DRSS CyberPatriot

Windows Server 2008 Checklist

**Before Competition**

* Identify personal computer assets for competition
* Develop competition schedule … only five competitors at any one time
* Confirm VMWare Version 6.07
* Identify latest operating system service packs
* Find service pack locations and download
* Identify patches for any applications
* Research Vulnerability Databases for possible competition vulnerabilities
  + National Vulnerability Database
  + Open Sourced Vulnerability Database
  + Vulnerability Notes Database
  + Others
* **Develop and test \*.inf script file**

**Competition Start**

**\*\* Study the Competition Read Me File and Forensics Questions \*\***

Type of system … what files, processes and services are appropriate?

Who are authorized users?

Other

Answer forensics question first if possible

* Run \*.inf script file
* Check Broadcast message on scoring engine screen

**Update System**

* Set Automatic Windows Update … do not install all optional updates unless needed
* Latest service packs (sometimes must be installed manually) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Update Third Party Applications (Adobe, Firefox, Flash, Notepad ++, etc.)**

**Antivirus/Antispyware (antimalware)**

* If not installed, install a version available to you (Microsoft Security Essentials)
* Update signatures

**Action Center**

* Configure Backup Utility
* Security Settings

**Remove unnecessary Windows features (depends upon README file)**

* Games
* Indexing Service
* Internet Explorer
* Internet Information Service
* Internet Information Service Hostable Web Core
* Media Features
* Microsoft .NET Framework 3.51
* MANY OTHERS POSSIBLE

**Configure Firewall**

* Windows Firewall
* Possible Firewall Exception (depending upon particular configuration)
  + File and printer sharing
  + Remote assistance (usually disabled)
  + Remote desktop (usually disabled)
  + UPnP framework (usually disabled)
  + Others
* Advanced Firewall Considerations
  + Network connection settings
  + Security logging
  + ICMP
  + Default settings

**Account Policy**

* Remove Unauthorized Accounts
* Authorized User accounts
  + Ensure accounts are running at least privilege level
  + Check for Guest Account (disable if not needed)
    - USUALLY DISABLE
    - If not disabled
      * Rename
      * Deny network access
      * Shutdown not permitted
      * Deny event log access
* Account Lockout Policy
  + Duration
  + Threshold
  + Account lockout counter reset value
* User Access Control (UAC) Set
* Page file is cleared at shutdown

**Password Policy**

* Accounts Password Protected
* Maximum Password Age
  + User accounts 90 days
  + Administrator account 30 days
* Minimum password age > 0 (recommend 5 days)
* Minimum Password Length >= 8 characters
* Password history – 5 passwords remembered
* Strong Passwords
  + Password complexity enabled
  + Reversible encryption disabled
* Screen Saver Password Protected and Timeout Set
* User cannot use same password when it expires
* Ensure passwords expire
* Check administrative account names (account names should not be root, admin, administrator, etc)
  + Obfuscate the account
  + Change password
  + Audit for weak passwords (john the ripper)
* Blank Passwords Limited to Console Access Only
* **Encrypt files if needed**

**Security Settings**

* Require Ctrl-Alt-Del to Login
* Check System Auditing (ensure it is set at required, if not standard, use DISA STIG)
  + Audit account logon events – enable to prevent random hacks or stolen passwords
  + Audit object access – enable to prevent improper access to sensitive files
  + Audit process tracking – enable to monitor attempts to modify program files to help detect virus outbreaks
  + Account management - enable to see if a change has occurred to an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group
  + Directory service access – enable to track accesses to an Active Directory® directory service object that has its own system access control list (SACL)
  + Logon events – enable to see when someone has logged on or off to the computer
  + Privilege use – enable to see when someone performs a user right
  + Policy change - enable to see attempts to change local security policies, user rights assignments, auditing policies, or trust policies
  + System events - enable to see when someone has shut down or restarted the computer, or when a process or program tries to do something it does not have permission to do
  + Recommended Audit Policy Settings
    - Windows 7 and Windows Server 2008 Users
      * Account logon events
      * Account management
      * Logon events
      * Policy change
      * Process tracking
      * System events
    - Windows Server 2008 Users Only
      * Directory service access
      * Object access
      * Privilege use
* Remove “everyone” access to computer
* UAC detect application installation and prompt for elevation setting enabled
* Restrict anonymouos access to named Pipes and Shares enabled
* Allow system to be shutdown without having to login in disabled
* RDP network level authentication enabled
* User must type CTRL+ALT+DEL to login
* Users are no longer allowed to install print drivers
* Automatic administrative logon at recovery console is disabled
* Internet Explorer Enhanced Security Configuration is enabled
* File sharing and permissions (drives, program files, other)
* **Server Backup Installed**

**Prohibited Files**

* View Hidden Files
* Target search based on README File and forensics question
* File Extensions
  + Audio - .mp3, .wma, .wav, .ra, .mpa, .mid, .m4a, .m3u, .iff, .aif + others
  + Video - .wmv, .vob, .swf, srt, .rm, .mpg, .mp4, .mov, .m4v, .flv, .avi, .asx, asf, .3gp, .3g2 + others
* Empty Recycle Bins
* **Check for illegal software archives (Nikto, NMAP and others) - .xml, .html,. .nbe, .csv or .txt files**

**Unnecessary Services**

* Task Manager
  + Applications
    - Close nonessential/harmful
    - Check associated processes ([www.processlibrary.com](http://www.processlibrary.com))
  + Stop & Disable Unnecessary and Insecure Services
    - IIS – web server capabilities
    - NetMeeting Remote Desktop Sharing - VoIP
    - Remote Desktop Help Session Manager
    - Remote Registry – allows remote users to edit registry
    - Routing and Remote Access - allows the system to be used as a router
    - Simple File Sharing
    - SSDP Discovery Service – plug and play
    - Telnet – allows remote users to log on
    - FTP – File Transfer Protocol
    - Universal Plug and Play Device Host – installation of plug and play devices
    - Windows Messenger Service – not necessary to use windows instant messenger; allows ‘netsend’ command to be used
    - SNMP Trap service
    - TFTP Server removed
    - Apache
    - World Wide Web Publishing
  + Performance Tab
  + Networking Tab
  + Users Tab
    - Terminate user’s connection
    - Logoff users

**Malware**

* Check Installed Programs
  + Control Panel > Programs > Programs and Features
  + C:\Program Files & C:\Program Files(X86)
  + Search for \*.exe files
* Vulnerability Scanners
  + Microsoft Baseline Security Analyzer
  + Malwarebytes
  + NESSUS
  + Microsoft Malicious Software Removal Tool
  + Open Port Check
    - NMAP – Check for open ports (nmap –sT <ip range> and nmap –sU <ip range>
    - Netstat
    - FPort
    - PsKill
  + Belarc Advisor
  + SHAVLIK LIMITED
* Check Start Up Configuration

**Access Control**

* SAM Accounts & Shares – Anonymous enumeration
* Last User Name Not Displayed on login
* Check Remote Desktop Sharing (README)
* Check Remote Registry

**File & Folder Characteristics**

* Check File Ownership (if needed)
* Check File Sharing … especially “everyone” pemissions
* Folder Permissions
* Check hosts file

**Security Configuration**

* Windows 2008 – Run Security Configuration Wizard (install Security Compliance Manager)
* Windows 2000/Vista/XP – Run Security Configuration and Analysis/Apply GPOs

**Validate Patching/Security configuration**

* Run Vulnerability Scans again and check results against previous results
* Run Secunia again
* Check Broadcast message on scoring engine screen

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Miscellaneous Information**

**Administrative Tools** (control panel to performance & maintenance to administrative tools)

* Local Security Policy
  + Password policy
  + Account lockout policy
  + Audit policies
  + Directory service access
  + Logon events
  + Privilege use
  + Policy change
  + System events
  + Remove “everyone” access to computer

**Performance monitoring** (Menu Bar -> Click Task Manager -> Applications Tab)

* + Allows you to see what processes may be over utilizing resources or not functioning properly
  + Monitor processes to see if unknown programs are running
  + Identify and diagnose the source of current system problems, or help you predict potential system problems
  + A common target for malware
    - Some malware processes (rootkits) will prevent themselves from being list in the task manager making them harder to detect
  + The Users tab
    - Shows all users currently logged into the system
    - Users can be disconnected and/or logged off via this tab
  + Sysinternals
    - A third-party tool that helps manage, troubleshoot and diagnose Windows systems and applications
    - File and disk utilities
    - Networking utilities
    - Process utilities
    - Security utilities
    - System information utilities

**Check file system**

* + Windows
    - Check Task Manager to examine .exe files or unknown processes running
    - Check ‘Startup’ to examine.exe files
    - Monitor .dll changes.

**Monitor open ports**

* + Free tools available for both linux and windows (i.e.,wireshark)
  + Trojan horse scanners typically attempt connections on high-numbered ports