Identify the offensive traffic.

1. Identify the traffic between your machine and the web machine:
    a. When did the interaction occur?
        i. **May 3, 2022, 12:05 AM**
    b. What responses did the victim send back?
        i. **401, 301, 207, 404, 200**
    c. What data is concerning from the Blue Team perspective?
        i. **Nmap/port scanning attempts. Connection attempts and successes.**

2. Find the request for the hidden directory.
    a. In your attack, you found a secret folder. Let's look at that interaction between these two machines.
    b. How many requests were made to this directory? At what time and from which IP address(es)?
        i. **17,102**
    c. Which files were requested? What information did they contain?
        i. **Password.dav. Contained Ryan username and hash which was his password.**
    d. What kind of alarm would you set to detect this behavior in the future?
        i. **Any requests for hidden directories from outside the company's network. Another alarm can be made for multiple, consecutive requests from a single IP address not on the network.**
    e. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
        i. **Username and password requirements especially for those that can access the hidden directories. There can also be encryption of the hidden directories to further harden the system.**

3. Identify the brute force attack.
    a. After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
        i. Can you identify packets specifically from Hydra?
            1. **Yes. Filter user_agent.oringal: "Mozilla/4.0 (Hydra)"**
        ii. How many requests were made in the brute-force attack?
            1. **17,098**
        iii. How many requests had the attacker made before discovering the correct password in this one?
            1. **17084, only 2 successful**
        iv. What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
            1. **Alarm for unauthorized attempts. Set max number. Especially for HTTP 401 unauthorized responses.**

b. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    i. **Username and password requirements, especially adding strength requirements for them. They should not be simple and easily guessed or cracked. Set a max number of attempts.**

4. Find the WebDav connection.
    a. Use your dashboard to answer the following questions:
        i. How many requests were made to this directory?
            1. **86**
        ii. Which file(s) were requested?
            1. **passwd.dav**
        iii. What kind of alarm would you set to detect such access in the future?
            1. **Alarm set for any requests or access to the WebDav directory from outside the local, internal network.**
    b. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
        i. **Configure the directory to accept uploads from only certain IP addresses that are predefined within the internal network.**

5. Identify the reverse shell and meterpreter traffic.
    a. To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
        i. Can you identify traffic from the meterpreter session?
            1. **Source.ip: 192.168.1.105 and destination.port: 4444. url.path:"/webdav/shell.php"**
        ii. What kinds of alarms would you set to detect this behavior in the future?
            1. **Alert for invalid file types and open ports. Alert for port 4444.**
    b. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
        i. **Disallow uploads to the network from outside IP addresses. Have controls for users for their privileges and access rights. Block executable files like .php.**