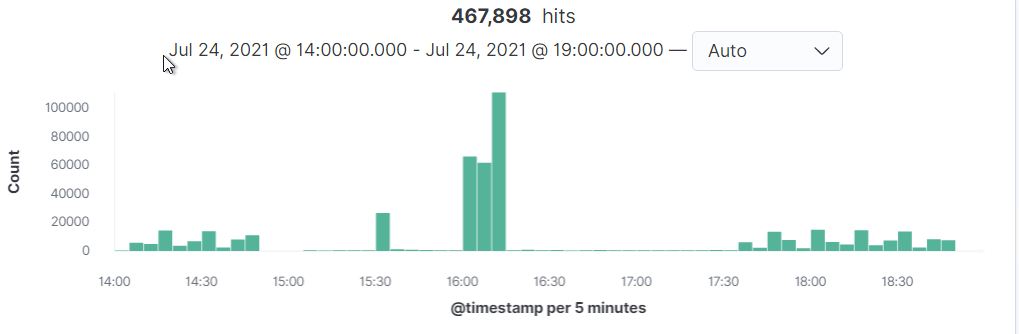
After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.

- Identify the traffic between your machine and the web machine:

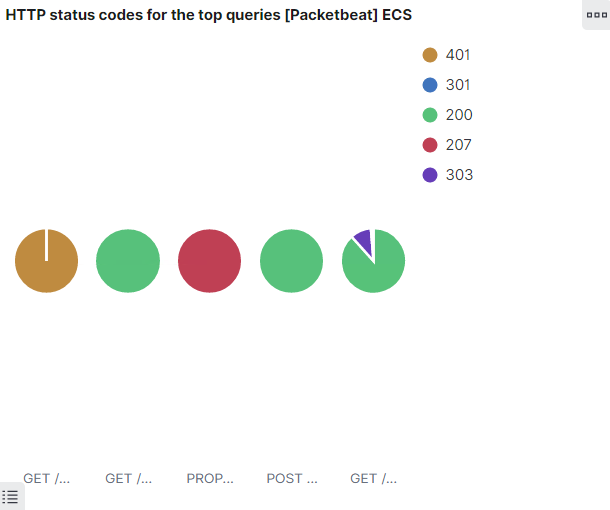
- When did the interaction occur?

Saturday 7/24 between 14:00 and 18:00



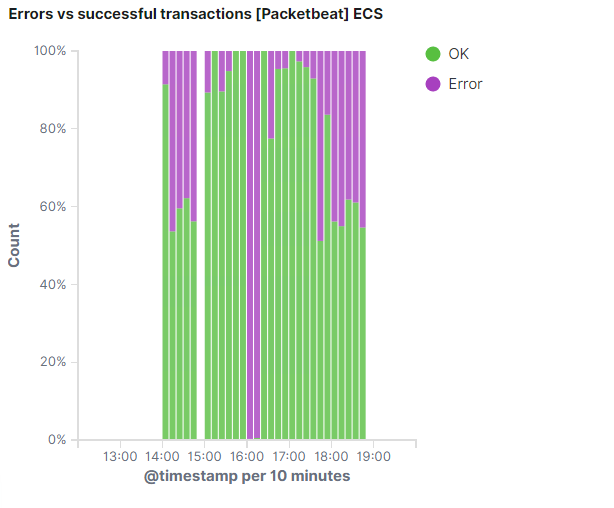
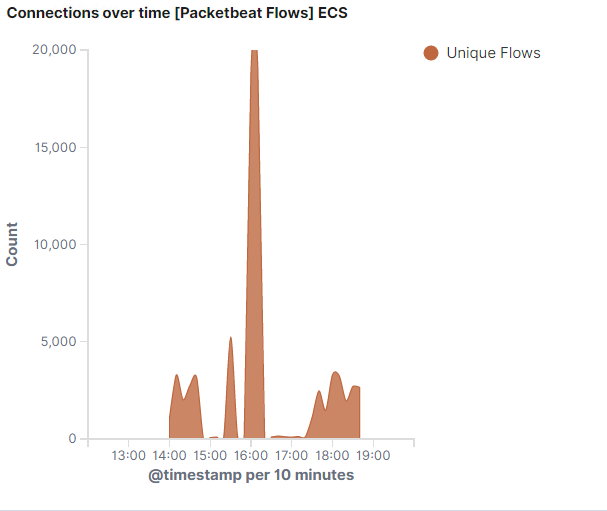
- What responses did the victim send back?

401, 301, 207, 303, and 200 are the top responses



- What data is concerning from the Blue Team perspective?

What is concerning about the data is the spikes in the connections over time chart and the errors vs successful transactions

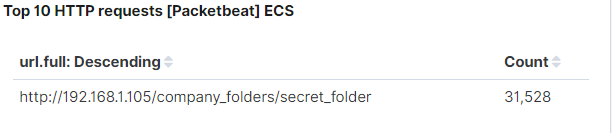


2. Find the request for the hidden directory.

- In your attack, you found a secret folder. Let's look at that interaction between these two machines.

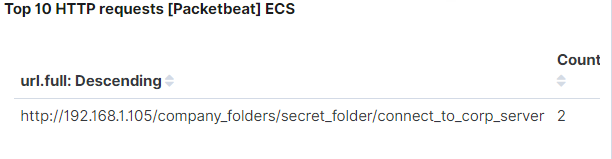
- How many requests were made to this directory? At what time and from which IP address(es)?

From the top 10 http requests dashboard it looks like the /company\_folders/secret\_folder was hit 31,528 times



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

They requested /company\_folders/secret\_folder/connect\_to\_corp\_server twice, which contained instructions on how to connect to the companies webdav.



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

I would really set an alert for anyone trying to access the /connect\_to\_corp\_server folder because of the importance of the information in the folder.

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

A major one would be for this file or directory to be deleted so no one would be able to see instructions on how to access this information.

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?

There were about 496 hits where “hydra” was the user agent in accessing “/secret\_folder”

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

There were 31,528 hits with 2 successful gaining access to the /connect\_to\_company\_server file

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

31,528

- What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?

I think an alert that detects more than 10 401 errors in 1 hour would be necessary because it indicates some form of attack or an alert that shows “hydra” as an user agent at any time would be necessary.

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

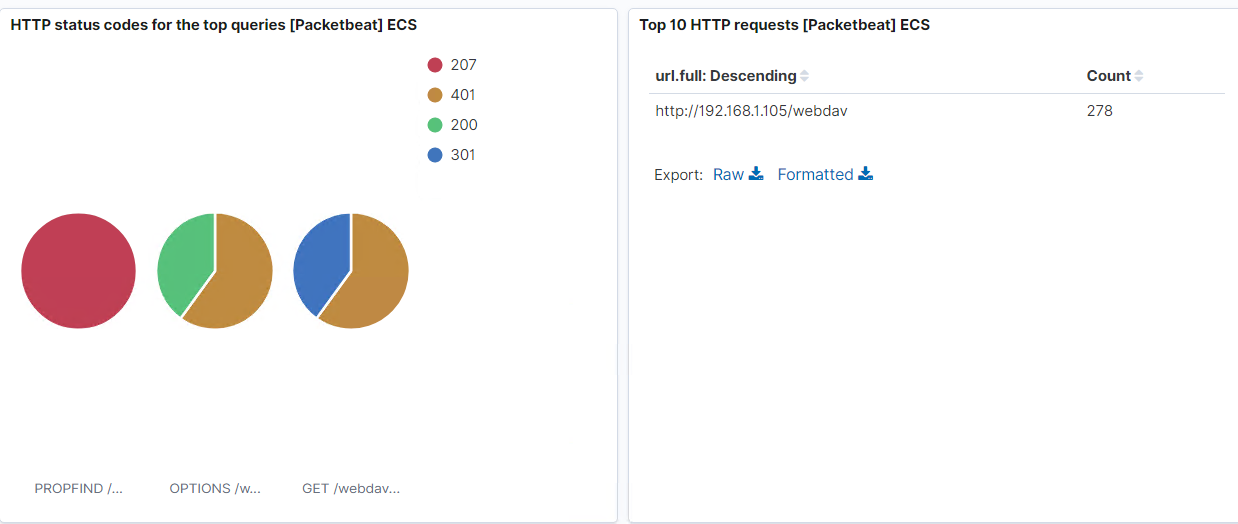
One way would be to lockdown an ip address or user agent after 3-5 attempts in one hour to try and prevent any brute force attacks.

4. Find the WebDav connection.

- Use your dashboard to answer the following questions:

- How many requests were made to this directory?

There were 278 requests made to the webdav directory



- Which file(s) were requested?

Shell.php and passwd.dv were both requested during the attack.

- What kind of alarm would you set to detect such access in the future?

I would set an alert for anyone accessing the Webdav directory, other than the machine that is supposed to.

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

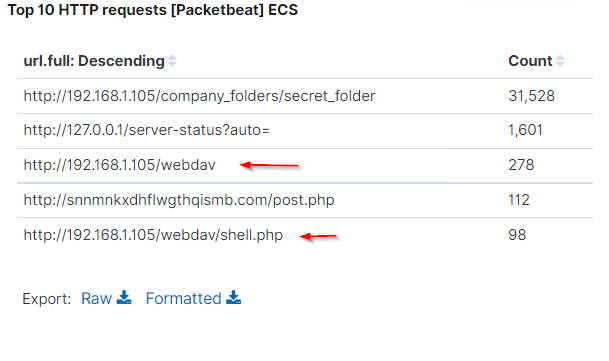
One way would be to create a firewall rule to only allow certain ip addresses to access it.

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?

With the source ip of 168.192.1.105 connecting to the webdav and shell.php we can look further into them and see that the destination port was 4444.



- What kinds of alarms would you set to detect this behavior in the future?

An alert to notify us of any traffic on port 4444 or of anyone uploading a .php file onto the network would be 2 great alerts.

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

One way would be to not allow anyone to upload anything to this directory over the web.