DRSS CyberPatriot

Windows 7 Checklist

4 October 2017

Before Competition

Update Checklist

- Download and review latest Center for Internet (CIS) Security Benchmark
- Install DISA STIG viewer on pre-competition computer
- Download DISA STIG Manuals (*.xml files)
  - Open STIG viewer
  - Review … update checklist

Custom Security Tools Development

- Develop Custom Setup (*.inf) Files
- Run Security Compliance Manger
  - Install Microsoft Security Compliance Manager on research computer
  - Download the latest SCM Baselines for Windows 7
  - Tailor SCM baselines

Create Competition Flash Drive

- Prepare Competition Flash Drive (separate folders)
- DISA STIG setup (*.inf) files
- Custom Security Templates
- MS Security Compliance Manager (SCM) Baselines
  - Install LGPO utility and scripts on flash drive
  - Transfer SCM Baselines as GPO backups to flash drive
- Service Pack
- Application Updates
- Nessus
- Freeware Security Tools
  - Microsoft Baseline Security Analyzer
  - Malwarebytes
  - Others

Other Preparations

- Identify personal computer assets for competition
- Develop competition schedule … only five competitors at any one time
- Confirm VMware Workstation 12.5.7
- Download CyberPatriot Training Briefings before start

- Study past vulnerabilities
- Install and configure Nessus on host computers

****

Competition Start

- ☐ Study the Competition README File and Forensics Questions
  - Type of system … what files, processes and services are appropriate?
  - Who are authorized users?
  - **Answer the forensics questions if possible**
- ☐ Check system date and time. Correct if necessary.
- ☐ Check Broadcast message on scoring engine screen

- ☐ Run DISA STIG (*.inf) Files
  - Record vulnerabilities
  - **Delete image and open another**

- ☐ Apply Custom Setup (*.inf) Files
  - Record vulnerabilities
  - Delete image and open another if necessary

- ☐ Apply Security Compliance Manager Baselines
  - Record vulnerabilities
  - Delete image and open another if necessary

- ☐ Automated Security Tools
  - Microsoft Baseline Security Analyzer
  - Malwarebytes
  - Run Nessus scans
  - CIS CAT-Lite Scanner (Windows 10 & Ubuntu 16 only)

Account Policies

(Microsoft Management Console (mmc) and secpol.msc)

- ☐ Secure Built-in Administrator Account
  - Change name
  - Add password
- ☐ Remove all from administrator group who do not belong
- ☐ Remove Unauthorized Accounts
- ☐ Authorized User accounts
  - Ensure accounts are running at least privilege level
  - Remove unnecessary accounts from the Administrators Group
  - Check Guest Account (disable if not needed)
    - USUALLY DISABLE (check README file)
    - If not disabled

- Rename (rename even if disabled)
- Deny network access
- Shutdown not permitted
- Deny event log access

- ☐ Accounts Password Protected
  - Password characteristics (three of following)
    - Numbers
    - Lower case letters
    - Upper case letters
    - Symbols
    - Symbols in the MIDDLE
- ☐ Password Policy
  - Password history: 5 passwords remembered
  - Maximum password age
    - User accounts 90 days
    - Administrator account 30 days
  - Minimum password age: 10-30 days
  - Minimum password length >= 10 characters
  - Strong Passwords
    - Password complexity enabled
    - Reversible encryption disabled
- ☐ Account Lockout Policy
  - Duration: 30 minutes
  - Account lockout threshold: 3-10 invalid login attempts
  - Account lockout counter reset value (Secure Account Lockout Observation Window): 30 minutes
- ☐ 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
- ☐ NTLM hash is not stored on next password change
- ☐ **Disable AutoPlay**

Audit Policy

- ☐ Ensure audit policy settings are configured correctly
- ☐ Audit Policy Settings (Windows 7)
  - Audit account logon events — Success, Failure
  - Audit account management — Success, Failure
  - Audit logon events — Success, Failure
  - Audit policy change — Success, Failure
  - Audit process tracking — Success, Failure
  - Audit system events — Success, Failure

- ☐ Audit Policy Settings (Windows 2008 Server)
  - Audit account logon events — Success, Failure
  - Audit account management — Success, Failure
  - Audit directory service access — Success, Failure
  - Audit logon events — Success, Failure
  - Audit object access — Success, Failure
  - Audit policy change — Success, Failure
  - Audit privilege use — Success, Failure
  - Audit process tracking — Success, Failure
  - Audit system events — Success, Failure
- ☐ Monitor Event Viewer
  - Applications
  - Security
  - Setup
  - System
  - Forwarded Events

Action Center

- ☐ Enable Messages for All Categories
- ☐ Install Antivirus/Antispyware (anti-malware) if not installed
  - Microsoft Security Essentials for Windows 7/Vista
  - Window Defender for 8, 8.1 and 10
  - Ensure signatures are up to date
- ☐ Configure Firewall
  - Activate all three (Home, Public and Work)
    - Customize settings for each type of network (e.g. Home, Public. Work)
    - Select to be notified when the firewall blocks a program
  - Enable any Firewall Exceptions (depending upon particular configuration)
    - Add trusted programs to Firewall Exceptions List
    - Avoid opening entire port
  - Common Exceptions
    - Core Networking
    - 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

Configure Backup Utility

- ☐ **Schedule automatic "full backups" (weekly) … use thumb drive**
- ☐ Could create a system repair disc

- Could create system image backup

File/Folder Permissions & Security

- Folder Permissions
  - C Drive
    - Adminstrators & System – all permissions
    - Users – (1) Read & execute, (2) List folder contests and (3) Read
  - Review subfolders for sensitivities
  - Only SYSTEM, Administrators and Owner should have "Full Control" and "Modify" permissions
- Encrypt MS Office Files (Word, Excel, Powerpoint or Access)
- **Encrypt other sensitive files with 7-Zip**
- Check hosts file
- Check Ownership
- Remove file sharing unless README indicates otherwise
- Check C Drive Sharing … especially "Everyone Group" sharing
  - Unless there is a good reason do not share drives

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**

Automated Vulnerability Tools

- Customize the start menu to add administrative tools
- Update folder options
  - Show hidden files, folders, or drives
  - Show file extensions
- Check Broadcast message on scoring engine screen
- Other

Security Settings (should be set through *.inf Setup Files)

- 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

Unnecessary Applications, Processes and Services

- Task Manager
  - Applications Tab - Close Nonessential/Harmful Applications
  - Processes Tab
    - Close Nonessential
    - Check associated processes (www.processlibrary.com)
    - Malware
      - Stop process
      - **Delete files with related name**
  - Services Tab
    - Stop & Disable Unnecessary and Insecure Services
      - Internet Information Services – 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
- DNS
- FreeSSD
- PS3 Media Server
- RPC Locator
- RIP Listener
- SNMP
- SMTP
-

  - Performance Tab
  - Networking Tab
  - Users Tab
    - Terminate user's connection
    - Logoff users

Malware

- ☐ Check Task Manager Processes
  - Stop malware process
  - **Search for and remove all related files**
- ☐ Check Installed Programs
  - Control Panel > Programs > Programs and Features
  - C:\Program Files & C:\Program Files(X86)
  - Search for *.exe files
- ☐ Vulnerability Scanners
  - 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
- ☐ Remove log.txt files and associated programs (Fishdown, Hotbar, etc.)
- ☐ Remove malware (check appendix)
- ☐ Remove malware data archives (Nikto, NMap etc.)

Access Control

- ☐ SAM Accounts & Shares – Anonymous enumeration (disable or enabled depending upon README
- ☐ Last User Name Not Displayed on login
- ☐ Check Remote Desktop Sharing (README)
- ☐ Check Remote Registry
- ☐ Check for AOL toolbar
- ☐ Remote access to CD drives
- ☐ Drive and folder sharing and permissions checked
- ☐ Logon Policy
    - Limit local use of blank passwords to console only
    - Message text for users attempting to logon set
    - Switch to the secure desktop when prompting for elevation
    - Do not require CTRL+ALT+DELETE
    - Last user name is no longer displayed when logging in
    - Disconnect clients when logon hours expire
    - Disable Let everyone permissions apply to anonymous users

Patch System (This can take a long time … do last)

- ☐ Set Automatic Windows Update … do not install all optional updates unless needed
    - Check for updates daily and automatically install
    - May accomplish other checklist items during update
- ☐ **May need to repeat update process several times to find all**
- ☐ Latest service packs (sometimes must be installed manually)
- ☐ Update any Microsoft products
- ☐ Replace Internet Explorer with Chrome or Firefox if permitted
- ☐ Update Third Party Applications from flash drive or Internet
    - Internet Explorer
    - Flash Player

Validate Patching/Security configuration

- ☐ Run Vulnerability Scans again and check results against previous results
- ☐ Run Nessus scans
- ☐ Check Broadcast message on scoring engine screen

Miscellaneous

- ☐ Unlock locked user account