CEH Engage - Part III

Part 3 of CEH Engage covers Session Hijacking, Evading IDS, Firewalls, and Honeypots, Hacking Web Servers, Hacking Web Applications, and SQL Injection modules. In this part, you must take over active network and application sessions, compromise firewall, IDS, and other perimeter defense mechanisms, and exploit the organization's web applications. 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 15 modules of the CEH program.

Flags

Challenge 1:

An attacker tried to perform session hijacking on a machine from 172.30.10.0/24 subnet. An incident handler found a packet capture file $_Jack.pcapng obtained from the victim machine which is stored in Documents folder of EH Workstation -1. You are assigned to analyse the packet capture file and determine the IP of the victim machine targeted by the attacker. (Format: NNN.NN.NN.NNN)

172.30.10.200 - Correct answer.

Challenge 2:

An attacker tried to intercept a login session by intercepting the http traffic from the victim machine. The security analyst captured the traffic and stored it in Downloads folder of EH Workstation -1 as Intercep_$niffer.pcapng. Analyse the pcap file and determine the credentials captured by the attacker. (Format: aaa/aaaa)

Lee/test - Correct answer.

Challenge 3:

A honeypot has been set up on a machine within the 192.168.10.0/24 subnet to monitor and detect malicious network activity. Your task is to analyze the honeypot log file, cowrie.log, located in the Downloads folder of EH Workstation -2, and determine the attacker IP trying to access the target machine. (Format: NNN*NN*NN*NN)

172.30.10.99 - Correct answer.

Challenge 4:

Conduct a footprinting analysis on the target website www.certifiedhacker.com to determine the content length. (Format: NNN)

347 - Correct answer.

Challenge 5:

You're a cybersecurity investigator assigned to a high-priority case. Martin is suspected of engaging in illegal crypto activities, and it's believed that he has stored his crypto account password in a file named $ollers.txt. Your mission is to crack the SSH credentials for Martin's machine within the 192.168.10.0/24 subnet and retrieve the password from the $ollers.txt file. (Hint: Search in the folders present on the Desktop to find the target file) (Format: aNaa**NNNNNAA*)

i2tr&^72546HJ* - Correct answer.

Challenge 6:

Attackers have identified a vulnerable website and stored the details of this website on one of the machines within the 192.168.10.0/24 subnet. As a cybersecurity investigator you have been tasked to crack the FTP credentials of user nick and determine the ID of the domain. The information you need has been gathered and stored in the w_domain.txt file. (Format: NNNNNNNNNN)

7867721010 - Correct answer.

Challenge 7:

You have identified a vulnerable web application on a Linux server at port 8080. Exploit the web application vulnerability, gain access to the server and enter the content of RootFlag.txt as the answer. (Format: Aa*aaNNNN)

Ch@mp2022 - Correct answer.

Challenge 8:

You are a penetration tester assigned to a new task. A list of websites is stored in the webpent.txt file on the target machine with the IP address 192.168.10.101. Your objective is to find the Meta-Author of the website that is highlighted in the list. (Hint: Use SMB service) (Format: AA-Aaaaaaa)

EC-Council - Correct answer.

Challenge 9:

You have recently joined GoodShopping Inc. as a web application security administrator. Eager to understand the security landscape of the company's website, www.goodshopping.com, you decide to investigate the security updates that have been made over time. Your specific task is to identify the attack category of the oldest Common Vulnerabilities and Exposures (CVEs) affected the website. (Format: aaaaa*aaaa aaaaaaaaaa (AAA))

cross-site scripting (XSS) - Correct answer.

Challenge 10:

You are a web penetration tester hired to assess the security of the website www.goodshopping.com. Your primary task is to identify the type of security policies is missing to detect and mitigate Cross-Site Scripting (XSS) and SQL Injection attacks. (Format: Aaaaaaa Aaaaaaaa Aaaaaa)

Content Security Policy - Correct answer.

Challenge 11:

You are part of a cybersecurity team investigating an internal website that has been copied from a legitimate site without authorization. One of your teammates, acting as a spy, has scanned the website using a smart scanner within the subnet 192.168.10.0/24. Your task is to identify the number of Directory Listing of Sensitive Files on this website. The report, named w_report.pdf, is available on the target machine.(Hint: He remembered the OS as Windows Server 19 while scanning the website) (Format: NN)

36 - Correct answer.

Challenge 12:

Perform a bruteforce attack on www.cehorg.com and find the password of user adam. (Format: aaaaaaNNNN)

orange1234 - Correct answer.

Challenge 13:

As a cybersecurity analyst, your task is to identify potential vulnerabilities on the moviescope.com website. Your manager has requested a specific number of risk categories. The required HTML file is located on EH Workstation 1. (Format: N)

3 - Correct answer.

Challenge 14:

Perform a SQL Injection attack on www.moviescope.com and find out the number of users available in the database. (Format: N)

5 - Correct answer.

Challenge 15:

Perform a SQL Injection vulnerability scan on the target website www.moviescope.com and determine the WASC ID for SQL Injection (Format: NN)

19 - Correct answer.