UT Chattanooga
Security Guidelines: Windows 2000 Server
7/18/05 Beta

Note: With the exception of security patches, Microsoft no longer actively supports Windows 2000. It is strongly recommended that all existing Windows 2000 Server installations be upgraded to Windows 2003 Server where possible.

Physical Security: Physical access to servers should be limited to the corresponding system administrators. Network access to KVM (keyboard-video-mouse) switches should be protected using ACLs (access control lists) where possible.

Disks: All hard disk partitions should be NTFS, not FAT32.

Time: All servers should synchronize their clocks with an accepted timeserver. This is critical to accurate network diagnostics and forensic recovery.

Patches: All installations of Windows 2000 Server should be patched to the fullest extent available. Currently this state is represented by Service Pack 4a patched with Security Rollout SP4. All Windows 2000 Server installations should also be checked using Microsoft's Baseline Security Advisor and those running a web server should be locked down using the IIS Lockdown Tool. All servers should have Automatic Updates enabled using the default site provided by Microsoft or UT Chattanooga's Windows Services Update Server.

Antivirus: While servers should not be used for daily activities such as email or word processing, they are still vulnerable to malware such as viruses and worms. Each server should be running the campus approved AV solution.

Passwords: All account passwords should be at least 7 characters long with a maximum age of 180 days and meet the Minimum Password Standard provided by UT Chattanooga's Information Technology Division. Each account should remember the previous 20 passwords to prevent password re-use. Accounts should be locked after three incorrect password attempts for a duration of 20 minutes. Passwords should not be stored in a format that allows "Reversible Encryption."

Services: Where applicable, all unnecessary services should be disabled. Examples include SMTP, SNMP, Telnet, Routing and Remote Access, Remote Desktop, Messenger, FTP, Alerter, and Clipboard. IIS (Web Server) should be hardened using UrlScan.

Administrator: Access to the Administrator account should be severely limited. The Administrator account should also be renamed.

Guest: The Guest account, as well as any user created equivalent accounts, should be disabled. Anonymous access via the network to the server should be explicitly denied. The Guest account should also be renamed.

Sessions: Automatic logon should be specifically disabled on all servers and all session should be protected using a password-enabled screensaver with an inactivity timer set to 15 minutes.

Network: All Windows 2000 Servers should be using NTLM v2 (Windows NT Lan Manager) only. Earlier methods of authentication (LM, NTLM v1) are vulnerable to attacks and considered to be insecure. Versions of Windows prior to 2000, such as 98 and ME, will need the Active Directory client to enable NTLM v2 authentication.

Event Logs: The total space reserved for all three Windows logs (Event, System, Security) should not exceed 120 Mb in size. Logs should be set to "Overwrite as Necessary" and Guest access to logs should be specifically disabled. Where possible, remote logging of Windows Security events should be done.

Backups: All critical content on a server should be archived regularly. Where possible, at least one fully archive set should be kept "off-site."

External References

Microsoft Baseline Security Analyzer:
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

IIS Lockdown Tool:
http://www.microsoft.com/technet/security/tools/locktool.mspx

Windows 2000 Services
http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp

Microsoft UrlScan
http://www.microsoft.com/technet/security/tools/urlscan.mspx

Windows 2000 Recovery Console
http://www.microsoft.com/windows2000/techinfo/administration/management/safemode.asp

Windows 2000 Authentication
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q239869

UT Chattanooga Password Policy:
http://itd.utc.edu/standards/passwords.php