Windows Checklist

***1. Turn on Windows Firewall***

a. After DC disables Group Firewalls run gpupdate /force on each machine

b. Configure Property for each separate box

i. Inbound AND Outbound

***2. Create Snapshots Right Away!***

***3. Account management***

1. Disable unneeded user accounts
2. ‘Check both local and AD accounts
3. Make sure accounts are in the correct groups
4. Set passwords for all user accounts
5. Rename built-in admin account
6. ‘Check sharing permissions.

***4. Install Firewall and defense software***

1. Make sure group policy is set so that individual firewall configuration is.

Allowed

1. Make sure Firewall rules work with group policies (Group Object

Editor)

***5. Check external facing services***

a. Visit your own hosted services and make sure you aren't exposing any

critical information}

b. Run netstat or KillSwitch, make sure you don't have any unneeded ports

open

***6. Make Backups of all critical services***

a. DNS Right Click Zone, Change to store locally, not in AD, copy, change

back to store in AD. File is Located in C:\Windows\Systom32\dns

1. dnscmd zonename /zoneexport Zone.com backup\zone1.com.dns.bak

b. Web

©. FIP

***7. Check Startup Programs***

a. Msconfig

b. Check Scheduled Tasks

i. Both of these are part of the comodo suite

***8. Patch Critical Vulnerabilities***

i. For XP, 2000 and 2003 patch MS08\_067

ii. For Vista and 2008 patch MSO9\_050

iii.For Windows Server 2012,2016, Windows 7,8,10 patch Eternal

***9. Set Policies – Active Directory – Add Group Policy Object MMC***

a. XPassword Policies

i. Min Length – 14

ii. Enforce password history – min 3