

# Security Threats, Attacks, and Vulnerabilities

This Security Threats, Attacks, and Vulnerabilities training covers how to recognize, compare, and contrast different types of cybersecurity vulnerabilities and threats and indicators associated with network attacks. This Security Threats, Attacks and Vulnerabilities training is derived from the first of CompTIA Security+ certification exam's five exam objectives and will prepare you in the broadest way possible.

[CBT Nuggets course material](#) →

## WEEK 1

### Social Engineering Techniques

155 min.

Introduction to Social Engineering	2
Phishing and Related Attacks	6
Low Tech Attacks	5
Why Social Engineering Works	4
The Top Social Engineering Tool	7
Identifying a Phishing Email	10
Social Engineering Toolkit	8
Review Quiz	5

### Cyber Attack Techniques

Overview	1
Introduction to Cyber Attack Techniques	1
Malware	8
Password Attacks	6
Password Attack Example	10
Cyber Physical Components	5
Adversarial AI	4
Supply Chain Security	2
Cryptographic Attacks	4
Review Quiz	8

### Application Attacks

Overview	1
Introduction to Application Attacks	1
Injection Attacks	3
Cross Site Scripting	2
Poorly Written Apps	5

Overflow Attack Demo	8
Poorly Written App Attack	4
Impersonation	3
Error Handling Attack	7
Additional Application Attacks	4
Password Recovery Fail	4
Review Quiz	6

### Network Attacks

Overview	1
Introduction to Network Attacks	1
Wireless Attacks	6

## WEEK 2

152 min.

In-line / On-path Attacks	6
Layer 2 attacks	8
Domain name system (DNS)	6
Distributed denial-of-service (DDoS)	4
Malicious code or script execution	2
Remediation Options	5
Review Quiz	8

### Threat Actors and Intelligence Sources

Overview	1
Introduction to Actors, Vectors, and Intelligence Sources	1
Threat Actors	6
Attack Vectors	7
Threat Intelligence Sources	10

Threat Maps	12
Additional Sources for Research	4
Review / Quiz	6

### Vulnerabilities and Security Risks

Overview	1
Introduction to Vulnerabilities and Security Risks	1
Cloud vs. On-prem Vulnerabilities	3
Zero-day Attacks	3
Weak Configurations	9
Telnet with IPsec Demonstration	10
Third-Party Risks	3
Patch Management	4
Vulnerabilities Review Quiz	13

### Techniques Used in Security Assessments

Overview	1
Introduction to Security Assessments	1
Vulnerability Scan Overview	6
Network Scan Demonstration	8

## WEEK 3

85 min.

Positive and Negative Scan Results	3
CVE and CVSS	5
Security information and event management (SIEM)	5
Threat hunting	3
Security orchestration, automation, and response (SOAR)	3
Security Assessment Review Quiz	11

## Penetration Testing Techniques

Overview	1
Introduction to Penetration Testing	1
Pen Testing Overview	11
OSSTMM	3
Resources from NIST	4
Penetration Testing Execution Standard	4
Pen Testing Demo	14
OWASP	4
Security Team Exercises	2
Pen Testing Review Quiz	9