Patching a Windows 2000 Install

April 2004

These are the initial steps taken to secure a Windows 2000 Professional box installed on an IBM T20 laptop. The OS was installed and Internet Explorer was used for several hours before taking these steps. This, most likely, accounts for the multiple items found by AdAware and Spybot upon installing and running these products.

One item of note was that if you connect your Windows box to the network and use the Windows Update service,then you are exposed without security patches for some period of time while downloading and installing. In my case the downloading, installing, and reboots took around 90 minutes.

The order taken was to turn off some services (Messenger and Telephony), run Windows Updates, install Norton Antivirus, install AdAware, and then install Spybot.

Notes follow:

```
Windows Updates
---------------
1.) Internet Explorer 6 Service Pack (16MB) and reboot. License Agreement required.
2.) W2K Service Pack 4 Express Install for End Users. (36MB). License Agreement required.
        - No indication of download progress for 36MB piece.
        - Install bar moves very, very, very, very slowly.
        - No informational messages.
        - Total install time: 45 minutes
        - Reboot required.
        - After this update Windows Update options suddenly became available for
          new hardware found Wizard dialogue.
        - Before install there were 14 critical updates to perform. After this
          had increased to 17.
3.) At this point I was able to do multiple updates at once. These included:
        - Cumulative Security Update for Outlook Express 6 Service Pack 1 (KB837009) (1.9 MB)
        - Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB832894) (2.8 MB)
        - Critical Update for Windows Media Player Script Commands (KB828026) (2.8 MB)
        - Security Update for Windows 2000 (KB837001) (290 KB)
        - Security Update for Windows 2000 (KB828741) (294 KB)
        - Security Update for Windows 2000 (KB835732) (295 KB)
        - Security Update for Microsoft Data Access Components (KB832483) (2.0 MB)
        - Security Update for Microsoft Windows (KB828749) (281 KB)
        - Security Update for Microsoft Windows 2000 (KB828035) (343 KB)
        - Security Update for Microsoft Windows 2000 (KB825119) (304 KB)
        - Security Update for Microsoft Windows 2000 (KB826232) (329 KB)
        - Security Update for Microsoft Windows (KB824105) (223 KB)
        - Security Update for Windows 2000 (KB823182) (359 KB)
        - 823559: Security Update for Microsoft Windows (382 KB)
        - Flaw In Windows Media Player May Allow Media Library Access (819639) (1.9mb)
        - 816093: Security Update Microsoft Virtual Machine (Microsoft VM) (5.1 mb)
        - 814078: Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP) (361KB)
        - Which adds up to 19.8 MB total. Download about 20 minutes. Install about 7 minutes.
        - Rebooted machine. The initial shutdown takes about an extra minute to save settings.
4.) Scanned for updates and another critical update appeared. This was:
        - Critical Update for Internet Explorer 6 Service Pack 1 (KB831167) (368KB)
        - Required reboot.
5.) Scanned and no more critical updates were required. Two recommended updates for Windows 2000
    were now available. These were:
        - 818043: Recommended Update for Windows 2000 (700 KB)
        - Recommended Update for Windows 2000 (822831) (243 KB)
    In addition updated a few other items, including:
        - Update for Windows Media Player 9 Series (KB837272)
        - Update for Windows 2000 (KB820888)
        - Root Certificates Update
        - Reboot was required.
6.) Scanned and installed the following update as it specified it was a security update:
        - DirectX 9.0b End-User Runtime*
        - Initial install was 293 KB, but then additional several MB of data was downloaded. The
          installer _did not_ indicate how much data was being downloaded.
        - Download and install took about 7 to 10 minutes.
        - Reboot was required.
7.) One final scan. All that was left were:
        - Microsoft Windows Journal Viewer (Windows 2000) (7.0 MB)
        - Microsoft .NET Framework version 1.1 (23.1 MB)
        - Note, if you go to http://www/windowupdate.com/ instead of http://www.windowsupdate.com/
          the site holding that name will leave you with two pop-up windows, one of them full-screen.

Summaries: 6 reboots required
           2 license agreemeents
           70 to 90 minutes (512Kbps connection)
```

```
          22 "critical" updates installed
          4 additional/recommended updates
          57.2MB (+/-) for critical updates
          Unknown (> 5 MB) for other updates


Norton Antivirus
----------------
1.) Ran the installer. Dealt with all the various requests for info, to register, etc. Updated
    all the various program and virus files.
2.) Forced to reboot before initial scan and/or install completed.
3.) Initial scan takes anywhere from a few minutes to much longer depending on number of files
    and type of machine.


Adaware
-------
1.) 2.1 MB download.
2.) Plugins are noted, but not obvious if necessary. They are not.
3.) Installed and ran. Noted that the reference file in use was 8 days old. Clicked "Check for
    updates now" option on main page and downloaded a newer reference file. Size was not indicated
    during download.
        - Noted that you cannot turn on "Ad-watch" without paying for the product.
        - Ran "Scan now" with default settings.
        - Found 10 items! 9 tracking cookies and 1 registry item. This was on a fresh system with
          just a few hours worth of use.
        - Immediately scanned again. No new objects found.

Spybot
------
1.) 3.6 MB download
2.) Installed. Defaults except told it not to install a Quick Launch icon.
3.) A message comes up that reads:

        If you remove advertisement robots with this program, you may not be
        allowed to continue using their host programs. Read their license
        agreements for further info.

        - Not exactly a clear message to and end-user.
        - You can choose not to see this message again.
        - Next message you get reads:

        You have AdAware installed. If you have the AdAware option to scan inside
        archives enabled, AdAware may find files in the Spybot-S&D folder. Spybot-S&D
        does not contain any spyware, but it creates backups of everything you fix (until
        you remove those backups from the Recovery list), and AdAware complains about these
        backups. You can safely ignore these backups found by AdAware.

        - This seems reasonable and relatively straight-forward.
        - Main screen opened. I clicked the "Updates" button first.
        - Five sets of updates were available (about 1.2 MB). Ran all five (one was not chosen).
          After downloading a DOS window appeared with no clear indication of what to do,
          then Spybot rebooted and showed the same opening screens again with prior choices
          forgotten.
        - The entire Spybot interface upon restarting had changed. I found the Updates option
          under the new "Online" tab (not obvious!), and scanned for updates just in case.
        - Now clicked the Spybot-S&D tab, then "Search & Destroy" button - nothing happened.
          Realized you need to click the much smaller "Check for problems" button at this
          point.
        - The scan took a few minutes. Three items were found. 1 file (related.htm), and 2
          Registry items. Decided to fix these.
4.) Poked around the Spybot files and decided to immunize against 505 items and to install
    resident download blocker. Not really sure what these do, but I wanted some active protection
    from Spybot.

Services
--------
* Turned off Messenger (on by default)
* Turned off Telephony
* Could not turn off RPC - Checked this after updates and still could not turn off RPC.
* Filter ports
   - inbound tcp/udp 135, 137, 139, 445, 161, 80, 443, 563, 1025, 1026, 1029.
   - Affects Windows fileshare, printing, and Microsoft Exchange email.
   - Us the ipsecpol tool to do this.
     Alternate port filtering method:
       + Start menu ==> Control Panel ==> Network and Dial-up Connections ==>
```

```
         Right-click on active network connection and choose Properties.
       + Under properties highlight Internet Protocol (TCP/IP)
       + Click on Properties.
       + Click on "Advanced..."
       + Click on Options tab
       + Highlight TCP/IP filtering
       + Click on Properties
       + Check "Enbable TCP/IP Filtering (All adapters)
       + Create the set of rules listed above that you need from this interface.
* Enable Automatic Updates
   - Start ==> Settings ==> Control Panel ==> Automatic Updates
* Disable UPNP Services (Universal Plug and Play Services)
```

Last udpated Sat Jan 1 12:00:53 CLST 2005