1. **Show all users**
   - *net user*
   - *Disable guest accounts*
2. **Change Passwords for ALL USERS**
   - Change administrators passwords first and then all users
   - Open start menu
   - Type cmd
   - Right click on cmd as "run as administrator"
   - *net user <user-name> **
   - *Change SQL Server passwords*
     - *Security->Logins->Right-click->Properties*
   - *Change passwords for web services*
3. **Security Updates**
   - Search for "check for updates"
   - Only downloaded recommended/important updates (uncheck)
   - Only check the updates that say "Security Update"
   - WINDOWS 10 "Advanced options > defer feature updates"
4. **Download and Install Malwarebytes**
5. **Firewall**
   - Search for "firewall"
   - Inbound and outbound rules
   - Setup this first rule to close all connections
     - Click *inbound rules* (on left side of window)
     - Click *new rule* (on right of window)
     - Click *port* and *next*
     - Click *all local ports*
     - *Click block the connection*
     - *Add name in UPPERCASE.*
   - *Proceed to add ports according to specific computer*
6. **Check for processes running (make a white list)**
   - *tasklist*
   - *taskkill -PID <pid-num> -f*
   - **DO NOT KILL the following ports**
   - *RPCss (135), eventlog service (49409), Spoolsv (49410), schedule (49411), lsass.exe (49414)*
7. **Check for ports open**
   - *netstat -anob*
8. **Group Policy Template**
   - User Account Policies
     - Set minimum password length.
     - Enable password complexity requirements.
     - Do not store passwords using reversible encryption. (Default)

        - Configure account lockout policy.
    - Make sure LM hash disabled

9. **Patch specific vulnerabilities**

XP	10	2003	Vista/2008	2012	7
MS08-067 MS06-040 MS12-020 MS03-026		MS09-050 MS08-067 MS06-040 MS03-026 MS10-061	MS09_050 MS12-020 MS10-061		MS09_050 MS12-020

    - **Download patches from here:**
    - http://www.catalog.update.microsoft.com/
    - http://www.wsusoffline.net/docs/

10. **Install EMET**

11. **Auditing Policy**
    - Group Policy - Domain Controller
    - Local Policy

12. **MBSA (Microsoft baseline security analyzer)**
    -

13. **SCM (Windows security compliance manager)**
    -

14. **Event Viewer: see how logins**
    - http://www.howtogeek.com/124313/how-to-see-who-logged-into-a-computer-and-when/
    -

Sources
https://github.com/lchack/CCDC/blob/master/windowshardening.txt
https://wikis.utexas.edu/display/ISO/Windows+Server+2012+R2+Hardening+Checklist