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
    f. Check For IOT Devices/Phones
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. 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.
        ii. Commands
            1. Enable and start
                a. Sc config mpsvc start=auto
                b. Net start mpsvc /y
            2. Enable logging
                a. Netsh advfirewall set allprofiles loggin droppedconnections enable
        iii. Netsh advfirewall set allprofiles settings remotemanagment disable

Windows Defender Firewall -

1. Ensure Windows Defender Firewall is on.
2. Restore Default Policy: Right-click "Windows Firewall w/ Advanced Security on Local Computer" and select "Restore Default Policy".
3. Disable every Inbound rule except:
    a. Allow Core Networking ICMPv4 in
    b. Allow Core Networking DHCP (Dynamic Host Config Protocol) in

    c. ADD Allow Port UDP 1514 in (Local Subnet Only: Right-click rule → Scope → Add Local IP)

4. Disable every Outbound rule except:
    a. Internet Explorer, TCP 80,443 | UDP 53
    b. ADD Allow Port UDP 1514 out (Local Subnet Only: Right-click rule → Scope → Add Local IP)

4. Items to Download

a. WINDOWS UPDATES!!!

b. Sysinternals Suite | http://bit.ly/GiveSys
c. Nmap | http://bit.ly/GivePorts
d. Wireshark | http://bit.ly/GiveShark
e. Nxlog | https://bit.ly/GiveLog
f. RSAT Tools | “Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online”

5. Sysinternals Suite

Autoruns: AutoRuns

- GatherNetworkInfo.vbs is OKAY (part of Autoruns)
- Check last modified date of files in System32 (very recent times = bad file)
- Colors:
    - Pink: No publisher information was found
    - Green: New item
    - Yellow: Startup entry is there but the file/job is not

Portmon: Monitor Port Activity

Process Explorer: View Running Processes

- Add the following columns: Autostart location, Users
- Options: Verify file signatures, replace task manager

Rootkit Revealer: Check for Rootkit(s)

TCPView: View TCP/UDP Endpoints

Boot Processes -

1. Enter System Configuration: **`msconfig.exe`**
2. Services Tab: Hide all Microsoft services; Disable unnecessary features
3. Startup Tab: Disable non-critical services

1. Search for “Turn Windows Features On or Off”.
2. Uncheck:
    a. Print and Document Services
    b. SMB 1.0/CIFS File Sharing Support
    c. Telnet Server & Client
    d. XPS Services

\

Block Future PSEXEC Connections

```
C:\> reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 0
```