CompTIA Sec+ SY0-501, Part 1 of 9: Overview and Malware

Meet the expert: Jason Dion, CISSP No. 349867, is a professor at University of Maryland University College with multiple information technology professional certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Digital Forensic Examiner (DFE), Digital Media Collector (DMC), CySA+, Security+, Network+, A+, PRINCE2 Practitioner, and ITIL. He holds a Masters of Science degree in Information Technology with a specialization in Information Assurance

Prerequisites: • Basic familiarity with computer networks, administration, and security is helpful (But, all required information will be covered during the course)
• Completion of the CompTIA A+ and Network+ certifications (Helpful, but not required)

Runtime: 01:45:07

Course description: In this course we will discuss an overview of Security+. We will discuss Malware, ransomware and malware infections and how to avoid interception and privilege escalation for the SY0-501 Exam.

Course outline:

Overview Of Security
• Introduction
• Welcome
• Overview of Security
• CIA Triad
• AAA of Security
• Security Threats
• Mitigating Threats
• Hackers
• Threat Actors
• Summary

Malware
• Introduction
• Malware
• Viruses
• Worms
• Trojan Horse
• Demo: Virus and Trojan
• Summary

Ransomware
• Introduction
• Ransomware
• Spyware
• Rootkits
• Spam
• Summary of Malware
• Summary

Malware Infections
• Introduction
• Malware Infection
• Common Delivery Methods
• Phishing
• Botnets and Zombies
• Active Interception and Privilege Escalation
• Summary

Privilege Escalation
• Introduction
• Privilege Escalation
• Backdoors and Logic Bombs
• Symptoms of Infection
• Removing Malware
• Preventing Malware
• Summary