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?
       1. Graphical user interface

          Description automatically generated with medium confidence
       2. 7/17/2021 at 1500
     + What responses did the victim send back?
     + A picture containing chart

       Description automatically generated
     + What data is concerning from the Blue Team perspective?
       1. That a single host created a huge spike in activity on the 17th.
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)?
     + Graphical user interface, text, application, email

       Description automatically generated
     + Which files were requested? What information did they contain?
     + Graphical user interface, text, application, email

       Description automatically generated
     + What kind of alarm would you set to detect this behavior in the future?
       1. Any alarm that would notify me whenever the secret\_folder directory was accessed through a GET command when the attacker uses a Curl Command or HTTP request
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Don’t allow the HTTP port to be open. Hide this folder inside a firewall.
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. Yes, because the first thing to look for would be port 80 abuse.
     + How many requests were made in the brute-force attack?
       1. 406 from port 9200
     + How many requests had the attacker made before discovering the correct password in this one?
       1. 356
     + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
       1. Alarm for 80, 443, and 9200 and any read or writes
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Don’t advertise the secretfile. Keep everything important off the public link. Put everything in important behind a firewall.
4. Find the WebDav connection.
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?
       1. 14
     + Which file(s) were requested?
       1. passwd.dav
     + What kind of alarm would you set to detect such access in the future?
       1. An alarm for any PHP file upload
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Deny traffic from port 4444. Provide a firewall that protects the Webdav connection.
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. Yes, through the source.ip of 192.168.90 and source.port 4444
     + What kinds of alarms would you set to detect this behavior in the future?
       1. Set alerts for port 80 and port 4444
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       1. Put port 80 on a network that is away from more important data and the port was checked. Port 80 would have its own network. Then deny traffic from port 4444.