Information Gathering and Vulnerability Scanning for Penetration Testing

This intermediate Information Gathering and Vulnerability Scanning for Penetration Testing training equips security technicians with the skills to gather critical system data and conduct effective vulnerability scans. Learn how to prepare for penetration tests, identify security flaws, and optimize test results. This cybersecurity training is a great resource for penetration testers and cybersecurity professionals.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Conduct Information Gathering Using Appropriate Techniques — 62 min.

Introduction to Information Gathering	1
Scanning Hosts	6
Enumerating Hosts for Specific Details	8
Digging Deeper into Fingerprinting and Cryptography	6
Eavesdropping for Data	7
Decompiling and Debugging for Data	5
Using Open Source Intelligence Gathering	8

Perform a Vulnerability Scan

Overview	1
Intro to Vulnerability Scanning	1
Identifying Types of Scans	6
Handling Scanning Permissions	4
Scanning Applications and Containers	4
Scanning Considerations	5

Analyze Vulnerability Scan Results

Overview	1
Intro to Analyzing Scan Results	1
Categorizing Assets	4
Adjudicating Scan Results	6
Prioritizing Vulnerabilities	5
Identifying Common Themes	6

Leverage Information for Exploitation

Overview	1

Intro to Exploitation	1
Mapping Vulnerabilities to Potential Exploits	5
Prioritizing Pentest Activities	2
Implementing Exploits	5
Learning Password Cracking Methods	8
Understanding Social Engineering	3

Explain Weaknesses Inherent to Specialized Systems

Overview	1
Intro to Specialized Systems	1
Understanding ICS and SCADA	4
Considering Mobile Devices	4
Embedded and Real-Time Devices	5
Utilizing IoT Devices	4
Understanding POS Device Weaknesses	4

Vulnerability Management Activities

Overview	1
Vulnerability Scans	11
Security Content Automation Protocol (SCAP)	12

WEEK 2

131 min.

Assessments	14
Patch Management	8
Information Sources	4

Vulnerability Assessments and Pentesting

Overview	1
Vulnerability Assessment vs Pentesting	7
Testing Methods	12
Pentesting: Post Exploit	7
Vulnerability Assessment Tools	7
Some Pentesting Tools	9
Vulnerability Assessments and Pentesting Requirements	5

Vulnerability Analysis and Mitigation

Overview	1
Common Software Vulnerabilities	13
Race Conditions	7
Cryptographic Vulnerabilities	5
Software Development Vulnerabilities	7
Web Application Attacks	8
VM and Network-Based Attacks	13