

SSU Windows Security Standards

Version: May 6, 2007

Requirements

1. Have a staff or faculty member as your primary system administrator. Student assistants can be trustworthy and valuable as assistant administrators, but their first priority is and should be their education. If you become too reliant upon a student assistant they will often be in class when you need them. Especially avoid having a student assistant be the only person who knows how to do something. This requirement is from the SSU Blue Paper Policy entitled “Computer and Network Usage” (<http://www.sonoma.edu/uaffairs/policies/computer&network.htm>)
2. Allocate resources (including time) for regular patch updates and maintenance.
3. Implement automatic Microsoft patching
4. All servers connected to the campus network are subject to network and local audits.
5. Run a currently supported version of Windows. (Note: Windows 95, 98, NT, and 2000 are no longer supported by Microsoft.)
6. Harden (and patch, when possible) new systems before attaching them to the network.
7. Don't run a service or server unless you are using it. If you need help with this contact the IT Helpdesk. Note: IT has created a security template to implement this and many other security features along with documentation. ⁱ
8. Take appropriate physical security measures. Remember: Physical access is total access.
9. Make sure all accounts have a non-empty, non-default password.
10. Create and retain backups. Test restoring periodically. If you are compromised, backups may be your only way to recover.
11. Avoid storing confidential data (e.g., social security numbers and credit card numbers) on your systems. More details can be found in the SSU Blue Paper Policy entitled “Personal Confidential Information” (<http://www.sonoma.edu/uaffairs/policies/pci.htm>). A good starting point to determine if you are storing this kind of data is to install and run the free Cornell Spider utility on your system (<http://www.cit.cornell.edu/computer/security/tools/>).

12. Force good passwords by implementing Microsoft's "password must meet complexity requirements" security setting. Note: IT has created a security template to implement this and many other security features along with documentation.ⁱⁱ
The minimum password requirements are:
 - a. Minimum length (8 characters). Recommend a minimum of 14 characters.
 - b. Minimum complexity (At least two of: lower, upper, numeric, punctuation)
 - c. No dictionary words
 - d. Do not contain all or part of the user's account name
 - e. No significant dates
 - f. No names of loved ones, pets, bands, movies, hobbies, heroes, etc.
13. Expire passwords every 90 days. Note: IT has created a security template to implement this and many other security features along with documentation.ⁱⁱⁱ
14. Avoid "Welcome to server <service name>" messages. Attackers have gotten off with the argument that since the message said "Welcome" they felt they were welcome to use the system. SANS recommends "Authorized uses only. All access may be logged." Note the word "uses" instead of "users".
15. Use Microsoft's remote desktop for remote access (version 6 or higher). If you can't use this for any reason contact SSU's Information Security Officer (iso@sonoma.edu).
16. Periodically identify what network services are running on what ports. One way to do this is to use these free utilities: the Microsoft netstat utility or fport (<http://www.foundstone.com/knowledge/proddesc/fport.html>) from Foundstone .
17. Subscribe to vendor mailing lists and stay up to date with vendor patches on an ongoing basis.
 - a. Microsoft (<http://www.microsoft.com/technet/security/bulletin/notify.asp>)
 - b. Microsoft (<http://www.microsoft.com/security/>)
 - c. Microsoft (<http://www.microsoft.com/technet/security/>)
18. Use a local firewall such as the facility that comes with Windows XP SP2
19. Run a current anti-virus utility and maintain a current subscription for updates
20. Do not use the Administrator account (or another account with the same privileges) as a normal user account for mail and surfing, etc. Use an administrative account for management tasks only.
21. Don't grant file permissions to the Everyone group
22. Carefully monitor the Windows Events log
23. Don't send plaintext (i.e., unencrypted) passwords over the network
24. Use EmplID's, Seawolf IDs, or RegIDs instead of Social Security Numbers.

Recommendations

1. Enable full logging. We recommend using Microsoft's EventCombMT utility to search (<http://www.microsoft.com/downloads/details.aspx?familyid=7AF2E69C-91F3-4E63-8629-B999ADDE0B9E&displaylang=en>)
2. Rename the Administrator account to make it more difficult for a hacker to gain an administrator's privileges.
3. Use NTP (<ftp://ftp.udel.edu/pub/ntp/>) to synchronize your clock with other computers on campus so that log file time stamps will match. (Currently we are using 130.157.1.1 and 130.157.253.253. We should include the DNS names of our official NTP servers.)
4. Implement System File Checker (SFC.EXE) integrity checking software. This gives an administrator the ability to scan all protected files to verify their versions. If System File Checker discovers that a protected file has been overwritten, it retrieves the correct version of the file from the cache folder. Windows installation source files, and then replaces the incorrect file.
5. Talk to us before running services that you do not know how to run.
6. Configure servers (such as mail or web servers) to hide their version numbers.
7. Run a password cracker to check for weak passwords
8. Disable guest accounts
9. Eliminate shared accounts
10. Minimize the number of user accounts on servers and "critical" hosts
11. Minimize the number of users with elevated privileges

ⁱ The Default SSU Template configures basic best practices security settings for workstations and servers. It is not all encompassing and can be added to but it is an excellent place to start. The following settings are configured:

Minimum Password Age = 10 days – A user cannot change their password within 10 days of setting it.

Maximum Password Age = 90 days – A password must be changed every 90 days.

Minimum Password Length = 8 characters – Passwords must be at least 8 characters long.

Password Complexity = 1 – Passwords must contain letters, numbers, at least one uppercase letter and a special character (e.g. !&\$#@)

Lockout Bad Count = 5 – After 5 failed login attempts the account will become locked.

Reset Lockout Count = 5 – After 5 minutes the count will be reset.

Lockout Duration = 30 – The account is locked for 30 minutes.

LSA Anonymous Name Lookup = 0 – This disables showing account information to non-authenticated users. This feature is not needed when running Windows 2000 and higher.

Enable Guest Account = 0 – The Guest account is disabled.

Audit System Events = 3 – Success and Failure of system event calls is audited.

Audit Logon Events = 3 – Success and Failure of logons to this server is audited.

Audit Account Logon = 3 – Success and Failure of logons authenticating to this server is audited.

LmCompatibilityLevel=4,4 – Machines request NTLMV2 but fail backwards to NTLMv1 authentication. Weak LM authentication is refused.

NoLMHash=4,1 – When a password is changed the LM hash is not stored on the local machine.

RestrictAnonymous=4,1 – Anonymous attempts to not get granted the same permissions as the “Everyone” group.

RestrictAnonymousSAM=4,1 – Anonymous users cannot enumerate the SAM (Security Accounts Manager). The following services are disabled: Messenger and Telnet.

Regular User accounts do not have write access to the Windows directory or the Windows\System32 directory.

ⁱⁱ The Default SSU Template configures basic best practices security settings for workstations and servers. It is not all encompassing and can be added to but it is an excellent place to start. The following settings are configured:

Minimum Password Age = 10 days – A user cannot change their password within 10 days of setting it.

Maximum Password Age= 120 days – A password must be changed every 120 days.

Minimum Password Length = 8 characters – Passwords must be at least 8 characters long.

Password Complexity = 1 – Passwords must contain letters, numbers, at least one uppercase letter and a special character (e.g. !& \$#@)

Lockout Bad Count = 5 – After 5 failed login attempts the account will become locked.

Reset Lockout Count = 5 – After 5 minutes the count will be reset.

Lockout Duration = 30 – The account is locked for 30 minutes.

LSA Anonymous Name Lookup = 0 – This disables showing account information to non-authenticated users. This feature is not needed when running Windows 2000 and higher.

Enable Guest Account = 0 – The Guest account is disabled.

Audit System Events = 3 – Success and Failure of system event calls is audited.

Audit Logon Events = 3 – Success and Failure of logons to this server is audited.

Audit Account Logon = 3 – Success and Failure of logons authenticating to this server is audited.

LmCompatibilityLevel=4,4 – Machines request NTLMV2 but fail backwards to NTLMv1 authentication. Weak LM authentication is refused.

NoLMHash=4,1 – When a password is changed the LM hash is not stored on the local machine.

RestrictAnonymous=4,1 – Anonymous attempts to not get granted the same permissions as the “Everyone” group.

RestrictAnonymousSAM=4,1 – Anonymous users cannot enumerate the SAM (Security Accounts Manager). The following services are disabled: Messenger and Telnet.

Regular User accounts do not have write access to the Windows directory or the Windows\System32 directory.

ⁱⁱⁱ The Default SSU Template configures basic best practices security settings for workstations and servers. It is not all encompassing and can be added to but it is an excellent place to start. The following settings are configured:

Minimum Password Age = 10 days – A user cannot change their password within 10 days of setting it.

Maximum Password Age= 120 days – A password must be changed every 120 days.

Minimum Password Length = 8 characters – Passwords must be at least 8 characters long.

Password Complexity = 1 – Passwords must contain letters, numbers, at least one uppercase letter and a special character (e.g. !& \$#@)

Lockout Bad Count = 5 – After 5 failed login attempts the account will become locked.

Reset Lockout Count = 5 – After 5 minutes the count will be reset.

Lockout Duration = 30 – The account is locked for 30 minutes.

LSA Anonymous Name Lookup = 0 – This disables showing account information to non-authenticated users. This feature is not needed when running Windows 2000 and higher.

Enable Guest Account = 0 – The Guest account is disabled.

Audit System Events = 3 – Success and Failure of system event calls is audited.

Audit Logon Events = 3 – Success and Failure of logons to this server is audited.

Audit Account Logon = 3 – Success and Failure of logons authenticating to this server is audited.

LmCompatibilityLevel=4,4 – Machines request NTLMV2 but fail backwards to NTLMv1 authentication. Weak LM authentication is refused.

NoLMHash=4,1 – When a password is changed the LM hash is not stored on the local machine.

RestrictAnonymous=4,1 – Anonymous attempts to not get granted the same permissions as the “Everyone” group.

RestrictAnonymousSAM=4,1 – Anonymous users cannot enumerate the SAM (Security Accounts Manager). The following services are disabled: Messenger and Telnet.

Regular User accounts do not have write access to the Windows directory or the Windows\System32 directory.