1. Identify the offensive traffic.  
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur? - 2-10-2021 at 06:00
     + What responses did the victim send back?- 201,204,400,401,404,200
     + What data is concerning from the Blue Team perspective? - there was access to a secret folder from an unknown IP address and the success of put from that ip address
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)? - 32,764, 2-10-2021 at 0900, 192.168.1.90
     + Which files were requested? What information did they contain? - connect\_to\_corp\_server was requested contained information on how to connect to the webdav server
     + What kind of alarm would you set to detect this behavior in the future? - an alarm to set would be any unknown IP address asking access or a threshold of attempts made on that file.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack. - one way to mitigate the attack to close ssh and create a jumpbox that only has access to this folder. The folder was meant for ashtons eyes only so ashton should be the only one with access.
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? yes
     + How many requests were made in the brute-force attack? - 32,754
     + How many requests had the attacker made before discovering the correct password in this one? - 32,750
     + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?- a threshold of attempts being made in a certain time frame would be made
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack. - again a jumpbox would be a good idea or a white list to only allow known ip addresses. Or after a certain amount of attempts made lock out the ip.
4. Find the WebDav connection.  
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory? - 24
     + Which file(s) were requested? - /webdav was requested and pst to /webdav was requested, and a put for shell.php
     + What kind of alarm would you set to detect such access in the future? - an alarm that an unknown ip address requested /webdav.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack. - again a hardened system would be to have a jumpbox with the only access to this folder, making a white/black list, and also to keep webdav updated
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? yes
     + What kinds of alarms would you set to detect this behavior in the future? - an alert should come up with a “Put” request and if the file is a php
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack. - again block unwanted access to the secret\_folder and the webdav server