Securing Windows Server 2016, Part 1 of 5: Overview and Users

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 is Part 1 of the series.

Runtime: 03:29:25

Course description: In this course we need to start off by thinking like an attacker and the attack phases. It will begin with a introduction to attacks, breaches and detection. Next, Users and User security with resources, authorization and credentials as well as controlling rights and privileges. It will round out with managing passwords and group managed service accounts.

Course outline:

Understanding Attacks
- Introduction
- Assume Breach
- Methods of Attack
- Attack Stages
- Prioritizing Resources
- Incident Response Strategy
- Ensuring Compliance
- Summary

Detecting Security Breaches
- Introduction
- Locating Evidence
- Event Logs
- Examining Other Configurations
- Summary

Using Sysinternals Tools
- Introduction
- Introducing Sysinternals
- Demo: Sysinternals
- Introduction to FSRM
- System Monitor
- AccessChk
- Autoruns
- LogonSessions
- Process Explorer
- Process Monitor
- Sigcheck
- Demo: Locating Systinternals
- Demo: LogonSessions
- Demo: Process Explorer
- Demo: Process Monitor
- Summary

User Rights and Priveleges
- Introduction
- Principle of Least Privilege
- Configuring User Rights
- Configuring Account Security Options
- Demo: Control Privileges
- Demo: Account Options
- Demo: Active Directory in PowerShell
- Demo: User Properties
- Account Security Controls
- Complexity Options
- Summary

Assigning Privileges
- Introduction
- Password and Lockout Policies
- Demo: Password Policies
- Configuring Fine-Grained Password Policies
- Understanding PSO Application
- Protected Users Security Groups
- Delegating Administrative Control
- Demo: Access Control Lists
- Local Administrator Password Solutions
- LAPS Requirements
- LAPS Process
- Configuring and Managing Passwords
- Demo: LAPS
- Demo: LAPS GPO
- Summary

Computer and Service Accounts
- Introduction
- What Is a Computer Account
- Computer Account Functionality
- Working with Secure Channel Passwords
- Service Account Tyoes
- Group MSAs
- Demo: Configure MSA
- Demo: MSA Continued
- Summary

Protecting User Credentials
- Introduction
- Introducing Credential Guard
- Credential Guard Requirements
- Configuring Credential Guard
- Verifying Credential Guard Operation
- Credential Guard Weaknesses
- NTLM Blocking
- Searching AD DS for Problem Accounts
- Demo: Locate Problem Accounts
- Summary

Privileged Access
- Introduction
- The Need for Privileged Access Workstations
- Privileged Access Workstations
- Jump Servers
- Securing Domain Controllers
- Summary