1. **Perform extensive scan of the target network and identify the FQDN of the Domain Controller.**
2. **While investigating an attack, you found that a Windows web development environment was exploited to gain access to the system. Perform extensive scanning and service enumeration of the target networks and identify the IP address of the server running WampServer**

3. **Identify a machine with SMB service enabled in the 192.168.0.0/24 subnet. Crack the SMB credentials for user Henry and obtain Sniff.txt file containing an encoded secret. Decrypt the encoded secret and enter the decrypted text as the answer. Note: Use Henry's password to decode the text.**

4. **An insider attack has been identified in one of the employees mobile device in 192.168.0.0/24 subnet. You are assigned to covertly access the users device and obtain malicious elf files stored in a folder "Scan". Perform deep scan on the elf files and obtain the last 4 digits of SHA 384 hash of the file with highest entropy value.**

5. **Perform a vulnerability scan for the host with IP address 172.20.0.16 What is the severity score of a vulnerability the indicates the End of Life of a web development language platform?**

6. **Exploit a remote login and command-line execution application on a Linux target in the 192.168.0.0/24 subnet to access a sensitive file, NetworkPass.txt Enter the content in the file as answer.**

7. **A forensic investigator has confiscated a computer from a suspect in a data leakage case. He found an image file, MyTrip.jpg. stored in the Documents folder of the "EH Workstation – 2" machine. He suspects that some confidential data is hidden in the image file. Analyse the**

8. Exploit weak credentials used for FTP service on a Windows machine in the 192.168.0.0/24 subnet. Obtain the file, Credentials.txt, hosted on the FTP root, and Enter its content as the answer.

9. You used shoulder surfing to identify the usernames and password of a user on the Ubuntu machine in the 192.168.0.0/24 network, that is, smith and L1nux123. Access the Machine, Perform vertical privilege escalation to that of a root user, and enter the content of the imroot.txt file as the answer.

10. During as assignment, an incident responder has retained a suspicious executable file "die-another-da" Your task as a malware analyst is to find the executable's Entry point (Address). The file is in the C:\Users\Admin\Documents directory in the "EH Workstation – 2" machines.

11. You are investigating a massive DDoS attack launched against a target at 10.10.1.10. Identify the attacking IP address that sent most packets to the victim machine. The network capture file "attack-traffic.pcapng" is saved in the Documents folder of the "EH Workstation – 1" (ParrotSecurity) machine.

12. Perform the SQL injection attack on your target web application cinema.cehorg.com and extract the password of a user Sarah. You have already registered on the website with credentials Karen/computer.

ile and extract the sensitive data hidden www.cehorg.com and enter the web
e data, an eight-character alpha-numeri 84. value a
agination" if you are stuck. application available at image
n the file. Enter the 13. Exploit t the page with page_id=sensiti
string, as the answer. the flag's Use "I

16. A file named Hast.txt has been uploaded through DVWA (http://172.20.0.16:8080/DVWA). The file is located in the "C:\wamp64\www\DVWA\hackable\uploads\" directory. Access the file and crack the MD5 hash to reveal the original message. Enter the decrypted message as the answer. You can log into the DVWA using the credentials admin/passwd.

17. Analyse the traffic capture from an IoT network located in the Documents folder of the "EH Workstation – 1" (ParrotSecurity) machine, identify the packet with IoT Publish Message, and enter the message length as the answer.

18. Your organization suspects the presence of a rogue AP in the vicinity. You are tasked with cracking the wireless encryption, connecting to the network and setting up a honeypot. The airdump-ng tool has been used, and the Wi-Fi traffic capture named "WirelessCapture.cap" is located in the Documents folder in the "EH Workstation – 1" (ParrotSecurity) machine. Crack the wireless encryption and identify the Wi-Fi password.

19. A disgruntled ex-employee has hidden a server access code in a Windows machine in the 192.168.0.0/24 subnet. You can not physically access the target machine. but you know that the organization administration purpose. Your task is to retrieve the "sa_code.txt" file from the target machine and enter the string in the file as the answer.

15. Perform SQL injection attack on a web application lag cybersec.cehorg.com, available at 172.20.0.22. Find the value in the F column in one of the DB tables and enter it as the answer.

14. Perform vulnerability research and exploit the web application training.cehorg.com, available at 192.168.0.64. Locate the Flag.txt file and enter its content as the answer.

20. A disgruntled employee of your target organization has stolen the company's trade secrets and encrypted them using VeraCrypt. The VeraCrypt volume file "Secret" is stored on the C: drive of the "EH Workstation – 2" machine. The password to access the volume has been hashed and saved in the file Key2Secret.txt located in the Documents folder in the "EH Workstation – 1" (ParrotSecurity) machine. As an ethical hacker working with the company. you need to decrypt the hash in the with the company. you need to decrypt the hash in the Key2Secret.txt file, access the VeraCrypt volume, and find the secret code in the file named Confindential.txt.