**Linux Hardening Policy**

1 PAGE MAX

*BIOS and Boot Loader Security*

1. Physical system security will be implemented by hardening the BIOs and preventing unauthorized users from booting from peripherals and by implementing a BIOS password for the GRUB to prevent physical access to the system

*Administrative*

1. Review users
2. Discover listening ports and the services running by using netstat

*Password Security*

1. Shutdown services/applications that are not needed to reduce possible vulnerabilities
2. Always keep the system updated with the latest release patches for security

*Available Network Services*

*Personal Firewalls*

1. Review logs and monitor user activity
2. 6. Enforce password policy

Windows Hardening Policy

1. Physical system security enabled by locking with BIOS password and implementing BitLocker encryption
2. Apply most recent updates pulled from catalog.update.microsoft.com
3. Enable two-factor authentication for domain users and (Windows 10/Server 2016 only) disable Microsoft Accounts
4. Set local security policies (including password policies) and (Server only) relevant GPOs
5. Disable SMBv2 and SMBv1
6. Enable Windows Firewall and set appropriate firewall rules in place including filtering client outbound traffic for RDP and VNC connections
7. Identify all listening ports (netstat) and disable unneeded services (services.msc)
8. (Server only) Remove unnecessary server roles
9. Remove unnecessary EXE/UWP applications including malicious tools, entertainment applications, and widgets (where applicable)