Microsoft

Securing Windows Client

Workshop*PLUS*

Overview

Security threats are increasingly a focal point for many enterprises. Cyber-crime, industrial espionage, and diversity of malware are expanding dramatically. There is no single tool that can protect your assets against all threats. However, by protecting your client infrastructure with defenses at different layers of security, you can significantly reduce the potential exposure.

Corporate client machines and devices can introduce significant security risk. This Workshop*PLUS* demonstrates Microsoft's technologies, tools, and methods which can be used to design, deploy, and control client-side security by significantly decreasing several risks in Windows 7, 8, 8.1, and 10 environments. Understand the full story behind Credential Theft and Pass the Hash (PtH) attacks and know all the mitigations and countermeasures available for Windows 7 and later operating systems

The three-day **Securing Windows Client** Workshop*PLUS* provides students with the skills required to protect Windows clients against unintended access or intrusion.

This Workshop*PLUS* covers:

- New mitigations in the current Windows client operating systems, including Windows 7, Windows 8, Windows 8.1 and especially Windows 10

Technical Highlights

After completing this WorkshopPLUS, you will be able to:

- Implement new security features and built-in tools of Windows 7, Windows 8, 8.1 and Windows 10 (auditing enhancements, Credential Guard, Device Guard, Microsoft Passport)
- Understand advanced Windows Firewall capabilities and how to use it to mitigate the risk of PtH attack on network layer, IPsec isolation, and Wi-Fi security.
- Security Compliance Manager (SCM) to evaluate and implement client security configurations.
- Effectively prioritize and implement Microsoft patches for desktops, laptops, and tablets.

Target Audience

This WorkshopPLUS is targeted at the following IT professionals who deploy, design, and implement Windows Client environments:

- *IT Administrators*
- *Windows Infrastructure Engineers*
- *Desktop administrators*
- *IT Security staff and Administrators*

Key Features and Benefits

- *Hands-on labs and demos*
- *Workshop structure is modularized and can be customized according to customer's needs*

Prerequisites

The students must possess knowledge of the following:

- *Security threats and vulnerabilities*
- *Patch management*
- *Group policy management*
- *Windows Firewall*
- *Network security concepts*

Hardware Requirements

- *Processor: Pentium IV 2.4 GHz*
- *RAM: 16 GB*
- *Free hard disk space: 140 GB*

Operating System Requirements

OS: Windows Server 2012 R2 with Hyper-V Role installed.

Syllabus

This Workshop*PLUS* suggested duration **three** full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Vulnerabilities, threats and PtH attack overview*:* This module provides an overview of general vulnerabilities, threats and layered security protection. It covers PtH attack mitigation techniques including the new Windows 10 feature Credential Guard.

Module 2: Securing Client in Application Layer: This module details tools that are available in Windows 7 (Address Space Layout Randomization (ASLR), User Account Control (UAC), Mandatory Integrity Control (MIC) , AppLocker, Session 0 isolation and File and Registry Virtualization) as well as some new features introduced in Windows 10 (auditing enhancements, Device Guard)

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

Module 4: Client Authentication Security Features: This module covers password challenges and alternatives and new features introduced in Windows 10 (Microsoft Passport, Windows Hello)

Module 5: Protecting Client Network Communication: This module focuses on securing the network layer by providing a deep insight of built-in Windows Firewall and IPsec capabilities, and an overview of secure wireless access, also how to use advanced capabilities of Windows Firewall to mitigate the risk of PtH attack

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 hotfix branching

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

Microsoft