DRSS CyberPatriot

Windows 8/8.1 Checklist

[Differences](Windows%208%20and%20%208.1%20Differences.pptx)

**Before Competition**

* [Windows 8 & 8.1 Overview](Windows%208%20&%208.1%20Overview.pptx)
* Identify personal computer assets for competition
* Develop competition schedule … only five competitors at any one time
* Confirm VMWare Version 6.07
* [Windows 8 & 8.1 do not have service packs. Windows update sufficient](file:///C:\Users\famle\Documents\CyberPatriot\Checklists\DRSS%20Checklists\Windows%20Checklists\Windows%208%20&%208.1\Latest%20Windows%208%20&%208.1%20Checklist\Service%20Packs.ppt)
* Download CyberPatriot Training Briefings for reference
* Ensure possession of latest past vulnerability history
* [Develop and test security templates for Windows 8 or 8.1](Custom%20Security%20Template.pptx)
* [Download DISA STIG files](DISA%20STIG%20Files.ppt)
* [Download Standard Microsoft Security Compliance Manager (SCM) Baselines](Local%20Group%20Policy%20&%20Security%20Compliance%20Manager%20-%2020%20December%202016.ppt)
* [Develop custom SCM Baselines](Local%20Group%20Policy%20&%20Security%20Compliance%20Manager%20-%2020%20December%202016.ppt)
* [Install Nessus on all competition host machines](Nessus%20Host%20Machine%20Installation.ppt)
* Download latest MalwareBytes version and host on a thumb drive
* [Download latest Secunia Personal Software Inspector (PSI) and host on a thumb drive](Secunia%20PSI.ppt)
* Download the latest Microsoft Security Baseline Analyzer (MSBA) and how on a thumb drive

**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?
  + Answer forensics question first if possible
* Pin control panel, command line and run icons to task bar
* [Run security templates and record vulnerabilities](Custom%20Security%20Template.pptx)
* Delete image and open second
* [Apply MS SCM Baselines and record vulnerabilities](Local%20Group%20Policy%20&%20Security%20Compliance%20Manager%20-%2020%20December%202016.ppt)
* [Apply DISA STIG Files and record vulnerabilities](DISA%20STIG%20Files.ppt)
* Check Broadcast message on scoring screen
* [Run Nessus scans](Nessus%20Scans.ppt)
* [Run the Microsoft Baseline Security Analyzer (MSBA)](MIcrosoft%20Baseline%20Security%20Analyzer.ppt)
* Other

**Configure/Patch System**

* Set Automatic Windows Update … do not install all optional updates unless needed
* [Run Secunia PSI scans](Secunia%20PSI.ppt)
* **Update Third Party Applications (Adobe, Firefox, Flash, Notepad ++, etc.)**
* Family Safety Settings
  + Activity Reports
  + Web Filtering
  + Time Limits
  + Game & Apps Restrictions
  + Desktop App Restrictions
* [Windows SmartScreen](SmartScreen.pptx)
* Privacy Settings
  + Location
  + Webcam
  + Microphone
* Bluetooth
* Secure Boot (may not be accessible in VMWare)
* File & Folder Auditing
* Problem reporting settings
* [Bitlocker encryption](Bitlocker%20Encryption%20in%20Windows%208.mp4)
* AppsLocker - <https://www.youtube.com/watch?v=HAts_oDDdfQ>
  + Executable Rules
  + Windows Installer Rules
  + Script Rules
  + Packaged Apps Rules
* Event Log Service
* [Backup Programs](Windows%20Backups.pptx)
* [Windows Backup Video](How%20to%20setup%20Windows%208%20Backup.mp4)

**Antivirus/Antispyware (antimalware)**

* [If not installed, install a version available to you (Microsoft Defender)](Windows%20Defender.pptx)
* Update signatures if needed

**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](Firewalls.ppt)
* 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 (rename even if disabled)
      * 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

**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

**Security Settings**

* Require Ctrl-Alt-Del to Login
* [Check System Auditing](Audit%20Policy.pptx) (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
* **Encrypt files if needed**

**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](Task%20Manager.ppt)
  + 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
  + 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](MalwareBytes.ppt)
  + 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
* 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” permissions
* Folder Permissions
* Check hosts file
* [File Encryption](File%20Encryption.ppt)

**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 screen

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