EHACKIFY
CYBERSECURITY RESEARCH & TRAINING

Practical Exam Manual:
Penetration Tester - Web Application and Network

Introduction:

The final practical exam from Ehackify Cyber Security Research and Training tests students' practical skills in web application and network penetration testing. These hands-on assessments are important because they allow students to apply what they've learned in real-world situations, helping them become better prepared for cybersecurity roles.

Exam Overview:

Exam Duration: The exam takes place over a period of 5 days from the time of enrollment and The main objective is to identify as many issues as possible.
Assessment Criteria: Students are evaluated based on their technical skills, how well they stick to the testing method, the quality of their reports, and the number of issues they discover.

Exam Objectives:

- Demonstrate proficiency in conducting web application and network penetration tests.
- Apply appropriate methodologies to identify and exploit vulnerabilities.
- Document findings effectively in a professional penetration testing report.
- Showcase competence in the report review session.

Exam Guidelines:

Lab Environment: Each candidate receives a virtual machine upon enrollment, enabling secure access to the exam environment. Additionally, candidates must export and return the virtual machine for activity review during the report review session.

Report Submission Cut-off: Candidates must submit their final reports before the exam period concludes. Failure to do so will lead to termination of the exam, with candidates possibly being offered a second opportunity.

Format:

1. **Reconnaissance:** Gather information about the target system, including network ranges, hostnames, and open ports. Techniques may involve passive reconnaissance, DNS enumeration, and publicly available information gathering.
2. **Scanning:** Scan the target system for open ports, services, and operating systems to identify potential entry points. Active scanning techniques are used to map out the network topology and identify vulnerabilities.
3. **Vulnerability Identification:** Identify and analyze potential vulnerabilities within the target system, including system configurations, web application code, and common vulnerabilities.
4. **Exploitation:** Exploit identified vulnerabilities to gain unauthorized access to the target system, leveraging known exploits, custom payloads, and bypassing security controls.
5. **Post-exploitation:** After gaining access, escalate privileges, gather sensitive information, and maintain access. Various post-exploitation techniques are used to explore the system and identify additional weaknesses.
6. **Reporting:** Document findings, including detailed vulnerability descriptions, exploitation techniques, and recommendations for remediation. The report must adhere to industry standards.
7. **Report Reviewing Session:** In this session, students' reports and activity performance on the exported virtual machine will be assessed.

We assess candidates on how well they follow testing methods, find vulnerabilities, and document their findings. During review sessions, they discuss their results, showing their understanding and communication skills. This helps determine if they're ready for penetration testing roles.

Report Submission:

To submit your report, please use this link: **https://forms.gle/TbNE1XpRSZxmXQML8**

Students, apply your skills confidently in real-world scenarios. We appreciate your dedication in completing the exam, ensuring a fair evaluation of your penetration testing skills by Ehackify Cyber Security Research and Training.