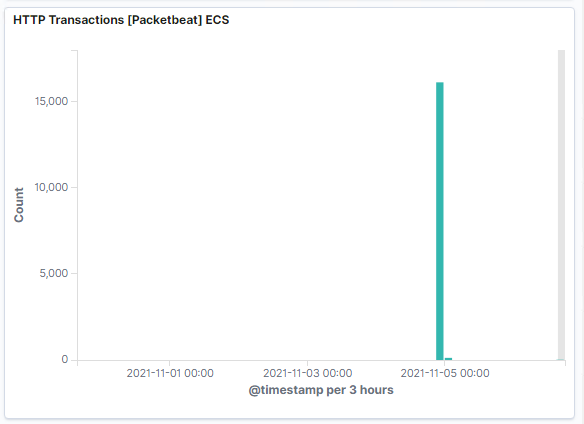
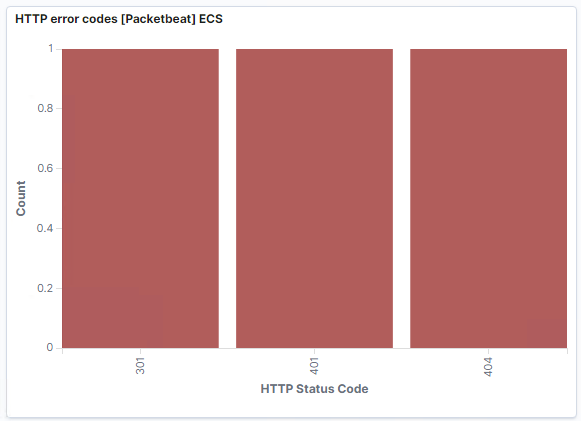
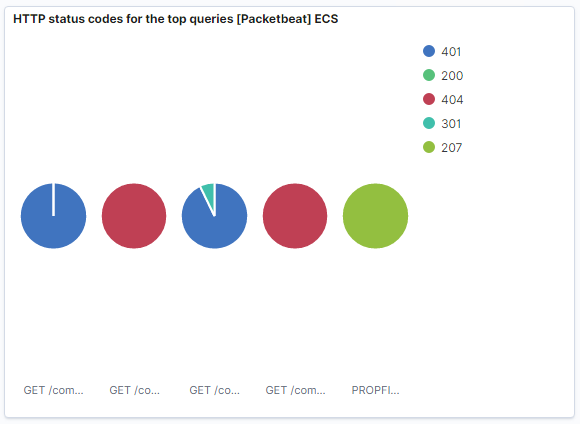
The remaining steps will be a process of self-discovery to be completed without screen shot examples.

Get familiar with running search queries in the Discover screen with Packetbeat. This will be located on your fourth tab in Chrome.

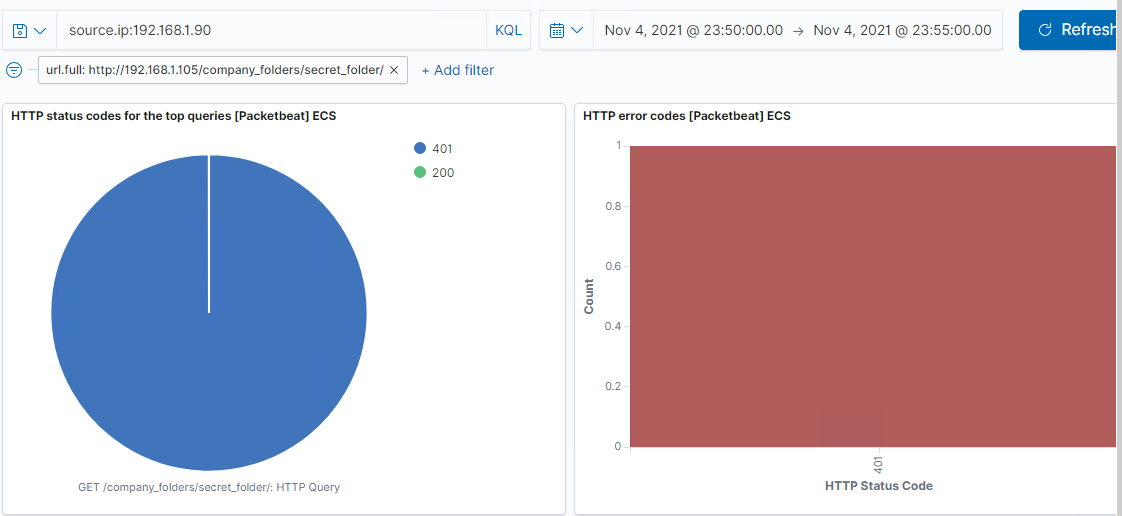
* On the Discover page, locate the search field.
* Start typing source and notice the suggestions that come up.
* Search for the source.ip of your attacking machine.
* Use AND and NOT to further filter you search and look for communications between your attacking machine and the victim machine.
* Other things to look for:
  + url
  + status\_code
  + error\_code

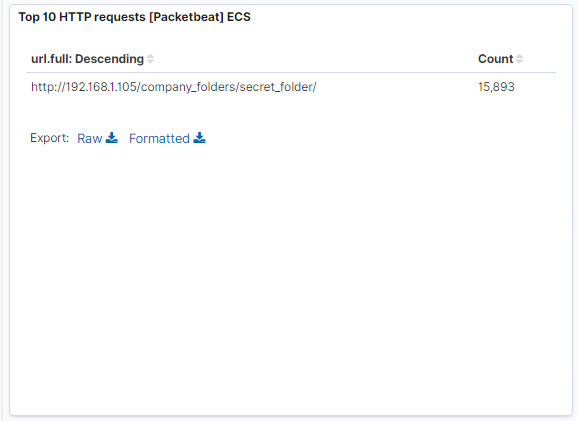
After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.  
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur?  
       2021-11-04 - 21:00  
       
     + What responses did the victim send back?  
       200, 207, 301, 401 and 404  
       

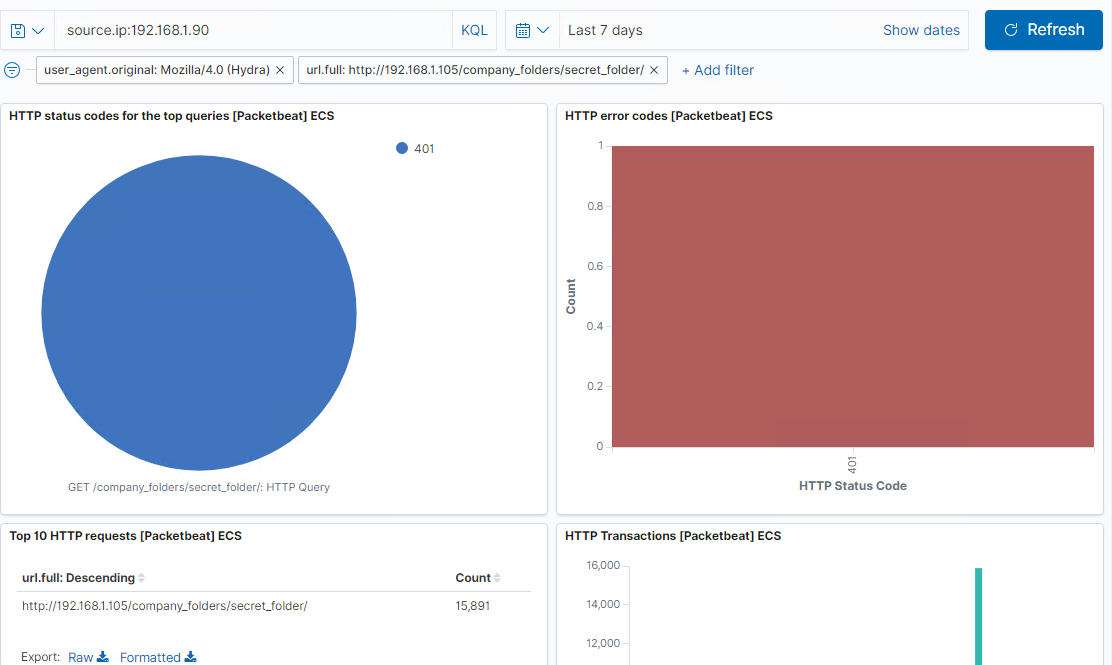
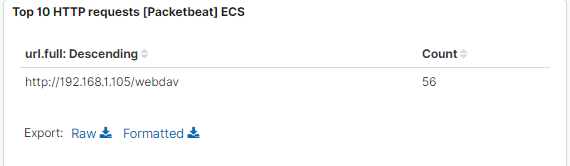
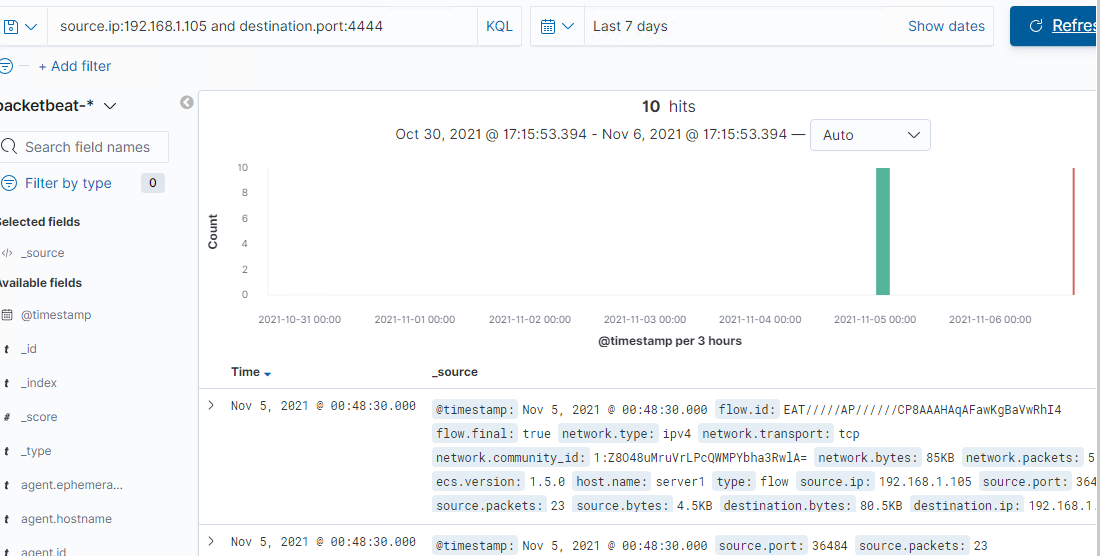


* + - What data is concerning from the Blue Team perspective?  
      The large amount of 404s.

1. 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)?  
       15,893 from 192.168.1.90 at 21:00  
       



* + - Which files were requested? What information did they contain?  
      text/html
    - What kind of alarm would you set to detect this behavior in the future?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

1. 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, with user\_agent.orginal = “Mozilla/4.0 (Hydra)”  
       
     + How many requests were made in the brute-force attack?  
       15891 requests
     + How many requests had the attacker made before discovering the correct password in this one?  
       15891 requests
     + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?  
       I would setup an alert to notify me when x number of 401s occur.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Set a maximum number of failed login attempts before the account is locked.
       2. Monitor for any traffic from Hydra user agent.
2. Find the WebDav connection.  
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?  
       56  
       
     + Which file(s) were requested?
     + What kind of alarm would you set to detect such access in the future?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Disable WebDav and use another secure file transfer option
       2. Use HTTPS
3. 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?
       1. Look for outbound traffic on port 4444
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Block known exploits