FANSHAWE

INFO-6003

O/S & Application Security

Week 08

Agenda

- Protected Processes
- Server Roles
- Server Core
- Security Baselines
- Microsoft Baseline Security Analyzer (MBSA)
- Security Compliance Manager (SCM)

Protected Processes

Protected Processes

- Security principals, or a process running on behalf of a security principal, are assigned an integrity level
- The integrity level is included in the SID
  - Server 2008 has four integrity levels
  - A process with a lower integrity level can not write to a process with a higher integrity level
    - System
    - High
    - Medium
    - Low

Protected Processes

- When a process is protected, other processes or threads with a lower integrity level cannot:
  - Inject a new thread into the process
  - Set or receive context information
  - Duplicate a handle from the protected process
  - Access the memory area of the protected process

Protected Processes

- Windows securable objects can now be assigned an integrity level
  - Files, registry keys etc.
- System objects have high integrity
- Most user services and applications run with medium integrity
- Normal users and applications cannot modify a system object
  - Medium can’t modify high

Protected Processes

- When a security principal (process) attempts to access an object the integrity level in the SID is checked
- If the integrity level is the **same or higher** than the integrity level of the object then the DACL of the object is examined
  - If the integrity level is **lower** no access is granted and the DACL is not examined
- As a result, integrity levels in the SID override DACL permissions

Integrity Levels in SID

- S-1-16-4096
  - SID for Low Integrity Level
- S-1-16-8192
  - SID for Medium Integrity Level
- S-1-16-12288
  - SID for High Integrity Level
- S-1-16-16384
  - SID for System Integrity Level

Protected Processes

- Since IE 7.0
  - in protected mode, IE 7 runs as a low integrity process
  - IE, its add-ons, toolbars, or child process cannot access a higher integrity level process
  - Temporary Internet Files cookies etc. all are marked with low integrity
- Malware that is downloaded on the browser can't break out and change system files
  - Stopped by SID integrity level

Control Flow Guard

- Since Windows 8.1, Microsoft introduced Control Flow Guard
- CFG is an attempt to mitigate the redirection of control flow to an unexpected location
- The O/S closes any program where the target address is invalid
- CFG mitigates a lot of common exploit techniques that overwrite a pointer

Credential Guard

- Windows 10 introduced a feature called Credential Guard in order to prevent credential theft attacks such as Pass-the-Hash
- Instead of storing secrets in the Local Security Authority (LSA), it isolates the data using virtualization-based security
- Remote Procedure Calls are used to interact with the isolated environment

Credential Guard

- Virtualization Extensions are required to use Credential Guard
- Intel VT-x or AMD-V are required to be enabled in the BIOS/UEFI
- A lot of HP laptops ship with Intel VT-x disabled and may also cause problems with VMWare Workstation if the feature is disabled

Credential Guard

- Credential Guard can be managed in several different ways including:
  - Group Policy
  - Command Prompt
  - Windows PowerShell
  - Windows Management Instrumentation (WMI)

Local Administrator Password Solution (LAPS)

- LAPS allows the management of local account passwords to be done by Active Directory
- Only authorized users are able to read the data or request resets
- This is also meant to thwart Pass-the-Hash credential replay attacks
- Stores the local Administrator's password in Active Directory and the computer is able to update it's password information in AD

Server Roles

Server Roles

- How you harden a server operating system will be determined by the Role the server is going perform
- A server could perform a number of roles
  - Web Sever
  - File Server
  - Domain controller
  - DNS
  - DHCP Server
- May have responsibility for a single role or a combination of roles

Server Roles

- Every role is different and requires a different configuration
  - Software or services installed and running
  - Configuration settings
- Prior to Server 2008 many separate and unrelated components had to be configured for a server to perform a specific role
  - e.g. File Server
- Since Server 2008 the administrator chooses the role and Server Manager loads the necessary components

Roles vs. Features

- With Microsoft a Role is a collection of services that enable the server to provide a specific function
- Features are software tools that perform certain tasks, and usually support a role
- Dependencies:
  - Some roles require certain features to work
  - Some features require other features to work
- If there are dependencies, Server Manager will alert you

Server Manager Win2k8R2

Server Manager

File Action View Help

Server Manager (GOZERALPHA)
- Roles
- Features
- Diagnostics
- Configuration
- Storage

Server Manager (GOZERALPHA)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary — Server Summary Help

Computer Information

Full Computer Name:	gozerAlpha.transpire.local
Domain:	transpire.local
Local Area Connection:	192.168.0.66, IPv6 enabled
Local Area Connection 2:	IPv4 address assigned by DHCP, IPv6 enabled
Remote Desktop:	Enabled
Server Manager Remote Management:	Enabled
Product ID:	55041-507-7012443-84234 (Activated)

Do not show me this console at logon

- Change System Properties
- View Network Connections
- Configure Remote Desktop
- Configure Server Manager Remote Management

Security Information

Windows Firewall:	Domain: Off
Windows Updates:	Install updates automatically using Windows Update
Last checked for updates:	Today at 12:49 AM
Last installed updates:	12/10/2015 3:04 AM
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users

- Go to Windows Firewall
- Configure Updates
- Check for New Roles
- Run Security Configuration Wizard
- Configure IE ESC

Last Refresh: Today at 5:11 AM Configure refresh

Roles and Features

Server Manager

File Action View Help

Server Manager (GOZERALPHA)
- Roles
- Features
- Diagnostics
- Configuration
- Storage

Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary — Roles Summary Help

Roles: 4 of 17 installed

- Active Directory Domain Services
- DNS Server
- File Services
- Network Policy and Access Services

Add Roles
Remove Roles

Active Directory Domain Services — AD DS Help

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status — Go to Active Directory Domain Services

Messages: 1
System Services: 8 Running, 2 Stopped
Events: 4 informational in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 1 installed — Add Role Services, Remove Role Services

Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed

Last Refresh: Today at 5:08 AM Configure refresh

Dependencies

Server Roles

- Server2008 R2 Enterprise has 18 Roles and 35 Features
- Example Roles:
  - Active Directory Domain Services
  - DHCP Server
  - Web Server (IIS)
- Example Features:
  - BITS (Background Intelligent Transfer Service)
  - Multipath I/O
  - Remote Assistance
  - .NET Framework

Adding Roles and Features

- On Server 2008 all the code required for a role or feature is copied to the hard drive during installation
  - Just not in the final location required
  - Stored in %systemroot%\winxs
- This prevents the need to have the installation media handy when adding roles or features

Adding Roles and Features on Server 2012

- On Server 2012 the code for all roles and features is not copied during installation
- Administrators have the ability to download the required files directly from Microsoft or a network location
- This also prevents the need to have the installation media locally when adding roles or features on Server 2012

Server 2012

- Although Server 2012 is the most secure Windows Server O/S, organizations tend to drag out the time to upgrade their systems
- One of the issues with Server 2012 is that it does not support software such as Exchange 2010 and SharePoint Server 2010

Server Core

Server Core

- Appeared as a separate edition with Server 2008
- Since Server 2008 R2 server core is now an installation option and can be used with any edition
  - Standard
  - Enterprise
  - Datacenter

Server Core

- Goal was to eliminate any services and other features that are not essential for the support of certain commonly used server roles
  - Reducing the attack surface
- Stripped down version with very limited Graphical User Interface
  - No Windows Explorer or Internet Explorer
  - No Windows Media Player or other consumer related programs

GUI Applications

- This is a list of all the GUI applications available in Server Core

GUI Application	Executable with Path
Command prompt	%WINDIR%\System32\Cmd.exe
Microsoft Support Diagnostic Tool	%WINDIR%\System32\Msdt.exe
Notepad	%WINDIR%\System32\Notepad.exe
Registry Editor	%WINDIR%\System32\Regedt32.exe
System Information	%WINDIR%\System32\Msinfo32.exe
Task Manager	%WINDIR%\System32\Taskmgr.exe
Windows Installer	%WINDIR%\System32\Msiexec.exe

Server Core Roles in 2008 R2

- Only 9 of 18 available in Enterprise Edition
  - AD Domain Services
  - AD Lightweight Directory Services
  - DHCP Server
  - DNS server
  - File Services
  - Hyper-V
  - Print Services
  - Streaming Media Services
  - Web Server (IIS)

Server Core Features in 2008 R2

- Only 10 of 35 available in Enterprise Edition
  - BitLocker Drive Encryption
  - Failover Clustering
  - Multipath IO
  - Network Load Balancing
  - Removable Storage Manager
  - SNMP Services
  - Subsystem for UNIX-based Applications
  - Telnet Client
  - Windows Server Backup Features
  - WINS Server

Server Core 2008 / 2008 R2

- Transitioning between the Full Server installation and Server Core in 2008 and 2008 R2 requires the Administrator to reinstall the O/S
- This can be troublesome if you wish to change it later on

Server Core 2012

- Transitioning between the Full Server installation and Server Core in 2012 can be done without reinstalling the Operating System
- One of the improvements since Windows Server 2008 and 2008 R2

Security Baselines

Security Baselines

- Security Baselines are a great guide to hardening the Operating System
- Specifications for how hardening should be done
- Different for different operating systems
- Different for different types of servers (webservers, mail servers, etc.)
- Needed because it is easy to forget a step

Security Template

- There are thousands of security settings
- To aid in securing both servers and workstations; various companies and organizations have developed security templates
  - Microsoft, SANS, CIS, NSA
  - These can be imported into the O/S and applied to the system, or used to compare the existing O/S settings to the template

Security Templates

- Template is an ASCII text configuration file
- Typical security settings
  - Password policies
  - Account lockout policies
  - Audit policies
  - Kerberos policies
- Microsoft Management Console – MMC
  - Has security template snap-in to view settings

MMC Snap-In

- Can be used to apply a template to the computer
- Settings should be tested on non-production environment machines
- You can compare your systems settings to the template without making any changes
- One limitation of this method is that you can’t apply the template across the network, you have to be on the local machine

Current Templates

- Since Server 2008, there are only 3 default templates, and only 2 of them are really used
  - Defltbase.inf (not really used)
  - Defltsv.inf (for servers)
  - Defltdc.inf (for DCs)
- These files are located at the following location on Windows Server 2008 and 2008 R2:
  - %systemroot%\inf.

Best Practice Analyzer

- BPA can be run on individual Roles to determine if they are properly configured
  - Meeting Microsoft's guidelines for best practices
- After running the scan you will get a list of alerts based on your current configuration
  - Error: the role is noncompliant and this is a critical problem or misconfiguration
  - Warning: the role is noncompliant
  - Compliant: the role meets current best practices
- You can exclude results you don't want to see again

Best Practice Analyzer

Best Practices Analyzer: 8 noncompliant; 0 excluded; 33 compliant Last Scan: 5/28/2014 2:28:20 PM

Noncompliant (8) | Excluded (0) | Compliant (33) | All (41)

Severity	Title	Category
Error	The PDC emulator master S2008-ismiley2.smiley.ca in this forest s...	Configuration
Warning	All domains should have at least two functioning domain controller...	Operation
Warning	The directory partition DC=smiley,DC=ca on the domain controlle...	Configuration
Warning	The directory partition CN=Configuration,DC=smiley,DC=ca on t...	Configuration
Warning	The directory partition CN=Schema,CN=Configuration,DC=smiley...	Configuration
Warning	The directory partition DC=DomainDnsZones,DC=smiley,DC=ca o...	Configuration
Warning	The directory partition DC=ForestDnsZones,DC=smiley,DC=ca o...	Configuration
Warning	The domain controller S2008-ismiley2.smiley.ca should comply wit...	Configuration

- Scan This Role
- Exclude Result
- Include Result
- Properties
- Copy Result Properties
- Help

Security Configuration Wizard

- Available since Server 2003 SP1
  - Only used for Server OSs
- Used to analyze a system and recommend changes
  - Running Services
  - Firewall Rules
  - Registry Settings
  - Audit Policies
  - Etc.

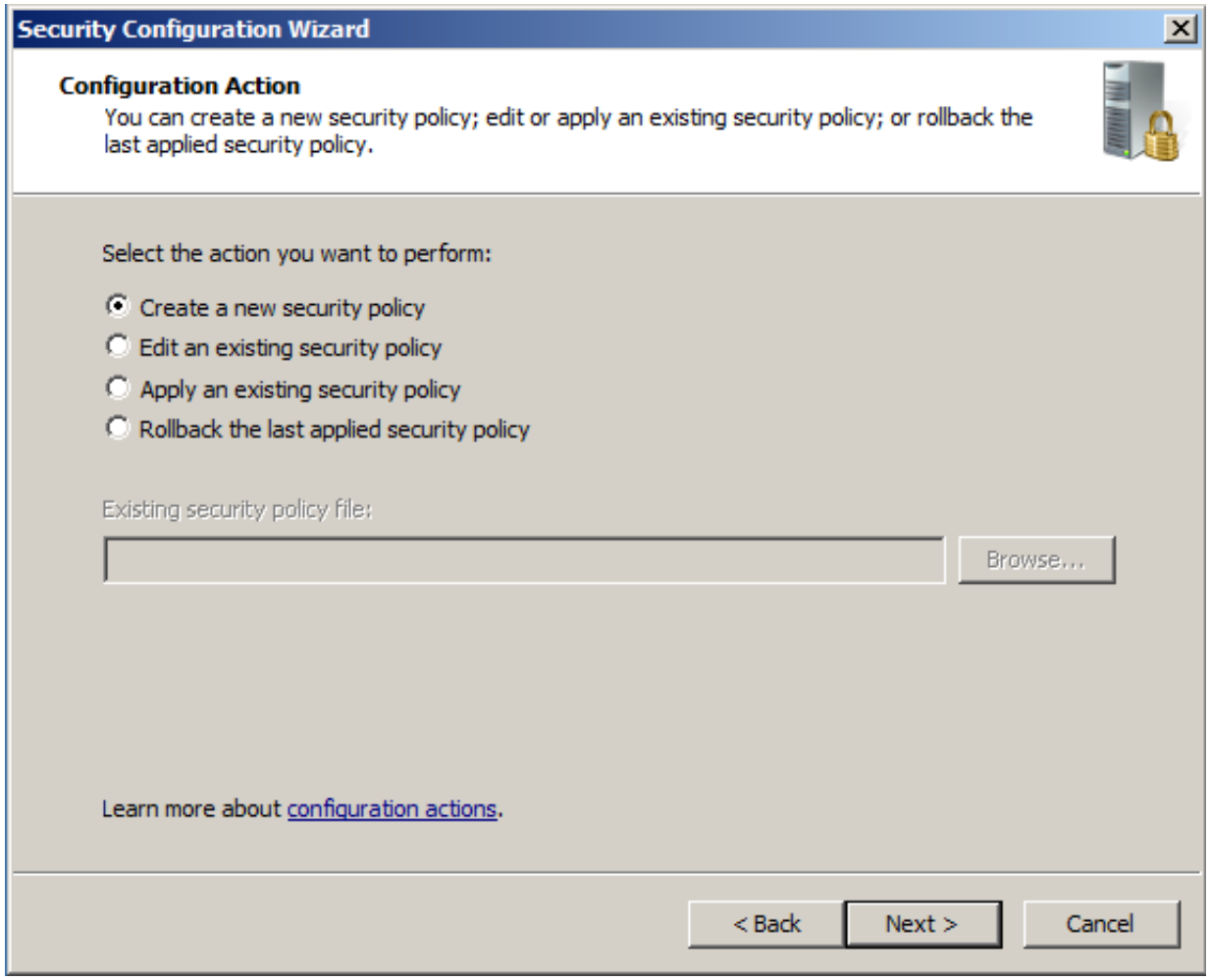
Security Configuration Wizard

- Helpful in configuring a server for a specific role
  - All services not required for the chosen Role are disabled
  - Ports not required for the role are blocked
  - Reduces exposure to SMB, LanMan & LDAP protocols risks
  - Limits IIS web extensions if not applicable to the Role
- Can be used to create a template the can be applied to other servers

Security Configuration Wizard

- You can deploy security policies that you create with SCW through Group Policy
- SCW does not install or uninstall the components necessary for the server to perform a role, rather configures the installed components
  - You install role-specific components through Server Manager.
- SCW detects role dependencies
  - If you select a role, it automatically selects dependent roles
- All applications that use the IP sockets must be running on the server when you run SCW

Security Configuration Wizard



Security Configuration Wizard

- The scwcmd command is used to convert existing SCW policies/templates into GPOs
- After running the command, the GPO will appear in the Group Policy Management Console
- The GPO can then be linked to a Site, Domain or OU, or other container
  - If you use SCW to create a policy/template for your Domain Controllers, you can convert it to a GPO and link it to the Default Domain Controllers OU / Container

MBSA

MBSA

- Microsoft Baseline Security Analyzer
- Tool to help secure the Windows operating system
  - Server and Workstation computers
- GUI and command line options
- Checks for common configurations errors
- Checks for Missing security updates
- Free download
  - www.microsoft.com/mbsa

MBSA

Microsoft Baseline Security Analyzer 2.2

Microsoft
Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: FOLusername\user (this computer)

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- [x] Check for Windows administrative vulnerabilities
- [x] Check for weak passwords
- [x] Check for IIS administrative vulnerabilities
- [x] Check for SQL administrative vulnerabilities
- [x] Check for security updates
  - [ ] Configure computers for Microsoft Update and scanning prerequisites
  - [ ] Advanced Update Services options:

Start Scan | Cancel

MBSA

- Scans 5 areas
  - Security updates
  - Windows administration vulnerabilities
  - IIS vulnerabilities
  - SQL vulnerabilities
  - Weak passwords

MBSA

- Security Updates
  - Security updates for IIS, SQL & Exchange
  - Internet Explorer security updates
  - Media player & MS Office security updates
- Weak passwords
  - Blank or simple passwords
  - Account password expiration
  - Number of administrator accounts
  - Guest account enabled
  - Restrict Anonymous Registry key settings

MBSA

- IIS Checks
  - Is the lockdown tool running
  - Are the sample applications & Admin virtual folder installed
  - Is scripts virtual directory installed
  - Is IIS logging enabled
  - Is IIS running on domain controller

MBSA

- SQL Checks
  - Is Administrators group assigned to the Sysadmin role
  - Is CmdExec role restricted to Sysadmin
  - Blank or simple passwords on SQL Server accounts
  - Does everyone group have access to SQL server Registry keys
  - Does Guest account have database access
  - Access permissions on SQL installation folders
  - Is SQL server running on a domain controller

MBSA

- Windows administration vulnerabilities
  - Internet Explorer zone settings for each local user
  - IE enhanced security setting for Administrator & non administrator accounts
  - Office product security zone settings for each local user
  - Restrict anonymous settings
  - File system type (FAT32 or NTFS)
  - Firewall status
  - Automatic update status
  - List shares and unnecessary services

Security Compliance Manager

SCM

- Security Compliance Manager
- Used in larger deployments
- Very powerful tool that allows organizations to configure and manage servers and workstations centrally
  - Matching them to predefined baselines
- Ties in with Group Policy and SCCM
  - System Center Configuration Manager

SCM

- Basic Features
  - Security settings are configured/documented in security baselines
    - Based on Microsoft security guide recommendations and industry best practices
    - Similar to templates
  - Security configurations are deployed using Group Policy
  - Security configurations are checked/verified/audited using DCM packs via SCCM
    - Desired Configuration Management

Homework

- Deploying Windows Server 2012

http://windowsitpro.com/windows-server-2012/windows-server-2012-deployment-roles

- Deploying Windows Server 2016

https://blogs.technet.microsoft.com/ausoemteam/2015/06/29/windows-server-essentials-microsoft-online-services-integration-versus-azure-active-directory-connect/

- Security Configuration Wizard

https://technet.microsoft.com/en-us/library/cc754997.aspx

- Local Administrator Password Solution

https://www.microsoft.com/en-us/download/details.aspx?id=46899

- Protect derived domain credentials with Credential Guard

https://technet.microsoft.com/en-us/library/mt483740%28v=vs.85%29.aspx

Lab 06 – MBSA, BPA, & SCW

Lab 06 Details

- Make sure you are taking snapshots
  - Otherwise you may have to redo your labs to recreate the required environments
- Set up MBSA on the domain from the GUI and the command line
- Use Microsoft's best practice analyzer
- Use SCW to create a baseline, then deploy it through a GPO

NON GENUINE SOLUTION

- Slmgr –rearm
-