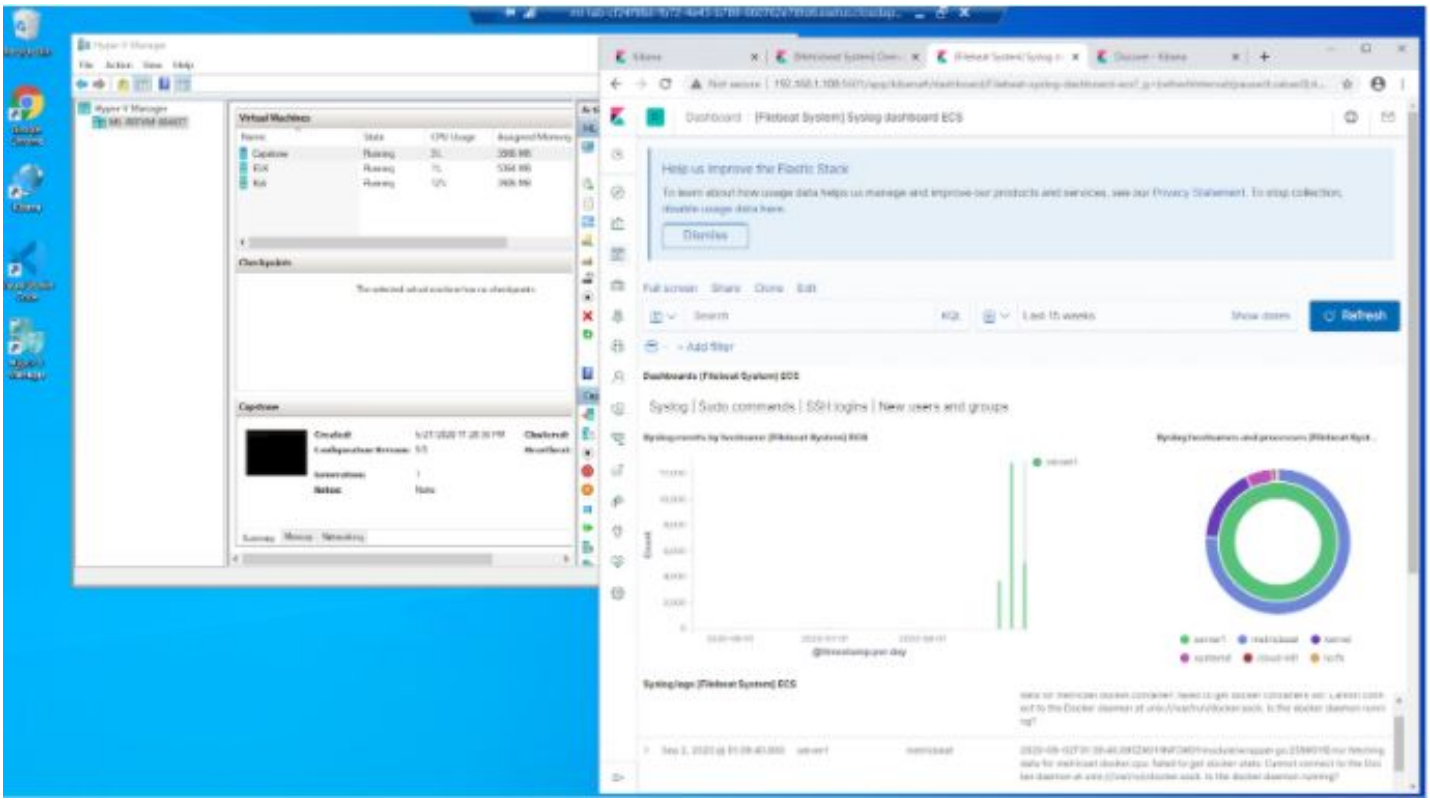
Defend

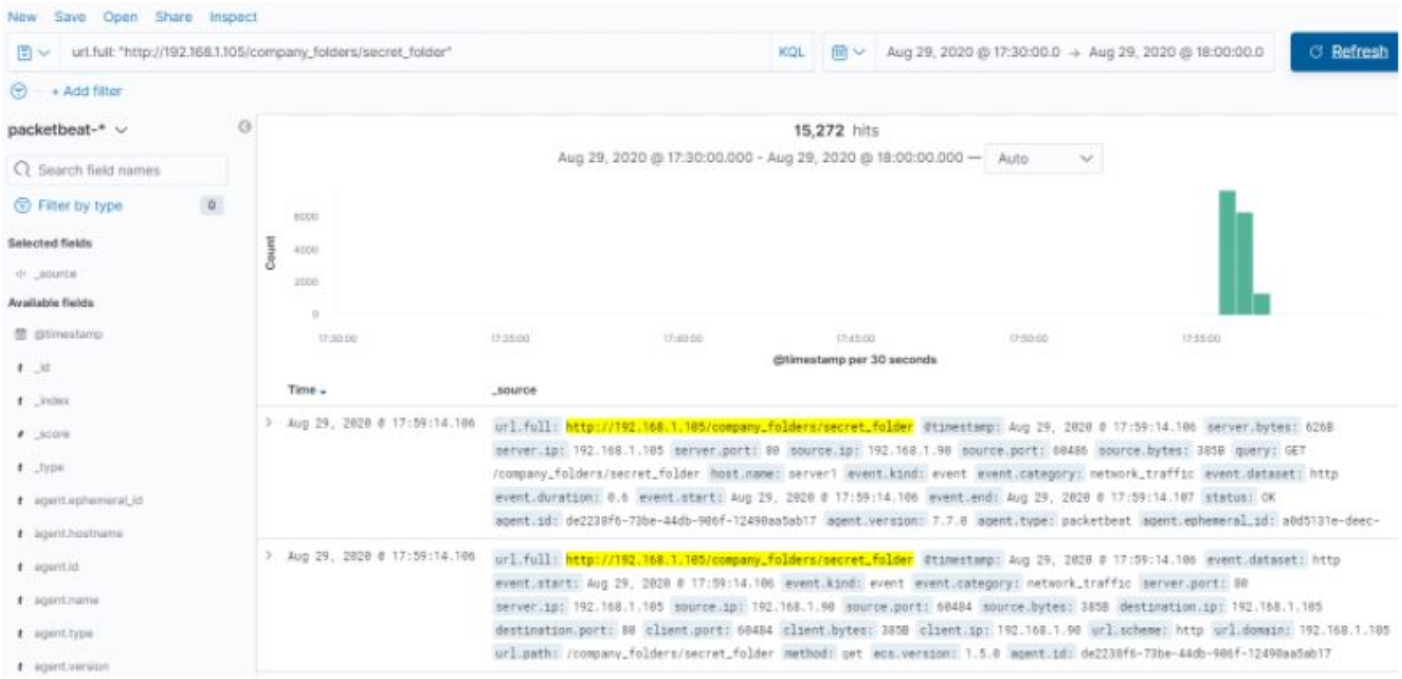
Set up:
Make sure that all three VM's are running



From the workstation, open the web browser and navigate to Kibana page (192.168.1.105:5601 -- the IP address of the vulnerable machine and the port in which its logs are being recorded to the ELK stack). Ensure to add the Kibana log data.

Create a dashboard with:

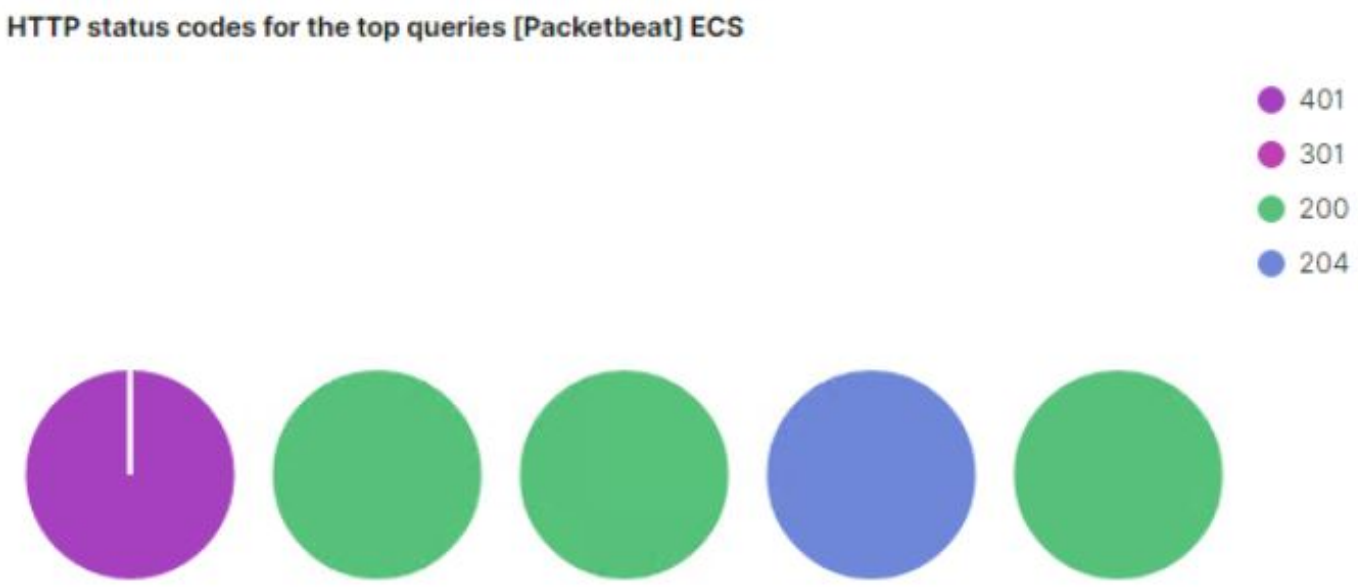
- HTTP status codes for the top queries [Packetbeat] ECS
- Top 10 HTTP requests [Packetbeat] ECS
- Network Traffic Between Hosts [Packetbeat Flows] ECS
- Top Hosts Creating Traffic [Packetbeat Flows] ECS
- Connections over time [Packetbeat Flows] ECS
- HTTP error codes [Packetbeat] ECS
- Errors default successful transactions [Packetbeat] ECS
- HTTP Transactions [Packetbeat] ECS



Summary:

Identify the offensive traffic.

- When did the interaction occur?
  - On August 29 from 17:30
- What responses did the victim send back?
  - HTTP response codes of: 401, 301, 200, and 204
  -



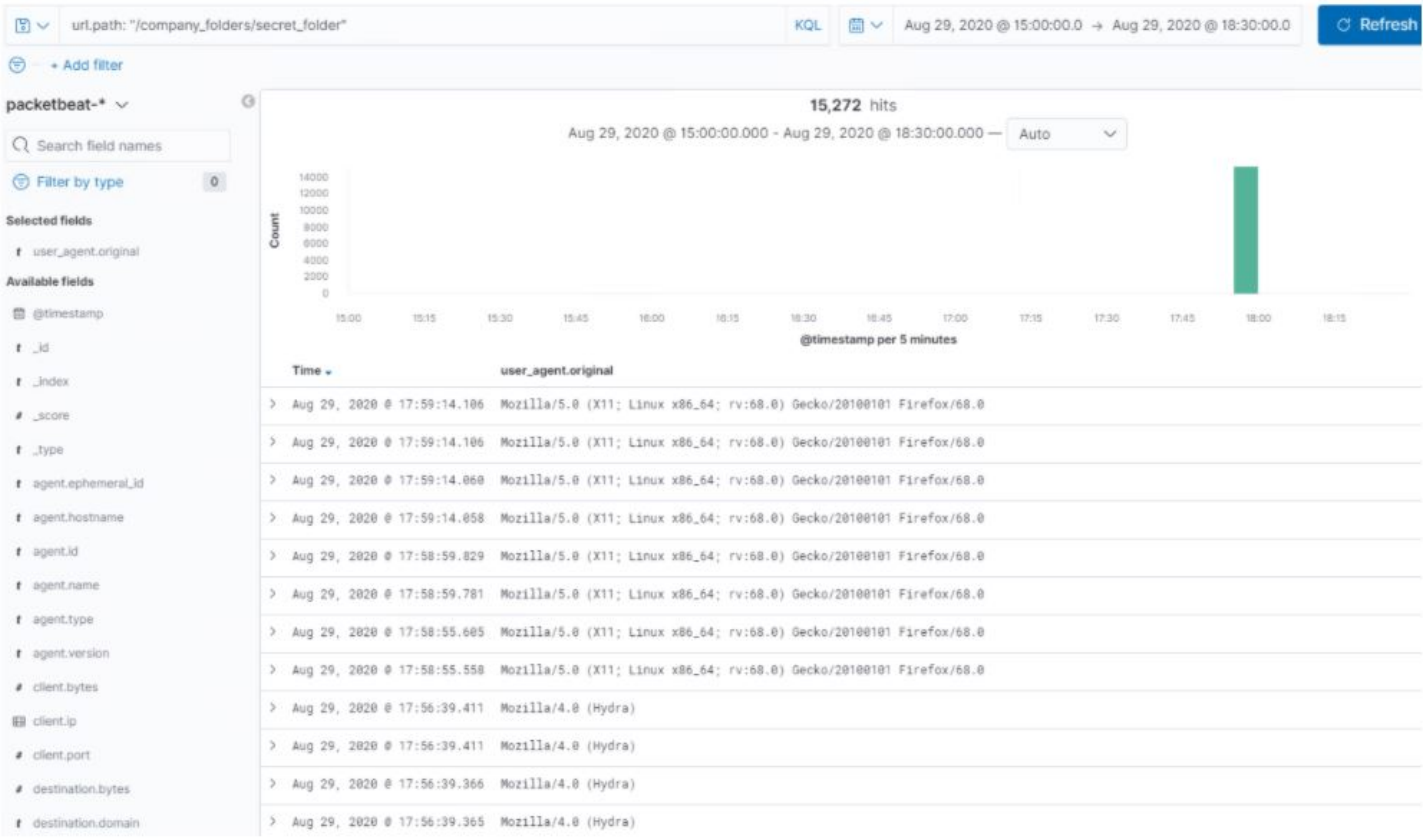
- What data is concerning from the Blue Team perspective?
  - The spike in abnormal traffic on the server and the access of the “secret_folder”, as well as the size of the data transferred

Find the request for the hidden directory

- In the attack, you found a secret folder. Let's look at the interaction between these two machines.
  - How many requests were made to this directory? At what time and from which IP address(es)?
    - At 17:50, 15,272 requests were made, from 192.168.1.90.
  - Which files were requested? What information did they contain?
    - An Alarm to detect when the HTTP requests exceed a threshold
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    - Disable access to root via SSH
    - Disable unused services
    - Limit connection rates

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
    -



  - How many requests were made in the brute-force attack?
    - 15,268
  - How many requests had the attacker made before discovering the correct password in this one?
    - 4
  - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
    - Alert that is triggered when the 401 unauthorized HTTP response code has reached its threshold.
    - Alert that identifies when the user-agent names that match password cracking software, like Hydra, John the Ripper, etc
    - Alert when login failure has reached its threshold.
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    - Once the HTTP response code 401 unauthorized has been produced 10 times, the IP address can be blocked.

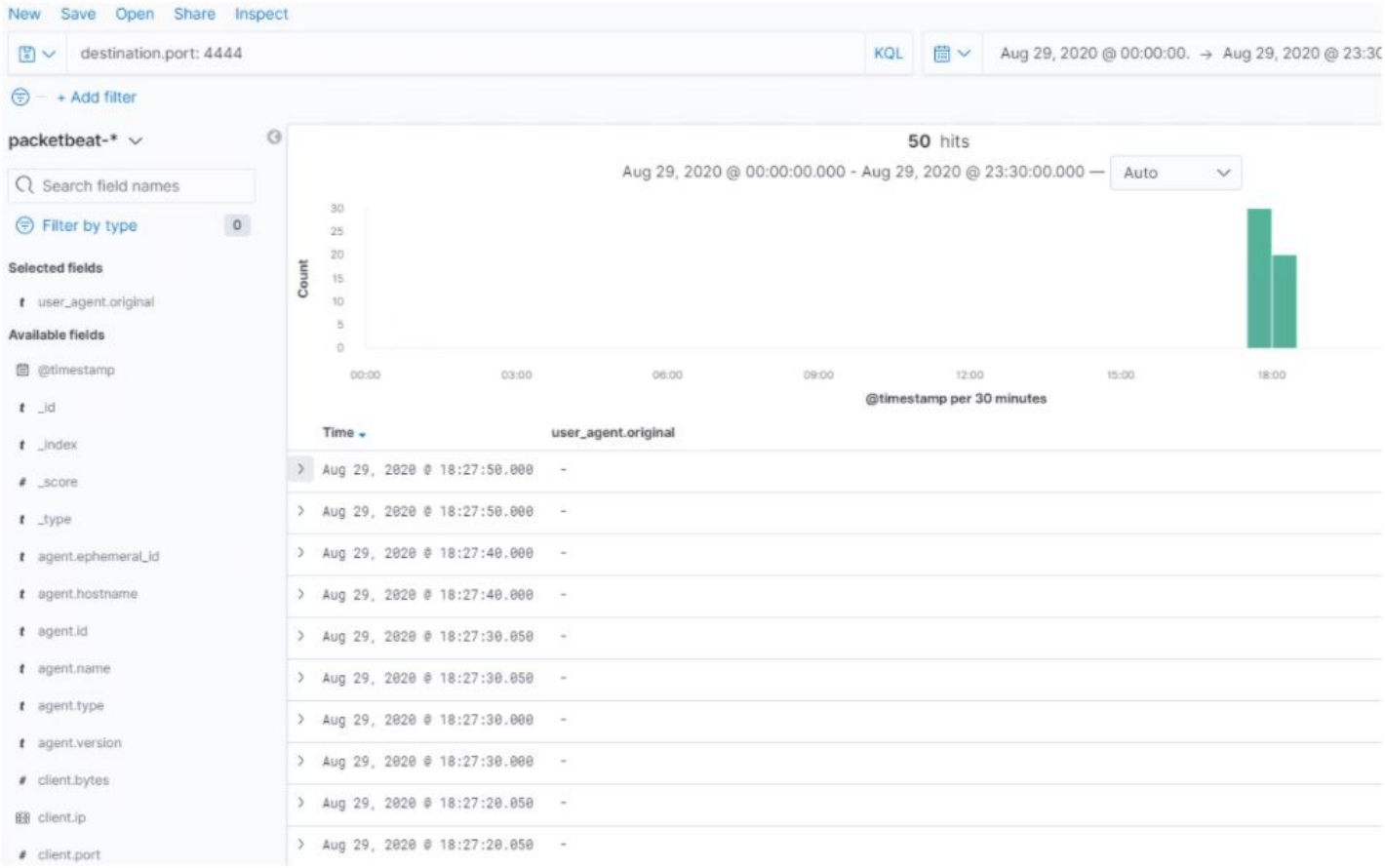
- Blocking User-agent names that match password cracking software, like Hydra, John the Ripper, etc.

Find the WebDav connection.

- Use your dashboard to answer the following questions:
  - How many requests were made to this directory?
    - 38
  - Which file(s) were requested?
    - shell.php
  - What kind of alarm would you set to detect such access in the future?
    - An alert when there has been an attempt to upload or download a file where the size exceeds the defined threshold and outside of the defined accepted file types.
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    - Updating WebDav and the apache server would be very helpful, as well as maintain up-to-date list of authorized users, and limit the size and type of files being uploaded and downloaded.

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?
    - Yes
    -



  - What kinds of alarms would you set to detect this behavior in the future?
    - Alert when .php files are uploaded to the server
    - Alert for traffic moving on port 4444
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

- Close port 4444
- Use of stronger passwords
- Two-factor authentication
- Unique login URLs
- Maintain updated and patched systems