1. Identify the offensive traffic.

    - Identify the traffic between your machine and the web machine:
        - When did the interaction occur? **First contact at 23:06 on 10/26**

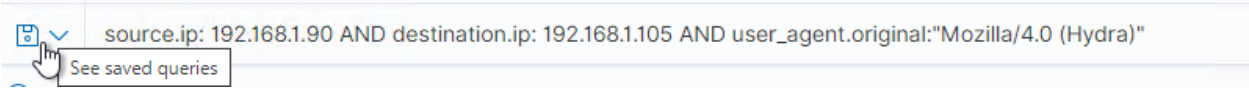
        - What responses did the victim send back? **200**
        - What data is concerning from the Blue Team perspective? **A random IP was able to find and gain access to the server IP**
2. Find the request for the hidden directory.

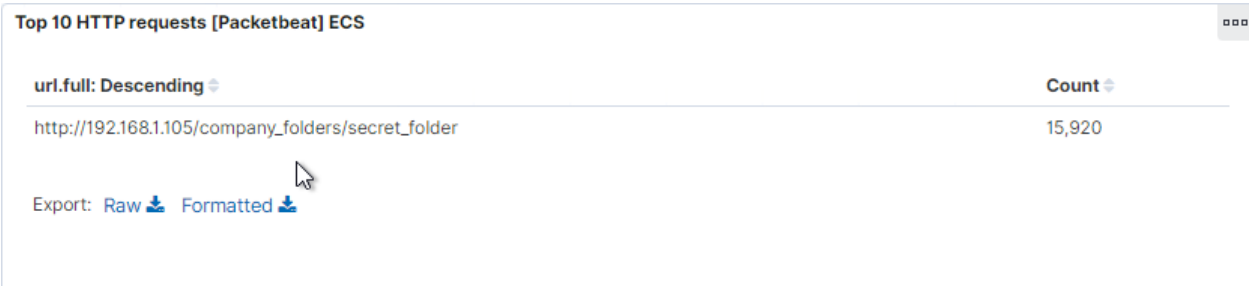
    - In your attack, you found a secret folder. Let's look at that interaction between these two machines.
        - How many requests were made to this directory? At what time and from which IP address(es)? **15928 requests starting at 23:16 on 10/26 from 192.168.1.90**

        - Which files were requested? What information did they contain?
        - What kind of alarm would you set to detect this behavior in the future? **I would set up an alarm that would trigger after a large amount of attempts at the server**
        - Identify at least one way to harden the vulnerable machine that would mitigate this attack. **I would set the page to lock out after 3 failed attempts.**
3. Identify the brute force attack.

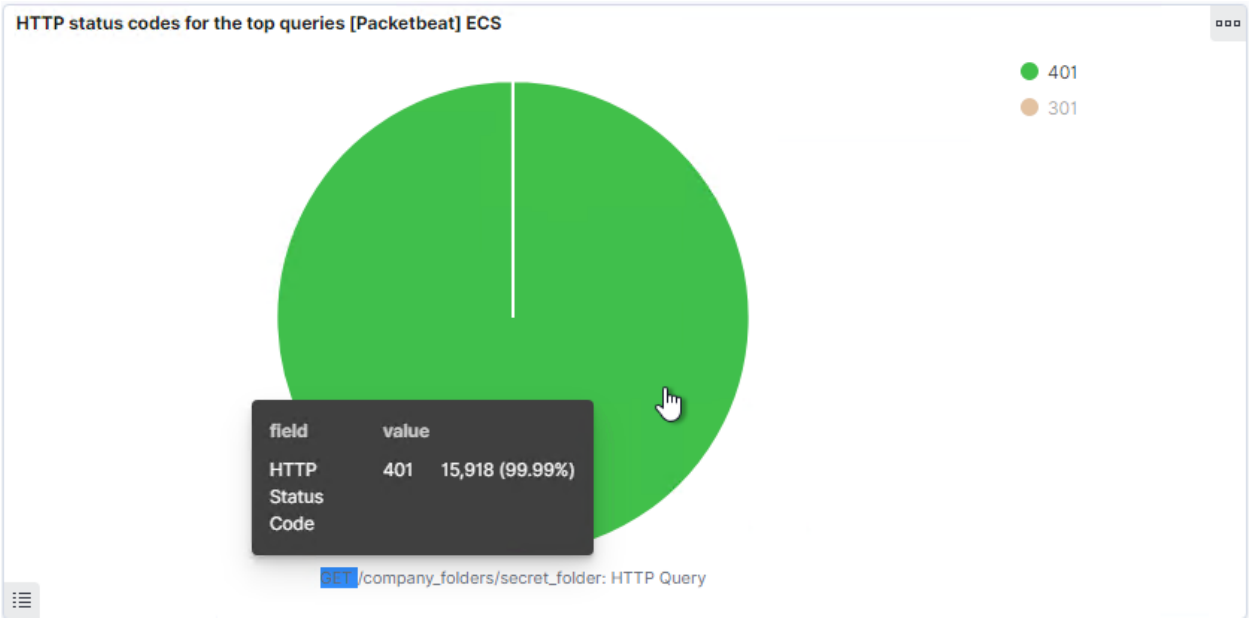
    - After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:

- Can you identify packets specifically from Hydra?





- How many requests were made in the brute-force attack? **15920**
- How many requests had the attacker made before discovering the correct password in this one? **15918**



- What kind of alarm would you set to detect this behavior in the future and at what threshold(s)? **I would set an alarm to trigger at if there are more than three 401 status in a five minute time frame**
- Identify at least one way to harden the vulnerable machine that would mitigate this attack. **I would lock out after five attempts for 15 minutes**

4. Find the WebDav connection.

    - Use your dashboard to answer the following questions:
        - How many requests were made to this directory? **168**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,928
http://192.168.1.105/webdav	168
http://192.168.1.105/webdav/windowsupdate.php	82
http://192.168.1.105/	50
http://192.168.1.105/webdav/redteam.exe	26

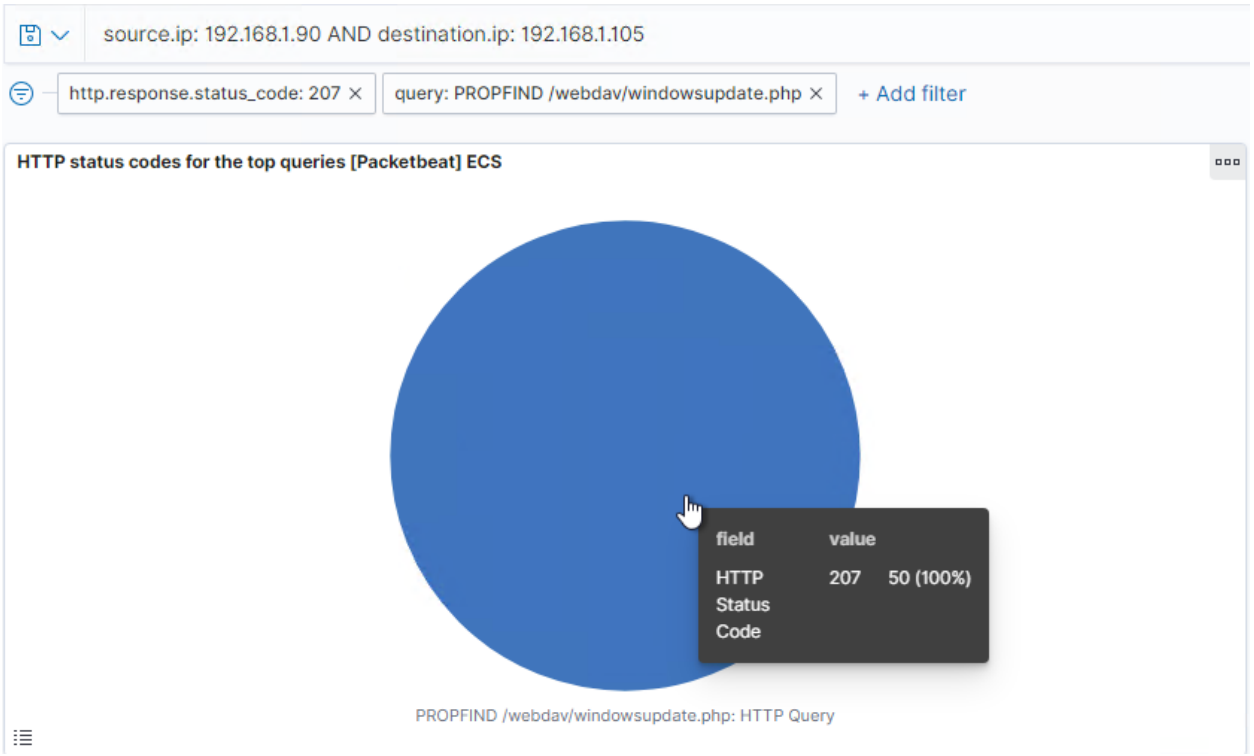
- Which file(s) were requested? **Windowsupdate.php, passwd.dav redteam.exe**

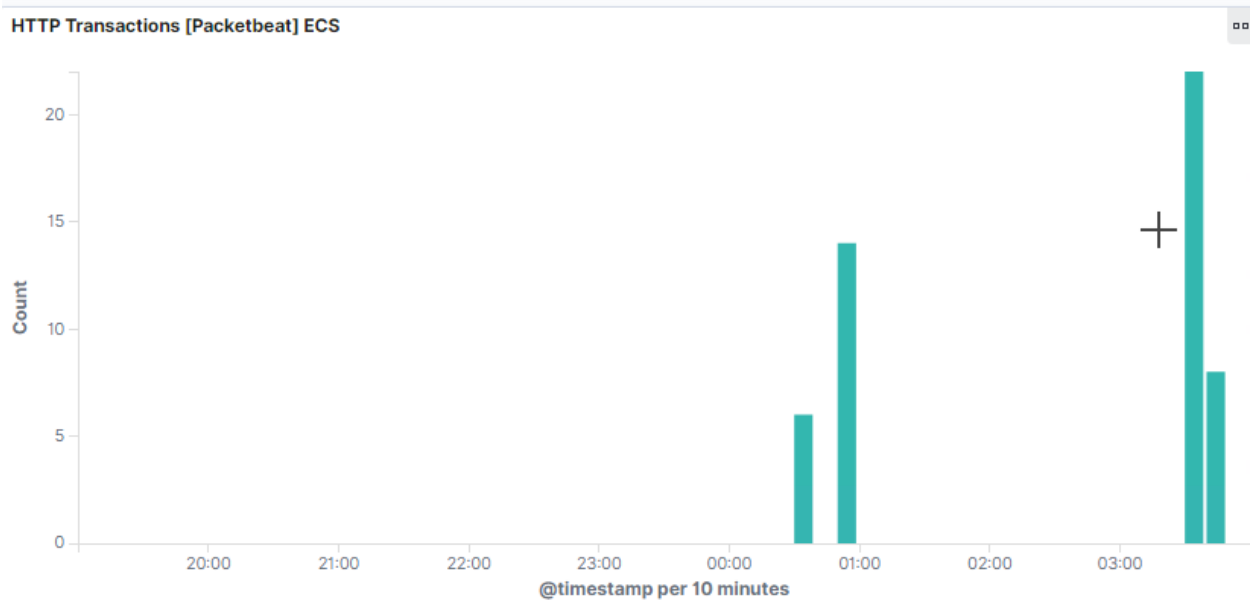
url.full: Descending	Count
http://192.168.1.105/webdav	150
http://192.168.1.105/webdav/windowsupdate.php	50
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/redteam.exe	14

- What kind of alarm would you set to detect such access in the future? **I would make a list of approved IPs (internal and external) and set an alarm whenever an IP not on this list accessed WebDAV**
- Identify at least one way to harden the vulnerable machine that would mitigate this attack. **Even with the whitelist, I would require MFA for WebDAV users.**

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? **Set an alert for HTTP 207 status codes from WebDAV**
- Identify at least one way to harden the vulnerable machine that would mitigate this attack. **Make a whitelist of IPs that are able to upload to WebDAV**