CEH Engage - Part IV

Part 4 of CEH Engage covers Hacking Wireless Networks, Hacking Mobile Platforms, IoT and OT Hacking, Cloud Computing, and Cryptography modules. In this part, you must analyze wireless packet captures, use different attack vectors to exploit mobile devices, and audit IoT and OT systems/networks for known threats. You need to note all the information discovered in this part of the CEH Engage.

Note: Attempt this part after completing all 20 modules of the CEH program.

Flags

Challenge 1:

An employee's mobile device within CEHORG has been compromised, leading to an encrypted message BCtetx.txt being placed on the Android operating system. The password needed to decrypt the file is saved on EH-workstation-1. As an ethical hacker, your task is to decrypt the file using the password and input the extracted information. (note: the password file pawned.txt is stored in documents folder). (Format: *aaaaAN*NaN)

(ryptD3(0d3 – Correct Answer.

Challenge 2:

A compromised Android device is suspected of containing malicious applications. As an ethical hacker, you are tasked with identifying and extracting all installed APK files. Within these APKs, you must locate and extract a specific CRC value ends with "614c" . This CRC value is believed to be a crucial component of a larger security breach investigation. Determine the complete CRC value as answer. (Format: NNaaNNNa)

Challenge 3:

A ZIP archive encompassing redundant images of a physical signature has been compromised signature.zip and stored in Documents folder of EH Workstation-1 machine. Your role as an ethical hacker involves a forensic examination of the archive's contents to pinpoint the image file associated with an MD5 hash value ends with sequence "24CCB". Determine the original signature file name as answer. (Format: aN*aaa)

k4.png – Correct Answer.

Challenge 4:

As a cybersecurity analyst, you are investigating a potential phishing campaign targeting Ruby, an employee at a local tech company. You have access to Ruby's call log from the past few days, stored on an Android device within the target subnet 192.168.10.0/24. Identify the call in the log that is most likely a phishing attempt and provide the suspected phone number. (Format: +N (NNN) NNN-NNNN)

Challenge 5:

An employee's mobile device has reportedly been compromised and is suspected of being used to launch a Denial of Service (DoS) attack against one of the company's internal servers. Your assignment is to conduct a thorough analysis of the network capture file "And_Dos.pcapng" located in the Documents directory of EH workstation-2 machine and identify the severity level/potential impact of the attack performed. (perform deep down Expert Info analysis). (Format: Aaaaaaa)

Warning – Correct Answer.

Challenge 6:

CEHORG manages multiple IoT devices and sensors to oversee its supply chain fleet. You are tasked with examining the file "MQTT.pcapng," located in the Home directory of the EH Workstation - 2 machine. Analyze the packet containing the "High_humidity" message and determine the alert percentage specified in the message. (Format: NN)

50 – Correct Answer.

Challenge 7:

An attacker had sent a file cryt-128-06encr.hex containing ransom file password, which is located in documents folder of EH-workstation-2. You are assigned a task to decrypt the file using cryp tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters. (Format: Aaaaaaa/**aa**aA*a)

Twofish/@!ph@|tE*t – Correct Answer.

Challenge 8:

A VeraCrypt volume file "MyVeracrypt" is stored on the Document folder of the EH Workstation – 1 machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume folder. (Hint: Password: veratest). (Format: N)

4 – Correct Answer.

Challenge 9:

An ex-employee of CEHORG is suspected of performing an insider attack. You are assigned a task to retrieve the contacts dump from the employee's Android phone. Using PhoneSploit, find the country code of the contact named "Maddy." (Note: Use option 'N' in PhoneSploit for next page.). (Format: NN)

61 – Correct Answer.

Challenge 10:

CEHORG manages multiple IoT devices and sensors to oversee its supply chain fleet. You are tasked with examining the file "MQTT.pcapng," located in the Home directory of the EH Workstation - 2 machine. Analyze the packet containing the "High_temperature" message and determine the topic length . (Format: NN)

16 – Correct Answer.

Challenge 11:

An ex-employee of CEHORG is suspected to be performing insider attack. You are assigned a task to attain KEYCODE-5 used in the employees' mobile phone. Note: use option N in PhoneSploit for next page. (Format: Aaaaa*Aaaaaa)

Power Button – Correct Answer.

Challenge 12:

An employee in CEHORG has secretly acquired Confidential access ID through an application from the company. He has saved this information on the Music folder of his Android mobile phone. You have been assigned a task as an ethical hacker to access the file and delete it covertly. Enter the account information present in the file. Note: Only provide the numeric values in the answer field. (Format: NNNNNNNN)

80099889 – Correct Answer.

Challenge 13:

An attacker has hacked an employee's Android device at CEHORG and initiated a LOIC attack from the device. As an ethical hacker, you have obtained a screenshot of the attack using a background application. Retrieve the screenshot of the attack using PhoneSploit from the compromised mobile device and determine the number of HTTP packets sent per second. (Format: NN)

Challenge 14:

You have received a folder named "Archive" from a vendor. You suspect that someone might have tampered with the files during transmission. The Original hashes of the files have been sent by the sender separately and are stored in a file named FileHashes.txt stored in the Document folder in the "EH Workstation – 2" machine. Your task is to check the integrity of the files by comparing the MD5 hashes. Compare the hash values and determine the file name that has been tampered with. Note: Exclude the file extension in the answer field. The answer is case-sensitive. (Format: Aaaaaa)

Quotes – Correct Answer.

Challenge 15:

A VeraCrypt volume file "secret" is stored on the Document folder in the EH Workstation – 2 machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test). (Format: N)

6 – Correct Answer.