CompTIA Sec+ SY0-401, Part 5 of 8: Security and Malware [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: 02:06:29

Course description: Take your first steps on the road to being a security professional. In this course, security expert Ryan Hendricks gives an overview of the world of threats and vulnerabilities. He will define and differentiate common types of attacks including worms, Trojans and other malware. He'll also discuss how hackers exploit the low-tech but effective techniques of social engineering in order to gain unauthorized access to enterprise data.

Course outline:

CIA Triad
- Introduction
- CIA Triad
- Confidentiality
- Confidentiality Support
- Confidentiality Attacks
- Integrity
- Integrity Support
- Integrity Attacks
- Availability
- Availability Support
- Availability Attacks
- CIA Triad
- Summary

Safety
- Introduction
- Fences
- Fences, Cont.
- Lighting
- Lighting, Cont.
- Locks
- Closed-Circuit Television
- Escape Plans
- Drills
- Escape Routes
- Testing Controls
- Summary

Physical Security
- Introduction
- Hardware Locks
- Hardware Locks, Cont.
- Mantraps
- Video Surveillance
- Video Surveillance, Cont.
- Fencing
- Proximity Readers
- Access List
- Proper Lighting
- Signs
- Guards
- Barricades
- Biometrics
- Protected Distribution
- Alarms
- Motion Dectectors
- Summary

Types of Malware
- Introduction
- Adware
- Virus
- Virus Types
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic Bomb
- Botnets
- Ransomware
- Polymorphic Malware
- Summary

Social Engineering
- Introduction
- Social Engineering
- Shoulder Surfing
- Dumpster Diving
- Tailgating
- Impersonation
- Hoaxes
- Phishing
- Demo: URL Manipulation
- Vishing
- Spear Phishing
- Whaling
- Pharming
- DNS Poisoning
- Principles
- Summary

Various Attacks
- Introduction
- Man-in-the-Middle
- Denial of Service (DoS)
- Distributed Denial of Service
- Replay
- Smurf Attack
- Spoofing
- Spam
- Spim
- Xmas Attack
- Privilege Escalation
- Malicious Insider Threat
- ARP Poisoning
- Watering Hole Attack
- Transitive Access
- Client-Side Attacks
- Password Attacks
- Typo Squatting/URL Hacking
- Summary