CompTIA Sec+ SY0-401, Part 6 of 8: Attacks and Mitigation [Deprecated/Replaced]

Meet the expert: Ryan Hendricks is an experienced instructor who teaches networking and security courses to IT professionals throughout the nation. He currently has the CompTIA Certified Technical Trainer (CTT+ Classroom) and the Cisco Certified Academy Instructor (CCAI) credentials. He holds certifications from (ISC)2, EC-Council, CompTIA, and Cisco. When not on the podium instructing, he delves into IT books, always looking to learn more and keep up with the latest security topics.

Prerequisites: This course assumes that the user has working knowledge of networks and networking. Ideally, the user should have their CompTIA Network+ certification, but can be replaced with networking experience.

Runtime: 01:48:36

Course description: In this course, certified technical trainer Ryan Hendricks delves into the multitude of ways an attacker can compromise an organization. Hendricks will discuss how session hacking is used to compromise Web servers and e-mail servers and also examine the security concerns regarding wireless and Bluetooth devices. This course will also reveal the tools that should be in every security professional’s tool belt as well as the latest mitigation, discovery, penetration and vulnerability testing techniques.

Course outline:

Wireless Attacks
- Introduction
- Rogue Access Points
- Jamming/Interference
- Evil Twin
- War Driving
- War Chalking
- Bluejacking
- Bluesnarfing
- IV Attack
- Packet Sniffing
- Near Field Communication
- Replay Attacks
- WEP/WPA Attacks
- WPS Attack
- Summary

Application Attacks
- Introduction
- Zero-Day Attack
- Cookies and Attachements
- Locally-Shared Objects
- Malicious Add-Ons
- Session Hijacking
- Header Manipulation
- Arbitrary Code Execution
- Summary

More Application Attacks
- Introduction
- Cross-Site Scripting
- Cross-Site Request Forgery
- Demo: Cross-Site Scripting
- SQL Injection
- Demo: SQL Injection
- Demo: Bypass Authentication
- XML Injection
- Directory Traversal
- Demo: Directory Traversal
- Command Injection
- Demo: Command Injection
- Buffer Overflow
- Integer Overflow
- Summary

Mitigation Techniques
- Introduction
- Event Logs
- Audit Logs
- Security Logs
- Access Logs
- Hardening
- Network Security
- Security Posture
- Reporting
- Detection vs. Prevention
- Summary

Discovery
- Introduction
- Security Assessment Results
- Tools
- Protocol Analyzer
- Vulnerability Scanner
- Honeypots
- Honeynets
- Port Scanner
- Passive vs. Active Tools
- Banner Grabbing
- Assessment Techniques
- Baseline Reporting
- Code Review
- Determine Attack Surface
- Review Architecture
- Review Designs
- Summary

Penetration Testing
- Introduction
- Penetration Testing
- Identify Vulnerability
- Verify a Threat Exists
- Bypass Security Controls
- Actively Test Security Control
- Exploit Vulnerabilities
- Vulnerability Scanning
- Passively Testing Security
- Identify Lack of Security
- Identify Common Misconfigs
- Intrusive vs. Non-Intrusive
- Credentialed vs. Non
- Black Box
- White Box
- Gray Box
- Summary