Basic Security Checklist – Windows 7 & Windows XP

Read the scenario, AND THEN read the scenario again!

- If the system logs straight on
    - netplwiz
- Updates (show how to set)
    - Service packs
    - Other OS updates
    - Non-OS updates
- User Accounts
    - Extra accounts deleted (disabled not for CyberPatriot)
    - Accounts have passwords
    - Changing default account names (not for CyberPatriot)
    - Check for group memberships
    - No auto login (netplwiz)
- Passwords
    - Secpol.msc
    - Length
    - Complexity
    - History
    - Lockout
- Firewall
    - Adding a rule
- Antivirus (MSE is quick and works well)
- Extra Programs
    - Start Menu
    - Add/Remove Programs (Programs in Windows 7)
    - Msconfig – startup tab
- Extra Services
    - Services.msc
    - Do not touch CyberPatriot Services
    - Look at scenario
    - Remember to sort by status & startup type
- Remote Access
    - Go through Computer -> Properties for CyberPatriot
- Auditing
    - Secpol.msc

- File System
    - NTFS preferred
        - Diskpart -> list volume (verify drive letter)
        - Vol drive letter
        - Convert drive letter: /FS:NTFS (error on our VM)
    - Create a partition (Computer Management)
        - Shrink or extend
- File Sharing
    - Check through Computer Management
    - Remove through Windows Explorer
    - Can remove in Computer Management for Windows 7
- Show File Extensions
    - Windows Explorer -> Organize
- Check Event Logs for out of the ordinary items
    - Event Viewer
- (win7) User Access Control
    - Control Panel -> User Accounts
    - Also from msconfig Tools tab
    - Use the help (especially to match something in a scenario)
- (win7) Action Center
    - Check for any issues
- Control Panel
    - Includes turning some Windows features on & off
    - Parental Controls
- Administrative Tools
    - Use Search Bar or change Start Menu properties
- Computer Properties
    - Device Manager
    - Remote Settings
    - System Protection
    - Advanced System Settings
- (win7) Network and Sharing Center
    - Task Bar 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)
- Rootkit removal – think SAFE MODE