Domain: Offensive Security

Question 1: Planning an Engagement

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

1. Restate the Problem - We are trying to gain access to

2. Provide a Concrete Example Scenario

    - In Project 2, which VMs were on the network?
        i. Kali, Capstone, ELK
    - What was the purpose of each? ELK holds the Kibana dashboards; Kali is used for penetration testing, Capstone is used for forwarding logs to the ELK machine

    - Which of these VMs did you have to infiltrate? Capstone

    - What was your goal in infiltrating each VM? Pentesting

    - Which tools did you use to perform the infiltration?
        i. Firefox
        ii. Hydra
        iii. Nmap
        iv. John the Ripper
        v. Metasploit
        vi. Curl
        vii. MSVenom

    - What kinds of security measures, if any, were enabled on the network?

3. Explain the Solution Requirements

    - How did you identify your targets? Port scanning

    - How did you identify vulnerabilities in each target and which did you exploit? Port scanning

    - What did you do after infiltrating? Elevated to root in order to have full permissions

4. Explain the Solution Details

    - Which tools and commands did you use to identify your targets and their vulnerabilities?

        i. Hydra - hydra -l ahston -P /root/Downloads/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder
        ii. Ifconfig
        iii. Nmap 192.168.1.105
    - Which exploits did you use against these vulnerabilities and how did you deliver them? Hashing, manual brute force,
    - How did you achieve your goal after infiltration? By capture the flag. Found files that we should not have access too and retrieved the contents of said file

5. Identify Advantages and Disadvantages of the Solution

    - Were your methods covert or detectable by monitoring solutions? Detectable

    - How could you achieve your goal with greater stealth?