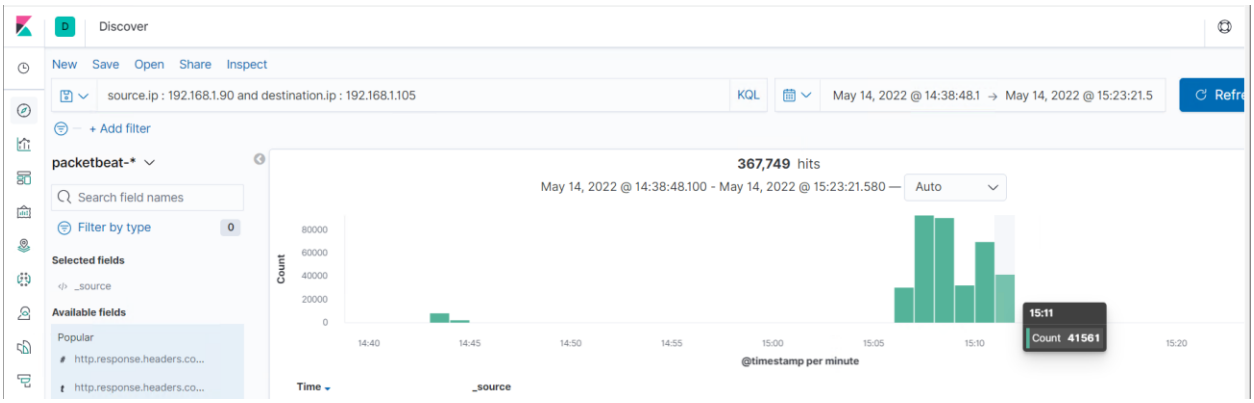
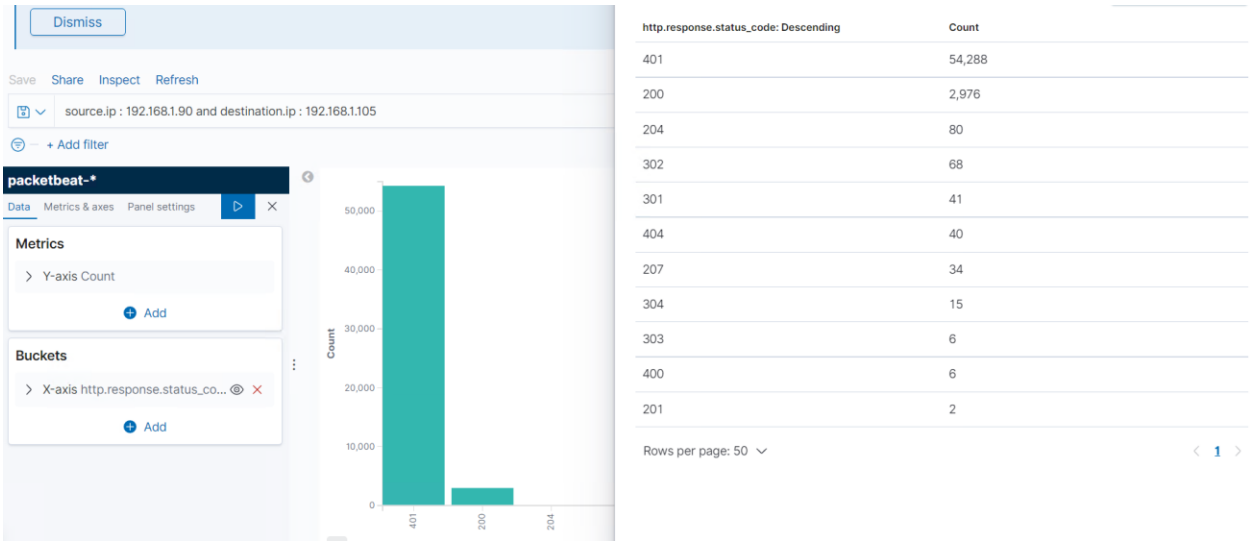
Day 2: Instructions

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?
            - May 14, 2022, between 15:06 and 15:12

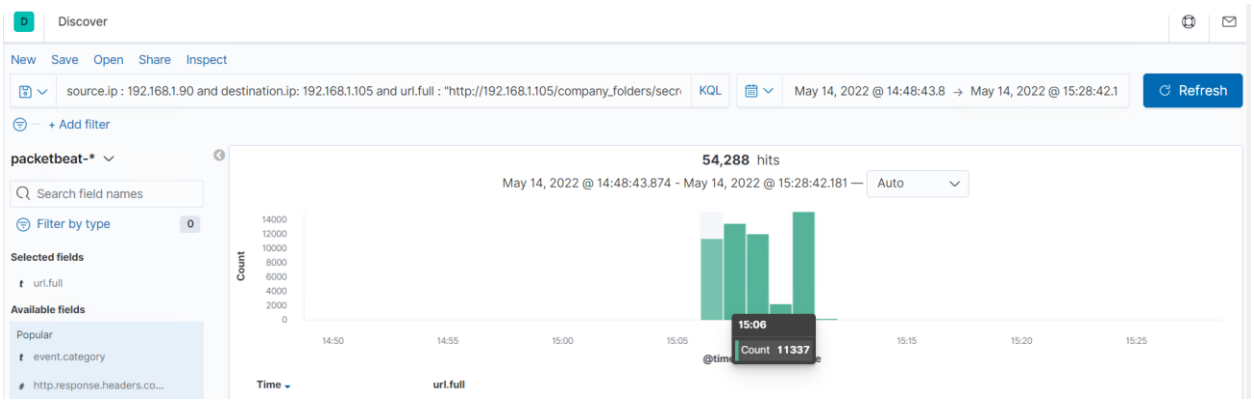


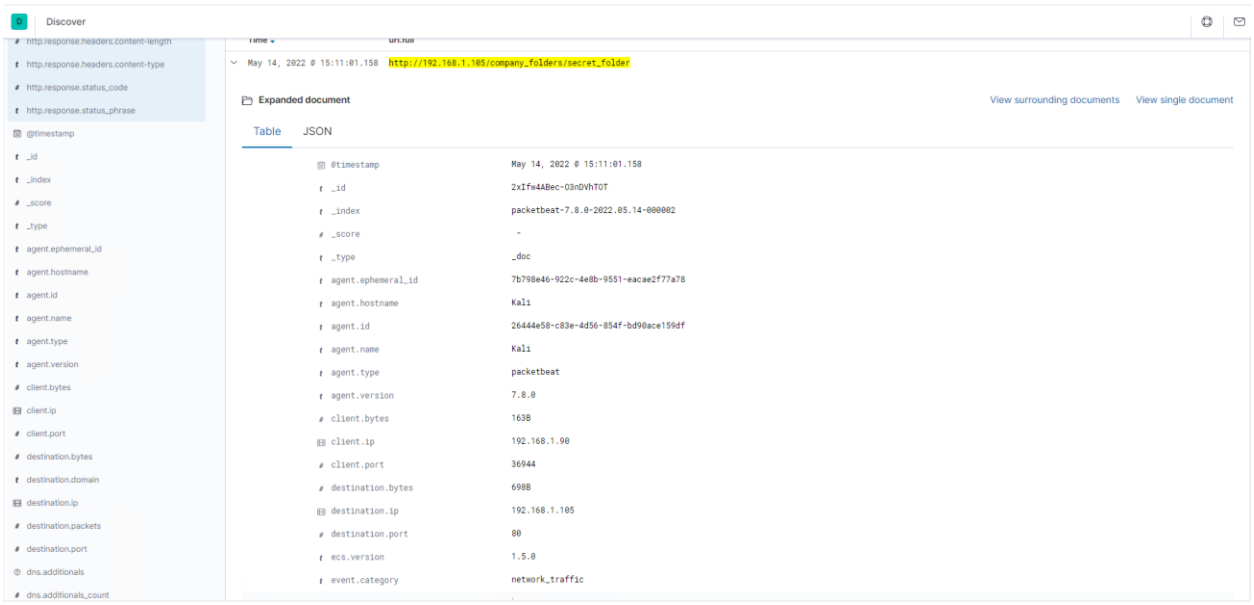
        - What responses did the victim send back?



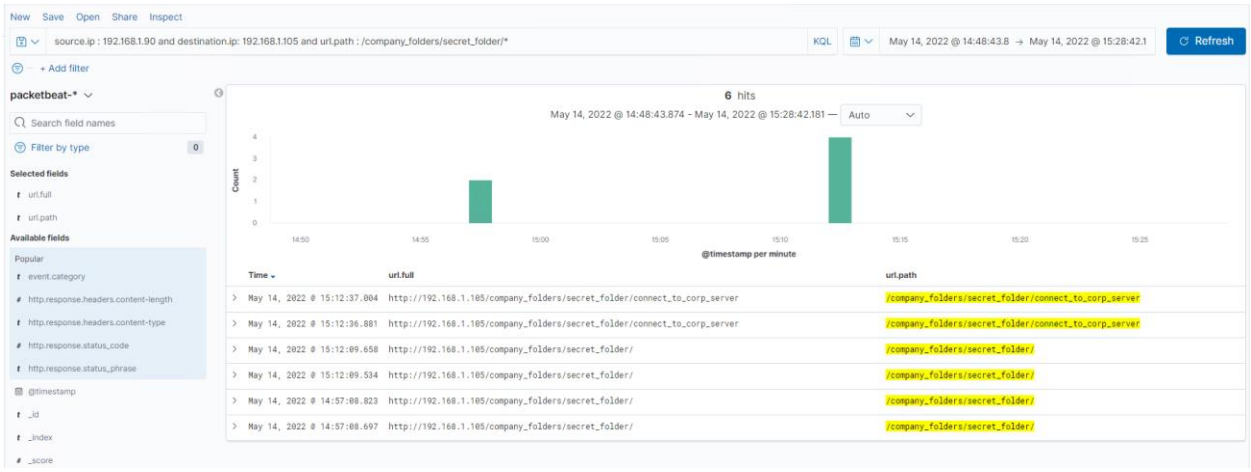
        - What data is concerning from the Blue Team perspective?
            - The increase in traffic from 192.168.1.90 to 192.168.1.105 and total count the 403 status code (unauthorised status)

2. Find the request for the hidden directory.





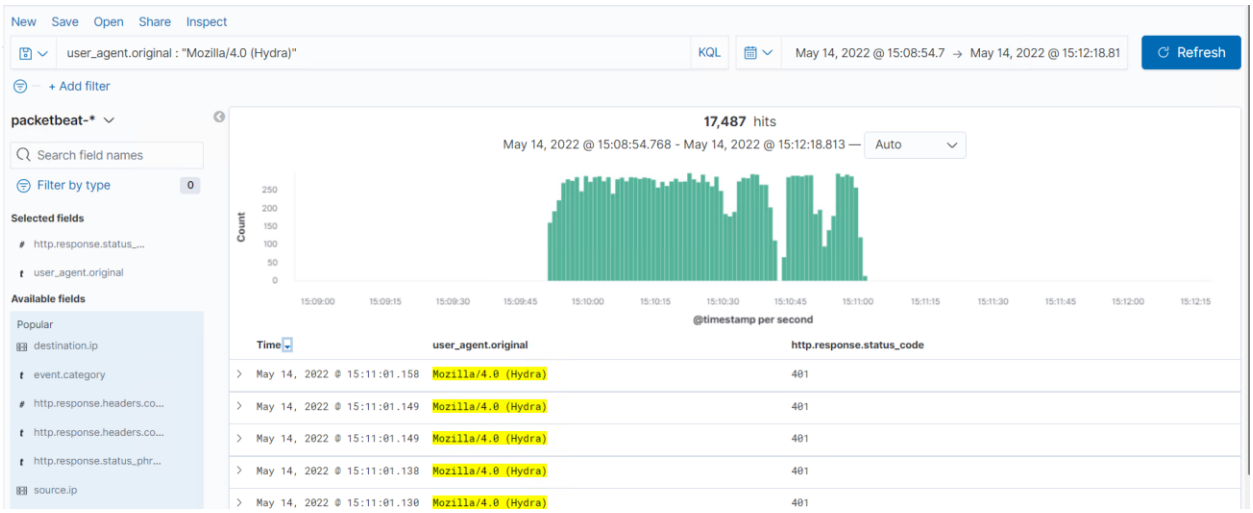
- In your attack, you found a secret folder. Let's look at that interaction between these two machines.
  - How many requests were made to this directory? At what time and from which IP address(es)?
    - The requests to the secret folder began at 15:06 and a total of 11337 requests were made
    - In total there were 54,288 requests made between 15:06 to 15:11
    - The request was made from 192.168.1.90 (attacking machine) to 192.168.1.105 (target machine)
  - Which files were requested? What information did they contain?



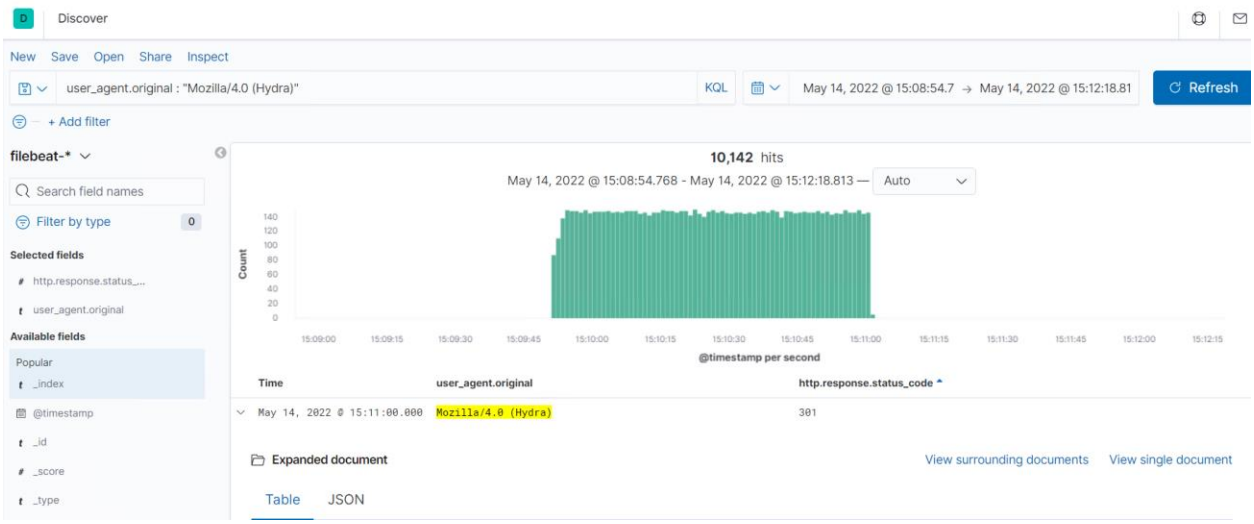
- /company_folders/secret_folder/connect_to_corp_server

- What kind of alarm would you set to detect this behavior in the future?
  - Notify when any ip addresses that are not whitelisted try to access the folder
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Remove the secret folder from the server and move it to a more secure server and change the names of the folder

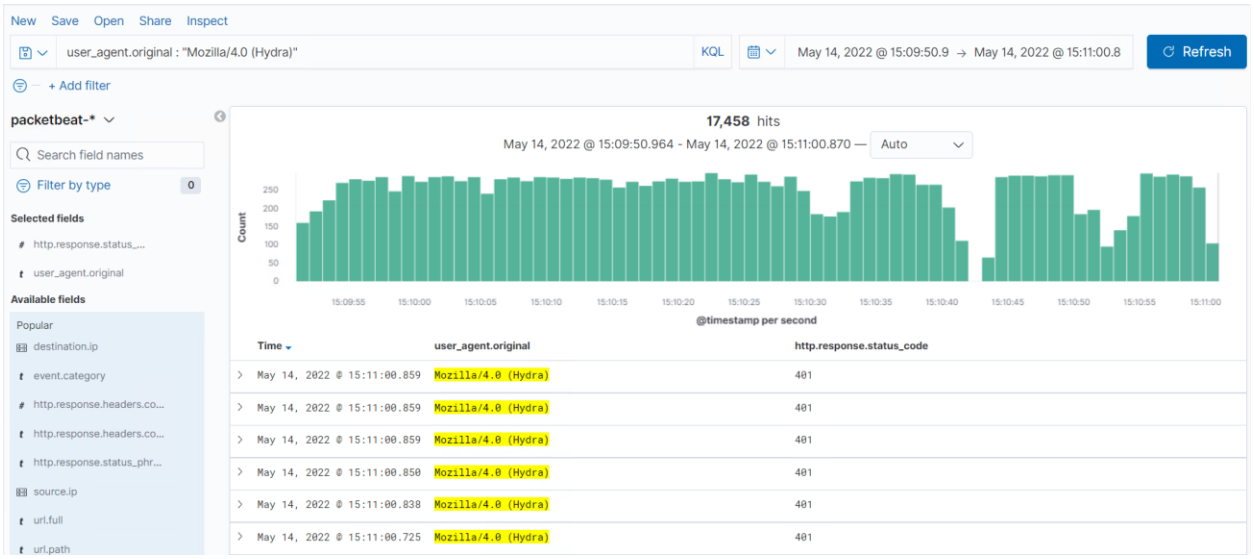
3. Identify the brute force attack.
   - After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
     - Can you identify packets specifically from Hydra?



- How many requests were made in the brute-force attack?
  - 17,487 requests made in the brute-force attack
- How many requests had the attacker made before discovering the correct password in this one?



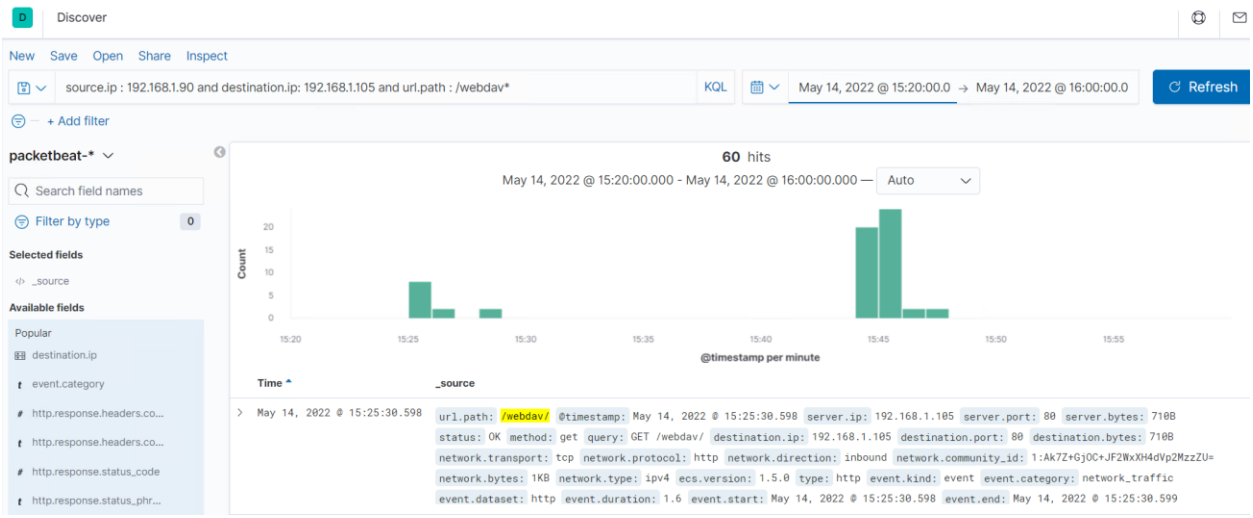
- 10,142 requests (Filebeat)



- Approximately 17, 458 (packetbeat)

- What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
  - An alarm would be triggered after 5 failed attempts within a 10 minute period
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Add two factor authentication and lock the account when the above certain threshold of failed attempts has been reached

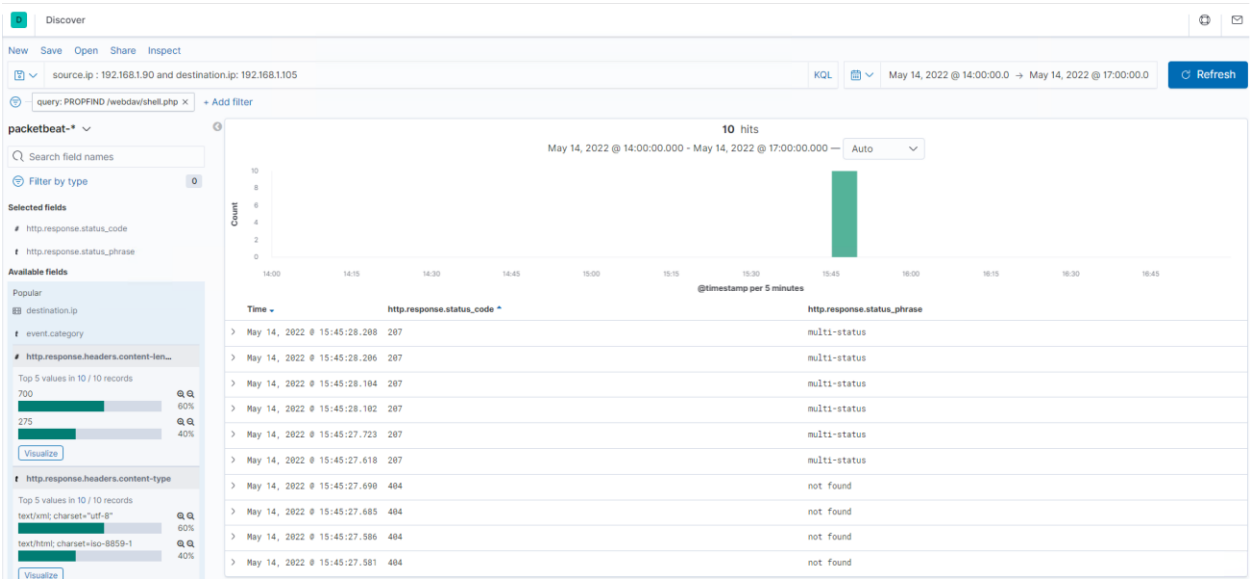
4. Find the WebDav connection.
   - Use your dashboard to answer the following questions:
     - How many requests were made to this directory?



- 60 requests were made

- Which file(s) were requested?
  - passwd.dav
  - shell.php
- What kind of alarm would you set to detect such access in the future?
  - Trigger when an unauthorized ip address attempts to access the server
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Whitelist all of authorized IP address and block any unauthorized IP address trying to access the server

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?



- What kinds of alarms would you set to detect this behavior in the future?
  - Trigger when a status code of 207 received
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - Have a list of IP addresses that are white-listed and make ports 22 and 80 unavailable to the other IP addresses