CEH Engage - Part I

Part 1 of CEH Engage covers Footprinting and Reconnaissance, Scanning Networks, Enumeration, and Vulnerability Analysis modules. In this part, you are required to perform passive and active reconnaissance of the target organization, enumerating services, shares, users, user groups, etc., and perform vulnerability analysis of the identified systems/networks on the target. 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.

Flags

Challenge 1:

An attacker conducted footprinting on a web application and saved the resulting report Dumpster.xlsx in the documents folder of EH Workstation-1. Your task is to analyze this report and identify the hostname associated with the IP address 173.245.59.176. (Format: aaaaa.aa.aaaaaaaaaa.aaa)

henry.ns.cloudflare.com - Correct answer.

Challenge 2:

Identify the number of live machines in 192.168.10.0/24 subnet. (Format: N)

5 - Correct answer.

Challenge 3:

Identify the IP address of a Linux-based machine with port 22 open in the target network 192.168.10.0/24 (Format: NNN.NNN.NN.NNN).

192.168.10.111 - Correct answer.

Challenge 4:

Find the IP address of the Domain Controller machine in 192.168.0.0/24. (Format: NNN.NNN.NN.NNN)

192.168.0.222 - Correct answer.

Challenge 5:

Perform a host discovery scanning and identify the NetBIOS_Domain_Name of the host at 192.168.0.222. (Format: AAAAA.AAA)

SKILL.CEH - Correct answer.

Challenge 6:

Perform an intense scan on 192.168.0.222 and find out the DNS_Tree_Name of the machine in the network. (Format: AAAAA.AAA.aaa)

SKILL.CEH.com - Correct answer.

Challenge 7:

While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.10.0/24. (Format: N.NaN)

8.9p1 - Correct answer.

Challenge 8:

During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database. Note: Target network 172.30.10.0/24 (Format: Aaaaaa)

Ubuntu - Correct answer.

Challenge 9:

Perform an intense scan on target subnet 192.168.10.0/24 and determine the IP address of the machine hosting the MSSQL database service. (Format: NNN.NNN.NN.NNN)

192.168.10.144 - Correct answer.

Challenge 10:

Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain. (Format: aaN.aaaaaaaa.aaa, aaN.aaaaaaaa.aaa)

ns1.bluehost.com, ns2.bluehost.com - Correct answer.

Challenge 11:

Find the IP address of the machine running SMTP service on the 172.30.10.0/24 network. (Format: NNN.NN.NN.NNN)

172.30.10.200 - Correct answer.

Challenge 12:

Perform an SMB Enumeration on 172.30.10.200 and check whether the Message signing feature is required. Give your response as Yes/No.

Yes

No - Correct answer.

Challenge 13:

Perform a vulnerability assessment on the 2023 CWE Top 25 most dangerous software vulnerabilities and determine the weakness ID of the last entry on the list. (Format: NNN)

276 - Correct answer.

Challenge 14:

Perform vulnerability scanning for the Linux host in the 192.168.10.0/24 network using OpenVAS and find the QoD percentage of vulnerabilitiy with severity level as medium. (Format: NN)

70 - Correct answer.

Challenge 15:

Perform a vulnerability scan on the host at 192.168.10.144 using OpenVAS and identify any FTP-related vulnerability. (Format: AAA Aaaaaaaaa Aaaaaaaaa Aaaaa)

FTP Unencrypted Cleartext Login - Correct answer.