WIndows:

<https://security.utexas.edu/os-hardening-checklist/windows-2016>

<https://security.utexas.edu/os-hardening-checklist/windows-r2>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/>

<https://www.hardenwindows10forsecurity.com/index.html>

<https://blanchard.productions/wp-content/uploads/2018/03/CyberPatriot-Windows-Checklist.pdf>

<https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc137720(v=msdn.10)>

<https://www.blackhat.com/presentations/win-usa-04/bh-win-04-milroy/bh-win-04-milroy.pdf>

<https://newhelptech.wordpress.com/2017/07/02/step-by-step-implementing-dns-security-in-windows-server-2016/>

<https://www.bleepingcomputer.com/news/security/windows-8-and-later-fail-to-properly-apply-aslr-heres-how-to-fix/>

Some of the Local Policies and Firewall stuff could work on actual CP

Also have to disable the services that are in the Services category

Advanced Auditing Policies

Group Policies in gpedit.msc check the next link for more specifics (Can disable Insider Preview Builds from there, could give us points)

<https://security.uri.edu/files/CIS_Microsoft_Windows_10_Enterprise_Release_1511_Benchmark_v1.1.0.pdf>

<http://techgenix.com/hidden_backdoors_trojan_horses_and_rootkit_tools_in_a_windows_environment/>

Active Directory:

<https://activedirectorypro.com/active-directory-security-best-practices/>

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

DNS:

<https://newhelptech.wordpress.com/2017/07/02/step-by-step-implementing-dns-security-in-windows-server-2016/>

Also coming up services on Windows 10 (Possibility):

SMB or FTP (We have to figure out how to secure this)

Services coming up on Server 2016 (Possibility):

DNS

Domain Controller (Active Directory [AD])

Have to figure out how to secure the above and configure properly

Linux:

<https://help.ubuntu.com/community/Security>

<https://security.utexas.edu/os-hardening-checklist/linux-7>

<https://iase.disa.mil/stigs/os/unix-linux/Pages/index.aspx>

<https://www.techrepublic.com/article/how-to-harden-ubuntu-server-16-04-security-in-five-steps/>

<https://ca-cyberhub.org/wp-content/uploads/SupportPortal/Boot-Up-Manager.pdf> <- boot up link could help

Advanced Linux:

<http://bookofzeus.com/harden-ubuntu/>  
<https://www.netacad.com/web/self-enroll/course-568755>  
<https://www.netacad.com/web/self-enroll/course-570281>  
<https://learn.cisecurity.org/benchmarks>  
<https://help.ubuntu.com/16.04/serverguide/>  
<https://www.uscyberpatriot.org/competition/training-materials/linux>  
<https://www.reddit.com/r/cyberpatriot/comments/5a9c85/custom_ubuntu_practice_image/>  
<https://support.ca-cyberhub.org/support/solutions/folders/33000201655/page/1?url_locale=>

Ports: <https://ca-cyberhub.org/wp-content/uploads/SupportPortal/What_About_Ports.pdf>

Ubuntu Services Possibility:

SSH

Samba

(Have to make both of those as secure as possible)

Debian Possible Upcoming Services:

LAMP (Linux, Apache2, MySQL, and PHP)

(Have to make both of those as secure as possible)

Bind9 is an important service to research on. Research will come under this soon.

Helpful Server Security:

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf>