Windows Protection Mechanisms: Section 1 Transcript

Introduction

1/2

Welcome to the Windows Protection Mechanisms module.

Windows hardening is a technique used to reduce the number of openings for malicious users to attack the system. In this module you will learn the importance of Windows File Protection (WFP) and its successor, Windows Resource Protection (WRP). Also, you will learn about Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), and how they relate to Windows security.

Throughout this module, you'll be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Describe Windows File Protection (WFP) and Windows Resource Protection (WRP),
- Discuss the differences between WFP and WRP,
- Explain Address Space Layout Randomization (ASLR),
- Explain Data Execution Prevention (DEP), and
- Identify how Microsoft defines critical system files.

Bypass Exam Introduction

2/2

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to begin the Bypass Exam.

If you do not wish to take the Bypass Exam, you can use the Content Menu to proceed to the next section of the module.

Windows Protection Mechanisms: Section 2 Transcript

Brief History of Windows Protection Mechanisms

1/8

Microsoft has a history of trying to keep up with the times to counter threats to its operating systems. In the beginning, its operating system had no form of protection. Here is a brief history of a few of their Windows protection mechanisms.

Note that protection mechanisms that were implemented in earlier versions were rarely removed; usually Microsoft built upon, renamed, or incorporated the protection mechanisms into later versions. In this module, you'll see how WFP was incorporated into a larger WRP system.

Windows 2000 and Windows XP, released in 2000 and 2001, incorporated new security features to protect selected files, applications, and other resources. Some of those features included Access Control Lists (ACLs), security groups, group policy, WFP and introduction of user-level privileges (i.e., Guest accounts).

Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, released in 2004 and 2005, introduced Data Execution Prevention (DEP) in order to add support for the No Execute (NX) bit which helps to prevent buffer overflow exploits. During these releases, Kernel Patch Protection was introduced (i.e., PatchGuard), which prevents third-party software from modifying the kernel, including kernel-mode drivers or any data structure used by the kernel.

Windows Vista, released in 2006, introduced Windows Defender, integrity levels in user processes, and obfuscation techniques such as Address Space Layout Randomization (ASLR) used to increase the amount of effort required by malware before successful system infiltration. This also marked the introduction of WRP, employing ACLs to provide file protection from modification, deletion, or replacement of essential system files, folders and registry keys. Protecting these files ensures the normal operation of the operating system and prevents operating system and application failures.

Windows 7, released in late 2009, introduced Microsoft Security Essentials (MSE). MSE replaced Windows Defender and incorporated real-time protection through anti-virus and Network Inspection System, which is a Network Intrusion Detection System (NIDS) that works on Vista and Windows 7.

Windows 8, released in October 2012, removed MSE and incorporated it into the underlying operating system. It introduced Secure Boot to prevent unauthorized firmware, operating systems, and drivers from running at boot time by leveraging the abilities of Unified Extensible Firmware Interface (UEFI). It also replaced the old Basic Input/Output System (BIOS) in modern computers . Secure Boot does this by requiring Authenticode digital signatures on the firmware modules, operating system loaders (boot manager), and UEFI drivers.

Windows Defender Antivirus

2/8

Windows Defender Antivirus was introduced in Windows 10 and provides several improvements over MSE that allow for a more holistic approach to enterprise antivirus protection. To do this, Windows Defender Antivirus uses a multi-pronged approach that consists of Cloud-delivered protection, Rich local context, Extensive global sensors, Tamper proofing, and Enterprise-level features.

Click each of the features to learn more about them.

- Cloud-delivered protection: Uses distributed cloud-based resources and machine learning to detect and block known and unknown malware.
- Rich local content: Used by Windows Defender Antivirus to monitor the contextual information (origin, current and past locations) of local files and processes.
- Extensive global sensors: Aggregates enriched context data from endpoints and uses this data to keep Windows Defender Antivirus aware of emerging threats.
- Tamper proofing: Uses protected processes to prevent untrusted processes from tampering with Windows Defender Antivirus components.
- Enterprise-level features: Provides tools and configuration options that are better suited for an enterprise-level antimalware solution.

Early Launch Anti-Malware

3/8

Some advanced malware has the ability to infect a system's boot drivers to load rootkits and other boot sector malware. This type of malware is difficult to detect and remove because it infects a system before the OS and antivirus software is loaded.

To address this, Microsoft's Early Launch Anti-Malware (ELAM) was introduced in Windows 8 and allows antivirus software to scan the boot drivers of a system for viruses before they are loaded. If antivirus software determines that a driver to be initialized is malicious, it can prevent the driver from loading. ELAM classifies drivers as good, bad, or unknown, and its policy can be configured to allow specific classifications of drivers to run.

Windows File Protection (WFP)

4/8

WFP is the original mechanism developed to prevent the replacement of critical Windows system files. The goal is to ensure that these critical system files are not accidentally deleted, modified, or renamed. WFP is a reactive system; it monitors for changes to critical system files and then reacts to these requested changes. For WFP, Microsoft defines critical system files as files that must not be replaced or overwritten because they are used by the operating system and other applications that ensure the normal function of the OS and prevents OS and application failures. This includes those files installed as part of the operating system; updates, hotfixes, service packs, and signed drivers.

Modified, missing, or bad files are replaced from a repository of known good entries, in the following order:

- The cache folder (by default, it is %systemroot%\system32\dllcache),
- The network install path, if the system was installed using network install, and
- The Windows CD-ROM, if the system was installed from CD-ROM.

WFP File Replacement

In Windows Server 2003 and Windows XP, replacement of WFP-protected system files is supported only through the following mechanisms:

- Windows Service Pack installation using Update.exe,
- Hotfixes installed using Hotfix.exe,
- Operating system upgrades using Winnt32.exe, and
- Windows Update.

Replacing protected files by means other than these specific methods result in WFP restoring the original files.

In this example, protection is triggered after WFP receives a directory change notification for a file in a protected directory. WFP then determines which file was changed and references the file signature in a catalog file to determine if the new file is the correct version. Normally, WFP replaces the file with the one from the dllcache, but this file was also modified, so WFP then prompts for the CD installation disc since the OS was installed from the CD-ROM. Additionally, these prompts indicate that an admin is logged on since these dialog boxes can only be displayed to an admin.

Without an installation disc available, the user selects Cancel and is prompted with the warning.

Protected Critical System Files

When a Windows operating system is installed on a computer, folders are created where critical system files are placed. These Microsoft Defined WFP-protected critical system files have the following file extensions:

- .dll (Dynamic Link Library),
- .exe (Executable),
- .ocx (Object Linking and Embedding, also known as OLE, control extension),
- .sys (Real-Mode Device Drivers), and
- Some True Type fonts.

Click each extension to learn about the protected files.

.dll: This file extension stands for Dynamic Link Library. An example protected file is Kernel32.dll (Windows Kernel).

.exe:This file extension stands for executable. An example protected file is cmd.exe.

.ocx: This file extension stands for Object Linking and Embedding (OLE) control extension.

.sys: Most .sys files are device drivers, but some are not. Here are some example files: MSDOS.SYS and IO.SYS (Core OS files in MS-DOS and 9x), CONFIG.SYS (Various configuration options and information about what drivers will be loaded), COUNTRY.SYS, etc.

Some True Type fonts: Micross.ttf - Microsoft Sans Serif True Type Font; Tahoma.ttf - Tahoma True Type Font; Tahomabd.ttf - Tahoma Bold True Type Font.

System File Checker Watcher Thread

WFP includes many components to fulfill its role as Microsoft's built-in integrity and accelerated system file deletion recovery mechanism.

WFP is started by Winlogon through the implementation of two DLLs: sfc.dll and sfc_os.dll. Sfc.dll is a wrapper for most of the file protection routines and acts as a proxy to sfc_os.dll, forwarding any exports to this file. Sfc_os.dll implements a watcher thread to monitor several directories for changes to key drivers, executables, and DLLs listed in the sfcfiles.dll. It uses the functionality of NTFS to detect changes to protected files.

Upon receipt of a change notification, sfc_os.dll passes the information to wintrust.dll, which verifies that the file is digitally signed. Subject Interface Packages (SIPs), in this case SHA-1 hashes, build the modified file. Note, this is not a hash of the whole file, rather this is a hash created from Microsoft proprietary file constructs. This hash is the file's signature. The file's hash is then compared to the hash for the files stored in CATROOT.

Through this process, the file is evaluated as either valid or not valid. If the file has a valid signature, then sfc_os.dll verifies that there is a good copy of the file stored in the dllcache folder. If a copy of the verified file is stored in the dllcache folder and its signature matches, no further action is taken. If a copy of the verified file is not present in the dllcache folder, then a copy of the verified file is saved into the dllcache folder, and the CATROOT directory is updated. If a copy of the verified file is present in the dllcache folder, but the signature of the copy is invalid, then the invalid file is replaced with a copy of the verified file and the CATROOT directory is updated.

If the operating system was installed via a network connection, then it checks to see if the network path is still valid and if the file can be located. Next, it checks the system's local removable media devices (such as CD-ROMs and DVD drives) for an installation disc. If the installation media is not found, then the user is prompted to install the installation media onto a drive (but only if the user is logged in with adminstrator credentials). Once a copy of the file has been located, sfc_os.dll copies the file to the protected file's appropriate location of \Windows\System32, writes a copy of the file into the dllcache folder, and updates the CATROOT directory with the correct hash of the file.

SfcFiles.dll is a database of Unicode strings, each one containing a filename and its path, which is protected under WFP. The Strings command, Sysinternals, can be used to view a list of protected files contained in sfcfiles.dll.

System File Checker (sfc.exe) is a command-line utility. At the end of a Graphical User Interface (GUI)-mode setup, sfc.exe scans all protected files to verify that they were not modified by other programs being installed during the unattended installations. If any are missing or damaged, WFP renames the affected catalog file and retrieves a cached version from the cache folder, or requests a new copy if it cannot retrieve a copy.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Protection Mechanisms: Section 3 Transcript

WFP and WRP Tools

1/3

There are several tools that are useful for viewing and manipulating files affiliated with WFP and WRP.

Sigcheck, part of MS Sysinternals, is the name of Windows' file-signature verification tool. It is a command-line utility that shows file version number, timestamp detail, and digital signature detail including certificate chains. Just like a credit card signature machine, sigcheck looks for and compares a file's signature to the original signature to ensure nothing unusual is going on.

But how does a signature even get attached to a code in the first place? That's where signtool, available with Microsoft Windows Software Development Kit, comes into play. Signtool is a command-line tool that digitally signs files, verifies signatures in files, and time stamps files.

Finally, the System File Checker tool (SFC.exe) performs a full-body scan of the system for protected files, or can set up the system to perform a scan in the next boot. This is done by setting the appropriate SFC values in the Windows subkey.

Check out the Windows Protection Mechanisms document in Resources to see a list of the command-line options for SFC.

WFP and WRP Registry Entries

2/3

For both WFP and WRP, the Registry Session Manager, HKLM\System\CurrentControlSet\Control\Session Manager, maintains a location for storing file names to be renamed and defines how the system determines whether to allow the file to be renamed.

The Session Manager adds entries in the PendingFileRenameOperations subkey of files pending a name change, if the named file is in use. The entry contains pairs of file names, wherein the first name of the pair is changed to be the same as the second name. These file names are maintained in the PendingFileRenameOperations subkey until the system is rebooted and the files are renamed. The AllowProtectedRenames subkey must be set to 1 before the PendingFileRenameOperations subkey does its job of renaming the files.

Exercise Introduction

3/3

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Protection Mechanisms: Section 4 Transcript

Windows Resource Protection (WRP) 1/6

Windows Resource Protection (WRP) became available with Windows Server 2008, Windows Vista, and later versions. It replaced WFP in Windows Server 2003, Windows XP, and Windows 2000. It was implemented to ensure the integrity of critical system files, and expanded the protection as the next generation WFP by the amount, type, and location of critical Operating System artifacts. While WFP is reactive, WRP is proactive and provides protection based on access control. Permissions for full access to modify WRP-protected resources is restricted to the TrustedInstaller account, and any attempts to modify protected Microsoft-defined critical files are denied by default.

Missing or bad files are replaced from a repository of known good files in the following order:

- The component store (%systemroot%\winsxs\Backup),
- The network install path, if the system was installed using network install, and
- The Windows CD-ROM, if the system was installed from CD-ROM.

How WRP Provides Protection 2/6

WFP is a reactive system that registers for notification of file changes. If changes to a protected system file are discovered, the modified file is restored from a cached copy located in a this compressed folder: %WinDir%\System32\dllcache.

In contrast, WRP is a proactive system that watches for and prevents attempts to replace or modify protected system resources such as files, folders, and registry keys.

This protection is based on Windows DACLs and ACLs that have been defined for the protected resource.

Permission for full access to WRP-protected resources is restricted to TrustedInstaller, and it can only be changed using the following supported resource replacement mechanisms with the Windows Modules Installer service, TrustedInstaller:

- Windows Service Packs,
- Hotfixes,
- Operating system upgrades, and
- Windows Update.

When using WRP, administrators no longer have full rights to system files. Applications and installers must use the SfcIsFileProtected and SfcIsKeyProtected function calls to determine if a file or registry key is protected.

In addition to files, WRP protects critical folders. A folder containing only WRP-protected files may be locked so that only TrustedInstaller can create or modify the files and subfolders in that folder, or the folder may be only partially locked so administrators can create files and subfolders in the folder.

WRP also protects essential registry keys. If a key is protected, all of its subkeys and values are protected, too.

Lastly, WRP copies files that are needed to restart Windows to the cache directory located in the following folder: %WinDir%\Winsxs\Backup. This directory contains copies of only those files needed to restart Windows.

WRP Supported Replacement Mechanisms 3/6

Applications and installers outside of TrustedInstaller that try to replace a WRP-protected resource are denied access and generate an Access Denied error message.

But when Microsoft-trusted, well-known installers try to replace WRP-protected resources, the error message may be suppressed, but no changes are applied to the WRP-protected resource.

The error may be suppressed for a well-known installer only when all of the following criteria are satisfied:

- It is a legacy application. The application does not include a manifest with a requestedExecutionlevel that identifies the application as designed for Windows Vista or Windows Server 2008,
- The Access Denied error is caused only by the attempt to modify a WRP-protected resource, and
- An administrator is installing the application.

Windows Resource Protection File Types 4/6

Here are some of the WRP protected file types. WFP protects around 3,000 files, such as DLLs, EXEs, and a few TTFs. WRP greatly expanded on WFP's scope of protections in both file types and numbers, and WRP also protects critical folders and registry keys.

Windows Resource Protection Components 5/6

Here are the components that Windows Resource Protection uses. Some of these components are the same or similar to those used by WFP, but some are quite different. Click each component to look at their individual roles and responsibilities.

Services.exe: The Service Control Manager Process (Services.exe) loads and initializes auto-start device drivers and Windows services during the boot process.

Sfc.dll: Sfc.dll is the wrapper for most of the file protection routines.

Sfc.exe: A command-line utility. At the end of a Graphical User Interface (GUI)-mode setup, the System File Checker tool (Sfc.exe) scans all protected files to verify they were not modified by other programs being installed during unattended installations. If any are missing or damaged, WRP renames the affected catalog file and retrieves a cached version from the cache folder, or requests a new copy if it cannot retrieve a copy.

Sfc_os.dll: Sfc_OS.dll watches for changes in protected directories. It runs whenever a protected directory is accessed.

TrustedInstaller Account: The only supported way to modify WRP protected files is through the Windows Modules Installer (WMI) service, which can run under the TrustedInstaller account. This service account is used for the installation of patches, service packs, hotfixes, and Windows Update. This account has access to the various protected files and is trusted by the system (as its name implies) to modify critical files and replace them. Administrator and SYSTEM do not have write/delete rights for WRP resources.

DACLs and ACLs: WRP functions by setting DACLs and ACLs defined for protected resources (protected files, directories, and registry keys), so only the TrustedInstaller account is able to modify or delete these files. As an application developer, you can use the SfcIsFileProtected or SfcIsKeyProtected application programming interface (API) to check if a file or registry key is locked down.

Protected Objects: Critical system files, directories, files, and registry keys that are installed as part of the Windows operating system. Microsoft expands that definition of Critical system files to include directories, files, and registry keys affiliated with updates, hotfixes, service packs, signed drivers, and files installed and/or modified by the "TrustedInstaller" account.

Protected Folders: A folder containing only WRP-protected files may be locked so that only the Windows trusted installer is able to create and /or modify files and subfolders in the folder. This folder may be partially locked to enable administrators to create files and subfolders in the folder.

Protected Registry Keys: If a key is protected, all its subkeys and values are protected. WRP copies files that are needed to restart Windows to the cache directory located in %WinDir%\Winsxs\Backup. This directory contains copies of only those files needed to restart Windows.

Wintrust.dll: Provides the core cryptologic functionality required by WRP. Builds SIPs and performs SHA-1 hashes from Microsoft proprietary file constructs. The SIP is a Microsoft proprietary specification for a software layer that enables applications to create, store, retrieve, and verify a subject signature. Subjects include, but are not limited to portable, executable (.exe) images, cabinet (.cab) images, flat files, and catalog files.

Security Catalogs: Microsoft's strategy is to add entries to the catalog files for any service packs, hotfixes, and updates, but never removes entries from the catalog. Note: Do not rename or delete the CATROOT folder!!!! The CATROOT2 folder is automatically recreated by Windows, however, CATROOT is not.

CATROOT: Contains the security catalog files. The cat files contained within are all the base, service pack, and hotfix signatures (SHA-1 hashes) of the protected files. Stores all the Microsoft-signed system-updates since the Windows operating system was first installed on the system.

CATROOT2: Contains the catalog database files. A database within this folder contains a list of all the catalog files in the CATROOT folder so that the system knows which signature (hashes) to verify the files against.

Winsxs/Backup (Cache Directory): Windows Side By Side (WinSxS) is the Windows component store used to replace or repair operating system binaries in the event they become corrupted or compromised instead of the 'dllcache' and 'i386' folders in Windows XP. This is the first location WRP references when attempting to restore a modified protected file. WRP copies files that are needed to restart Windows to the cache directory located at %WinDir%\Winsxs\Backup. The size of the cache directory and the list of files copied to the cache cannot be modified.

Section Completed

6/6

Windows Protection Mechanisms: Section 5 Transcript

Bitlocker 1/5

Bitlocker is a technology that encrypts and protects data on full disks and containers. Bitlocker is currently integrated within many versions of the Windows Operating System, including Windows Vista and 7 Ultimate and Enterprise Editions, Windows 8 through 10 Pro, Enterprise and Education Editions, and Windows Server 2008 and later.

Bitlocker uses AES 128 or 256 bit to encrypt and protect data. It offers the most complete protection when it is used with a Trusted Platform Module (TPM) version 1.2 or newer. However, systems that are without a TPM chip can still take advantage of the benefits of Bitlocker by:

- Implementing the USB Startup key, which contains the Bitlocker encryption key,
- Using the system volume password, on Windows 8 or higher, or
- Entering a PIN during the initial boot process.

Bitlocker Encryption States 2/5

To use Bitlocker to encrypt the volume containing the operating system, the system must have at least two volumes: an unencrypted volume used for booting the system and another encrypted volume which contains the operating system.

The unencrypted volume contains the boot manager and the Boot Configuration Data (BCD). The boot manager reads the boot data from the BCD. The system then starts the boot loader from the system reserved partition, which then loads Windows. Note that during the boot process, the encrypted volume is decrypted in order for Windows to load.

Bitlocker: VHD and Existing Volume Usage 3/5

In addition to encrypting the boot volume, Bitlocker offers users the option of encrypting a Virtual Hard Disk (VHD) or existing volume.

Bitlocker To Go 4/5

"Bitlocker To Go" is a technology that allows users to encrypt external media, such as a USB drive, and restrict access with a password. When the encrypted device is connected to a system which is capable of supporting Bitlocker, the user is prompted for a password. When the user enters the password correctly, they gain access to the data contained on the device.

Exercise Introduction 5/5

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Protection Mechanisms: Section 6 Transcript

Address Space Layout Randomization (ASLR) 1/4

In the past, hackers and malicious users used to target specific and predictable memory locations for exploitation, due to core processes consistently being loaded into the same locations in older versions of Windows. But since the release of Windows Vista, Address Space Layout Randomization (ASLR) has been implemented to randomly arrange the positions of key data areas. This makes it more difficult for an attacker to predict target addresses and write exploits.

In the example shown, you can see that after rebooting a system, various core system processes have moved their memory locations.

Win32 Process Memory Map 2/4

An important result of the ASLR design in Windows Vista+ is that some address space layout parameters, such as PEB, stack, and heap locations are selected once per program execution. Other parameters, such as the location of the program code, data segment, BSS segment, and libraries change only between reboots.

ASLR is complementary to DEP because:

- It randomizes the base of the executable and the positions of libraries, heaps, and stacks in a process's address space,
- It defends against return-to-libc attacks and shellcode injection,
- Memory addresses are obscured from attackers, and the values have to be guessed, which could cause crashes, and
- Security is improved by increasing the search space.

When an application creates a heap in Windows Vista and later, the heap manager creates that heap at a random location. When a thread starts in a process linked with /DYNAMICBASE, Windows Vista and later moves the thread's stack to a random location. DEP/ASLR creates a stronger defense against memory manipulation vulnerabilities by defending against stack and heap overflows and underflows, format string vulnerabilities, array index overflows, and uninitialized variables.

Address-space randomization (ASR) is a promising solution to defend against memory corruption attacks that have contributed to about three-quarters of the USCERT advisories in the past few years.

How it Works 3/4

The ASLR uses a processor Time Stamp Counter (TSC)-derived value as the key-plus algorithm to generate random memory locations for the following:

- The image load offset (EXE/DLL),
- A threads stack location,
- The initial process's heap, and
- Process Environment Block (PEB).

The TSC is a 64-bit register present on all x86 processors since Pentium. It counts the number of cycles since reset.

ASLR randomizes the location of system files and other programs that are often targets of exploits because they have predictable locations.

The random image load offset is determined by a random global image offset set by TSC.

Exercise Introduction

4/4

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Protection Mechanisms: Section 7 Transcript

Data Execution Prevention (DEP) 1/7

Data Execution Prevention (DEP) is a security feature that helps prevent damage from external security threats. It monitors programs to ensure that system memory is being used safely. When DEP notices something unusual happening in a program, such as incorrect memory usage, it stops the program and tells the user about the activity.

Hardware DEP 2/7

There are two types of DEP: hardware and software.

The hardware DEP is also known as No Execute page protection. It occurs at the Central Processing Unit (CPU), and must be supported by the CPU and OS. The CPU marks the memory's Page Table Entry (PTE) to No Execute (NX). Older processors may not support hardware DEP.

Hardware DEP prevents certain types of malware from exploiting bugs in the system through the execution of code placed in a data page, such as the stack.

Software DEP 3/7

Software-based DEP provides specific protections against attacks that function through code exceptions with Structured Exception Handling (SEH). If the program's image files are built with Safe Structured Exception Handling (SafeSEH), then the software-enforced DEP ensures that before dispatching an exception, the exception handler is registered in the function table located within the image file. If the program's image files are not built with SafeSEH, software-enforced DEP ensures that, before dispatching an exception, the exception handler is located within a memory region marked as executable.

Configurable Settings 4/7

The configurable settings for DEP on Windows Service Pack 2 and 3, located in the Boot.ini file, can be queried using bootcfg, and can be set with this command: bootcfg /raw "/noexecute=policy_level".

The configurable settings for DEP on Windows Vista and above are located in BCD, and can be set using bcdedit.exe /set {current} nx policy_level.

Policy Levels 5/7

The DEP configuration is controlled through switches in the Boot.ini file, but if you are logged in as an administrator, then you can go to the System dialog box in the Control Panel to modify the DEP settings.

Windows supports four configurations for hardware DEP and software DEP. They are OptIn, OptOut, AlwaysOn, and AlwaysOff. Microsoft recommends that admins configure DEP to operate in either the AlwaysOn or OptOut setting.

To learn more about these four settings, access the Windows Protection Mechanisms Supplemental Document located in Resources.

Supported OSs

6/7

Different CPUs implement different protection systems. Starting from Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, in the 32-bit versions of Windows:

- AMD chipsets use the No-Execute page-protection (NX) processor feature, and
- Intel chipsets use the Execute Disable Bit (XD) processor feature.

In order for either of these processor features to be active, the processor must be running in Physical Address Extension (PAE) mode, which Windows automatically enables in order to support DEP.

Exercise Introduction

7/7

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Protection Mechanisms: Section 8 Transcript

Credential Guard

1/3

The Credential Guard, a feature introduced in the Windows 10 Enterprise, protects an isolated version of the Local Security Authority (LSA), known as the Local Security Authority Subsystem Service (LSASS).

Prior to Windows 10, the operating system communicated directly with the LSASS, which resided in the process memory. With the advent of Windows 10, the Credential Guard began storing the system's secrets in an isolated LSASS, which is protected by using virtualization-based security and is not accessible to the rest of the operating system.

Windows Defender Application Guard

2/3

Designed for Windows 10, Application Guard provides hardware isolation to the Microsoft Edge and Internet Explorer web-browsers. Using Hyper-V virtualization, untrusted websites will run within a temporary virtualized windows container. This container includes a separate copy of the Windows operating system with the minimum platform services to operate the Edge browser. However, all trusted, or whitelisted, websites will operate normally on the host operating system. Application Guard provides a next-level type experience in-terms of browser isolation, thus thwarting malicious attacks to the Windows system.

Section Completed

3/3

Windows Protection Mechanisms: Section 9 Transcript

Summary

You have completed the Windows Protection Mechanisms module.

During this module, you learned about the various techniques and countermeasures that Windows uses for protection and the tools available to implement them.

You should now be able to:

- Describe Windows File Protection (WFP) & Windows Resource Protection (WRP),
- Discuss the differences between WFP and WRP,
- Explain Address Space Layout Randomization (ASLR),
- Explain Data Execution Prevention (DEP), and
- Identify how Microsoft defines critical system files.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam.

Click the NEXT section button to begin the Module Exam.