Basic Security Checklist – Windows Server 2008 R2 Focus

Read the scenario, AND THEN read the scenario again!

● Make Internet Explorer Work for You (IE Enhanced Security Configuration) ○ Server Manager to turn off

○ Consider another Browser if allowed by scenario

● Turn off Shutdown Event Tracker

○ Group Policy Editor (gpedit.msc)

○ Computer Configuration\Administrative Templates\System

○ Display Shutdown Event Tracker

● Updates (show how to set)

○ Service packs

○ Other OS updates

○ Non-OS updates

● User Accounts (Server Manager -> Configuration -> Local Users and Groups) ○ Extra accounts deleted (disabled not for CyberPatriot)

○ Accounts have passwords

○ Changing default account names (not for CyberPatriot)

○ Check for group memberships

○ Remote Control Tab

● Passwords

○ Secpol.msc

○ Length, Complexity, History, Lockout

● Firewall

○ Adding a rule

● Antivirus (MSE not supported)

○ Look for Kapersky or Avast Trials (watch supported OS List)

● Extra Programs

○ Start Menu

○ Add/Remove Programs (Programs and Features in Windows Server 2008) ○ Msconfig – startup tab

● Extra Services

○ Services.msc

○ Do not touch CyberPatriot Services

○ Remember to sort by status & startup type

● Remote Access

○ Go through Computer -> Properties -> Remote Settings for CyberPatriot

● Auditing

● Searching for files

● File Sharing

○ MMC -> Shared Folder Snap-In (and remove with right-click)

● Show File Extensions

Cyber Patriot VI Checklist (Windows Server 2008 R2) Page 1

○ Windows Explorer -> Organize -> Folder & Search Options -> View tab

● Check Event Logs for out of the ordinary items – watch for cleared logs

● User Access Control (On or Off only)

○ Control Panel -> User Accounts

● Add/Remove Windows Features – Server Manager

● Administrative Tools

○ Available from Start Menu by Default

○ Server Manager

● Computer Properties

○ Device Manager

○ Remote Settings

○ System Protection/Restore – Not in Server 2008!

○ Advanced System Settings

● Network and Sharing Center

○ Taskbar - Network icon or Search

○ Advanced Sharing Settings

○ Be sure to look at all network profiles

● MBSA

○ Short download

○ Activate update settings

○ Scans in less than 10 minutes (depends on the number of users)

● Security Templates

○ Found in Windows/inf

○ Three of them

■ defltbase

■ defltdc

■ defltsv

○ Security Configuration & Analysis Snap-In (SCA)

■ Create own template for competition

● Service Packs

○ Find them before competition

● Removing Rootkits – think SAFE MODE!

Cyber Patriot VI Checklist (Windows Server 2008 R2) Page 2