

Rules for Win2K security

Rule 1

Remove all unnecessary programs and Windows Components. You can do this via the Control Panel's Add/Remove Programs module. (Why patch a service or program that shouldn't be running in the first place?)

Rule 2

Disable unneeded services. A significant number of services and background processes are installed and started by default; disable any services that aren't absolutely necessary for your server's everyday performance. This is done via the Services module under Administrative Tools.

For a complete listing of Windows 2000 services and a description of their purpose, take a look at Microsoft's [Glossary of Windows 2000 Services](#).

Rule 3

Change User Rights. By default, User Rights is wide open. Close this hole with the following recommendations for specifying Group or User rights.

1. Access this computer from the network--Remove the Everyone Group and replace it with a group that's more restrictive, such as Authenticated Users.
2. Bypass Traverse Checking--Remove the Everyone Group and replace it with Authenticated Users.
3. Create Permanent Shared Objects--Replace with Administrators Group only.
4. Logon Locally--Replace with Administrators by username and Service Accounts. I recommend by username because this creates an additional security mechanism in case a rogue user tries to gain console access with a tool that escalates the user's privilege to Administrator.
5. Shutdown System--Replace with Administrators Group only.

Rule 4

Synchronize your clocks and enable auditing. If you're going to compare logs from different systems after a security incident, all of your systems must have the same time. Auditing will track changes to your system when employed properly. At a minimum, audit these events for both Success and Failure:

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access (monitor for failure only)
- Policy change
- Privilege use
- Restart, Shutdown, and System

Rule 5

Disable unnecessary file sharing. Unless absolutely necessary, remove hidden drive letters and remote admin shares (ADMIN\$, C\$, D\$, etc.). To remove these admin shares permanently, set the registry key AutoShareServer to 0. This key is found at:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer
\Parameters

If the key isn't present, add a value of type REG_DWORD and set that to 0. This permanently disables all automatic hidden shares.

Rule 6

Set and enforce strict file level and registry permissions. Go through your directories and verify that only specific groups have access to the information contained within them. Restrict anonymous users from accessing the registry. This can be done by a registry key:

HKLM\System\CurrentControlSet\Control\LSA\restrictanonymous

Or via a Group Policy:

Group Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Additional restrictions for anonymous connections

The values for the registry key or the Group Policy Object are:

1=Do not allow enumeration of SAM accounts and shares.

2=No access without explicit anonymous permissions.

Rule 7

Minimize your servers' exposure to denial of service attacks. Windows 2000 allows you to adjust the TCP/IP parameters to have greater control over connection state. Take advantage of this by modifying the following hive with these registry entries:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

1. SynAttackProtect: REG_DWORD=2. Drops third packets of the TCP/IP handshake in an attempt to consume available session handles.
2. TcpMaxHalfOpen: REG_DWORD=500. Limits the number of half-opened TCP sessions.
3. EnablePMTUDiscovery: REG_DWORD=0. Prevents the use of nonstandard Path Maximum Transmission Unit size for all external connections.
4. Netbt\Parameters\NoNameReleaseOnDemand: REG_DWORD = 1. Prevents an external host request for the server's NetBIOS name.
5. EnableDeadGWDetect REG_DWORD = 0. Prevents a server from switching gateways and allowing an attacker to hijack a session.
6. EnableICMPRedirects: REG_DWORD = 0. Prevents an external host from modifying the server's routing table.
7. DisableIPSourceRouting: REG_DWORD=1. Disables client source routing attempts.

Patching a poor configuration is useless until you add the first layer of security to your operating system: Locking down the operating system is the start of any deployment. After your operating system is secure, verify that your server isn't listening on any ports that aren't integral to its day-to-day operation and block all nonessential traffic from the Internet to your system. Security is a layered approach, and this list is by no means complete. But it's a start to hardening Internet-exposed servers.