N10-008 CompTIA Net+, Part 6 of 7: Network Security

Meet the expert: Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

Prerequisites: This course assumes the user has some experience with computer hardware, software, and understands the concept of a computer network.

Runtime: 01:24:23

Course description: This course is a part of the CompTIA Net+ body of knowledge focusing on the N10-008 Exam. This course covers: network security fundamentals, planning security, identify threats and vulnerabilities and how to protect the network.

Course outline:

Network Security Fundamentals
- Introduction
- Intro to Network Security
- CIA Triad
- Network Threats
- Network Vulnerabilities
- Understanding Risks
- What is AAAA
- Cryptography
- Algorithms and Keys
- Digital Signatures
- Best Practices for Permissions
- Best Practices for Employees
- Defense in Depth
- Summary

Planning for Network Security
- Introduction
- Planning for Network Security
- Threat Vulnerability Pairs
- Identifying Vulnerabilities
- Types of Vulnerabilities
- Mitigating Risks
- Risk Assessments
- Summary

Identifying Threats and Vulnerabilities
- Introduction
- Threat Categories
- Software Attacks
- Malicious Code Attacks
- Types of Malicious Code
- Network Attacks
- Port Scanning
- IP Spoofing
- Denial of Service
- On-Path Attacks
- Human Attacks
- Wireless Vulnerabilities and Threats
- Summary

Protecting the Network
- Introduction
- Protecting the Network
- Implement Physical Protection
- Physical Security Options
- Anti-Malware
- Network Hardening
- SEcuring Network Communications
- Wireless Security
- Authentication
- Authentication Factors
- Network Access Control
- Demo: Anti Malware Options
- Demo: Hardening and IPSec
- Summary