CompTIA NET+ Cert, Part 09 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: This course assumes the user has some experience with computer hardware, software, and understands the concept of a computer network. The user should have also viewed CompTIA NET+ Cert: System Security course before viewing this course.

Runtime: 01:11:22

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

You need to be able to identify network security mechanisms and devices as a network technician. In this course we are going to look at a number of different network defenses which are implemented at various levels in the organization. You are going to be able to identify these network devices as well as implement network security controls to protect your users and the data contained on the corporate network.

Course outline:

Network Perimeter Security
- Introduction
- NAT
- The NAT Process
- IP Filtering
- MAC Filtering
- Firewalls
- Firewall Types
- Firewall Types (Cont)
- Common Firewall Features
- Demo: Firewall
- Demo: New Firewall Rule
- DMZs
- Proxy Servers
- Web Proxy Features
- Web Proxy Features (Cont)
- Website Caching
- NAC
- Physical Network Security
- Summary

Intrusion Detection Prevention
- Introduction
- Intrusion Detection
- IDSs
- Types of IDSs
- Passive and Active IDSs
- IPSs
- Port Scanners
- Vulnerability Assessment Tools
- Network Scanners
- Summary

IPSec
- Introduction
- IPSec
- IPSec Protection Mechanisms
- IPSec Modes
- IPSec Transport Protocols
- IKE
- Security Associations
- IPSec Policies
- IPSec Policy Rules
- IPSec Policy Rules (Cont.)
- Windows IPSec Components
- Demo: IPSec on Active Directory
- Demo: IPSec Windows Firewall
- Summary