



Penetration Tester

Job Description

Penetration testers, also called pen testers, assist organizations in identifying and resolving security vulnerabilities in their digital assets. Several professionals work in-house, serving on internal cybersecurity or information technology (IT) teams. Other pen testers work for firms that provide client services.

Key Responsibilities

- Conducting penetration tests on computer systems, networks, and applications.
- Developing new testing methods for identifying vulnerabilities.
- Identifying areas that require physical protection for systems, servers, and other network devices.
- Identifying methods and entry points that attackers use to exploit vulnerabilities.
- Hunting for weaknesses in common software, web applications and proprietary systems.
- Researching, evaluating, documenting and discussing answers with IT teams and administration.
- Evaluating and delivering feedback for information security fixes.
- Establishing expansions for existing security services that include hardware, software, policies, and procedures.
- Classifying areas where improvement is required in security education and awareness for users.
- Staying updated on the latest malware and security risks.

Qualifications Needed

Knowledge of programming languages, including:

- Python
- Powershell
- Google Go
- Bash

Knowledge of mobile penetration testing of iOS and Android systems, network operating systems, Windows, Linux, and MacOS, communications protocols, firewalls, IPS/IDS systems, virtual environments, and data encryption.

Understanding of popular application security and pen testing technologies, including:

- Kali
- Metasploit
- The Burp Suite
- Utilizing Wireshark
- Website Inspect
- Utilizing Network Mapper (NMAP)
- Nessus and other characters

Employers frequently look for professional credentials from organizations like the EC-Council, OSCP (Offensive Security Certified Professional), SANS Technology Institute, IEEE (Institute for Electrical and Electronic Engineers), and GIAC (Global Information Assurance Certification).