Cisco Certificate in Ethical Hacking v1.0

Challenge Description: The Cisco Certificate in Ethical Hacking is designed to validate a candidate's skills and knowledge necessary to identify, exploit, and mitigate cybersecurity vulnerabilities in a variety of environments using real-world scenarios. The Capture the Flag challenge, together with its required preparatory Ethical Hacker course and materials, equips candidates to handle sophisticated offensive cybersecurity events in various environments including network systems, web applications, and cloud technologies.

The following areas are general guidelines for the content likely to be included on the Capture the Flag challenge. However, other related topics may also appear during any specific scenario in the Capture the Flag challenge. To better reflect the contents of the scenarios in a Capture the Flag challenge and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Information Gathering and Reconnaissance

1.1 Use OSINT tools to gather information about a target (such as Google dorking, Shodan)

1.2 Analyze DNS and WHOIS records to gather intelligence

1.3 Perform network scanning and enumeration using tools such as Nmap and enum4linux

1.4 Employ various techniques for active reconnaissance including port scanning and DNS lookups

2.0 Vulnerability Scanning and Analysis

2.1 Conduct web application vulnerability scans using tools such as OWASP ZAP and Nikto

2.2 Perform network and host vulnerability assessments using tools such as Nmap and Greenbone Vulnerability Management (GVM)

2.3 Prioritize vulnerabilities based on CVSS scores and potential impact

3.0 Exploitation and Post-Exploitation

3.1 Exploit network, web application, and cloud vulnerabilities using tools such as Metasploit, SQLmap, and Pacu

3.2 Apply various post-exploitation techniques to maintain access and escalate privileges, utilizing tools such as Netcat and PowerSploit

3.3 Identify vulnerabilities and weaknesses involving AI, IoT, mobile, and firmware issues

4.0 Reporting and Mitigation

4.1 Construct comprehensive penetration testing reports based on findings

4.2 Prioritize remediation strategies to mitigate identified vulnerabilities

4.3 Prioritize findings and recommendations to stakeholders

5.0 Scripting and Code Analysis

5.1 Develop scripts in Bash, Python, and PowerShell to automate cybersecurity tasks

5.2 Analyze code samples to determine functionality and potential security flaws