Green Plan

All Commands Prompt unless specified Powershell will not be used

1. **Check Physical Stuff**
   a. Check for tape under the mouse
   b. Suspicious things connected to the computer
   c. USB
   d. ETC.
   e. Don’t open the box
2. **Users**
   a. Local users
      i. Change passwords. Don’t change passwords with command line
      ii. Disable unnecessary users but don’t delete
         1. “net user <username> /active:no”
   b. Domain Users
      i. Create Domain Admin accounts for each windows server admin
      ii. Find out, total users. Look in all OUs for hidden users. Services Accounts that aren’t service accounts.
      iii. Change passwords for scored users.
      iv. (Bluck) Disable unnecessary users but don’t delete
3. **Firewall**
   a. Enable firewall service
      i. Windows firewall (Advanced Security)
         1. Right-click top level and turn all profiles on.
   b. Restore Default Policy: Right-click “Windows Firewall w/ Advanced Security on Local Computer” and select “Restore Default Policy”.
   c. Commands
      i. Enable and start
         1. Sc config mpsvc start=auto
         2. Net start mpsvc /y
      ii. Enable logging
         1. Netsh advfirewall set allprofiles loggin droppedconnections enable
      iii. Netsh advfirewall set allprofiles settings remotemanagment disable
   d. Disable every Inbound rule except:
      i. Allow Core Networking ICMPv4 in
      ii. Allow Core Networking DHCP (Dynamic Host Config Protocol) in
      iii. ADD Allow Port UDP 1514 in (Local Subnet Only: Right-click rule → Scope → Add Local IP)
   b. Disable every Outbound rule except:
      i. Internet Explorer, TCP 80,443 | UDP 53

4. **Items to Download**
    a. Windows Update
    b. Tools:
        i. Can either browse to link or use Invoke-WebRequest -OutFile
        ii. Sysinternals Suite | https://tinyurl.com/GiveSysSuite | .zip
        iii. Nmap | https://tinyurl.com/GivePorts | .exe
        iv. Wireshark | https://tinyurl.com/GiveShark | .exe
        v. RSAT Tools | “Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online”
5. **Sysinternals Suite**
    a. Autoruns: AutoRuns
        i. GatherNetworkInfo.vbs is OKAY (part of Autoruns)
        ii. Check last modified date of files in System32 (very recent times = bad file)
        iii. Colors:
            1. Pink: No publisher information was found
            2. Green: New item
            3. Yellow: Startup entry is there but the file/job is not
    b. Portmon: Monitor Port Activity
    c. Process Explorer: View Running Processes
        i. Add the following columns: Autostart location, Users
        ii. Options: Verify file signatures, replace task manager
    d. Rootkit Revealer: Check for Rootkit(s)
    e. TCPView: View TCP/UDP Endpoints
6. **Boot Processes**
    a. Enter System Configuration: **`msconfig.exe`**
    b. Services Tab: Hide all Microsoft services; Disable unnecessary features
    c. Startup Tab: Disable non-critical services
7. **Windows Features**
    a. Search for “Turn Windows Features On or Off”.
    b. Uncheck:
        i. Print and Document Services
        ii. SMB 1.0/CIFS File Sharing Support
        iii. Telnet Server & Client
        iv. XPS Services
8. **Block Future PSEXEC Connections**
    a. reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0
9. **Inventory**
    a. OS

b. Services
c. Users
d. Installed applications

10. Git for Backups

a.