Occupation-Specific Information - Penetration Tester (Cybersecurity)

https://www.onetonline.org/link/summary/15-1299.04

Job-Description

Evaluate network system security by conducting simulated internal and external cyberattacks using adversary tools and techniques. Attempt to breach and exploit critical systems and gain access to sensitive information to assess system security.

Tasks

- Assess the physical security of servers, systems, or network devices to identify vulnerability to temperature, vandalism, or natural disasters.
- Collect stakeholder data to evaluate risk and to develop mitigation strategies.
- Conduct network and security system audits using established criteria.
- Configure information systems to incorporate principles of least functionality and least access.
- Design security solutions to address known device vulnerabilities.
- Develop and execute tests that simulate the techniques of known cyber threat actors.
- Develop infiltration tests that exploit device vulnerabilities.
- Develop presentations on threat intelligence.
- Develop security penetration testing processes, such as wireless, data networks, and telecommunication security tests.
- Discuss security solutions with information technology teams or management.
- Document penetration test findings.
- Evaluate vulnerability assessments of local computing environments, networks, infrastructures, or enclave boundaries.
- Gather cyber intelligence to identify vulnerabilities.
- Identify new threat tactics, techniques, or procedures used by cyber threat actors.
- Identify security system weaknesses using penetration tests.

- Investigate security incidents by using computer forensics, network forensics, root cause analysis, or malware analysis.
- Keep up with new penetration testing tools and methods.
- Maintain up-to-date knowledge of hacking trends.
- Prepare and submit reports describing the results of security fixes.
- Test the security of systems by attempting to gain access to networks, web-based applications, or computers.
- Update corporate policies to improve cyber security.
- Write audit reports to communicate technical and procedural findings and recommend solutions.

Detailed Work Activities

- Develop testing routines or procedures.
- Analyze security of systems, network, or data.
- Prepare scientific or technical reports or presentations.
- Stay informed about current developments in field of specialization.
- Analyze risks to minimize losses or damages.
- Develop computer or information security policies or procedures.
- Develop computer or information systems.
- Develop organizational policies or programs.
- Discuss design or technical features of products or services with technical personnel.
- Evaluate characteristics of equipment or systems.
- Examine records or other types of data to investigate criminal activities.
- Interpret design or operational test results.
- Investigate illegal or suspicious activities.
- Prepare analytical reports.
- Prepare technical or operational reports.
- Search files, databases or reference materials to obtain needed information.

- Test computer system operations to ensure proper functioning.
- Test performance of electrical, electronic, mechanical, or integrated systems or equipment.