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?
       1. 11/09/2021 16:00-19:00 PM
     + What responses did the victim send back?
       1. HTTP Status Code 401: 15,981
       2. HTTP Status Code 301: 2
       3. HTTP Status Code 200: 952
       4. HTTP Status Code 207: 12
       5. HTTP Status Code 404: 6
     + What data is concerning from the Blue Team perspective?
       1. 15,987 HTTP requests to <http://192.168.1.105/company_folders/secrets_folder>
       2. 2 successful attempts (Code 301)
       3. The data above is concerning because it shows repeated unsuccessful transaction attempts, and a spike in unique flow traffic, indicating a possible Brute Force attack.
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)?
       1. 15,987 HTTP requests to <http://192.168.1.105/company_folders/secrets_folder>
       2. 11/09/2021 16:00-19:00 PM
       3. Source IP: 192.168.1.1
     + Which files were requested? What information did they contain?
       1. The file within the secrets-folder is connect\_to\_corp\_server. This file has ryan’s hashed password as well as other information.
     + What kind of alarm would you set to detect this behavior in the future?
       1. Set an alarm if the folder is accessed
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. This directory and file should be removed from the server all together.
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?
       1. User\_agent.original = Mozilla/4.0 (Hydra)
     + How many requests were made in the brute-force attack?
       1. 15,987 HTTP requests
     + How many requests had the attacker made before discovering the correct password in this one?
       1. 469
     + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
       1. Set an alarm based on the threshold for the number of HTTP requests
       2. Set an alert when the user\_agent.original includes Hydra
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. After the limit of 10 401 Unauthorized codes have been returned from a server, that server can automatically drop traffic from the offending IP address for a period of 1 hour. We could also display a lockout message and lock the page from login for a temporary period of time from that user.
4. Find the WebDav connection.  
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?
       1. 18
     + Which file(s) were requested?
       1. The file that was within 192.168.1.105/webdav/ is shell.php
     + What kind of alarm would you set to detect such access in the future?
       1. Set an alert anytime this directory is accessed by a machine other than the machine that should have access.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Connections to this shared folder should not be accessible from the web interface.
       2. Connections to this shared folder could be restricted by machine with a firewall rule.
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?
       1. source.ip: 192.168.1.105 and destination.port: 4444
     + What kinds of alarms would you set to detect this behavior in the future?
       1. We can set an alert for any traffic moving over port 4444.
       2. We can set an alert for any .php file that is uploaded to a server.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Removing the ability to upload files to this directory over the web interface would take care of this issue.