CompTIA NET+ Cert, Part 15 of 17: Network Security[replaced]

page 1

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: Parts 1 through 14 of the CompTIA NET+ series

Runtime: 02:07:42

Course description: ** this course is updated for current certification N10-008 with parts 1 through 7 starting at https://www.learnnowonline.com/course/npe**

This course will focus on Domain 3.0 of the CompTIA NET+ Certification Exam N10-006, a largely changed objective which has been considerably expanded. Areas to be explored include risk assessment, business continuity, disaster recovery, and high availability, as well as mitigating risk utilizing network hardening on operating systems and devices. In addition, the fundamentals of network forensics to ascertain a compromised system will be discussed.

Course outline:

Overview of Network Security
- Introduction
- Objective Overview
- Subdomains
- Summary

Risk Related Concepts
- Introduction
- Risk Related Concepts
- Threats
- Vulnerabilities
- Identifying Vulnerabilities
- Risk
- User Awareness
- Regulatory and Legislative Requirements
- Continuity and Recovery
- Summary

Vulnerabilities and Threats
- Introduction
- Identifying Threats and Vulnerabilities
- Types of Attackers
- Types of Threats
- Malicious Code Attacks
- Common Categories of Attacks
- Network Threats
- Port Scanning and Eavesdropping
- Denial of Service
- Man-in-the-Middle Attacks
- Wireless Vulnerabilities and Threats
- Vulnerability Types
- Summary

Network Hardening
- Introduction
- Network Hardening
- Anti-Malware Software
- Network Devices
- Network Communications
- Summary

Physical Security
- Introduction
- Physical Security Controls
- Elements of Physical Security
- Summary

Basic Firewalls
- Introduction
- Basic Firewalls
- Firewall Types and Capabilities
- Summary

Network Access Control
- Introduction
- Network Access Control Models
- Concepts of Network Access Control
- Summary

Computer Forensic Fundamentals
- Introduction
- Computer Forensic Fundamentals
- The Forensics Process
- First Steps
- Other Forensics Concepts
- Summary