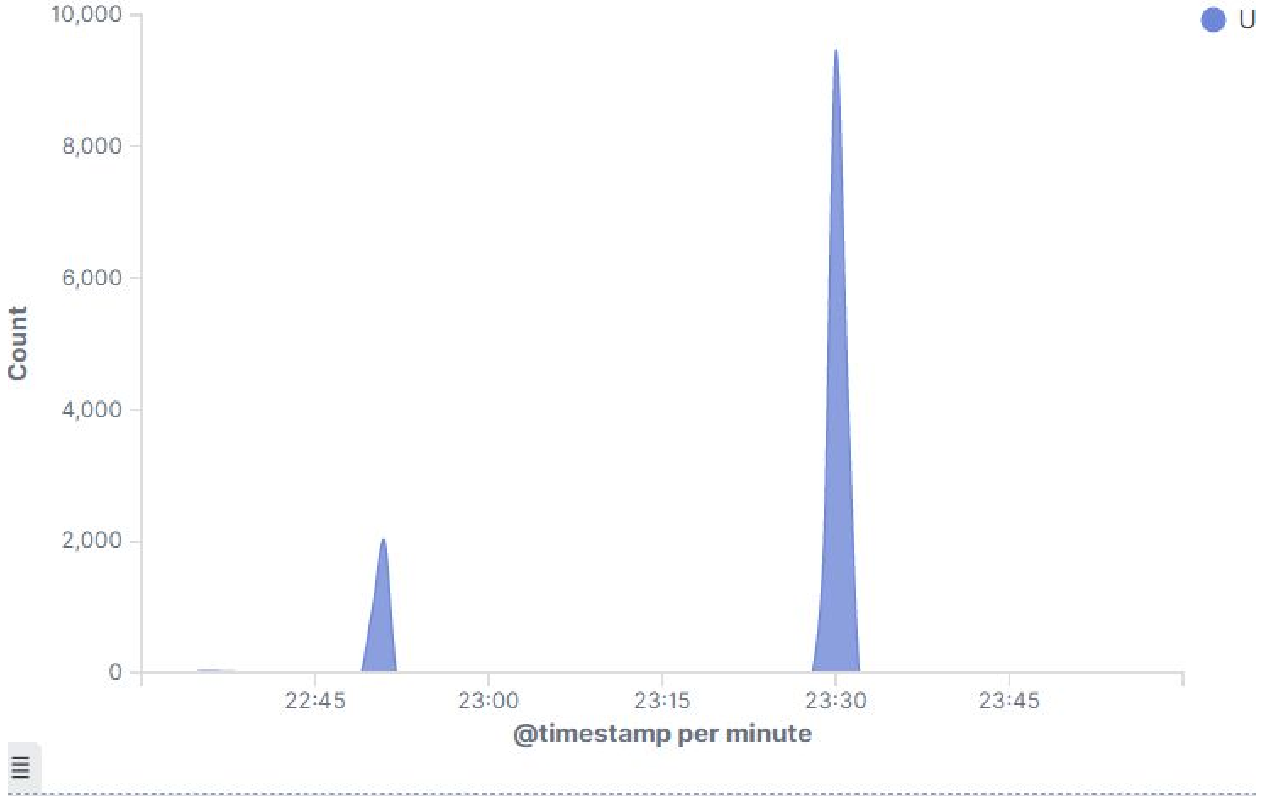
HTTP Query	Count	HTTP Status Code	Count
GET /company_folders/secret_folder/	6,531	401	6,529
GET /company_folders/secret_folder/	6,531	200	1
OPTIONS *	12	200	12

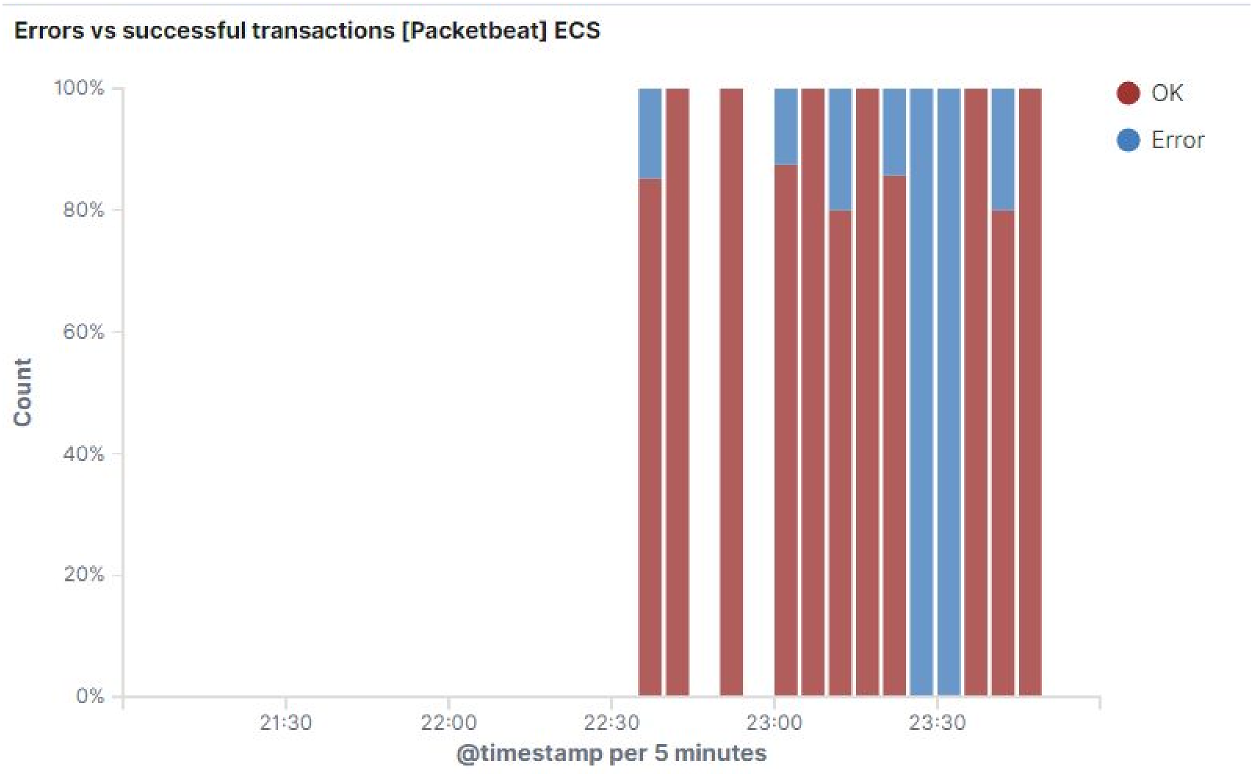


GET /company_folders/secret_folder/: HTTP Query

Also, there was a distinct spike in connection activity and errored transactions during the brute-force attack (around 23:30 on 7/2).

Connections over time [Packetbeat Flows] ECS





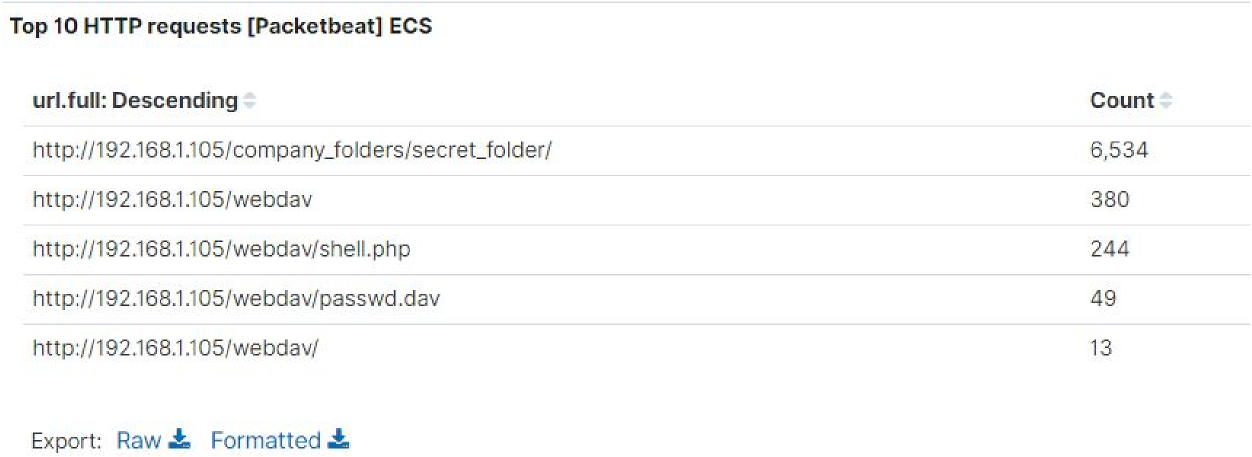
- What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
  - Set up an alert anytime one value within the user_agent.original field contains ‘Hydra’ or contains ‘Mozilla 4.0’. Most if not all company machines run Mozilla version 5.0
  - Set up an alert anytime a large or unusual amount of 401 (Unauthorized) status codes are generated from one MAC or IP address. The alert can be set off (have a threshold) when 10 401 codes are generated within 10 minutes.

- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Once the threshold has been reached, block all traffic from the offending IP address for a specified period of time (30-60 minutes).

4. Find the WebDav connection.

    - Use your dashboard to answer the following questions:
        - How many requests were made to this directory?

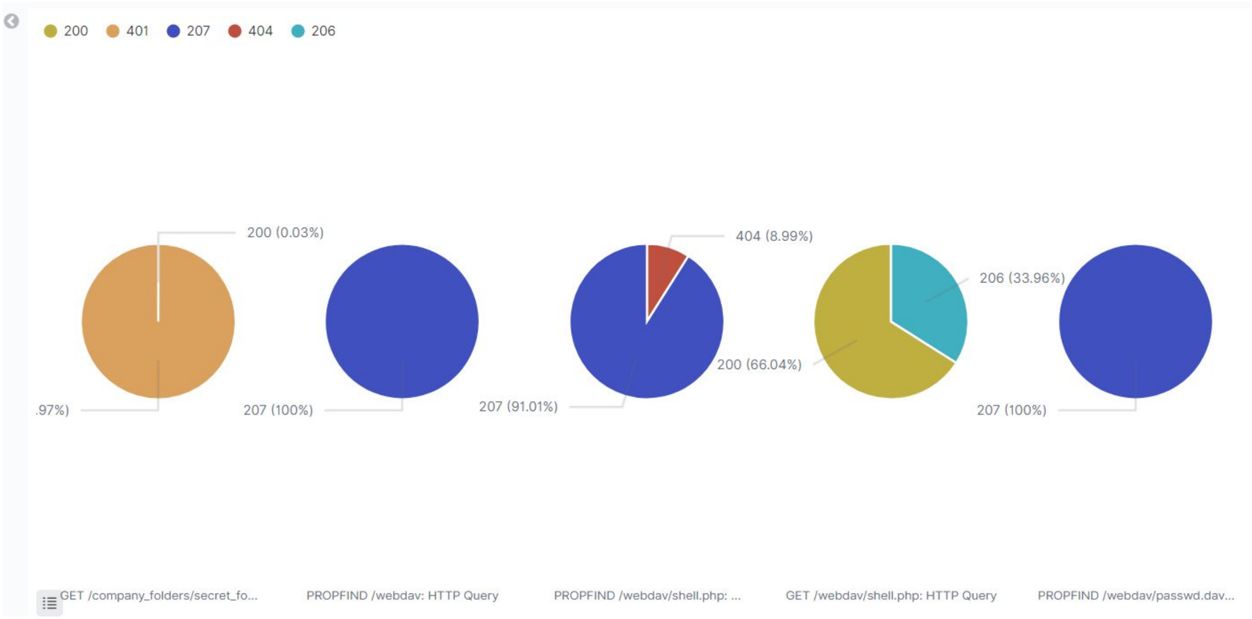
          198 requests were made to this directory during the second attack period from 7/5 at 19:00 through the end of 7/7.

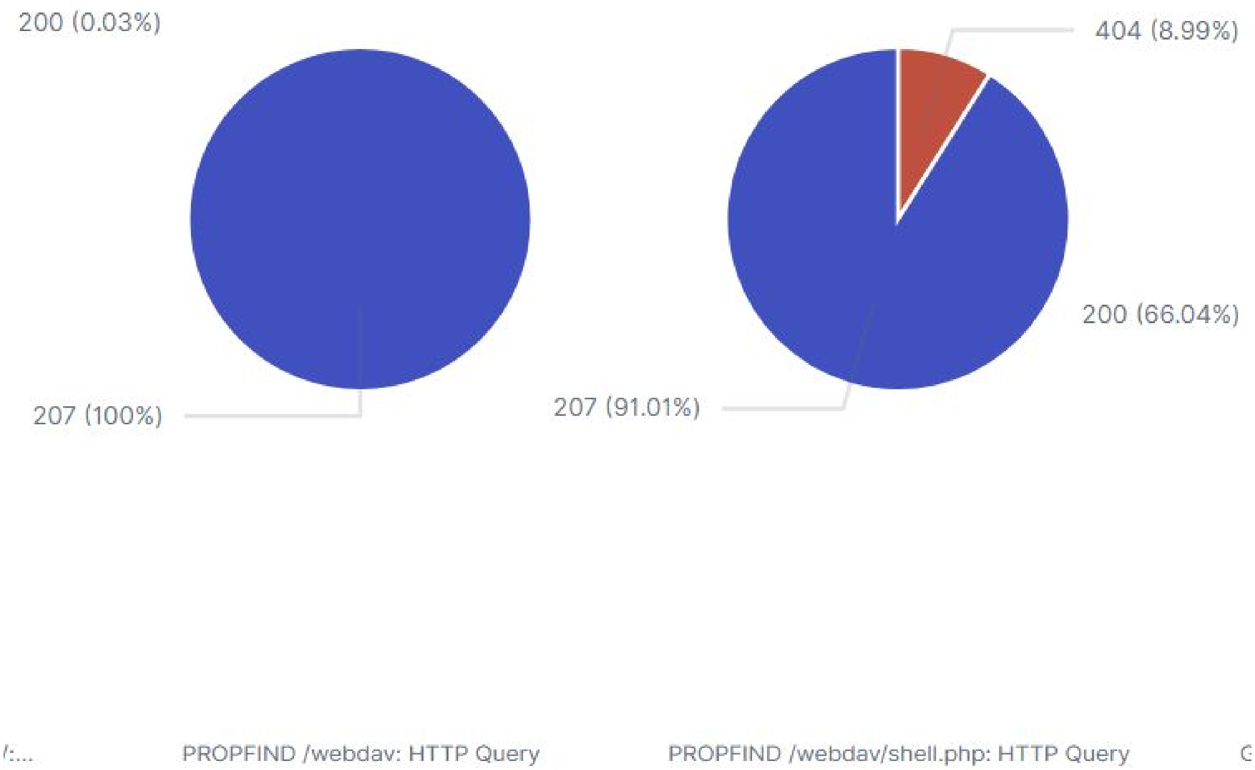


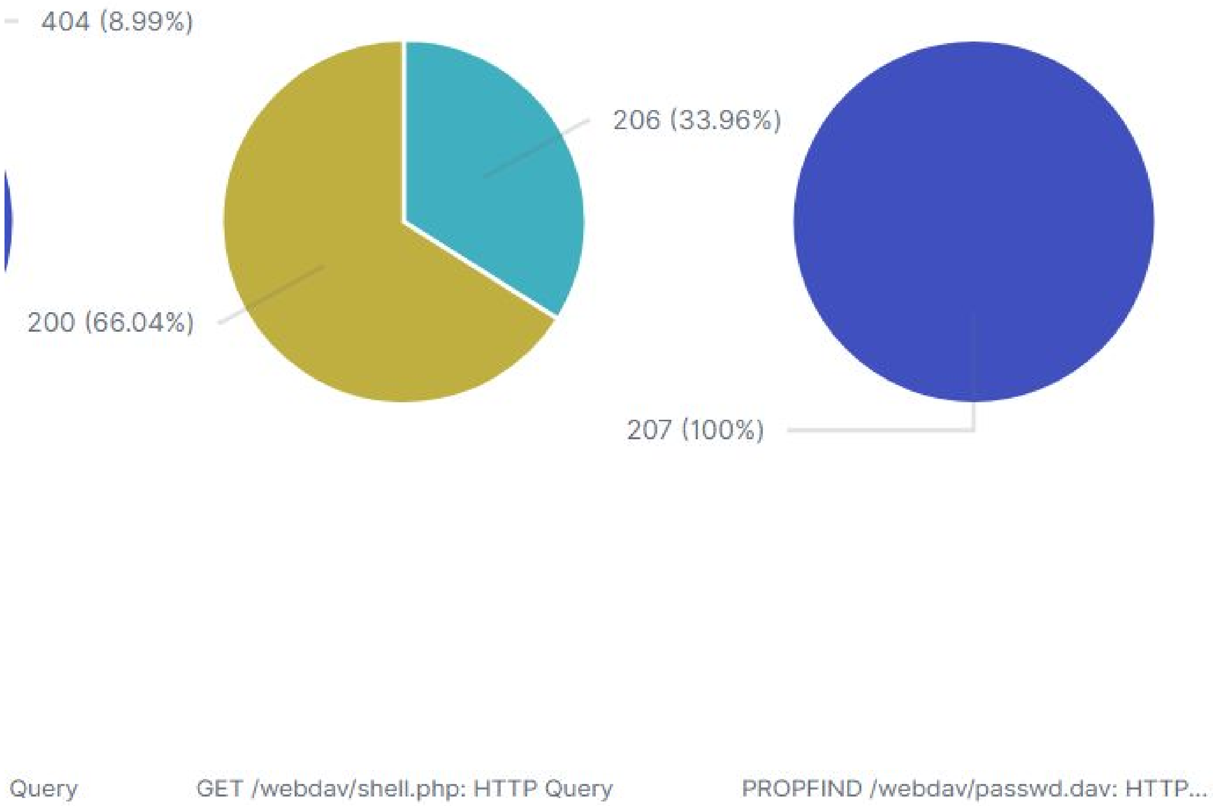
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,534
http://192.168.1.105/webdav	380
http://192.168.1.105/webdav/shell.php	244
http://192.168.1.105/webdav/passwd.dav	49
http://192.168.1.105/webdav/	13

The HTTP status response codes show successful, multi-status (code 207) for the webdav requests, while returning a 404 status (Request Cannot be Found) for 8 requests to shell.php request.


200
401
207
404
206
200 (0.03%)
.97%)
207 (100%)
404 (8.99%)
207 (91.01%)
206 (33.96%)
200 (66.04%)
207 (100%)
GET /company_folders/secret_fo...
PROPFIND /webdav: HTTP Query
PROPFIND /webdav/shell.php: ...
GET /webdav/shell.php: HTTP Query
PROPFIND /webdav/passwd.dav...


200 (0.03%)
404 (8.99%)
200 (66.04%)
207 (100%)
207 (91.01%)
/:...
PROPFIND /webdav: HTTP Query
PROPFIND /webdav/shell.php: HTTP Query
G



- Which file(s) were requested?

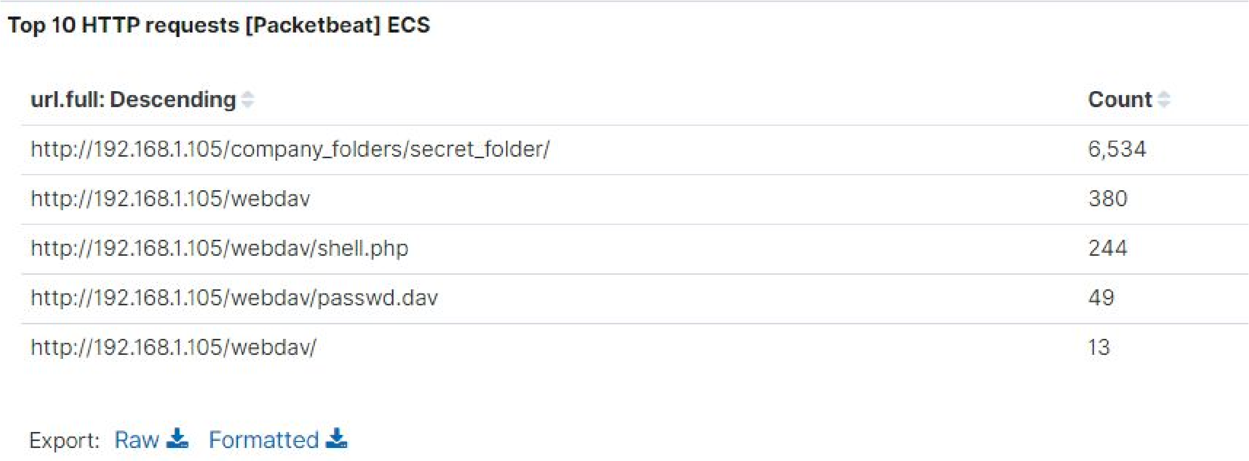
  A file named shell.php was requested 158 times, while the passwd.dav file was requested 25 times.

- What kind of alarm would you set to detect such access in the future?
  - Set up an alert anytime any IP address outside of the company requests the webdav directory.
  - An alert can also be set to notify anytime an unauthorized employee requests this directory.
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Block access to the webdav directory from a web browser or other GUI interface.
  - Block access to the directory via a firewall rule to all parties other than those employees with approved access to the directory.

5. Identify the reverse shell and meterpreter traffic.

- To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
  - Can you identify traffic from the meterpreter session?

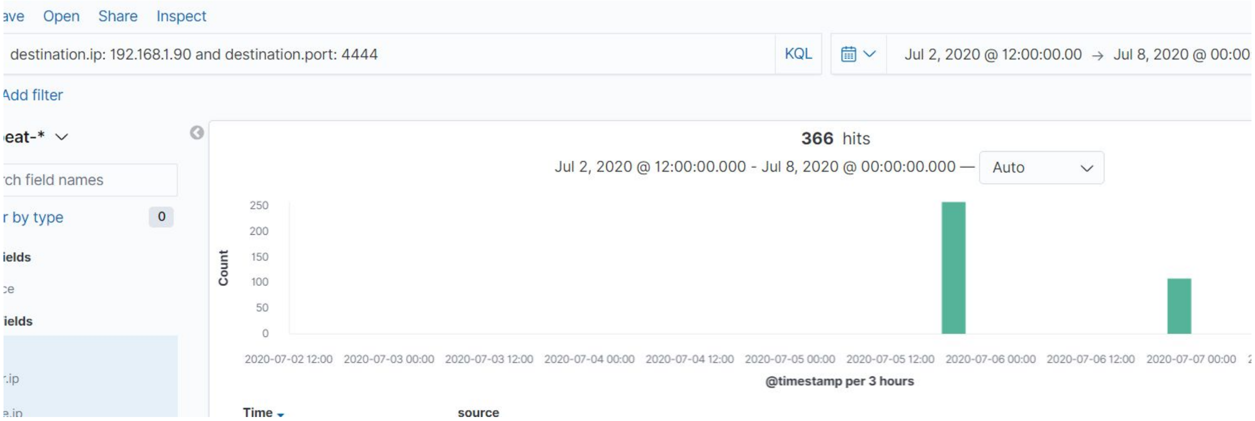
    158 requests were made on the reverse shell (shell.php).



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,534
http://192.168.1.105/webdav	380
http://192.168.1.105/webdav/shell.php	244
http://192.168.1.105/webdav/passwd.dav	49
http://192.168.1.105/webdav/	13

Also, traffic from the meterpreter session moved over port 4444. When searching for destination.ip of 192.168.1.90 and destination.port: 4444, we receive 366 results over the 7/5-7/7 time period

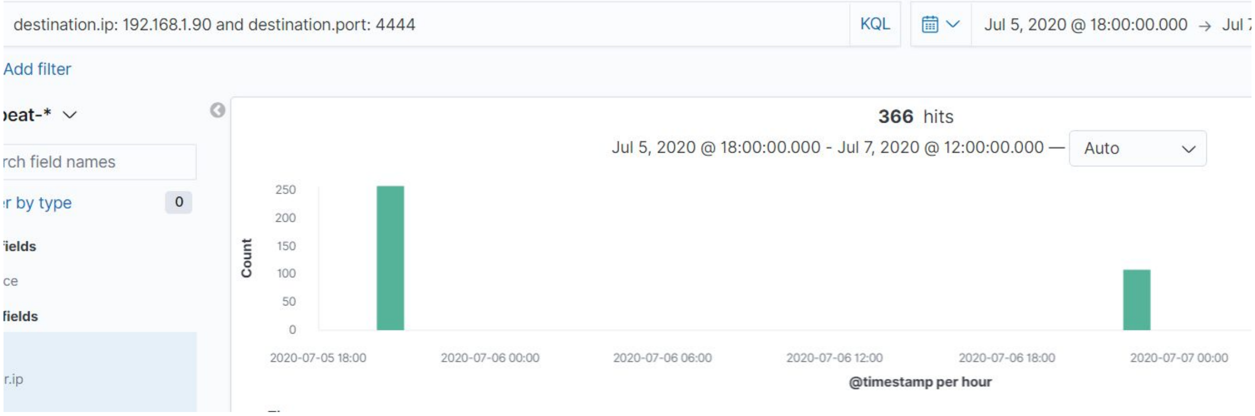


destination.ip: 192.168.1.90 and destination.port: 4444

Jul 2, 2020 @ 12:00:00.00 → Jul 8, 2020 @ 00:00

366 hits

Jul 2, 2020 @ 12:00:00.000 - Jul 8, 2020 @ 00:00:00.000 —

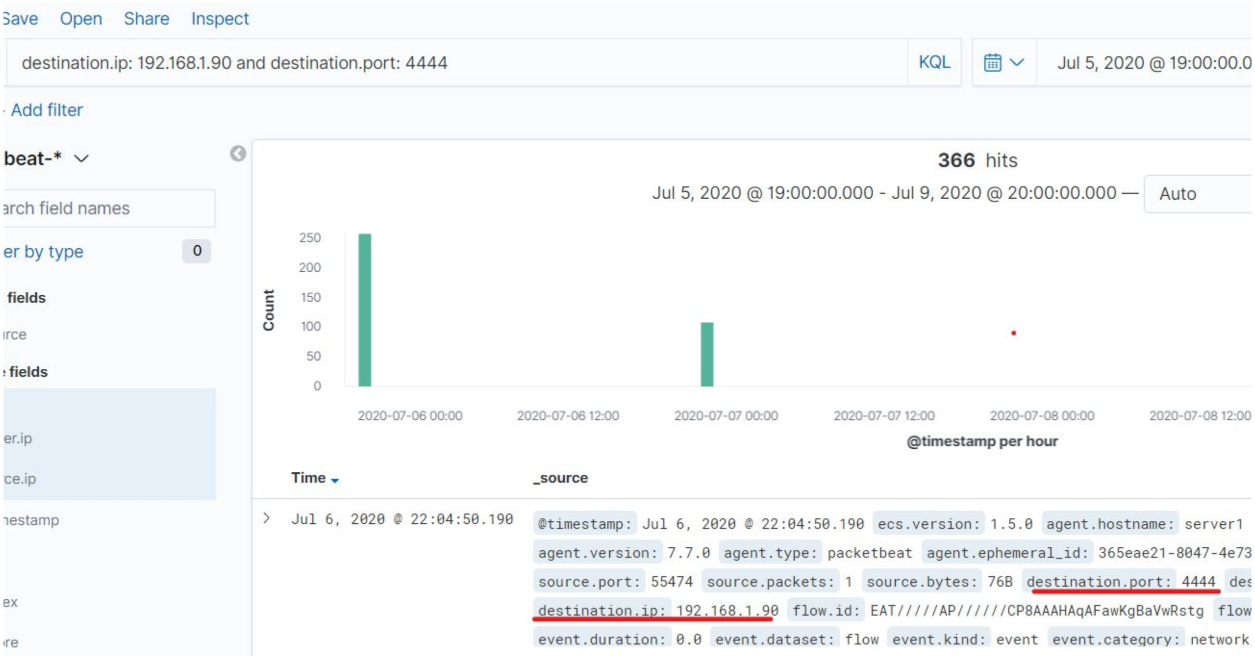


destination.ip: 192.168.1.90 and destination.port: 4444

Jul 5, 2020 @ 18:00:00.000 → Jul 7

366 hits

Jul 5, 2020 @ 18:00:00.000 - Jul 7, 2020 @ 12:00:00.000 —



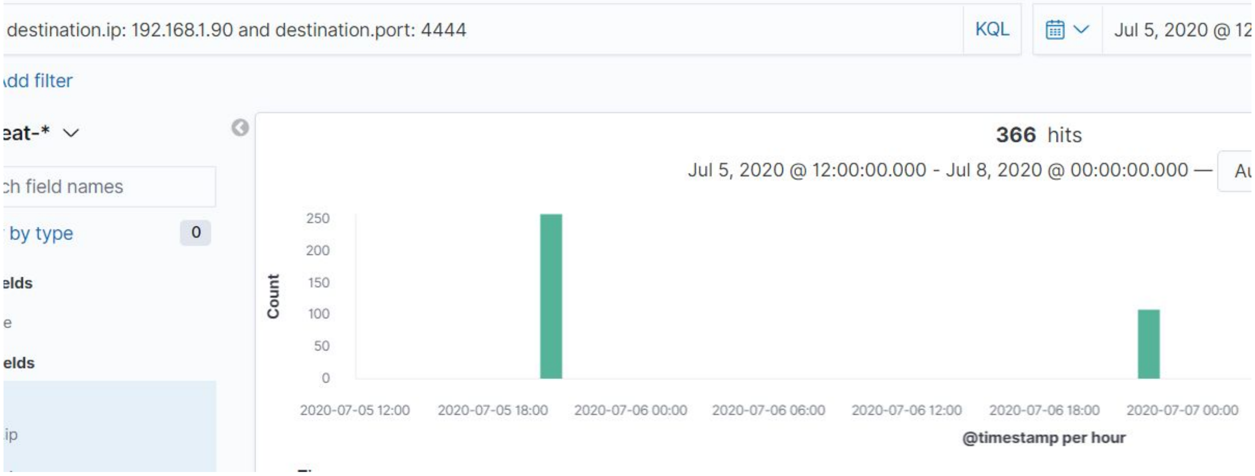
destination.ip: 192.168.1.90 and destination.port: 4444

Jul 5, 2020 @ 19:00:00.0

366 hits

Jul 5, 2020 @ 19:00:00.000 - Jul 9, 2020 @ 20:00:00.000 —

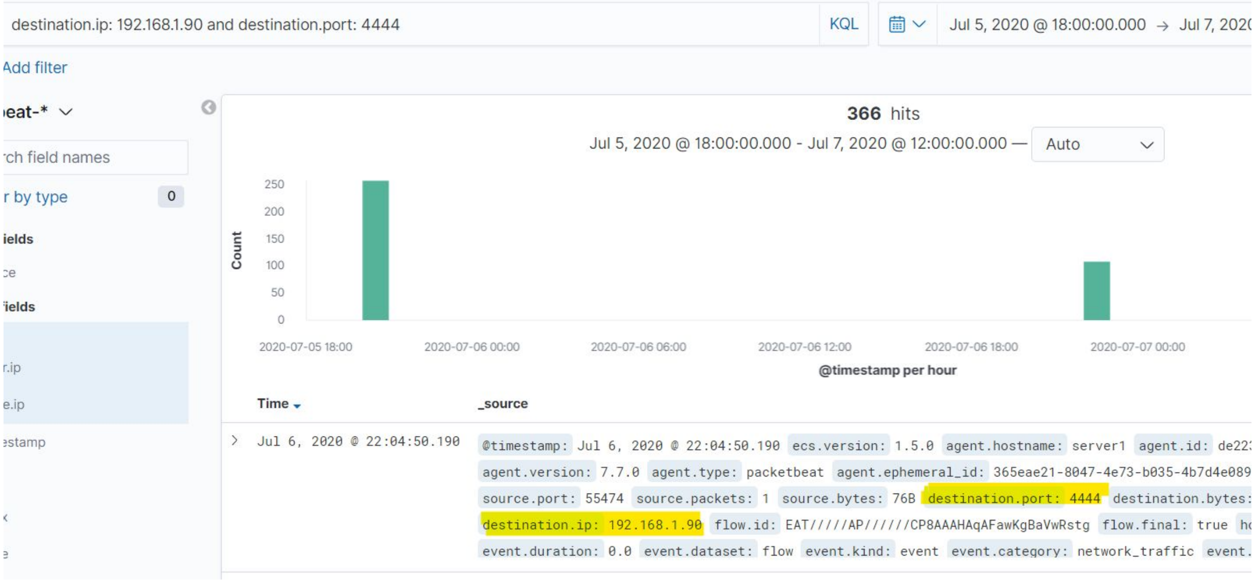
```
Time                        _source
> Jul 6, 2020 @ 22:04:50.190  @timestamp: Jul 6, 2020 @ 22:04:50.190 ecs.version: 1.5.0 agent.hostname: server1
                            agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 365eae21-8047-4e73
                            source.port: 55474 source.packets: 1 source.bytes: 76B destination.port: 4444 des
                            destination.ip: 192.168.1.90 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRstg flow
                            event.duration: 0.0 event.dataset: flow event.kind: event event.category: network
```



destination.ip: 192.168.1.90 and destination.port: 4444

366 hits

Jul 5, 2020 @ 12:00:00.000 - Jul 8, 2020 @ 00:00:00.000 —



destination.ip: 192.168.1.90 and destination.port: 4444

366 hits

Jul 5, 2020 @ 18:00:00.000 - Jul 7, 2020 @ 12:00:00.000 — Auto

```
Time        _source
Jul 6, 2020 @ 22:04:50.190   @timestamp: Jul 6, 2020 @ 22:04:50.190 ecs.version: 1.5.0 agent.hostname: server1 agent.id: de22
                             agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 365eae21-8047-4e73-b035-4b7d4e089
                             source.port: 55474 source.packets: 1 source.bytes: 76B destination.port: 4444 destination.bytes:
                             destination.ip: 192.168.1.90 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRstg flow.final: true hc
                             event.duration: 0.0 event.dataset: flow event.kind: event event.category: network_traffic event.
```

- What kinds of alarms would you set to detect this behavior in the future?
    - Set up an alert anytime traffic is moving over port 4444.
    - Set up an alert anytime a php. file is located on the webdav server.
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    - Set up a firewall rule to block any traffic moving from port 4444.
    - Disable the ability to add or remove any files on this directory from a web browser or GUI interface.
    - Restrict access to this directory to only specific, authorized users.