1. Identify the offensive traffic.
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur?
       - **It started at 23:51 server time.**
     + What responses did the victim send back?
       - **Mostly 200 responses with a few 400 responses included.**
     + What data is concerning from the Blue Team perspective?
       - **The user agent shows as NMAP, which would indicate someone is looking for an attack vector.**
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)?
       - **6,625 requests starting at 00:06 server time all 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?
       - **An alert when there is a spike in login attempts in a short time.**
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       - **Create a lockout after several incorrect login attempts.**
     + Identify the brute force attack.
       - **There is a large number of unsuccessful login attempts at essentially the same time with all showing Hydra as the user agent which indicates a brute force attack.**
   1. 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. The user agent specifies Hydra and they all happen at almost the exact same time.**
      * How many requests were made in the brute-force attack?
        + **6,625 requests starting at 00:06 server time all from 192.168.1.90**
      * How many requests had the attacker made before discovering the correct password in this one?
        + **6,622**
      * What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
        + **Send an alert to the security team after 5 consecutive unsuccessful attempts.**
      * Identify at least one way to harden the vulnerable machine that would mitigate this attack.
        + **Create a lockout and require password reset.**
3. Find the WebDav connection.
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?
       - **116**
     + Which file(s) were requested?
       - **passwd.dav**
     + What kind of alarm would you set to detect such access in the future?
       - **Alert any time anything is uploaded to server.**
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       - **Do not store passwords on the machine. Do not allow files to be uploaded remotely.**
4. 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?
       - **I did not use metasploit for this attack, so there was no meterpreter traffic. There was netcat traffic though.**
     + What kinds of alarms would you set to detect this behavior in the future?
       - **Alert any time there is any traffic that is not HTTP or HTTPS**
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
       - **Restrict outbound traffic from any ports except 80 or 443**