Basic Security Checklist – Windows Server

- For Windows 2016 – remember to use the advanced menu by
  - Pressing Windows + X
  - Right-Click the Start Menu
- 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
- Malware
  - Antivirus (WinClam, MSE, Server Trial version - depends on Server version)
    - You can use a trial version – just be sure it supports your OS!
  - Antimalware (MalwareBytes)
  - Rootkit removal – think SAFE MODE
- Unauthorized Software
  - Start Menu
  - Control Panel -> Programs
    - Windows Features (Server Manager)
      - Remove Role Services
  - Microsoft Configuration Utility (msconfig.exe)
  - Startup Folder
  - Registry Entries (regedit)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
    - Run and Run Once
- Users (Server Manager -> Configuration or Computer Management)
  - Decide who should have access to what (scenario)
  - Disable extra accounts (why not delete?)
  - Insure all accounts have a password (Password1234)
  - Changing the default names – why?
  - Check group memberships
  - Prevent auto-login with netplwiz (also classic login)
- Updates
  - Four choices (none, alert only, download only, **automatic**)
    - Server 2016 - options not available
  - Other Microsoft updates
  - Service Packs (download ahead of time)
  - Other OS Updates
  - Non-Microsoft updates (watch the scenario)
- Passwords – Local Security Policy (secpol.msc)
  - Length
  - Complexity
  - History

- Account Lockout – Local Security Policy
    - Duration
    - Threshold
    - Reset lockout counter
- Security options – Local Security Policy
- Computer Properties
    - Remote Access (Remote Desktop, Remote Assistance)
- Auditing (secpol.msc)
- Firewall
    - Check rules – look for something out of the ordinary
    - Insure it is on for all profiles
- Extra Services (services.msc, Server Manager)
    - Do not touch CyberPatriot Services
    - Look at scenario
    - Look for “strange” services
    - Remember to sort by status & startup type
- Unauthorized File Sharing
    - Check through Shared Folder Snap-In
    - Use MMC or Computer Management
    - Note the location before removing the share!
- Show File Extensions and Hidden Files
    - Windows Explorer -> Organize -> Folder & Search Options
    - Windows Explorer -> View tab -> find checkboxes
- Check Event Logs for out of the ordinary items
    - Security log…
- Finding Unauthorized File (graphics, videos, etc.)
    - For Server need to insure that File Services Role is on
    - Display the file extensions Search techniques (kind, type)
- User Access Control (User Accounts)
- Action Center