



SEEKSADMIN WINDOWS HARDENING

1) Installing all Security Patches and Service Packs.

2) Disabling Null sessions to prevent unauthorized access to user list on machine, which can be used with a password cracker to gain illegal access to machine.

3) Installing URL Scan to prevent malicious requests from getting to IIS and causing a buffer overflow.

(URL Scan – Security Tool for IIS - <http://www.microsoft.com/technet/security/tools/urlscan.msp>)

4) Configuration of ASP.Net 1.1 and ASP.Net 2.0 and enabled ASP.NET impersonation, Running them in Medium Trust so that clients can't access other customers directories and can't run unmanaged code.

- ASP.NET Folder Permissions
- ASP.NET Impersonation Settings
- ASP.NET 2 Applications Isolation

ASP.Net 1.1 - <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch09.asp>

ASP.Net 2.0 - <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/PAGHT000020.asp>

5) Hardening of the TCP/IP stack against Denial of Service Attacks.

Microsoft KB Article : <http://support.microsoft.com/default...b;en-us;324270>

6) IIS Modifications/Permissions/Various Log File Generation, Disable Rapid Fail Protection, Full W3SVC Log Generation for AWStats and other Stats Program.

7) Mail Server Security/Mail Relaying settings to protect SPAM, Abuse Detections setup. Microsoft IIS SMTP Security and Relay Settings and Log Generations.

8) Installing MBSA 2.0 to check other security related issues and Vulnerability.

9) Disabling some Unwanted Services like :

- Distributed File System
- Distributed Link Tracking Client
- Distributed Link Tracking Server
- Error Reporting Service
- Fax Service
- Indexing Service
- Netmeeting Remote Desktop Sharing
- Print Spooler
- Telnet

10) Disabling some unused accounts. Disabling the Guest, Support_XXX, and ASPNET accounts. Some of these are disabled by default, and the ASPNET account is only used if IIS 6.0 is run in IIS 5.0 isolation mode (which we don't). IIS 6.0 now uses "Network Services" account instead of ASPNET.

11) Restricted the system tools that are commonly used by attackers to assist with both the initial compromise and expansion beyond the server. tftp(.exe), ftp(.exe), cmd.exe, bash, net.exe, remote.exe, and telnet(.exe).

12) Disabling Windows Shell Execution. Also restricting WMI and ADSI as per setup.

13) Configuring Windows 2003 Internet Connection Firewall.

14) Installing Microsoft Windows Defender (Antispy Program).

15) Installing Antivirus.

16) MS DNS Server Security - Disabling Recursion and Forwarders.

If using SimpleDNS - Enabling Recursion to local IPs and Subnets only and other Security settings etc.

17) NTFS Hacks and Tuning like Turning off NTFS 8.3 Name Generations etc.

18) MySQL Server Security. Disabling Anonymous Accounts, etc.

19) Audit Setups : Local Audit Policies Setups like :

- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy change
- Privilege Use
- Process Tracking
- System Events

20) Lots of User Rights Assignments settings like :

- Audit the access of global system objects
- Interactive Logon to not to display last user name
- Check that the administrator users have strong password

21) NIC Settings/ LAN Connection Settings :

- Disabling Client for MS Networks
- Disabling LMHOSTS lookup
- LAN-Connection shows ICON in Tray when connected (easier access)

22) Assigning restrictive permissions possible at root of drive and other application folder and system folders.

Drive Root Permissions

Domains Folder Permissions

Microsoft IIS Folder Permissions

Microsoft FTP Folder Permissions

CDONTS/CDOSYS Folder Permissions

PHP Folder Permissions

Perl Folder Permissions

Python Folder Permissions etc.

If there are any additional software packages that are not included in the standard package for a web server (Something different from the web hosting control panel, FTP server, Mail server, DNS server, IIS or Apache) we check any permissions and security problems with it.