CCDC 2015

Windows XP/Windows Server 2003

**Basic Set Up and How To’s**

1. **Set up IIS (Windows XP)**

Prerequisites:

* The Domain Name System (DNS) service
* Microsoft Frontpage for creating and editing webpage
* Microsoft Visual InterDev for creating and developing web apps

Installation

* Start > Control Panel > Add or Remove Programs
* Add/Remove Windows Components. A friendly Windows Components Wizard appears, do you accept?
* Follow his every word, and profit.

1. **Set up SQL (Windows 2003)**

* In SQL Server Installation Center, click Installation.
* Click New SQL Server stand-alone installation or add features to an existing installation.
* In Setup Support Rules, click Ok.
* In Product Key, enter your product key and click Next.
* In License Terms, check I accept the license terms and click Next.
* In Setup Support Files, click Install.
* In Setup Support Rules, click Next.
* In Feature Selection, check the features you want to install and click Next.
* In Instance Configuration, click Next.
* In Disk Space Requirements, click Next.
* In Server Configuration, specify the Account Name and Password for the SQL Server Database Engine service and click Next.
* In Database Engine Configuration, specify the Authentication Method to use and the SQL Server administrators and click Next.
* In Error and Usage Reporting, click Next.
* In Installation Rules, click Next.
* In Ready to Install, click Install.

1. **Writing Inbound Port Rules for XP and 2003**
   * **On a computer that has the Group Policy Management feature installed, click Start, click Administrative Tools, and then click Group Policy Management.**
   * **If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.**
   * **In the navigation pane, expand Forest: *YourForestName*, expand Domains, expand *YourDomainName*, expand Group Policy Objects, right-click the GPO in which you want to create the rule, and then click Edit.**
   * **In the Group Policy Management Editor, expand Computer Configuration, expand Policies, expand Administrative Templates, expand Network, expand Network Connections, and then expand Windows Firewall.**
   * **Expand Domain Profile or Standard Profile. Rules created in the Domain Profile section apply whenever the client computer is connected to a network on which it can contact a domain controller for its assigned Active Directory domain. Rules created in the Standard section apply when the computer cannot contact a domain controller for its domain.**
   * **In the details pane, double-click Windows Firewall: Define inbound port exceptions.**
   * **On the Setting tab, click Enabled, and then click Show.**
   * **In the Show Contents dialog box, click Add.**
   * **In the Add item dialog box, type the string that represents the port on which you want to allow inbound network traffic. The text string must conform to the following syntax, with each parameter separated by a colon (:).**
   * **Port:Transport:Scope:Status:Name**
     1. **Port - The decimal port number to which inbound network traffic is allowed.**
     2. **Transport - The protocol for the port number. Either TCP or UDP.**
     3. **Scope - Select one of the following options:**

* **An asterisk (\*) to represent all networks.**
* **A comma-separated list of IP address or subnets, such as: 10.0.0.1, 10.2.3.0/24.**
* **The string localsubnet.**
  + 1. **Name - The name for the rule.**

1. **Backing up Utilities**
   * **Windows XP**
     1. The backup utility can be found in Start-All Programs-Accessories-System Tools. The figure below shows the window that first opens. In this dialog box, you have a choice between Microsoft's step-by-step "Wizard" or the "Advanced Mode".
   * Windows Server 2003
     1. Click **Start**, click **Run**, type **NTBackup**, and then click **OK**.
     2. This process opens the **Backup or Restore Wizard**.
2. **Mitigating MS 09-050**

* Vulnerabilities in SMBv2 Could Allow Remote Code Execution
* Workaround is to disable SMB v2
  + Click **Start**, click **Run**, type **Regedit** in the **Open** box, and then click **OK**.
  + Locate and then click the following registry subkey:
    - HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services
  + Click **LanmanServer**.
  + Click **Parameters**.
  + Right-click to add a new **DWORD (32 bit) Value**.
  + Enter **smb2** in the **Name** data field, and change the **Value** data field to **0**.
  + Exit.
  + Restart the "Server" service by performing one of the following:
    - Open up the computer management MMC, navigate to **Services and Applications**, click **Services**, right-click the **Server** service name and click **Restart**. Answer **Yes** in the pop-up menu.
    - From a command prompt and with administrator privileges, type **net stop server** and then **net start server**.

**The Game Plan (WIN ONE FOR THE GIPPER!)**

1. Set up IIS and MSQL (unless already installed and/or configured)
2. network sharing center > right click interface > properties > uncheck IPv6
3. uncheck the file/printer sharing box
4. Patch MS08-067
   1. SERVER 2003
      1. Requires service pack 2 for x64 and x32
      2. <http://bit.ly/2nGaqb6> (32 bit)
      3. <http://bit.ly/2ofMTii> (64 bit)
      4. reboot required
      5. registry key for verification: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB958644\Filelist
   2. XP
      1. Requires at min service pack 2 for x32 only
      2. <http://bit.ly/2oF9BNw> (32 bit)
      3. <http://bit.ly/2nQZcB4> (64 bit)
      4. reboot required
      5. registry key for verification: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP4\KB958644\Filelist

(x64) HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP Version 2003\SP3\KB958644\Filelist

1. Re-enable file and printer sharing
2. Patch MS03-026
   1. SERVER 2003
      1. <http://bit.ly/2nRfx8R> (32 bit just in case)
      2. <http://bit.ly/2mUHo8S> (64 bit)
      3. Reboot immediately after
      4. <http://bit.ly/2oFdFgL> (Microsoft Security Baseline manager, unless already installed)
      5. To check if patch is installed, go to baseline manager, and check the following key exists: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP1\KB823980
   2. XP Professional
      1. Block UDP ports 135, 137, 138, 445
      2. Block TCP ports 135, 139, 445, 593
      3. disable COM Internet Services (CIS) and RPC over HTTP, which listen on ports 443 on XP
      4. Control RPC port allocation
         1. From the Start menu, point to Programs, point to Administrative Tools, and then click Component Services to start Component Services.  
            Click to expand the Component Services and Computers nodes. Right-click My Computer, and then click Properties.  
            On the Default Protocols tab, click Connection-oriented TCP/IP in the DCOM Protocols list box, and then click Properties.  
            In the Properties for COM Internet Services dialog box, click Add.  
            In the Port range text box, add a port range (for example, type 5000-5020), and then click OK.  
            Leave the Port range assignment and the Default dynamic port allocation options set to Internet range.  
            Click OK three times, and then restart your computer.
         2. Block port range incoming from firewall
3. Add Sysinternals Suite
   1. http://bit.ly/2onXQfc
4. Follow Windows Hunting Document
5. Injects?

**Need Service Packs?**

* Windows 2003 Service Pack 2 x86
  + http://bit.ly/2nG9tjg
* Windows 2003 Service Pack 2 x64
  + http://bit.ly/2nlZ4pg
* Windows XP Service Pack 2 x64
  + http://bit.ly/2ofHmbK