Basic Security Checklist – Windows

- **(Win 10) Advanced Menu – Windows + X or right-click start menu**
- Users – **use Computer Management not Users applet**
  - Decide who should have access to what (scenario)
    - **Organizational Policies**
  - Disable extra accounts (why not delete?)
  - Insure all accounts have a password (Password1234)
  - Changing the default names – why?
    - **For graded hands-on do not change user names**
  - Check group memberships
  - Prevent auto-login with netplwiz (also classic login)
- Unauthorized Software
  - Start Menu
  - Control Panel -> Programs
    - Don't forget Windows Features
  - Microsoft Configuration Utility (msconfig.exe)
    - **(Win 10) Start up programs – use Task Manager**
  - Startup Folder
    - **(Win 10) shell:startup**
  - Registry Entries
    - **Run and RunOnce**
    - **HKLM and HKCU**
    - **Ignored in safe mode**
    - **RunOnce name with "!" at start = defer deletion until run**
- Malware
  - Antivirus (MSE, AVG Free, **Avast! Free**)
    - **Offline installation**
  - Antimalware (MalwareBytes)
  - Defender (built-in)
  - SmartScreen filter (IE 9 and later)
- Updates
  - **(Win 7)** Four choices (none, alert only, download only, **automatic**)
    - **(Win 10) Metered connection**
    - **(Win 10) Update Settings**
    - **(Win 10) Configure Automatic Updates**
      - **No autorestart**
      - **Configure automatic updates**
  - Service Packs (download ahead of time)
  - Other OS Updates
  - Non-Microsoft updates (Secunia PSI)

- Passwords – Local Security Options (secpol.msc)
    - Length
    - Complexity
    - History
- Account Lockout
    - Duration
    - Threshold
    - Reset lockout counter
- Computer Properties
    - Remote Access (Remote Desktop, Remote Assistance)
    - System Protection
- Auditing
- Firewall (built-in, ZoneAlarm Free)
- Unauthorized File Sharing
    - Check through Computer Management
    - Note the location before removing the share!
- Local Security Policy (secpol.msc)
    - Local Policies – Security Options
- Services (services.msc, Computer Management)
    - Look for “strange” services
    - Sort by type & startup status
    - Do not touch CyberPatriot Service
- Finding Unauthorized File (graphics, videos, etc.)
    - Display the file extensions Search techniques (kind, type)
- Event Viewer (filter)
    - Watch for cleared Security Log
- User Access Control (User Accounts)
- Action Center
- Network & Sharing
    - Be sure to check on all three network types
- Additional Helpful Software
    - MBSA (version 2.2)
    - CCleaner
    - WinPatrol
- Rootkit removal – think SAFE MODE
- Security Configuration & Analysis Snap-In (SCA)
    - Possibly create template for competition