1. Identify the offensive traffic.

    - Identify the traffic between your machine and the web machine:
        - When did the interaction occur?

          April 22nd at 2am

        - What responses did the victim send back?

          401- Invalid credentials indicating a brute force attack

        - What data is concerning from the Blue Team perspective?

          Unauthorized access through a brute force attack. Indicated by the 401 response code.

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)?

          16,516 requests from IP address 192.168.1.105

        - Which files were requested? What information did they contain?

          The Secret folder

        - What kind of alarm would you set to detect this behavior in the future?

          An alarm to trigger after a certain amount of 401 response codes, preventing a brute force in the future.

        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

          Setting a limit on how many failed login attempts are allowed before locking the account.

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?

          16,516 requests

        - How many requests had the attacker made before discovering the correct password in this one?

          16,508 requests

        - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?

          An Alarm for 401 error codes with a threshold in increments of 6,000 requests at a time.

        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

          Limit password attempts to 5 attempts and 2-factor authentication.

4. Find the WebDav connection.

    - Use your dashboard to answer the following questions:
        - How many requests were made to this directory?

          106 requests

        - Which file(s) were requested?

          The shell.php, password.dav files

        - What kind of alarm would you set to detect such access in the future?

          Alarm indicating when the same file is repeatedly opened

        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

          White-listing server IP Addresses

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, through the Errors vs. Successful Transactions table

        - What kinds of alarms would you set to detect this behavior in the future?

          Alarm for detecting a .php file being uploaded/accessed

        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

          White-list specific machines with granted access to the server