CompTIA NET+ Cert, Part 10 of 17: Security Threats and Attacks[replaced]

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: Network Security course before viewing this course.

Runtime: 01:12:17

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

In this course we are going to provide an overview of the huge number of threats and vulnerabilities that exist in modern networks. We will begin by looking at security concepts such as threats, vulnerabilities, risks, and how to deal with them. We will also look at various attacks and discuss how they work and how you can implement defense mechanisms to minimize risk for your organization.

Course outline:

Security Threats and Attacks
- Introduction
- Physical Security
- Physical Security (Cont.)
- Threats and Vulnerabilities
- Social Engineering Attacks
- Social Engineering Types
- Social Engineering Types 2
- Social Engineering Types 3
- Malicious Code Attacks
- Malicious Code Attacks,Types
- Malicious Code Attacks,Types 2
- Malicious Code Attacks,Types 3

- Types of Viruses
- Types of Viruses (Cont.)
- Summary

Network Attacks
- Introduction
- Buffer Overflow
- Password Attacks
- Types of Password Attacks
- Types of Password Attacks 2
- IP Spoofing Attacks
- Session Hijacking Attacks
- DoS Attacks
- DDoS Attacks
- Man-in-the-Middle Attacks
- Port Scanning Attack
- Replay Attacks
- FTB Bounce Attacks
- ARP Poisoning Attacks
- Wireless Security
- Wireless Vulnerabilities
- Wireless Vulnerabilities 2
- Wireless Vulnerabilities 3
- Wireless Vulnerabilities 4
- Wireless Vulnerabilities 5
- Summary

Threat Mitigation
- Introduction
- Software Updates
- Patch Management
- Antivirus Software
- Internet Email Virus Protectio
- Anti-Spam Software
- Security Policies
- Common Security Policy Types
- Security Policy Types (cont.)
- Security Incident Management
- IRPs
- Change Management
- Employee Education
- User Security Responsibilities
- Summary