



CyberPatriot Windows 10 Toolkit

★ <https://www.uscyberpatriot.org/competition/training-materials/training-modules> ★

<https://www.wired.com/2015/08/windows-10-security-settings-need-know/> ★

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/how-to-configure-security-policy-settings>

★ <https://msdn.microsoft.com/en-us/library/ff648641.aspx>

★ http://www.lacapnm.org/Cadets/STEM/CyberPatriot/SeasonVIII/CyberPatriot_Windows_CheckList.pdf

☐ **Forensic Question**

☐ **Updates**

☐ Start> search “Windows update”> check for updates

☐ **Update Policy**

☐ Start> search “Windows Update”> Advanced settings

☐ **Choose when to be notified**

☐ Start> search “User Account Control Setting”> Slide bar to “Always Notify”

☐ **User’s Files**

☐ File Folder Icon>This PC> C Drive AKA “OS(C:)”>Users> Select Suspicious User

☐ **Delete User**

☐ File Folder Icon>This PC> C Drive AKA “OS(C:)”>Users>left click bad user 1 time> right click 1 time> Delete

☐ **User Accounts**

☐ Start> search “Control Panel”> User Accounts

☐ **Administrative/Standard**

☐ (Your Account)Start> search “Control Panel”> User Accounts>Change account type

☐ (Other Account)Start> search “Control Panel”> User Accounts>Manage another account>select user>change the account type

☐ **Users And Groups**

- ☐ Start>search “Command Prompt”> type in “LUSRMGR” (Casing doesn’t matter)

☐ **Change Passwords**

- ☐ Start>search “Control Panel”> User Accounts> Make changes to my account in PC settings > sign-in options
- ☐ Start> search “Control Panel”> User Accounts>Manage another account>select user> Create a password
- ☐ Ctrl+Alt+Delete> Change a password

☐ **Password Policy**

- ☐ Start>search “Command Prompt”> type in “SECPOL.MSC” (Casing doesn’t matter)>Password Policy

☐ **Account Lockout Policy**

- ☐ Start>search “Command Prompt”> type in “SECPOL.MSC” (Casing doesn’t matter)>Account Lockout Policy

☐ **Firewall Settings**

- ☐ Start>search “Control Panel”> Windows Firewall

☐ **Turn On Firewall/ Install Maintenance**

- ☐ Start>search “Control Panel”> Windows Firewall> Security and Maintenance (bottom left corner)

☐ **Antivirus**

- ☐ Start>search “Windows Defender”
- ☐ Start>Settings>Update & Security>Windows Defender>Open Windows Defender Security Center
- ☐ **Disable Ports using the firewall(port 53 is used by the FTP protocol)**

CyberPatriot Competition Checklist

Manual	Automated
<input type="checkbox"/> Read the Read Me file- highlight, take notes	<input type="checkbox"/> User Rights – update registry
<input type="checkbox"/> Answer Forensics Question(s)	<input type="checkbox"/> MalwareBytes for malware
<input type="checkbox"/> Turn on Firewall	<input type="checkbox"/> Automatic Updates – download and install
<input type="checkbox"/> Action Center	<input type="checkbox"/> AV scan
<input type="checkbox"/> User Account Control	
<input type="checkbox"/> Secure Users and Groups (Guest/Admin, etc.)	
<input type="checkbox"/> Passwords for accounts	
<input type="checkbox"/> Password Policies	
<input type="checkbox"/> Remove/Disable Insecure Services	
<input type="checkbox"/> Local Security Policy (if not by .inf file)	
<input type="checkbox"/> Update appropriate software	
<input type="checkbox"/> Uninstall unnecessary software	
<input type="checkbox"/> Search for inappropriate files – media, hack tools, etc.	
<input type="checkbox"/> Secure File and Directory Shares	
<input type="checkbox"/> Check Open Ports	
<input type="checkbox"/> Check for Anti-Virus Program	
<input type="checkbox"/> Check for abnormal behavior	

Ensure you are not rebooting the machine for the updates with less than an hour to go!!

Document each and every action you perform – whether the setting works or not.

Write notes here. Use the back of this paper and ask for a new sheet if you run out of room!!



Securing Windows 7 Secure Windows Password (Press start and search for local security policy or go to the control panel\System and Security\Administrative tools)

• Password History 5 Days

• Maximum Password age 30-90 days

• Minimum Password age 5 days

• Minimum Password Length 8 char.

• Password Complexity Enabled

• Reverse Encryptions Disabled Account Lockout Policies(Right under Password policies)

• Account Lockout Duration 30 minutes

• Account Lockout Threshold 3

• Reset account lockout counter 30 minutes Set up Windows Audit Policies (Right under Account Policies in Local Policies)

• Audit Logon Events Failure

• Audit Account Management Success

• Audit Directory Service ND

• Audit logon Events Failure

• Audit Objects Access ND

• Audit Policy Change Success

• Audit Privilege use success failure

• Audit Process tracking Success Failure

• Audit System Events failure Security Options (Beneath User Rights Assignment in Local Policies)

• Disable Administrator account

• Disable Guest account • Rename administrator and guest accounts

• Shutdown Without Log on.

☐ TURN ON WINDOWS FIREWALL DUMBY!!!

☐ Change Passwords for Each User (User policy)

☐ Install automatic updates (Control Panel Action Tools under System in security.) Update Windows Programs (i.e. PowerShell, IE all the way to 10) ☐

Set local user Admin password to not expire and account enable Admin tools\Computer management\users and group\use R

☐ Disable and Stop Services in the services menu

• RDP

• ICS

• RDP User Mode

- Remote Registry

- RD Configuration

- SSDP Discovery

- UPnP Device Host

- Remote Desktop

- WWW Publishing Service

Clean the Host File (C:\Windows\System32\drivers\etc\host.txt

Deny Following Ports

- FTP

- SSH

- TelNet

- SNMP

- LDAP

- RDP

Windows 7 Service packs Installed