Microsoft

Securing Windows Client

Workshop*PLUS*

Target Audience:

This course is targeted to IT Admins, Windows Infrastructure Engineers, Desktop administrators, IT Security staff and administrators who deploy, design and implement Windows Client environments.

Prerequisites:

Understating of security threats and vulnerabilities, patch management, group policy management, windows firewall and network security concepts.

Overview

The **Securing Windows Client** 4-day WorkshopPLUS course provides students with the skills required to manage Windows clients against unintended access or intrusion. This workshop covers common security threats and vulnerabilities, and details how to protect your client infrastructure. This workshop also covers new mitigations in current Windows client operating systems, including Windows 7 and Windows 8.

Security threats are increasingly a focal point to many enterprises. Cyber-crime, industrial espionage, and diversity of malware is expanding dramatically. There is no single tool that can protect assets against all threats, however by protecting your client infrastructure with defenses at different layers of security, we can significantly reduce the potential exposure. Corporate client machines and devices can introduce significant security risk. This course demonstrates Microsoft's technologies, tools, and methods which can be used to design, deploy and control client-side security by significantly decreasing many risks in Windows 7 and Windows 8 environments.

Key Features and Benefits

- Identifying and discuss differing layers of security for clients
- Understand built-in Microsoft client security technologies
- Build, deploy and configure clients to significantly reduce security risk
- Prepare a client environment for security audits and certification
- Identify tasks for client hardening and compliance analysis

Technical Highlights

After completing this course, you will be able to:

- Implement new security features and built-in tools of Windows 7 and Windows 8
- Understand advanced Windows Firewall capabilities, IPsec isolation and WiFi security
- Utilize Security Compliance Manager to evaluate and implement client security configurations
- Effectively prioritize and implement Microsoft patches for desktops, laptops and devices

Syllabus

Hardware Requirements:

Processor: Pentium IV 2.4 Gigahertz (GHz)
RAM: 8 Gigabytes (GB) of RAM
Free Hard Disk Space: 100-GB hard disk

Operating System Requirements

Operating System: Windows 2008 R2 or Windows 2012 and Hyper-V Role

This workshop runs **four** full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Information Security and Information Risk Management*:* This module provides an overview of general Information Security concepts, security definitions, risk management, vulnerabilities and layered security protection.

Module 2: Securing Client in Application Layer: This module details tools that are available in Windows 7 (ASLR, UAC, MIC, AppLocker, Session 0 isolation, FARV) and some new feature that were introduced in Windows 8.

Module 3:Securing Client in File/Data layer: This module presents file and data layer security and protections against offline attacks against client assets. Technologies reviewed in this module include Bitlocker and Unified Extensible Firmware Interface (UEFI) boot protections.

Module 4: Certificate management and new client security features: This module covers methods to secure user authentication, harden client systems via Group Policy templates, the use and deployment of client certificates, and new Windows 8 PKI features.

Module 5: Protecting client network communication: This module focuses on network layer by providing deep insight of built/in Windows Firewall and IPsec capabilities, overview of secure Wireless access, and controlled secure remote asset access with VPN and DirectAccess

Module 6: Patch Management and Protecting Against Client Vulnerabilities: This module provides useful information on Microsoft Support Lifecycle, Microsoft Security update release process, client patch management practices, and WSUS basics.

Module 7: Client Baseline Management and Managing Compliance with SCM and DCM : This module covers a detailed overview of Microsoft Security Compliance Manager (SCM). You will understand how to deploy and monitor security baselines of your Windows client infrastructure as well as implement Desired Configuration Manager (DCM) packs created with SCM to evaluate ongoing compliance with System Center Configuration Manager (SCCM).

Microsoft