GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Linda VanHorn
Windows NT Security: Step-by-Step. Practicum

**Disable Nonessential Devices and Services to Reduce Exposure to DoS attacks**

How many of you work in universities, where Primary Domain Controls (PDC) pop up like dandelions? What services and protocols are these domain controllers running? Where do department system administrators find information to understand and evaluate the necessity of drivers, services, protocols, and bindings when many security instructions just say "disable nonessential services?" How do you convince system administrators to invest the time? This paper collects and compares guidelines from a variety of management, performance tuning and security papers on evaluating and disabling nonessential drivers, services, protocols, and bindings.

Why bother? Although SANS defines vulnerable systems and recommends stripping all unnecessary services [1], how does one convince department system administrators to carry out the recommendations? Departments may not be using servers for sensitive information so no one allocates time to research and plan service management. When asked, a system administrator may reply "I don't know what the service effects, so I'm not going to risk turning it off." If a server hasn't been cracked, the risk of losing data or service availability may be considered low.

The most persuasive argument for the busy system administrator is timesavings. There are enough core resources on a server [2,3] for system administrators to monitor and patch promptly. The few hours planning and disabling nonessential services for a PDC at installation can save the system administrator hours of work and increase the network availability for users. In the last year alone, the system administrator may have had to patch the domain controllers for LSA DoS, Source Routing, TCP/IP Sequence Numbers, service.exe DoS, SysKey, RDisk Race Condition, Loose Registry Permissions, Buffer Overflow in cmd.exe, IP Fragment Reassembly, and Master Browser DoS. We don't have a crystal ball for determining what may need to be patched in the future, so save valuable time by turning off or removing unused devices and services.

**What can/should be disabled?**

"Exactly which services and options can be disabled on a particular server depends upon the purpose(s) of that server and the custom applications running on it."[1] The security requirements of your organization may determine what you are allowed to run on a PDC. Even if servers do not need to be C2 [4,5] or ITSEC FC2-E3 [6] compliant, their security guidelines provide insight for securing devices, services and protocols. These combined with Managing Server Security [7], Windows NT Security Step-by-Step [8,] and the Navy's Guide to Securing NT [9] round out Microsoft's Domain Controller Configuration Checklist [10].

The sequence of disabling or removing device drivers and services counts. Remove device drivers before services. Some services have dependencies; the dependent services must be removed first. A common example on a Windows NT 4.0 workstation is to remove the Server before removing the Computer Browser.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

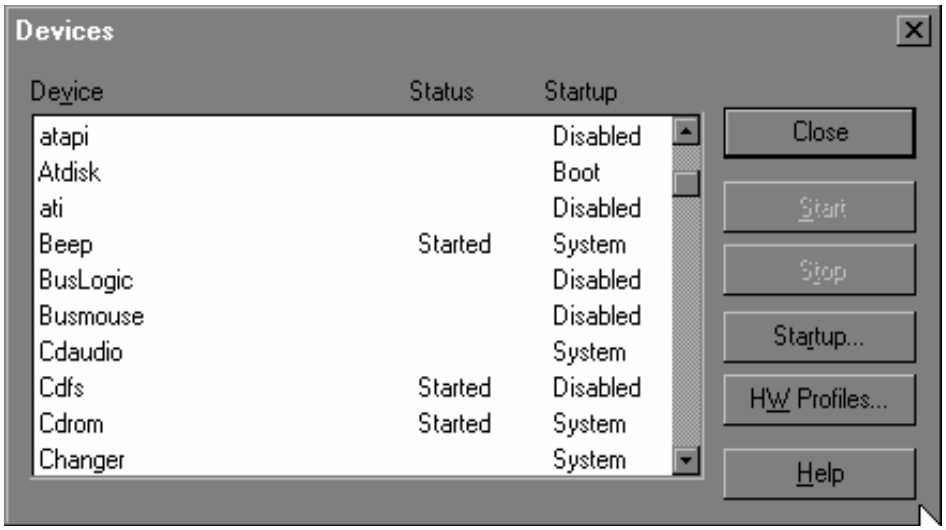
**1. Devices**

Devices refer to the physical equipment and software drivers installed on the domain controller. CERT [11] points out that, "New and reassigned systems often arrive with optional hardware that is not required. " These can complicate configuring the server and may give crackers another door into the system. Experts do not recommend modems and removable media devices for primary domain controllers. Physically remove these and their associated drivers and software.

All security guidelines agree that protecting the devices involved in the boot process is critical. The first step, if at all possible, is to place servers in a locked room with limited access. When this is not possible, secure the server with a power on password and consider the disablement of boot from the floppy drive. If the system doesn't need the floppy drive, remove it.

Rootkit authors target device drivers because they run in the kernel space with access to most of the system functions. DoS attacks can be a smoke screen for intruders replacing device drivers with trojans, rootkits, or DDoS tools after a system reboot. Any drivers left on a system should be secured with registry scripts and the use of such tools as Tripwire[12] or Intact[13].

The ITSEC F2-E3 [6] of the IT Security Evaluation Criteria is one measure of a secure operating system used in the U.K. and many European countries. This guideline is restrictive in that it states; "Only devices that are found on the Windows NT Installation CD may be enabled in the evaluated configuration." To see which drivers are installed by default on your PDC, from the Start button, select Settings, select the Control Panel, and then select Devices. The following screen appears showing the device name, its current status and the configured startup behavior.




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The C2-evaluated configuration, used as a measurement in the U.S., consists of specified hardware, software, programs and network services. Like its European cousin, its narrow definition (which also excludes NetBIOS) may not provide enough network service. Nevertheless, the list of thirty-five allowable devices [5] is a useful guide to see how few devices one really needs for a server.

Table 1: Allowable drivers under C2

| Service name | Driver |
|---|---|
| AFD Networking Support | afd.sys |
| IDE or EIDE storage systems | atapi.sys |
| Beep | beep.sys |
| CD file system | cdfs.sys |
| CD-ROM | cdrom.sys * |
| Compaq NetFlex-3 Driver | netflx3.sys |
| Compaq Array | cpqarray.sys |
| Disk | disk.sys * |
| Fastfat | fastfat.sys * |
| Floppy | floppy.sys |
| HP 4mm DAT tape device | hpt4qic.sys |
| i8042 keyboard and PS/2 mouse port | i8042prt.sys |
| keyboard class driver | kbdclass.sys |
| security device drive | ksecdd.sys |
| Microsoft NDIS driver | ndis.sys |
| mouse class driver | mouclass.sys |
| ms file system | msfs.sys |
| multiple UNC provider | mup.sys |
| device detector | netdetect.sys |
| Netware print and file service | npfs.sys |
| NT file system | ntfs.sys |
| null | null.sys |
| | |

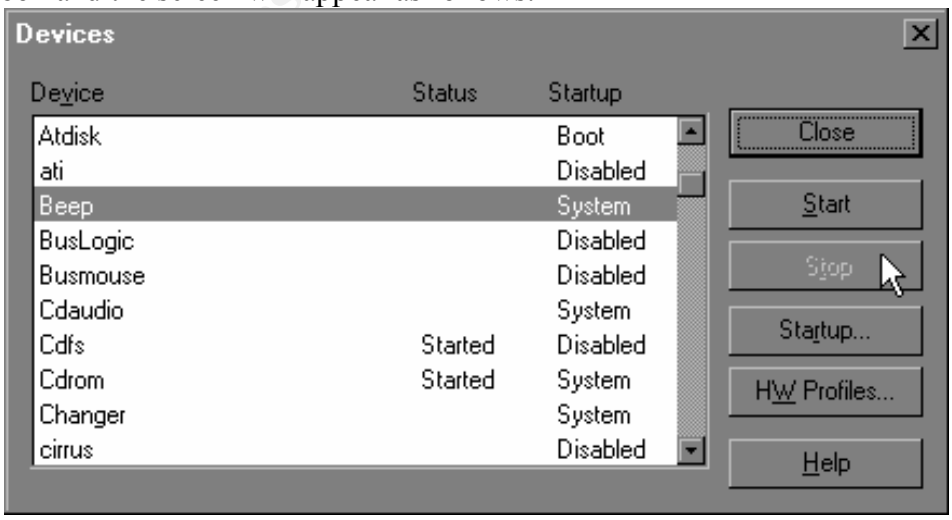
© SANS Institute 2000 - 2002, Author retains full rights.

| | |
|---|---|
| parallel port | parallel.sys |
| parallel port | parport.sys |
| redirector | rdr.sys |
| serial port | serial.sys |
| services | srv.sys |
| Symbios PCI-SCSI controller | symc810.sys |
| TCP/IP network service | tcpip.sys |
| VGA monitor | vga.sys * |
| WINS Client | netbt.sys |
| tape | tape.sys |
| 4mm DAT tape drive | 4mmdat.sys |

So there are resources for identifying the purpose of a driver and which ones may be disabled or removed. Drivers marked with an asterisk should not be disabled according to the Microsoft Knowledge Base article Q166238 [14].This document also discusses how to repair device drivers set to start at Boot or System but in fact never started. Although dangerous to remove carelessly, if the operations manager has banned beeping from the computer center, one can remove beep.sys. Another innovative solution is Pedestal Software's Integrity Protection Driver (IPD)[15]. After driver installation, devices can not be added, changed or deleted without a rebuild.

**How to Disable Drivers**

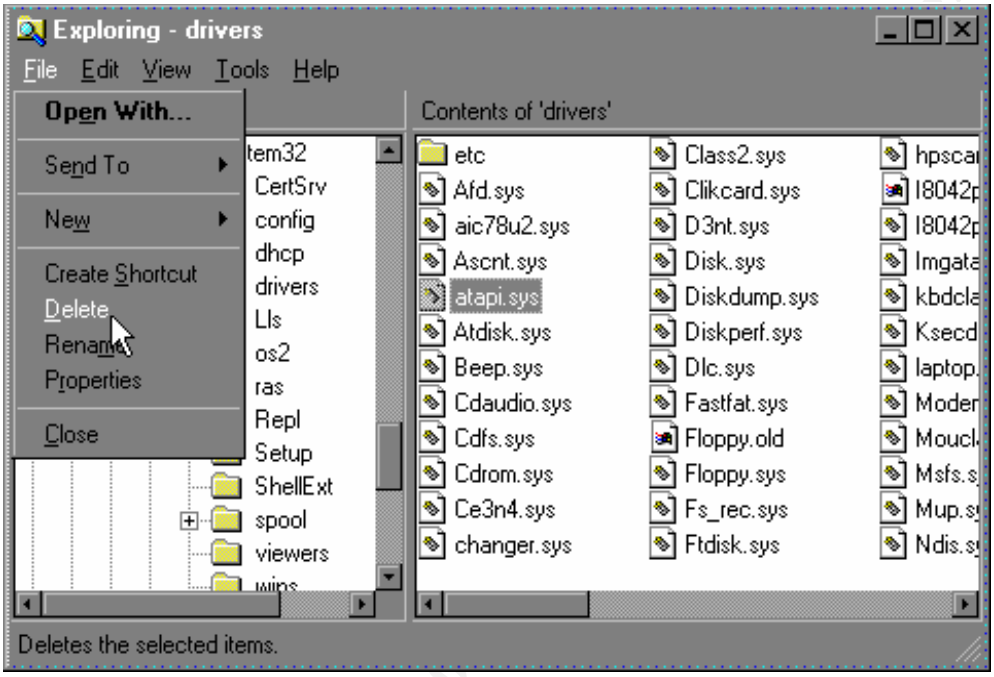
Once research is complete, and you've determined that security requires disabling a driver, select the Start button, Settings, the Control Panel and select the Devices icon. The following Devices screen appears. Highlight the device to disable, then select the Stop button. Answer yes to the pop-up box and the screen will appear as follows.




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**How to Remove Drivers**

In some cases security requirements dictate that a device must be removed. It's a good idea to have the Microsoft Knowledge Base article Q166238 [14] available. Begin by right clicking on the Start button, select Explore, scroll down and expand the system32 folder in the left panel, then select drivers. Highlight the device driver name in the right panel, select File, and then select Delete.

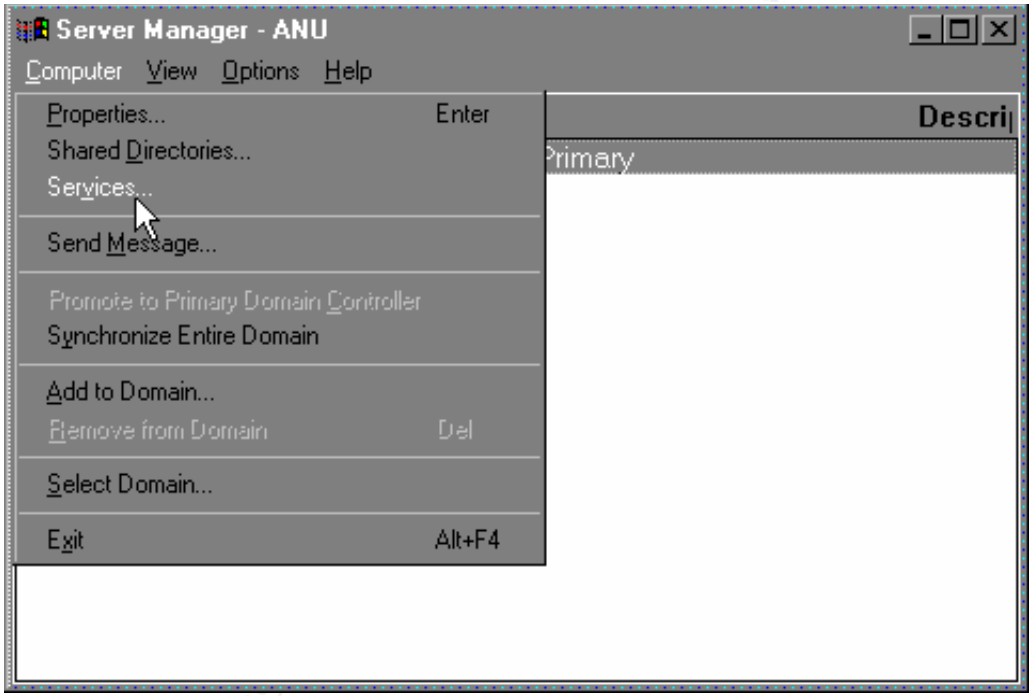



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

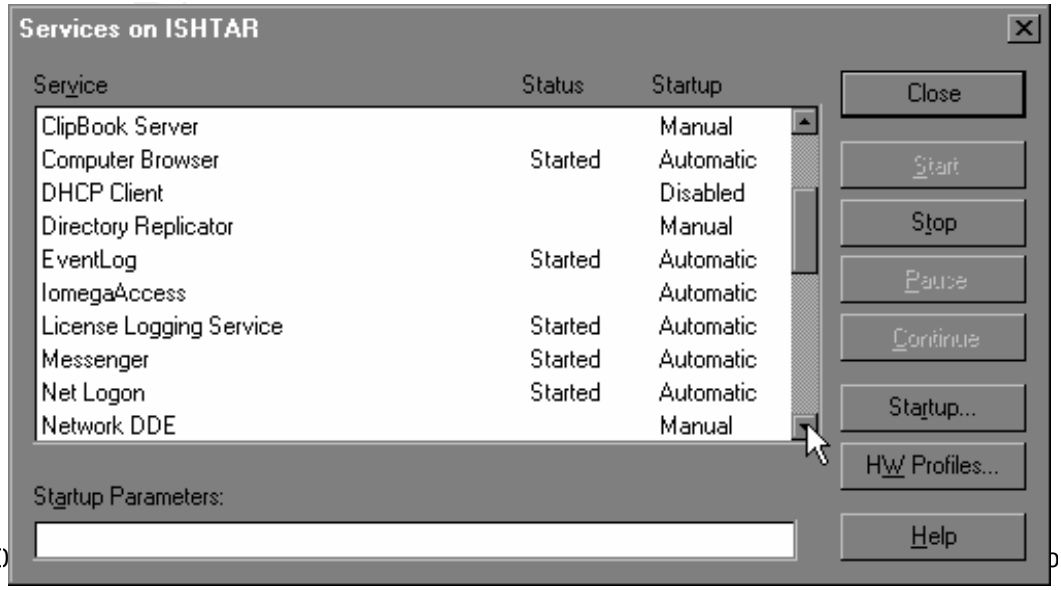
**2. Services**

Like devices, services are tempting targets. The threats may include DoS vulnerabilities, service account mis-configuration, trojan horses and social engineering ruses. SANS[8] recommends verifying that the PDC has the latest versions of each service. Installing the latest service pack updates and repairs services. Although Microsoft's Domain Controller Configuration Checklist[14] only recommends securing the Scheduler Service, Microsoft's Security Audit and Control[7] as well as the C2 [5] and ITSEC FC2-E3 [6] checklists provide additional suggestions.

To see the installed services, from the Start button, Programs, open Administrative Tools and then the Server Manager. With the Primary Domain Controller of a real (rather than a laptop) network, a system administrator can manage all the domain controllers and member servers from the Server Manager screen. To view the services for the PDC, highlight it then select Computer and Services.




The following scrollable list of built-in and application services appears.




© SANS Institute 2000 ... or retains full rights.

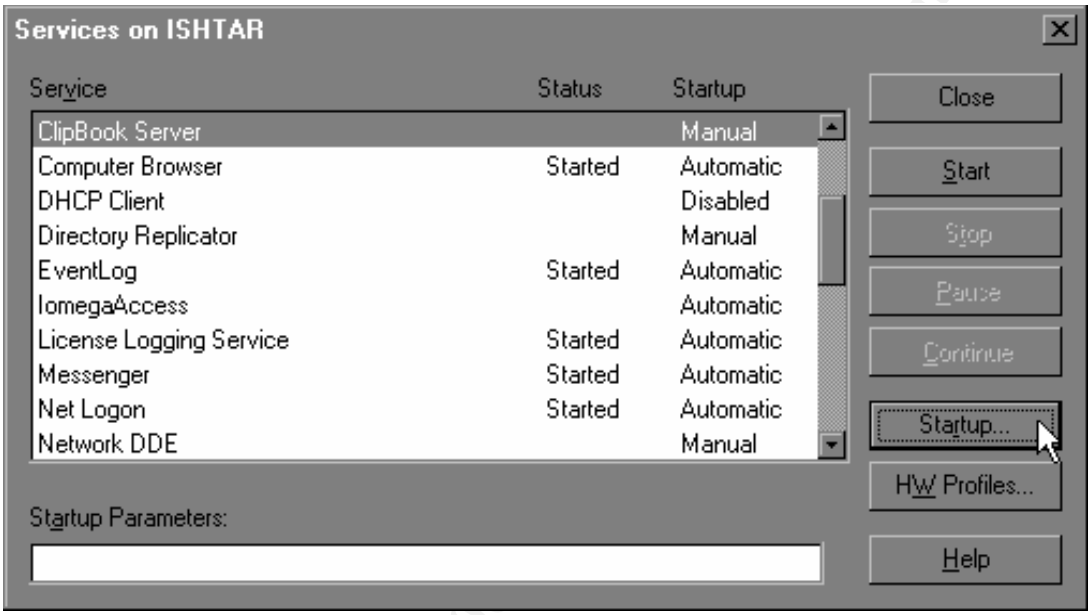
Table 2: Comparison of Service Recommendations:

| | DC [10] Checklist | Managing Server Security [7] | ITSEC FC2-E3 [6] | C2 Checklist [5] |
|---|---|---|---|---|
| Alerter | | Consider disabling | Allow | Remove |
| Clipbook viewer | | Disable | Remove | Remove |
| Computer Browser | | Allow | Allow | Allow |
| DDE | | Not required | Remove | Remove |
| DDEDSDM | | Not required | Remove | Remove |
| DHCP Client | | | Allow | Remove |
| Directory Replicator | | Secure | Remove | Remove |
| Event Log | | Require | Require | Require |
| License Logging | | | | |
| Messenger | | Allow | Remove | Remove |
| MS DNS | | | Only if DNS Server | Only if DNS Server |
| Net Logon | | Allow | Allow | Allow |
| NTLM SSP | | Allow | Allow | Allow |
| Plug & Play | | | Allow | Remove |
| Protected Storage | | | Allow | Remove |
| RPC Locator | | May use account | Allow | Allow |
| RPC Service | | May use account | Allow | Allow |
| Scheduler | Secure | Secure | Remove | Remove |
| Server | | Allow | Allow | Allow |
| Spooler | | May use account | Allow | Allow |
| TCP/IP Netbios He | | Allow | Allow | Allow |
| UPS | | Not required | Remove | Remove |
| WINS | | | Only if WINS Server | Only if WINS Server |

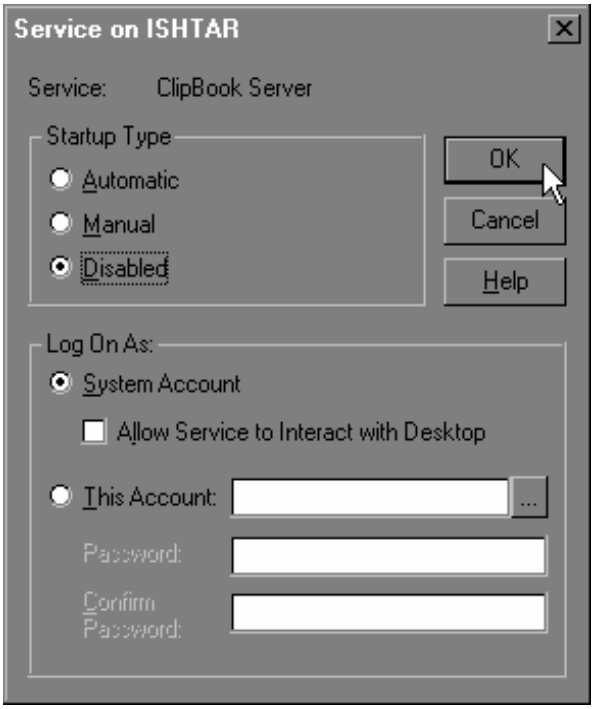
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Service Dependencies**
Aerter, Messenger and Net Logon depend on the Workstation service. Remote Procedure Call Locator and the NT LM Security Support depend on the Remote Procedure Call Service. Computer Browser depends on the Server Service. Although seldom required, the Network DDE services depends on Network DDE DSDM. Jumes in Managing Service Security [7] and The ARS Technica [16] web sites provide clear information on services and their functions.

**How to change the status of a service**
While in the Server Manager, Services screen, highlight the service. Select the Startup button.

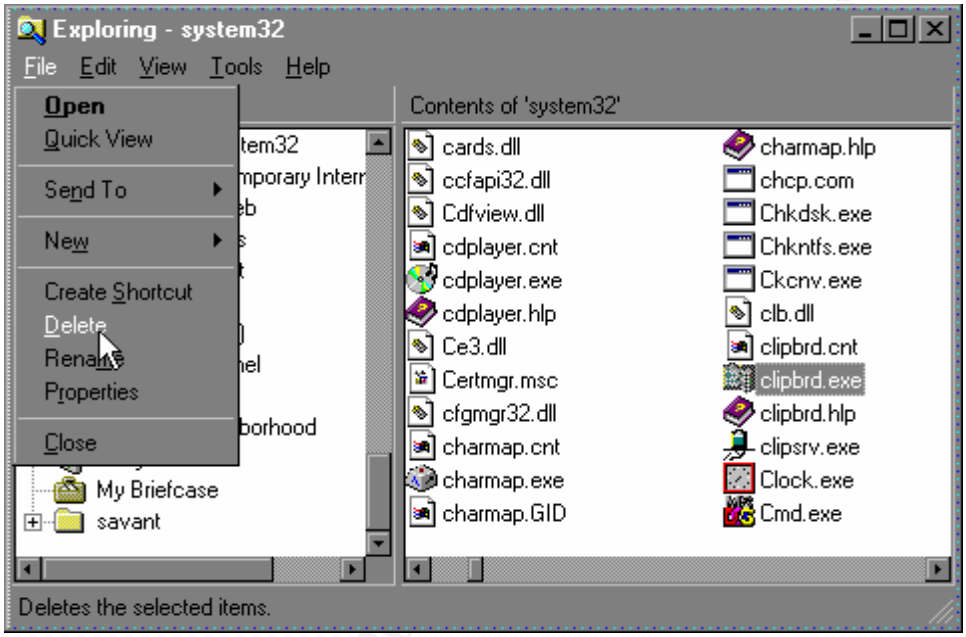



The Service description box appears. Click on the Startup Type radio button for Disabled, then select OK.




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**How to Remove the Clipbook Viewer Service**
For some systems, disabling a service is not enough. Guidelines, such as the ITSEC FC2-E3, may require system administrators to remove a service. Using Explore, find the file CLIPBRD.EXE in the system32 directory of the server root. Delete it and empty the Recycle Bin unless you have already implemented the "Do not move files to the Recycle Bin" option for the recycle bin properties sheet. You might also remove the clipsrv.exe while you're here.



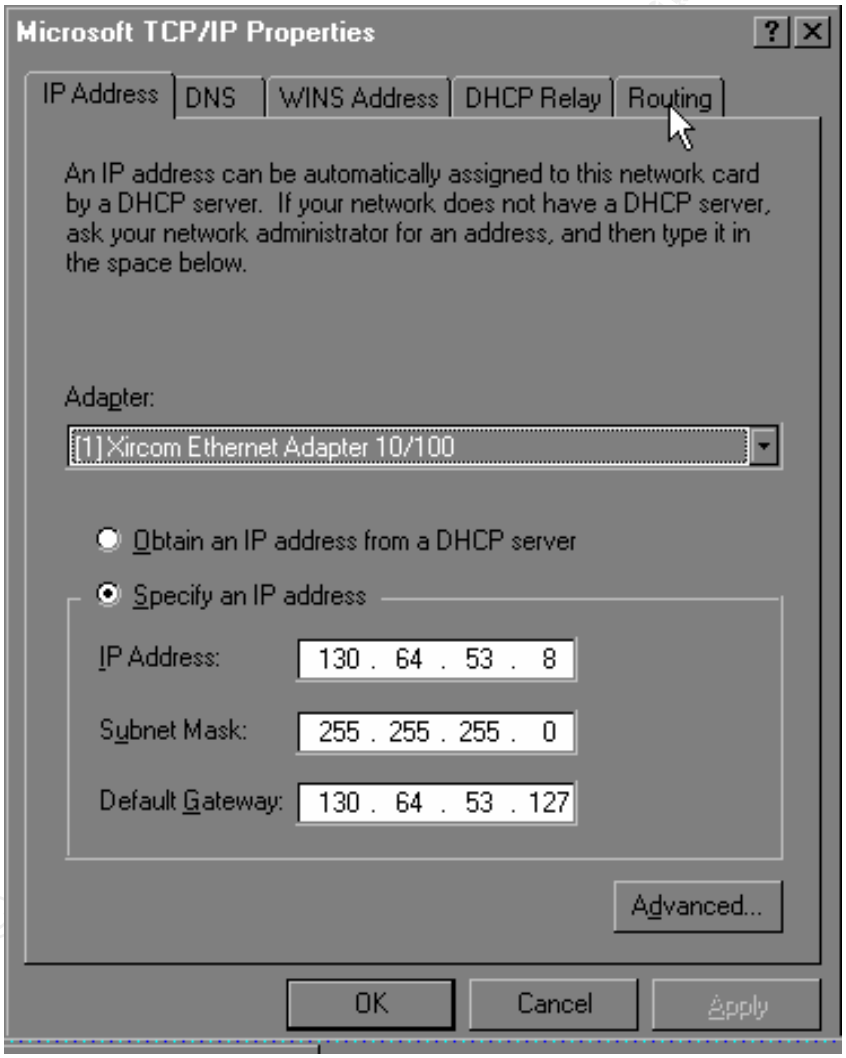

**Securing Services**
As the comparison table illustrates, several guidelines recommend securing services such as the Directory Replicator and Scheduler. That topic is beyond the scope of this paper, but Microsoft's Windows NT 4.0 Domain Controller Configuration Checklist [10] provides guidelines for securing the Scheduler. Jumes in Managing Service Security [7] describes how to secure the Directory Replicator. Look for additional instructions in the Microsoft Knowledge Base, SANS or at software vendor sites on securing specific built-in or application services. Services are critical to the controllers' security.

**3. Network Services, Protocols and Bindings**
Only run the protocols you need. Since C2 and ITSEC FC2-E3 standards cover stand-alone hosts, they are not particularly useful for network services. The default PDC installation will include the Computer Browser, NetBIOS interface, RPC configuration, Server and Workstation "services". The only protocol is TCP/IP. The network bindings include NetBIOS Interface, Server and Workstation.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

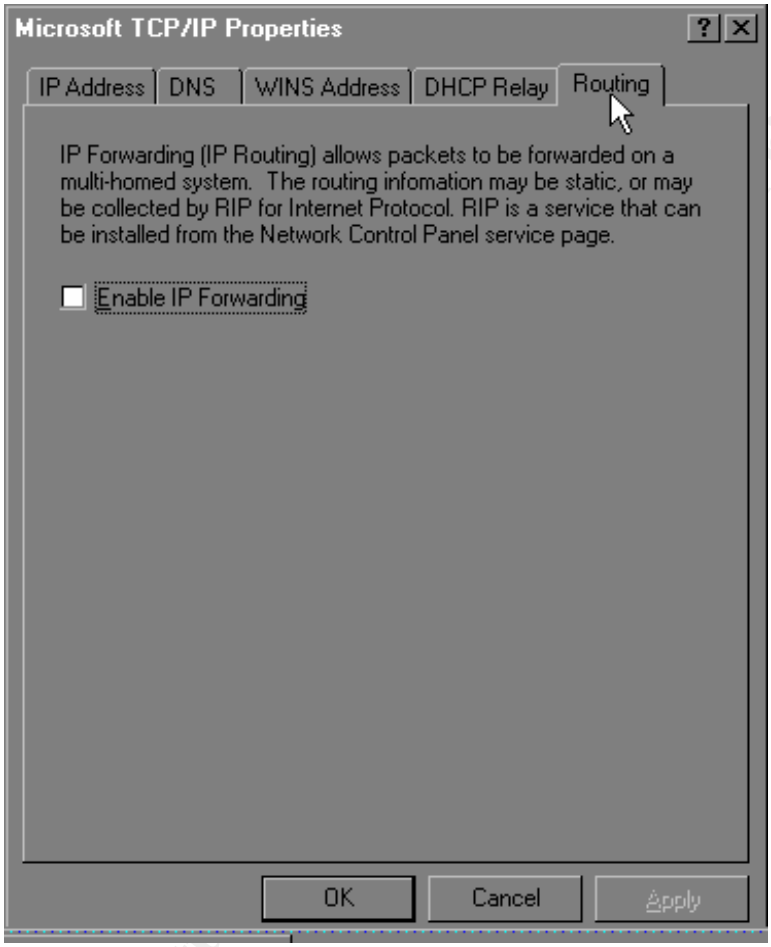
Don't be tempted to enable Simple TCP/IP Service, which include some of crackers' favorite protocols- Chargen, Daytime and Echo. These are rarely needed. Plan the local domain design so that TCP/IP Printing and Remote Access Service run on a resource server. Never run the Internet Information Server on a domain controller. And last but not least, there's always the anecdote about the clueless administrator who thought Services for Macintosh had to be enabled and brought down an entire school's subnet

**Make sure that TCP/IP forwarding is turned off.**
Selecting the Start button, then Setting, the Control Panel, and then selecting the Network icon access the Network screen. From the main Network screen, select the Protocol tab and then select Properties. The Microsoft TCP/IP Properties screen appears select Routing.




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In the Routing tab screen, make sure that the Enable IP Forwarding box is not checked.

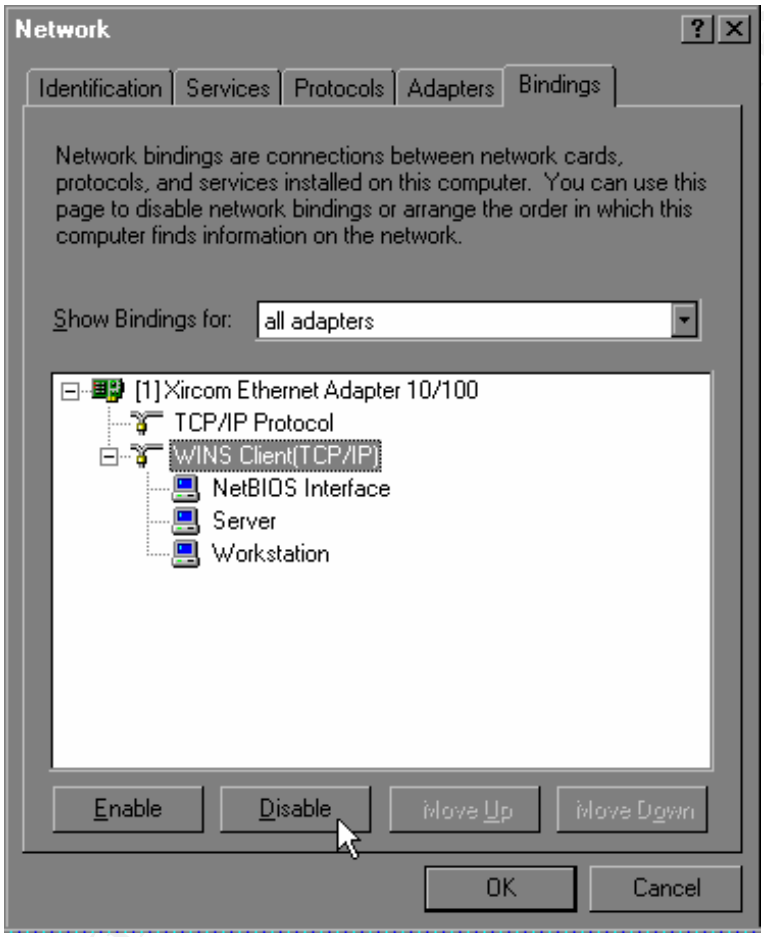



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Removing Bindings**

Guidelines frequently recommend that a PDC with two internal NIC cards, unbind NetBIOS on the external card to protect Windows NT networking data and SMB/NetBIOS services.

From the Taskbar, select the Start button, then Settings, and then the Control Panel. Double-click on the Network icon and then select the Bindings tab. Click on NetBIOS Interface and click on the Disable button. Select Close.




This is just a small piece of securing a domain controller. By gathering information into one paper for busy system administrators, hopefully we will be able to persuade more of them to save time and disable unneeded devices, services and protocols.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Resources**

1. Fossen, Jason and Johannson, Jesper. Windows NT Security: Step-by-Step. SANS GIAC Track 6 Syllabus, May 11-13, 2000.

2. NT Security News. Available: http://www.ntsecurity.net/.

3. Microsoft Security Bulletins. Available: http://www.microsoft.com/technet/security/.

4. Malisow, Ben. DoD-Certified Trusted Systems and You. Feb. 8, 2000. Available: http://www.securityfocus.com/ select Microsoft, NT, Securing and then DOD-Certified.

5. Windows NT C2 Configuration Checklist. April 5, 2000. Available at http://www.microsoft.com/TechNet/security/c2config.asp

6. ITSEC FC2-E3 Installation of Windows NT Workstation 4.0 and Windows NT Server 4.0. Version 2.4 June 1999. Available: http://www.microsoft.com/TechNet/winnt/winntas/ntitsec.asp

7. James J. Jumes, et. al, Managing Service Security, Chapter 10 in Windows NT 4.0 Security, Audit and Control, c1998, Microsoft Press.

8. SANS Windows NT Security, Step-by-Step v.2.0 Feb 9, 1999

9. U.S. Navy Secure Windows NT Installation and Configuration Guide. Version 1.3. December 1998. Available" http://infosec.navy.mil/comusec/ntsecure.html.

10. Microsoft's Windows NT 4.0 Domain Controller Configuration Checklist. March 29, 2000. Available: http://www.microsoft.com/technet/security/dccklst.asp.

11. CERT. Preparing for the initial installation of Windows NT 4.0 Systems. Available: http://www.cert/org/security-improement/implementations/i025.01.html.

12. Tripwire. Available: http://www.tripwire.com.

13. Intact. Available: http://www.pedestalsoftware.com.

14. Microsoft Knowledge Base article Q166238 - Problems Caused by Disabling Original Profile on Some Devices. Available: http://search.support/microsoft/com/kb/

15. Integrity Protection Driver. Available: http://www.pedestalsoftware.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 27th, 2017

# Upcoming Training

| | | | |
|---|---|---|---|
| **SANS Security West 2017** | **San Diego, CA** | **May 09, 2017 - May 18, 2017** | **Live Event** |
| **SANS Northern Virginia - Reston 2017** | **Reston, VA** | **May 21, 2017 - May 26, 2017** | **Live Event** |
| **SANS Cyber Defence Canberra 2017** | **Canberra, Australia** | **Jun 26, 2017 - Jul 08, 2017** | **Live Event** |
| **SANSFIRE 2017** | **Washington, DC** | **Jul 22, 2017 - Jul 29, 2017** | **Live Event** |
| **SANS Virginia Beach 2017** | **Virginia Beach, VA** | **Aug 21, 2017 - Sep 01, 2017** | **Live Event** |
| **SANS Network Security 2017** | **Las Vegas, NV** | **Sep 10, 2017 - Sep 17, 2017** | **Live Event** |
| **San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation** | **San Francisco, CA** | **Nov 27, 2017 - Dec 02, 2017** | **vLive** |
| **SANS San Francisco Winter 2017** | **San Francisco, CA** | **Nov 27, 2017 - Dec 02, 2017** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |