

Checklist

1. Install X-Netstat Pro
2. Install Sygate Personal Firewall / Configure Windows Advanced Firewall
3. Install Sophos Anti-Virus
4. Install Belarc Advisor
5. Install latest Service Pack for operating system
 - a. 2000 -> SP4
 - b. XP -> SP3
 - c. Vista -> SP2
 - d. Win 7 -> SP1
 - e. Server 2003 -> SP2
 - f. Server 2008 -> SP2
 - g. Server 2008R2 -> SP1
 - h. If latest SP is already installed run Belarc Advisor and install critical updates
6. DC Only -> Remove bad accounts, add new admin account, change passwords
7. Check services.msc and shutdown / disable on startup all non needed services
8. Shutdown RDP
9. Check registry location HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and RunOnce for anything out of the ordinary and remove as necessary
10. Check windows\temp folder and remove anything there
11. After up to date with latest service pack run Belarc Advisor and install critical updates
12. Use Deepfreeze to freeze configuration
13. Continue to monitor X-Netstat Pro and Sygate for possible attacks and compromises

FTP Server: strihm.dyndns-server.com

GitHub: <http://github.com/Xandrax6>