Item	NIST 800-53 R4	800-171	CMMC	Status (Met, NotMet, N/A)	Remediation Recommendation/Notes
Windows Server					
Windows Server must have antivirus.	X	X	X	Met	
A host-based firewall must be installed and enabled on the system.	X	X	X	NotMet	Install and enable host-based firewall.
Fax server role must not be installed. (Windows)	X	X	X	Met	
Server Message Block (SMB) v1 must not be installed.	X	X	X	Met	
The roles and features requried by the system must be documented.	X	X	X	NotMet	Create docuument and document every changes.
PowerShell 2.0 must not be installed.	X	X	X	Met	
Local Accounts with blank passwords are not allowed.	X	X	X	NotMet	Create passwords for Local Accounts. No allow authentication with blank passwords.
Local Administrator account must be renamed.	X	X	X	NotMet	Rename Local Admin account.
Local Guest account must be renamed.	X	X	X	NotMet	Rename Local Guest account.
Allow log on via RDP allowed only to members of Administrators Group	X	X	X	Met	
Passwords must be set to expire (Non Udacity Accounts)	X	X		NotMet	Set up password expiration.
Password minimum age must be set to more than 1 day.	X			NotMet	Set up password minimum age for 90 days.
Minimum Password length must be 14 digits.	X			NotMet	Set up password minimum length for 14 digits.
Application Event Log must be 32768KB or greater.	X			NotMet	Set up Application Event Log size for 50MB.
Security Event Log must be 196608KB or greater.	X			N/A	
System Event Log must be 32768KB or greater.	X			NotMet	Set up System Event Log size for 50MB.
Local Guest account must be disabled.	X			NotMet	Disable Local Guest account.
User Account Control must alert.	X			N/A	
Windows Server built-in password complexity enabled.	X			N/A	
Windows Smartscreen must be enabled.	X	X	X	NotMet	Enable Windows Smartscreen.
Windows 10					
Windows 10 systems must be maintained at a supported service level (Microsoft supported build n	X	X	X	NotMet	Update a newer version.
Local volumes must be formatted with NTFS.	X	X	X	Met	
Accounts must be configured to require password expiration. (Non Udacity Accounts)	X	X	X	NotMet	Set up password expiration.
Firewall must be enabled on the system.	X	X	X	NotMet	Enable Firewall.
Windows 10 account lockout duration must be configured to 15 minutes.	X	X	X	N/A	
Number of bad logon attempts must be 3 or less.	X	X	X	Met	
Minimum Password length must be 14 digits.	X	X	X	NotMet	Set up password minimum length for 14 digits.
Wi-Fi Sense must be disabled.	X	X	X	N/A	
Built-In Administrator account must be disabled.	X	X	X	NotMet	Disable Built-In Admin account.
Local Guest account must be renamed.	X	X	X	NotMet	Rename Local Guest account.
App and Browser Control Must be Enabled.	X	X	X	Met	
Exploit Protection mitigations in Windows 10 must be configured for wordpad.exe	X	X	X	NotMet	Configure Exploit Protection mitigations for wordpad.exe.
Application Event Log must be 32768KB or greater.	X			NotMet	Set up Application Event Log size for 50MB.
Local Guest account must be disabled.	X			NotMet	Disable Local Guest account.
CentOS					
Current on security updates.			X	Met	
Ensure separate partition exists for /var			X	NotMet	Move/mount /var to another partition. sudo fdisk /dev/sdX sudo nano /etc/fstab UUID=<UUID_of_new_partition> /newvar ext4 defaults 0 2 sudo mount /dev/sdX /mnt/newvar sudo cp -a /var/. /mnt/newvar/. sudo umount /mnt/newvar sudo reboot
Disable Automounting of drives.			X	NotMet	Disable Automounting of drives in fstab. lsblk or fdisk -l vim /etc/fstab Comment out(#) or remove entries Save and exit
Ensure AIDE is installed			X	NotMet	Install and configure AIDE. sudo yum install aide sudo aide --init vim /etc/aide.conf (edit and save it)
Ensure daytime services are not enabled			X	Met	
Ensure echo services are not enabled			X	Met	
Ensure tftp server is not enabled			X	Met	
Ensure CUPS is not enabled			X	Met	
Ensure DHCP Server is not enabled			X	Met	
Ensure FTP Server is not enabled			X	Met	
Ensure Samba is not enabled			X	Met	
Ensure TCP Wrappers is installed			X	NotMet	Install and configure TCP Wrappers. sudo yum install tcp_wrappers vim /etc/hosts.allow (edit and save it) vim /etc/hosts.deny (edit and save it)
Ensure DCCP is disabled			X	Met	
Ensure iptables is installed			X	Met	
Ensure audit log storage size is configured			X	Met	
Ensure audit logs are not automatically deleted			X	Met	

Windows Servers

Item	Details	Notes
Machine name	**Use it to distinguish your machines.(example Win2016-SRV-01)**	
OS version	**Use it to define your server roles and features and fit your organization security. (example Windows Server 2016 Datacenter)**	
Minimum RAM requirement	**Use it to define your server RAM requirement. (example 16GB RAM)**	
CPU requirement	**Use it to define your server CPU requirement. (example 16 Core - 32 Thread)**	
Roles and features	**Use it to define your server services. (example Samba File Sharing, IIS, Active Directory, DNS)**	
IP address	**Use it to define your Public and Private interface configuration.**	
Disk size	**Use it to define your server disk size. (example for OS: 1TB SSD and User data: 2TB SSD)**	
Disk Partition	**Use it to separate your server configuration data and data of your organization. (example for OS: C drive, User data: D drive)**	
Disk encryption	**Use it to set up your server disk encryption. (example BitLocker)**	
Back Up	**Use it to define your back up plans. (what kind of data and where store it)**	
Users	**Use it to list all of your users who have access your servers. (example IT Admins)**	
Permissions	**Use it to define access rules of your organization data. (Groups, file and folder permissions - HR's, Other employees, CEO's)**	
Users Password Complexity	**Use it to define Password Complexity (example a-z,A-Z,0-9, and specific characters)**	
Users Minimum Password Length	**Use it to define Minimum Password Length (example 15 character of Minimum Password Length)**	
Users Password expiration	**Use it to define Password expiration (example 6 moth of Password expiration)**	
Users Lockout Duration	**Use it to define Lockout Duration (example 15 min Lockout Duration)**	
Users number of bad log-in attempts	**Use it to define number of bad log-in attempts (example 3 number of bad log-in attempts)**	
Logging	**Use it to define what logging, where store it and size of log files. (example Application, Security, System)**	
Firewall Rules	**Use it to define inbound and outbound rules of your firewall. (example use VPN connection to reach server)**	
Updates	**Use it to identify how and when patches are installed from repository. (example check update every day)**	

Linux Servers

Item	Details	Notes
Machine name	**Use it to distinguish your machines.(example Ubuntu-SRV-01)**	
OS version	**Use it to define your server roles and features and fit your organization security. (example Ubuntu 22.04.4 LTS)**	
Minimum RAM requirement	**Use it to define your server RAM requirement. (example 8GB RAM)**	
CPU requirement	**Use it to define your server CPU requirement. (example 8 Core - 16 Thread)**	
Roles and features	**Use it to define your server services. (example Samba File Sharing, Apache, LDAP)**	
IP address	**Use it to define your Public and Private interface configuration.**	
Disk size	**Use it to define your server disk size. (example for OS: 1TB SSD and User data: 2TB SSD)**	
Disk Partition	**Use it to separate your server configuration data and data of your organization. (example for OS: sda1, User data: sda2)**	
Disk encryption	**Use it to set up your server disk encryption. (example LUKS)**	
Back Up	**Use it to define your back up plans. (what kind of data and where store it)**	
Users	**Use it to list all of your users who have access your servers. (example IT Admins)**	
Permissions	**Use it to define access rules of your organization data. (Groups, file and folder permissions - HR's, Other employees, CEO's)**	
Users Password Complexity	**Use it to define Password Complexity (example a-z,A-Z,0-9, and specific characters)**	
Users Minimum Password Length	**Use it to define Minimum Password Length (example 15 character of Minimum Password Length)**	
Users Password expiration	**Use it to define Password expiration (example 5 moth of Password expiration)**	
Users Lockout Duration	**Use it to define Lockout Duration (example 15 min Lockout Duration)**	
Users number of bad log-in attempts	**Use it to define number of bad log-in attempts (example 3 number of bad log-in attempts)**	
Logging	**Use it to define what logging, where store it and size of log files. (example Application, Security, System)**	
Firewall Rules	**Use it to define inbound and outbound rules of your firewall. (example use VPN connection to reach server)**	
Updates	**Use it to identify how and when patches are installed from repository. (example check update every day)**	
AIDE	**Use it to enable and set up AIDE (Advanced Intrusion Detection Environment).**	
Automounting of drives	**Use it to disable automounting of any drives.**	