The Quick Lockdown

Securing Windows Servers
Derek Milroy
derek.milroy@corp-sec.net
www.corp-sec.net
All checklists and scripts referenced in this presentation are available at:
www.corp-sec.net

The approach presented focuses on both efficiency and effectiveness, without breaking application functionality. The presenter has implemented hardening on several hundred servers across multiple companies.
Why Harden Hosts?

- Hardening: Altering the default configuration of an operating system to move it closer to a “deny all by default” security posture.
- Worms
- Script kiddies
- Cross-platform vulnerability aggregation
Checklist Types

Member Server Hardening Checklist
Domain Controller Hardening Checklist
Web Server Hardening Checklist
Terminal Server Hardening Checklist
Section 1

- Reboot the server to make sure there are no pre-existing issues with it. If you have (easy) physical access to the server, do a complete power-down. Otherwise, do a shutdown and restart.
Go to Indexing Service properties and turn off all directories for the system partition.

Right Click On “My Computer” and choose “Manage”

(start…run…ciadv.msc)

Expand the Services and Applications section on the right side of the window

Click on Indexing Service (below the Services and Applications Item)

Delete all catalogs that appear in the right window
W2K - Select the “Log on Screen Saver” after 15 minutes, require password to unlock
W2K3 – Windows 2003 Screen Saver after 10 minutes, require password to unlock

Change log sizes –
  Application: 5120, overwrite as needed
  Security: 10240, overwrite as needed
  System: 5120, overwrite as needed

For W2K3 set all three to 131072

Rename Administrator to standard and get rid of the default descriptions.
  Create a “new” Local User named Administrator, inserting the default descriptions from the real Administrator account – set to user cannot change password, password never expires – make it 14 characters (15+ for W2K3)…strong.
Handling Local Administrator Passwords

- Why rename the Administrator account?
  - Detect automated attacks and worms
- Consider using different naming convention standard for Internet facing vs. Internal domains/forests
- Make passwords for local administrator accounts separate from domain administrator accounts
- Make the passwords 15 character, strong, random – or use a passphrase
- Do not log on regularly with local administrator accounts
- Script regular password changes for local administrator account passwords or use a commercial product like User Manager Pro
- Use random passwords
- Store local administrator passwords in an encrypted database like the one found at: [http://www.schneier.com/passsafe.html](http://www.schneier.com/passsafe.html)
Account Policies:

Password Policy:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>45 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>5 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>8 characters</td>
</tr>
<tr>
<td>Passwords must meet complexity requirements</td>
<td>Enabled***</td>
</tr>
<tr>
<td>Store password using reversible encryption for all users in the domain</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

***At the Domain level, this setting may have to be the same as the weakest link in the chain if you have password synchronization software in your environment. (Some platforms can’t enforce alphanumeric passwords with upper and lower characters required.)

Account Lockout Policy:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account lockout duration</td>
<td>60 minutes</td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>5 invalid logon attempts</td>
</tr>
<tr>
<td>Reset account lockout counter after</td>
<td>60 minutes</td>
</tr>
</tbody>
</table>
Audit Policy: FOR all servers **EXCEPT** Print and Proxy Servers:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Success, Failure</td>
</tr>
</tbody>
</table>

Audit Policy: **PRINT SERVERS AND PROXY SERVERS**:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Success, Failure</td>
</tr>
</tbody>
</table>
User Rights Assignment:

**Policy**

Access this computer from the network

- Authenticated Users
- Backup Operators
- Administrators
- IWAM_"Computername"
- IUSR_"Computername"

Act as part of the operating system

- Authenticated Users
- Backup Operators
- Administrators
- IWAM_"Computername"
- IUSR_"Computername"

**Bypass traverse checking**

- Backup Operators
- Administrators
- Authenticated Users
- Users

**Change the system time**

- Backup Operators
- Administrators
- Authenticated Users
- Users

Create a pagefile

- Backup Operators
- Administrators

Create a token object

- Backup Operators
- Administrators

Create Global Objects

- Backup Operators
- Administrators

Create permanent shared objects

- Backup Operators
- Administrators

Debug programs

- Backup Operators
- Administrators

Deny access to this computer from the network

- Backup Operators
- Administrators
Deny logon as a batch job
Deny logon as a service
Deny logon locally
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Generate security audits
Impersonate a client after authentication
Increase quotas
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Log on as a service
**Log on locally**

Manage auditing and security log
Modify firmware environment values

**Profile single process**
Profile system performance
Remove computer from docking station

Replace a process level token
Restore files and directories

**Shut down the system**

Synchronize directory service data
Take ownership of files or other objects

Administrators

**Administrators**
Administrators
Users
Power Users
Administrators

Backup Operators
Administrators

Backup Operators
Administrators
### Security Options:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Additional restrictions for anonymous connections</strong></td>
<td><strong>Do not allow enumeration of SAM accounts and shares</strong></td>
</tr>
<tr>
<td>Allow server operators to schedule tasks (domain controllers only)</td>
<td>Not defined</td>
</tr>
<tr>
<td>Allow system to be shut down without having to log on</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allowed to eject removable NTFS media</td>
<td>Administrators</td>
</tr>
<tr>
<td>Amount of idle time required before disconnecting session 15 minutes</td>
<td>Disabled</td>
</tr>
<tr>
<td>Audit the access of global system objects</td>
<td>Disabled</td>
</tr>
<tr>
<td>Audit use of Backup and Restore privilege</td>
<td>Disabled</td>
</tr>
<tr>
<td>Automatically log off users when logon time expires (local)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Clear virtual memory pagefile when system shuts down</td>
<td>Disabled</td>
</tr>
<tr>
<td>Digitally sign client communication (always)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Digitally sign client communication (when possible)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Digitally sign server communication (always)</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Digitally sign server communication (when possible)</strong></td>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td>Disable CTRL+ALT+DEL requirement for logon</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Do not display last user name in logon screen</strong></td>
<td><strong>Send LM &amp; NTLM – use NTLMv2 session security if negotiated</strong></td>
</tr>
<tr>
<td><strong>LAN Manager Authentication Level</strong></td>
<td><strong>Message text for users attempting to log on</strong></td>
</tr>
<tr>
<td>Attempting to log on</td>
<td>In Legal Message title for users attempting to log on</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Number of previous logons to cache</td>
<td>0 logons</td>
</tr>
<tr>
<td>Prevent system maintenance of computer account password</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent users from installing printer drivers</td>
<td>Enabled</td>
</tr>
<tr>
<td>Prompt user to change password before expiration</td>
<td>14 days</td>
</tr>
<tr>
<td>Recovery Console: Allow automatic administrative logon</td>
<td>Disabled</td>
</tr>
<tr>
<td>Recovery Console: Allow floppy copy and access to all drives and all folders</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rename administrator account</td>
<td>TO Standard</td>
</tr>
<tr>
<td>Rename guest account</td>
<td>TO Standard</td>
</tr>
<tr>
<td>Restrict CD-ROM access to locally logged-on user only</td>
<td>Enabled</td>
</tr>
<tr>
<td>Restrict floppy access to locally logged-on user only</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure channel: Digitally encrypt or sign secure channel data (always)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure channel: Digitally encrypt secure channel data (when possible)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure channel: Digitally sign secure channel data (when possible)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure channel: Require strong (Windows 2000 or later) session key</td>
<td>Disabled</td>
</tr>
<tr>
<td>Send unencrypted password to connect to third-party SMB servers</td>
<td>Disabled</td>
</tr>
<tr>
<td>Shut down system immediately if unable to log security audits</td>
<td>Disabled</td>
</tr>
<tr>
<td>Smart card removal behavior</td>
<td>Lock Workstation</td>
</tr>
<tr>
<td>Strengthen default permissions of global system objects (e.g. Symbolic Links)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unsigned driver installation behavior</td>
<td>Warn</td>
</tr>
<tr>
<td>Unsigned non-driver installation behavior</td>
<td>Warn</td>
</tr>
</tbody>
</table>
For More Details on User Rights and Security Settings Sections

Q823659
“Client, Service, and Program Incompatibilities That May Occur When You Modify Security Settings and User Rights Assignments”

http://support.microsoft.com/default.aspx?scid=kb;en-us;823659
You’ll notice that restrict anonymous is set to 1 “Do not allow enumeration of SAM accounts and shares” instead of 2 “No access without explicit anonymous permissions”. This is to account for mixed mode environments.

Setting restrict anonymous interferes with printing. Setting restrict anonymous to 2 also causes problems with browsing on server segments that have both NT 4.0 and Windows 2000 servers but no domain controllers. If a Windows 2000 server with restrict anonymous set to 2 wins the election, your browsing will not function properly. Many administrative tools and functions rely on proper browsing. (A necessary evil in larger environments?)

Everyone says setting restrict anonymous to 2 is highly important.

No matter how many times they fix it, someone breaks it. So is having it set to one a big deal in a mixed mode environment? Probably not.
Section 2

Registry Modifications
Secure the event logs (application, system, and security) from Guest Access (ADD 3 keys, one for each.)
Hive: HKEY_LOCAL_MACHINE\System
Key: \CurrentControlSet\Services\EventLog\%LOGNAME%
Value Type: REG_DWORD
Value Name: RestrictGuestAccess
Value: 1

Disable CD-ROM Autorun (MODIFY this value.) (This can be done via policy under admin templates…system)
Hive: HKEY_LOCAL_MACHINE\System
Key: \CurrentControlSet\Services\CDRom
Value Type: REG_DWORD
Value Name: Autorun
Value: 0
Disable 8.3 Filename Creation – Modify **Sometimes applications need this value re-enabled for installs or upgrades**
Hive: HKEY_LOCAL_MACHINE\System
Key: \CurrentControlSet\Control\Filesystem
Value Type: REG_DWORD
Value Name: NTFSDisable8dot3NameCreation
Value: 1

Enable Syn Attack Protect (Q142641) - Add
Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\Tcpip\Parameters\Name: SynAttackProtect
Type: REG_DWORD
Value: 2
NOTE: If the SynAttackProtect key modification proves to be ineffective or a specific resources are being continuously hit by SYN Attacke, see MS Q142641. Also consider changing the TcpMaxPortsExhausted value to 1 and the TcpMaxDataRetransmissions value to 3 (see regentry.chm from the WIN2K resource Kit).
Configure Dead Gateway Protection
Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\Tcpip\Parameters
Name: EnableDeadGW Detect
Type: REG_DWORD
Value: 0

Disable Router Discovery
Note: Make sure IDRP is not in use in the client’s perimeter network.
Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[InterfaceName]\PerformRouterDiscovery
Name: PerformRouterDiscovery
Type: REG_DWORD
Value: 0

Disable ICMP Redirects - Change the value… the key is already there.
(Q225344)
Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\Tcpip\Parameters
Name: EnableICMPRedirect
Type: REG_DWORD
Value: 0
→ Disable IP Source Routing
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: DisableIPSourceRouting
Type: REG_DWORD
Value: 2

→ Tune the TCP/IP KeepAlive Time
Note: This setting is most appropriate to web servers, but may apply to other applications.
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: KeepAliveTime
Type: REG_DWORD
Value: 300000

→ Disable External Name Release
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: NoNameReleaseOnDemand
Type: REG_DWORD
Value: 1
→ Enable PMTU Discovery*
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: EnablePMTUDiscovery
Type: REG_DWORD
Value: 0

→ TcpMaxConnectResponseRetransmissions (default)
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: TcpMaxConnectResponseRetransmissions
Type: REG_DWORD
Value: 2

→ TcpMaxDataRetransmissions
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: TcpMaxDataRetransmissions
Type: REG_DWORD
Value: 3
Disabling PMTU Discovery

- This setting makes the default MTU size = 576. The default (with PMTU Discovery enabled) is 1500.
- In segmented environments (lots of VLANs), this can triple the amount of packets on your network. It can also adversely affect applications accessed via WAN links.
- Issues:
  - Setting MTU back to 1500 is interface specific
  - Not easily scriptable (if at all)
  - If a NIC is replaced the settings may not be
TCPMaxPortsExhausted (default)
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: TCPMaxPortsExhausted
Type: REG_DWORD
Value: 5

Disable All Autorun
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoDriveTypeAutoRun
Type: REG_DWORD
Value: 0xFF

ADDITIONAL EDIT FOR W2K3

Enable Kerberos Logging
Hive: HKEY_LOCAL_MACHINE\System
Key: \CurrentControlSet\Control\LSA\Kerberos\Parameters
Value Type: REG_DWORD
Value Name: LogLevel
Value: 1
For More Details on TCP/IP Stack Hardening

- Q120642
  “TCI/IP and NBT Configuration Parameters for Windows 2000 or Windows NT”
Section 3

Registry Permissions
Restrict permissions for the following registry locations: YOU MUST USE REGEDT32!
Be sure to remove “allow inheritance” prior to applying permissions, choose “copy” rather than remove.

The Permissions should all be set to the following:
Administrators (Full Control)
SYSTEM (Full Control)
Creator Owner (Full Control) [leave alone on Run, Run Once, Run Once Ex, Uninstall, and AeDebug]
ADD: Authenticated Users (Read)

Creator Owner (Full Control) leave alone on Run
Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows\CurrentVersion\Run

Creator Owner (Full Control) leave alone on Run Once
Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows\CurrentVersion\RunOnce

Creator Owner (Full Control) leave alone on Run Once Ex
Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows\CurrentVersion\RunOnceEx
Creator Owner  (Full Control) leave alone on Uninstall
   → Hive: HKEY_LOCAL_MACHINE\SOFTWARE
         Key: \Microsoft\Windows\CurrentVersion\Uninstall

Creator Owner  (Full Control) leave alone on AeDebug
   → Hive: HKEY_LOCAL_MACHINE\SOFTWARE
         Key: \Microsoft\Windows NT\CurrentVersion\AeDebug

   → Hive: HKEY_LOCAL_MACHINE\SOFTWARE
         Key: \Microsoft\Windows NT\CurrentVersion\Winlogon

   → Use REGEDT32 to set permissions on the following registry key.

Permissions should be set to:
   Administrator & System = Full Control
   Authenticated Users = Read

HKLM\Software\Microsoft\Rpc

ALL OF THESE ARE DONE BY DEFAULT FOR W2K3
Section 4

File System ACLs
(See the SANS WIN2K Step-By-Step Guide. This is a sub-set from that checklist.)

→ Change NTFS permissions for C:\ to Administrators and System: Full control and Authenticated Users with Read & Execute
→ Change NTFS permissions on C:\boot.ini, C:\ntddetect.com, and C:\ntldr
→ Change NTFS permissions on C:\Program Files to Administrators and System: Full control and Authenticated Users with Read & Execute
→ Change NTFS permissions for %systemroot%\repair to only Administrators and System: Full control Also, EXPLICITLY set permissions for the IUSR and IWAM (and any other web site service accounts) to NO ACCESS
→ Change NTFS permissions on directory %systemroot%\security to only Administrators and System with Full Control
→ Change NTFS permissions on directory %systemroot%\system32\config to only Administrators and System with Full Control Also, EXPLICITLY set permissions for the IUSR and IWAM (and any other web site service accounts) to NO ACCESS
→ Change NTFS permissions on directory %systemroot%\system32\dllcache to only Administrators and System with Full Control
→ Change NTFS permissions on directory %systemroot%\system32\logfiles to only Administrators and System with Full Control

ALL OF THESE ARE DONE BY DEFAULT FOR W2K3
Section 5

Utilities, Service Packs/Hot Fixes, and Services
→ Copy passprop.exe to the winnt\system32 directory and run passprop (start, run, passprop /complex /adminlockout

→ Run the Set Version Batch File

The set version batch writes information to the registry:
  compliance reporting via Retina or LANGuard v3.0
  information for troubleshooting
Set permissions to the local administrator account for the following command-line utilities. Also, consider EXPLICITLY setting permissions for the IUSR and IWAM users (and any other web site service accounts) to NO ACCESS. (For highly secure environments, consider moving, renaming, or deleting any command-line utilities.)

The following tools are usually found in the Winnt\System32 directory:

| append.exe | arp.exe  | at.exe   |
| attrib.exe | cacls.exe | change.exe |
| chcp.com   | chglogon.exe | chgport.exe |
| chguser.exe| chkdisk.exe | chkntfs.exe |
| cipher.exe | cluster.exe | cmd.exe   |
| compact.exe| command.com | convert.exe |
| cscript.exe| dcpromo.exe | debug.exe |
| dfscmd.exe | diskcomp.com | diskcopy.com |
| doskey.exe | edlin.exe | exe2bin.exe |
| expand.exe | fc.exe    | find.exe  |
| findstr.exe| finger.exe | forcedos.exe |
| format.com | ftp.exe   | hostname.exe |
| iisreset.exe| ipconfig.exe | ipxroute.exe |
| label.exe  | logoff.exe | makecab.exe |
The following tools are usually found in the Winnt directory:
Regedit.exe

W2K3 has more utilities  (IIS even more)

Install the latest Service Packs and Hot Fixes
Disable unnecessary services and features. The services in bold are stopped and disabled:

Alerter
Automatic Updates
Background Intelligent Transfer Service
ClipBook
Computer Browser
DHCP Client – not yet
Distributed File System
Distributed Link Tracking Client
Distributed Link Tracking Server
Fax Service
File Replication
FTP Publishing Service
Indexing Service
Internet Connection Sharing
Intersite Messaging
Kerberos Key Distribution
Messenger
Net Meeting Remote Sharing
Network DDE
Network DDE DSDM
Print Spooler – done in build
QoS RSVP
Remote Access Auto Connection Manager
Remote Access Connection Manager – not on Compaq Servers
Remote Registry Service  (DO NOT DISABLE THIS – Update Software must have this.)
Removable Storage
Routing and Remote Access
RunAs Service
Smart Card
Smart Card Helper
TCP/IP NetBIOS Helper (Bastion only)
Task Scheduler  (DO NOT DISABLE THIS – Update Software must have this.)
Telephony – not on Compaq Servers
Telnet

Many of these are disabled by default in W2K3
Section 6

OS/2 and POSIX Subsystems Removal
Run the script, “S6.windows2000.OS2POSIX.subsystem.removal.part.1.cmd” is in the \Lockdown\W2K directory.

**WAIT for the Windows File Protection pop-up window to appear.**
When it appears and prompts to restore those files from the Windows CD, click “Cancel” and click “Yes” to confirm.

Reboot the system.

Run the script, “S6.windows2000.OS2POSIX.subsystem.removal.part.2.cmd” is in the \Lockdown\W2K directory.

**WAIT for the Windows File Protection pop-up window to appear.**
When it appears and prompts to restore those files from the Windows CD, click “Cancel” and click “Yes” to confirm.

Reboot the system.

SP3 Completely Replaces both subsystems
Section 7

Resource Kit
Remove the following Resource Kit Components:

Via Add/Remove Programs:
- De-select: “Tool Documentation”
- De-select: “Deployment Tools”
- De-select: “Computer Management Tools”
- De-select: “Network Management Tools”
- De-select: “Diagnostic Tools”
- De-select: “File and Disk Tools”
- De-select: “Debug Tools”
- De-select: “Desktop Tools”
- De-select: “Remote Administration Scripts” ***VERY DANGEROUS!!!***
- Scripting Tools
  - De-select: “KiXtart 95”
  - De-select: “POSIX Utilities”
  - De-select: “Active Perl”
  - De-select: “AutoEXNT Service”
  - De-select: “Internet Information Services”
  - De-select: “Security Tools”

Use only the files you need with ACLs in d:\Program Files\reskit
Section 8

Other Items to Consider:

- Configure TCP/IP Filters, Consider the use of IPSEC Policies
- Tune your virus protection, scan all inbound files, set exclusions as needed.
- Scan the server with one or more of the following: MBSA, LANGuard Network Scanner, Nessus
Section 9

- TSE Admin Settings for all servers
- Must be done manually
- Delete the TSInternet user first – SPs add it back?
(Start…run…tscc.msc…double click on the RDP-Tcp Connection)

→ RDP Connection Settings: Modify the following items, leave the rest of the defaults.

→ On the General Tab: Set encryption to high

→ On the Sessions Tab: Check the First “Override user settings” box and set the following values:
  → End a disconnected session: 30 minutes
  → Active session limit: Never (no limit)
  → Idle session limit: 1 day

→ On the Sessions Tab: Check the Second “Override user settings” box and set the following values:
  → When a session limit is reached or connection is broken: End session

→ On the Remote Control Tab, select:
  → Do not allow remote control
→ On the Client Settings Tab, make sure the following options are disabled:
  Disable the following:
→ Windows printer mapping
→ LPT port mapping
→ COM port mapping (default)
→ Clipboard mapping
→ Audio Mapping **W2K3**

→ On the Permissions Tab: Click the advanced button, select the auditing tab, and click add

→ Set focus to the local machine and select the administrators group

→ Select the following options: (select both Successful and Failed for all items below)
  ○ Remote Control
  ○ Logon
  ○ Logoff
  ○ Connect
  ○ Disconnect
Section 10

Registry Modifications

IIS Specific
- Enable Logging of SSL Events (errors and warnings)
  Hive: HKEY_LOCAL_MACHINE
  Key: System\CurrentControlSet\Control\SecurityProviders\SChannel
  Name: EventLogging
  Type: REG_DWORD
  Value: 3

- Disable use of the Command shell with #exec
  Hive: HKEY_LOCAL_MACHINE
  Key: System\CurrentControlSet\Services\W3SVC\Parameters
  Name: SSIModeEnableCMDDirective
  Type: REG_DWORD
  Value: 0
Enable settings for Afd.sys (as per the MS Windows 2000 Security Operations Guide)

- **Hive:** HKEY_LOCAL_MACHINE
  **Key:** System\CurrentControlSet\Services\AFD\Parameters
  **Name:** DynamicBacklogGrowthDelta
  **Type:** REG_DWORD
  **Value:** 10

- **Hive:** HKEY_LOCAL_MACHINE
  **Key:** System\CurrentControlSet\Services\AFD\Parameters
  **Name:** EnableDynamicBacklog
  **Type:** REG_DWORD
  **Value:** 1

- **Hive:** HKEY_LOCAL_MACHINE
  **Key:** System\CurrentControlSet\Services\AFD\Parameters
  **Name:** MinimumDynamicBacklog
  **Type:** REG_DWORD
  **Value:** 20

- **Hive:** HKEY_LOCAL_MACHINE
  **Key:** System\CurrentControlSet\Services\AFD\Parameters
  **Name:** MaximumDynamicBacklog
  **Type:** REG_DWORD
  **Value:** 20000
Section 11

IIS Settings

- Most scripted in sections.
- Custom for each set of application servers.
- Logging should be enabled on all web servers.
Move the webroot files to a non-system partition

- Stop IIS-related services. If you stop IIS Admin Service, all other IIS-related services stop, too.
- Copy `c:\inetpub` to `d:\` (Use `robocopy` with the `/SEC switch`)
- Start the IIS Admin snap-in under MMC
- Redirect all IIS application parameters to `d:\inetpub\...(Default Web Site Properties – Home Directory Tab – Change the local path setting)`
- Register `metautil.dll`
- Run MetaEdit
- Find all references to `c:\inetpub\... Change to `d:\inetpub\...`
- `UN_REGISTER metautil.dll`
- `Shift + Delete metautil.dll`
- Restart the server
- `Shift + Delete c:\inetpub`

Or use ver 2.2 and add/remove programs
Perform the following for all Web Servers: Intranet or Internet (Bastion Host):

- Use the following rule of thumb for NTFS file permissions on the Web Server:
  - Another rule of thumb is to separate these file types into separate directories and apply the permissions to the Directories instead of individual files:

<table>
<thead>
<tr>
<th>File Type</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGI Files, etc.</td>
<td>( .EXE, .DLL, .CMD, .PL) Everyone (X) Administrators (Full Control) System (Full Control)</td>
</tr>
<tr>
<td>Script Files</td>
<td>( .ASP etc ) Everyone (X) Administrators (Full Control) System (Full Control)</td>
</tr>
<tr>
<td>Include Files</td>
<td>( .INC, .SHTML, .SHTM ) Everyone (X) Administrators (Full Control) System (Full Control)</td>
</tr>
<tr>
<td>Static Content</td>
<td>( .HTML ) Everyone (R) Administrators (Full Control) System (Full Control)</td>
</tr>
<tr>
<td>Images</td>
<td>( .GIF, .JPEG ) Everyone (R) Administrators (Full Control) System (Full Control)</td>
</tr>
</tbody>
</table>

CAUTION: When a folder has both write and execute IIS Permissions, an attacker can upload any executable and run it on the server. If two virtual folders are mapped to the same physical folder, and one virtual folder has Write and the other virtual folder has Execute, attackers can still upload any executable and run it on the server.
→ Set the Web Server Logging to W3C Extended Format and log the following properties:
Leave the New Log Time Period set to Daily
Select: “Use local time for naming and rollover”
Make sure the defaults for logging are enabled and add the ones in bold:
→ Client IP Address
→ User Name
→ **Service Name**
→ **Server Name**
→ Server IP Address
→ Server Port
→ Method
→ URI Stem
→ URI Query
→ Protocol Status
→ User Agent
→ **Cookie**
→ **Referer**
→ **ALL s-events under the Process Accounting Box**
Follow these steps to disable IP Address in the Content Location header: This secures against providing “Hidden” (internal NAT’ed addresses) in the web page header. The following fix will change the header to display the FQDN instead. See Q218180

- Open a command window.
- Change to the winnt\system32\inetsrv\adminsamples directory
- Type this command: “cscript adsutil set w3svc/UseHostName True”
- Type net stop iisadmin /y
- Type net start w3svc
Remove all IIS Sample Applications i.e. delete the following directories:

- \InetPub\AdminScripts
- \InetPub\iisamples
- \WINNT\System32\inetsrv\iisadmin (check with server/application owner)
- \WINNT\System32\inetsrv\iisadminpwd (check with server/application owner)
- \WINNT\Help\iishelp

Perform the following removals from within IIS Administrator:

- Remove the IISamples sub-object of the “Default Web Site”
- Remove the IISAdmin sub-object of the “Default Web Site”
- Remove the Printers sub-object of the “Default Web Site”
- Remove the IIS Help sub-object of the “Default Web Site”
- Disable Internet Printing
  - Delete the Printers Virtual Directory located at: %systemroot%\web\printers

- Perform the following registry edit:
  Hive: HKEY_LOCAL_MACHINE
  Key: Software\Policies\Microsoft\Windows NT\Printers
  Name: DisableWebPrinting
  Type: REG_DWORD
  Value: 1

NOTE: Internet Printing can be configured via group policy as well as via the Internet Services Manager. If there is a conflict between the GPO and Internet Manager settings, the GPO will take precedence. If you remove Internet Printing via the Internet Services Manager, be sure to verify that it won’t be re-enabled by either local or domain GPOs. (The default group policy neither enables nor disables Internet Printing.) In the MMC Group Policy snap-in, check Computer Configuration | Administrative Templates | Printing | Web Based Printing.
Disable Parent Paths: go to the root of each web site, right click, Properties | Home Directory | Configuration | App Options and uncheck “Enable Parent Paths” Ignore the IIS Help message…do NOT select it.
Remove unused script mappings from the Internet Services Manager. File extension mappings for script types that are not being used could be exploited by an intruder to gain access to the system.

(Below is an excerpt from the Microsoft IIS 5.0 Security Checklist)

IIS is preconfigured to support common filename extensions such as .ASP and .SHTM. When IIS receives a request for a file of one of these types the call is handled by a DLL. If you don't use some of these extensions or functionality you should remove the mappings by open Internet Services Manager then right-clicking the Web server | Properties | Master Properties | WWW Service | Edit | HomeDirectory | Configuration and remove these references:

If you don’t use: Remove this entry:
Web-based password reset .htr
Internet Database Connector .idc
Server-side Includes .stm, .shtm, .shtml
Internet Printing .printer
Index Server .htw, .ida, .idq

NOTE: The ISAPI Extension Mappings shown above may reappear whenever ANY Windows Component is added or removed via the Add/Remove Utility in the Control Panel.
- Change Application Protection to “Medium Pooled” on the Home Directory tab for all web sites (this is the default setting…double check it)

- Disable WebDAV, unless needed…Using it is NOT recommended!!!
  (Q241520)
  Hive: HKEY_LOCAL_MACHINE
  Key: System\CurrentControlSet\Services\W3SVC\Parameters
  Name: DisableWebDAV
  Type: REG_DWORD
  Value: 1
When possible, install IIS using an unattended install with the following answer file

[Components]
iis_common=on
iisdbg=off
iis_doc=off
iis_ftp=off
iis_htmla=off
iis_inetmgr=on
iis_nntp_docs=off
iis_pwmgr=off
iis_smtp=off
iis_smtp_docs=off
iis_www=on
iis_www_vdir_msadc=off
iis_www_vdir_printers=off
iis_www_vdir_scripts=off
iis_www_vdir_terminalservices=off

[InternetServer]
PathWWWRoot=D:\Inetpub\WWW Root
RDS Keys

RDS Keys: (Used for direct connections between the client and the database server, rarely used. Recommended against by Microsoft.) Note: Upgrading to MDAC v2.6 or greater should nullify this vulnerability but it is not a good idea to rely solely on patches i.e. the entries should still be deleted. (see Q184375)
Remove MDAC: IF it’s not used in the Client’s Environment! Consult with the server/application owner prior to implementation.

- Delete the /msadc virtual directory from the default Web site
- Delete the Samples Directory at:
  C:\Program Files\Common Files\System\msadc\Samples
- Remove the following registry keys (if present) from the IIS Server

  Hive: HKEY_LOCAL_MACHINE\SYSTEM
  Key: CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer. DataFactory

  Hive: HKEY_LOCAL_MACHINE\SYSTEM
  Key: CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

  Hive: HKEY_LOCAL_MACHINE\SYSTEM
  Key: CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
Section 13

- FTP Settings
- Standards for FTP and SMTP are in progress.
Dedicate ANY volume accessible by the FTP server explicitly to the FTP Service, if possible.

Enable Directory Annotation. (You must add this key)
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\MSFTPSvc\Parameters
Name: AnnotateDirectories
Type: REG_DWORD
Value: 1

Implement a banner that states the company that owns the FTP site and that unauthorized use is prohibited.

Whenever possible, disable anonymous access, use NTFS and FTP site permissions to restrict access granted for specific users as much as possible.
Troubleshooting

- Restrict Anonymous (Printing)
- File system ACLs
IISLOCKDOWN.exe Usage

- GUI
- Unattended
- URLScan
URLScan Troubleshooting

- Start with the URLScan log
Vulnerability Management

- Regression Testing
- Dev and AQ Implementation
- Exception Handling
- Tools
  - Commercial
  - MS Sec OPS Guide - scripts
References:

Securing Windows NT/2000 Servers for the Internet
Stephan Norberg  (ISBN:  1-56592-768-0)

Hacking Exposed Third Edition
Stuart McClure, Joel Scambray, George Kurtz  (ISBN:  0072193816)

Hacking Web Applications Exposed – Web Application Secrets and Solutions
Joel Scambray, Mike Shema  (ISBN:  007222438X)

Hacking Exposed Windows 2000 (Hacking Exposed)
Joel Scambray, Stewart McClure  (ISBN:  0072192623)

Hack Proofing Windows 2000 Server
Chad Todd, Norris L. Johnson Jr.  (ISBN:  1931836493)

Hackers Challenge – Test Your Incident Response Skills Using 20 Scenarios
Mike Schiffman  (ISBN:  0072193840)

Anti-Hacker Toolkit
Keith J. Jones, Mike Shema, Bradley C. Johnson  (ISBN:  0072222824)
Web Hacking Attacks and Defense  

Incident Response – Investigating Computer Crime  
Kevin Mandia, Chris Prosise  (ISBN:  0072131829)

Writing Secure Code  

Windows NT/2000 Thin Client Solutions: Implementing Terminal Services and Citrix MetaFrame  
Todd W. Mathers  (ISBN:  1578702399)

Maximum Windows 2000 Security  

Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses"  
Ed Skoudis  (ISBN:  0130332739)

IIS Security  
AeDebug Vulnerability
  http://www.wiretrip.net/rfp/p/doc.asp?id=15&iface=2

RDS Attack Defense
  http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2

**Securing Windows 2000 Step by Step (version 1.5)**
  The SANS Institute

“Hardening Windows 2000 in the Enterprise” series published on
  www.securityfocus.com
    Tim Mullen

Building a Windows NT Bastion Host in Practice
  Stefan Norberg, HP Consulting

Windows NT Security Guidelines
Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments
  Trusted Systems Services
Secure Windows NT Installation and Configuration Guide
Windows NT for Navy IT-21…version 1.3

NIST Special Publication 800-44 “Guidelines on Securing Public Web Servers”

All guides @ W2Kguides@nsa.gov

The “Internet Information Server (IIS) Security” module from the SANS 2001 GSEC Course

Module 5.4 “Securing Internet Information Server 5.0” from the Track 5 – Securing Windows 2000 SANS Curriculum

SANS Score Windows 2000 Auditing Document

SANS Score Auditing Web Applications Document


Designing and Planning Windows NT External Security by Tom Dodds, Eric Miyadi, and Tom Fuchs*

Securing Windows NT Installation (White Paper by Microsoft)*
Microsoft Windows NT C2 Configuration Checklist*

Microsoft Internet Information Server 5.0 Security Checklist*

Microsoft IIS 5.0 Baseline Security Checklist*

Q189271 List of Services Needed to Run a Secure IIS Computer*

Microsoft Windows 2000: From Blueprint to Fortress: A Guide to Securing IIS 5.0 by John Davis*

Q186433 Clarification of Winreg Operation in Windows NT*

Q153183 How to Restrict Access to the Registry for a Remote Computer*

* Available from Microsoft’s web site

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*

Windows Server 2003 Security Guide*
Questions?

If you have any questions you think of later send an e-mail to:
  - derek.milroy@corp-sec.net

Best effort for answers, usually within a week
Thank You