CEH Engage - Part II

Part 2 of CEH Engage covers System Hacking, Malware Threats, Sniffing, Social Engineering, and Denial-of-Service modules. In this part, you must exploit vulnerabilities identified in the last part and use various network/system/human exploitation techniques to gain access to the target's systems. You have to perform lateral and vertical privilege escalations and install malicious apps and utilities to maintain access and clear logs to avoid detection. You will need to create and use malicious applications against the target and will also be required to analyze any malware discovered on any of the targets. You need to note all the information discovered in this part of the CEH Engage and proceed to the subsequent phases of the ethical hacking cycle in the next part of the CEH Engage.

Note: Attempt this part after completing first 10 modules of the CEH program.

Flags

Challenge 1:

You are assigned to perform brute-force attack on a linux machine from 192.168.10.0/24 subnet and crack the FTP credentials of user nick. An exploitation information file is saved in the home directory of the FTP server. Determine the Vendor homepage of the FTP vulnerability specified in the file. (Format: aaaaa://aaa.aaaaaaaa.aaa/)

https://www.crushftp.com/ - Correct answer.

Challenge 2:

An intruder performed network sniffing on a machine from 192.168.10.0/24 subnet and obtained login credentials of the user for moviescope.com website using remote packet capture in wireshark. You are assigned to analyse the Mscredremote.pcapng file located in Downloads folder of EH Workstation-1 and determine the credentials obtained. (Format: aaaa/aaaaa)

kety/apple - Correct answer.

Challenge 3:

You are assigned to analyse a packet capture file ServerDoS.pcapng located in Downloads folder of EH Workstation-2 machine. Determine the UDP based application layer protocol which attacker employed to flood the machine in targeted network. Note: Check for target Destination port. (Format: Aaaaa Aaaaaaa Aaaaaaaa)

Quake Network Protocol - Correct answer.

Challenge 4:

A severe DDoS attack is occurred in an organization, degrading the performance of a ubuntu server machine in the SKILL.CEH network. You are assigned to analyse the DD_attack.pcapng file stored in Documents folder of EH workstation -2 and determine the IP address of the attacker trying to attack the target server through UDP. (Format: NNN.NNN.NN.NNN)

192.168.10.144 - Correct answer.

Challenge 5:

You are assigned to analyse PyD_attack.pcapng file stored in Downloads folder of EH Workstation -2 machine. Determine the attacker IP machine which is targeting the RPC service of the target machine. (Format: NNN.NN.NN.NN)

172.30.10.99 - Correct answer.

Challenge 6:

An incident handler identified severe DDoS attack on a network and provided report using Anti-DDoS Guardian tool. You are assigned to analyse the reports submitted by the IH team which are stored in "C:\Users\Admin\Documents\Anti-DDoS" directory of the EH Workstation-1 and determine the attacker IP which has transmitted more number of packets to the target machine. (Format: NNN.NNN.NN.NNN)

192.168.10.222 - Correct answer.

Challenge 7:

You are assigned to analyse the domain controller from the target subnet and perform AS-REP roasting attack on the user accounts and determine the password of the vulnerable user whose credentials are obtained. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: aNaaN*NNN)

c3ll0@123 - Correct answer.

Challenge 8:

A client machine under the target domain controller has a misconfigured SQL server vulnerability. Your task is to exploit this vulnerability, retrieve the MSS.txt file located in the Public Downloads folder on the client machine and determine its size in bytes as answer. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: N)

7 - Correct answer.

Challenge 9:

You are assigned to crack RDP credentials of user Maurice from the target subnet 192.168.10.0/24 and determine the password as answer. Note: use Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: Aaaaaaa@NNNN)

Pumpkin@1234 - Correct answer.

Challenge 10:

You are assigned to perform malware scanning on a malware file Tools.rar stored in Downloads folder of EH workstation-2 machine and determine the last four digits of the file's SHA-256 hash value. (Format: aNNN)

d282 - Correct answer.

Challenge 11:

You are assigned to monitor a suspicious process running in a machine whose log file Logfile.PML is saved in Pictures folder of the EH Workstation -2. Analyse the logfile and determine the Parent PID of the malicious file H3ll0.exe process from the log file. (Format: NNNN)

6952 - Correct answer.

Challenge 12:

You are assigned to analyse a ELF executable file Tornado.elf stored in Downloads folder of EH Workstation -2. Determine the Entropy value of the file as answer. (Format: N*NNNNN)

2.87903 - Correct answer.

Challenge 13:

You are assigned to scan the target subnets to identify the remote packet capture feature that is enabled to analyse the traffic on the target machine remotetly. Scan the target subnets and determine the IP address using rpcap service. (Format: NNN.NNN.NN.NNN)

192.168.10.144 - Correct answer.

Challenge 14:

An insider attack occurred in an organization and the confidential data regarding an upcoming event is sniffed and encrypted in a image file stealth.jpeg stored in Desktop of EH Workstation -2 machine. You are assigned to extract the hidden data inside the cover file using steghide tool and determine the tender quotation value. (Use azerty@123 for passphrase) (Format: NNNNNNN)

3965222 - Correct answer.

Challenge 15:

Perform vulnerability search using searchsploit tool and determine the path of AirDrop 2.0 vulnerability. (Format: aaaaaaa/aaa/NNNNN.a)

android/dos/46445.c - Correct answer.