SystemEXPERTS

Hardening Windows 2000

Philip Cox

Phil.Cox@SystemExperts.com

4 Steps to Practical Win2K Security

- Locate Windows system
- Insert *nix CD
- Reboot
- Follow installation prompts ☺

- But if that is not an option …

Hardening Win2K

- Out of the box
- Physical Security
- OS Install
- System Tighten
- Testing
- The goal: one service, one system
  - The reality is though that many people will not heed this advice, and will run systems that support multiple functions, because either they do not see the problem with it, or they have financial constraints that prohibit them from doing it the right way

Win2K Out of the Box

- Syskey
- Authentication
  - Kerberos for Domain authentication
  - NTLM for local and backward compatable
- Authorization
  - Fair File system permissions
- Auditing
  - None, unless set by Group Policy

Win2K Server Out of the Box

- Services
  - CIFS/SMB with NetBIOS
  - IIS : WWW, Front page extensions, & SMTP
  - Index server

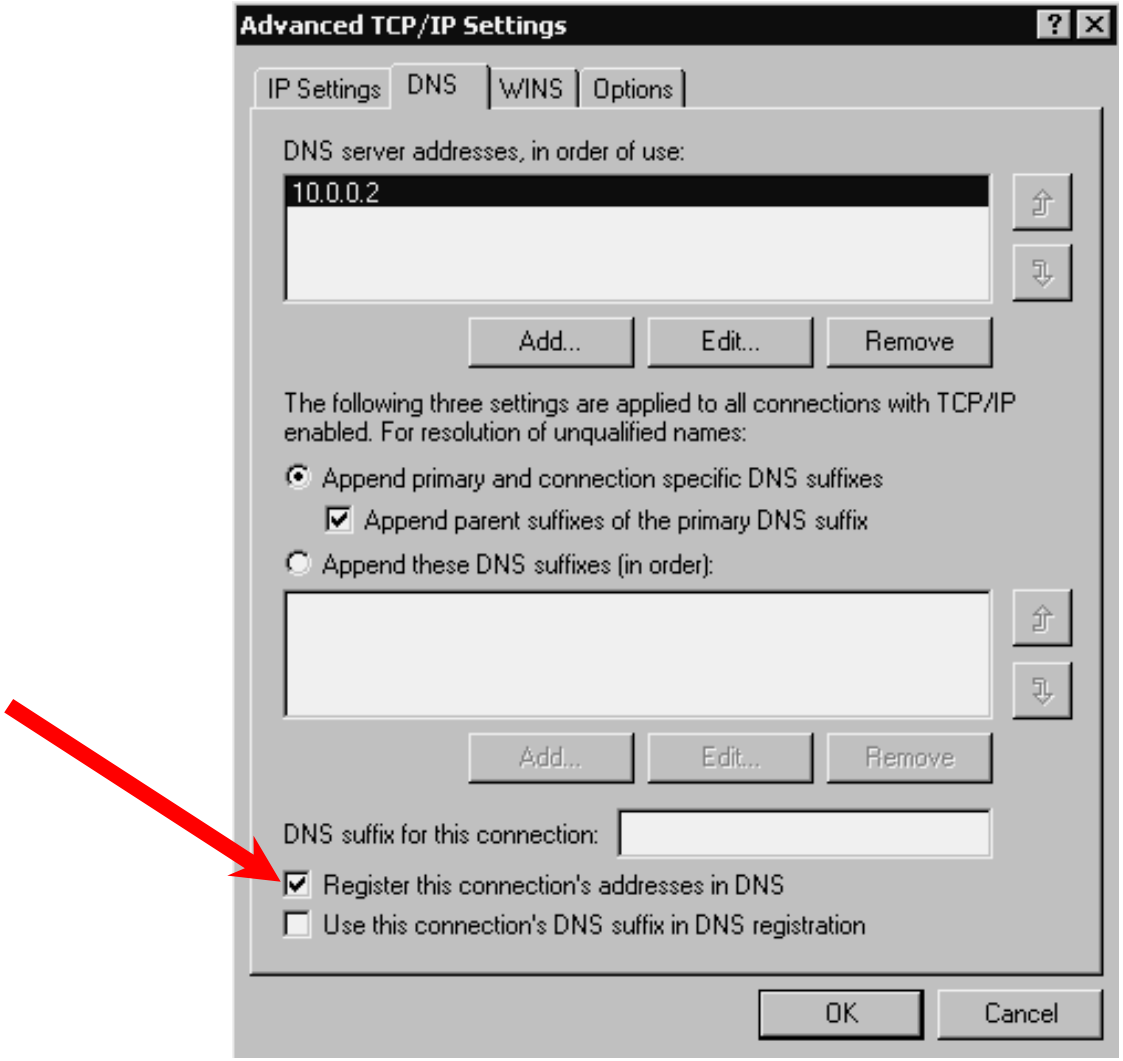
Physically Secure It

- Install case locks on all publicly accessible systems
- Put critical or highly sensitive systems in cages
- If removable media (i.e. floppies, CDs, ZIP drives) is allowed, then you should set the hardware to boot from the hard drive first
- Set the EEPROM boot password

Install the Operating System

- Use NTFS
- Use Separate data and OS partitions
- Set Good Admin password
- Install only required Network services
- Use static IP addresses for high secure systems
- Choose your DDNS settings
- Disable LMHOSTS lookup and NetBIOS over TCP/IP
- Become a domain member

DNS Settings



What About a Domain?

- You may want to use a separate Forest (i.e. AD)
- If you do, here are some guidelines
  - Make sure it is a new domain, in a new forest
  - Validate that there are no trust relationships established
  - Run an internal DNS server on that domain
  - Use screening routers and DNS configurations to block request/updates from external networks
  - Configure DNS to Only accept secure updates from host on the isolated network
  - If you require trust, then use the older WinNT method, and establish specific one-way trusts that are not transitive.

What About Upgrades

- It is harder than fresh installs, but is doable
- Configure the system using the Local Security Policy tool
- Use the security policy templates to reconfigure the system
  - setup *security.inf* for all systems
  - Use *DC security.inf* in addition for Domain Controllers

Harden Services

- What is running?
  - Try the Services Control Panel
  - Try Fport, netstat, Tcpview. (others?)

- For each service that exists on a Win2K system, you set
  - Startup option and account

Harden Services

High

- **DNS Client**
- **EventLog**
- **Logical Disk Manager**
- **Protected Storage**
- **Plug & Play**
- **Security Accounts Manager**
- **IPSec Policy Agent**
- **Protected Storage***
- **Remote Procedure Call***

Medium

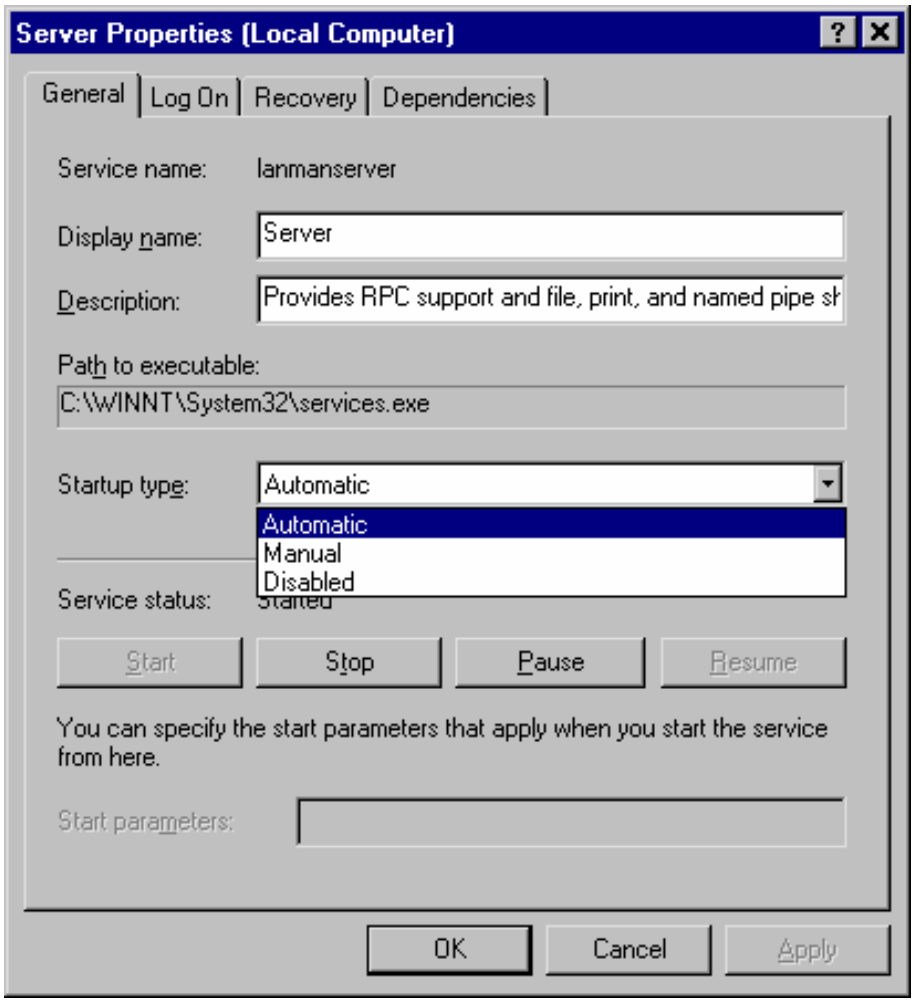
- Network Connections Manager
- Remote Registry Service
- RunAs service

DC

- Kerberos Key Distribution Center
- DNS Server
- Windows Time
- NT LM Service Provider
- File Replication Service (>1DC)
- RPC Locator
- Net Logon
- TCP/IP NetBIOS helper
- Server (when sharing resources or running the AD)
- Workstation

Disable Services

- Done via the Services Control Panel/Snap-in
- Change the Startup type field to Disabled
- Also `SC.exe` from the command line

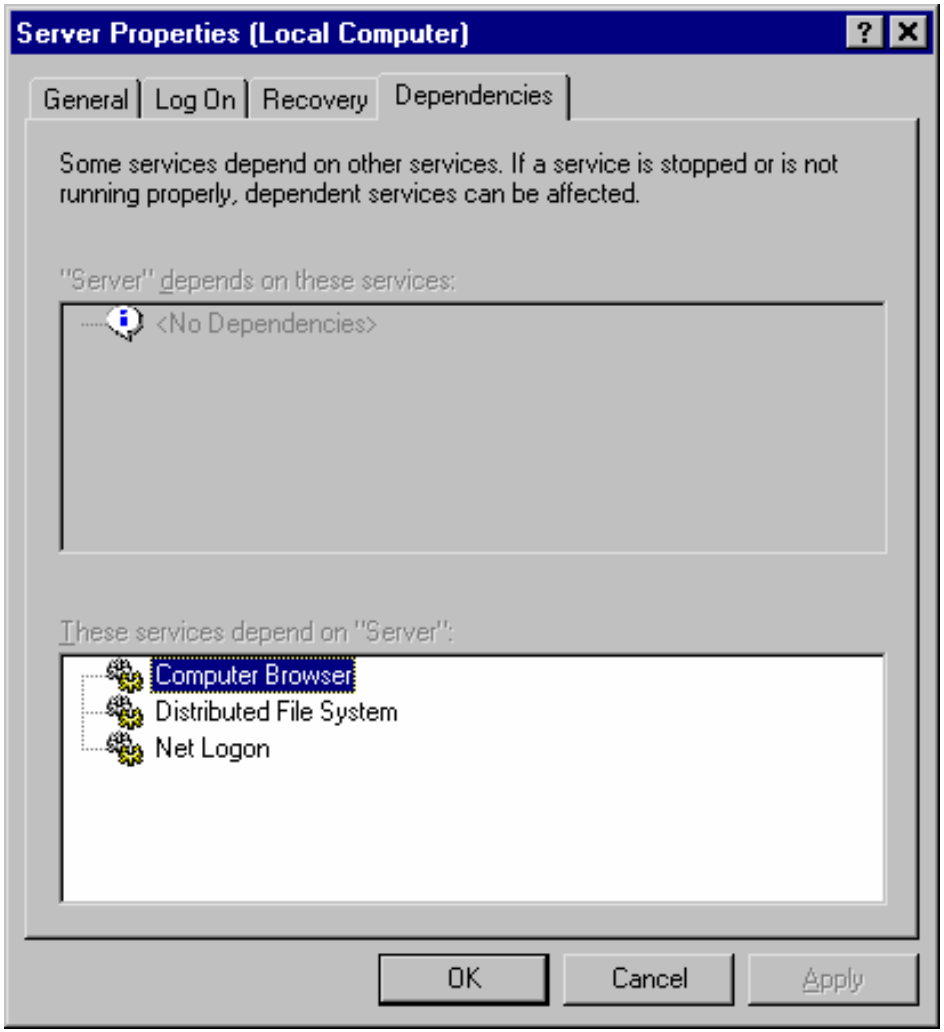


Disable or Delete?

- Is it best to disable or delete a service?
- A disabled service can be restarted by enabling, then starting it
  - If you have the right permissions on the system
- Whereas a deleted service cannot be started until it in re-installed
  - Thus it is significantly harder to have this happen maliciously, especially for Win2K core services
- The problem is that it is very hard (impossible?) to actually remove some of the services

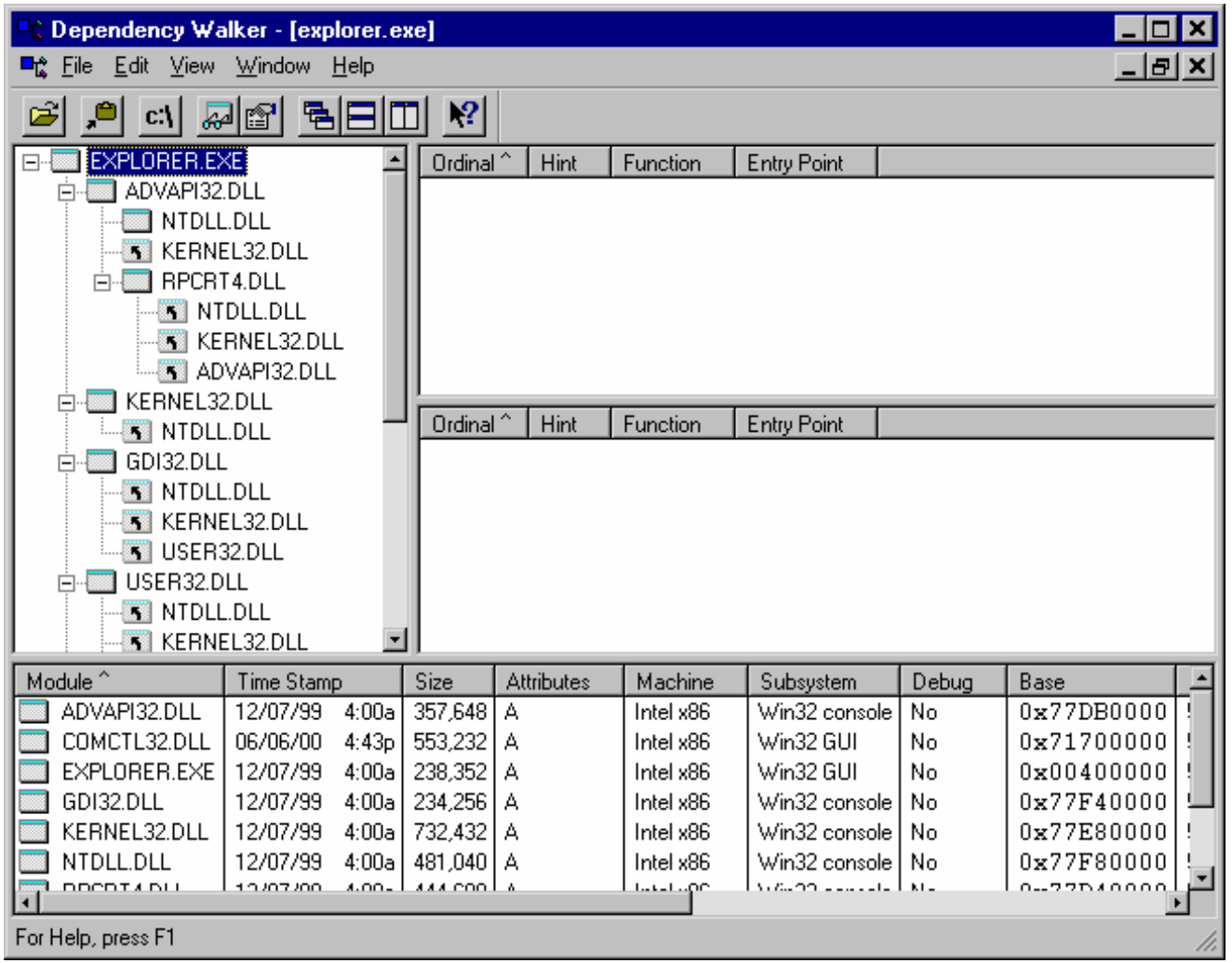
Finding Dependencies

- One of the major problems with Microsoft services has been the (in)ability to determine, easily, what services relied on other services



Application Dependencies

- Use depends from Resource Kit
- See the help associated with the tool form details on its use



Set System Policy

- Password Policies
  - Enforce password history 5
  - Maximum password age 60
  - Minimum password age 5
  - Passwords must meet complexity requirements
  - Store password using reversible encryption (Disabled)

- Account Lockout Policies
  - Account lockout threshold 5
  - Account lockout duration 30
  - Reset account lockout threshold after (Disabled)

Set System Policy

- Audit Policy
  - Audit account logon events
  - Audit account management
  - Audit logon events
  - Audit policy change
  - Audit system events
- Audit Log settings
  - Ensure that there is adequate space
  - Remember to set your rotation policy as well
- All should be consistent with whatever policy you have

User Rights

- Validate which Users and Groups have the following User Rights
  - Access this computer from the network
  - Act as part of the operating system
  - Back up files and directories
  - Change the system time
  - Create a token object
  - Debug programs
  - Force shutdown from a remote system
  - Increase scheduling priority
  - Load and unload device drivers

User Rights

- Log on as a service
- Log on locally
- Manage auditing and security log
- Modify firmware environment values
- Profile single process
- Profile system performance
- Replace a process level token
- Restore files and directories
- Shut down the system
- Take ownership of files or other objects

User Rights

- Additionally, if your systems are part of a domain, you should validate:
  - Add workstations to domain
  - Deny access to this computer from the network
  - Deny logon locally
  - Enable computer and user accounts to be trusted for delegation
  - Synchronize directory service data

Security Options

- Check the following (Security Options->Local Policy)

Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow system to be shut down without having to log on	Disabled
Audit use of Backup and Restore privilege	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled (for high security)
Digitally sign client communication (when possible)	Enabled (for medium security)
Digitally sign server communication (always)	Enabled (for high security)
Digitally sign server communication (when possible)	Enabled (for medium security)

Security Options

Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled (for multi-user systems)
LAN Manager Authentication Level	Send NTLMv2 responses only / refuse LM & NTLM
Message text for users attempting to log on	Get from your legal department
Message title for users attempting to log on	Get from your legal department.
Number of previous logons to cache (in case domain controller is not available)	0
Prevent users from installing printer drivers	Enabled
Recovery Console: Allow automatic administrative logon	Disabled
Rename administrator account	Rename this to something other than “admin” or “administrator”

Security Options

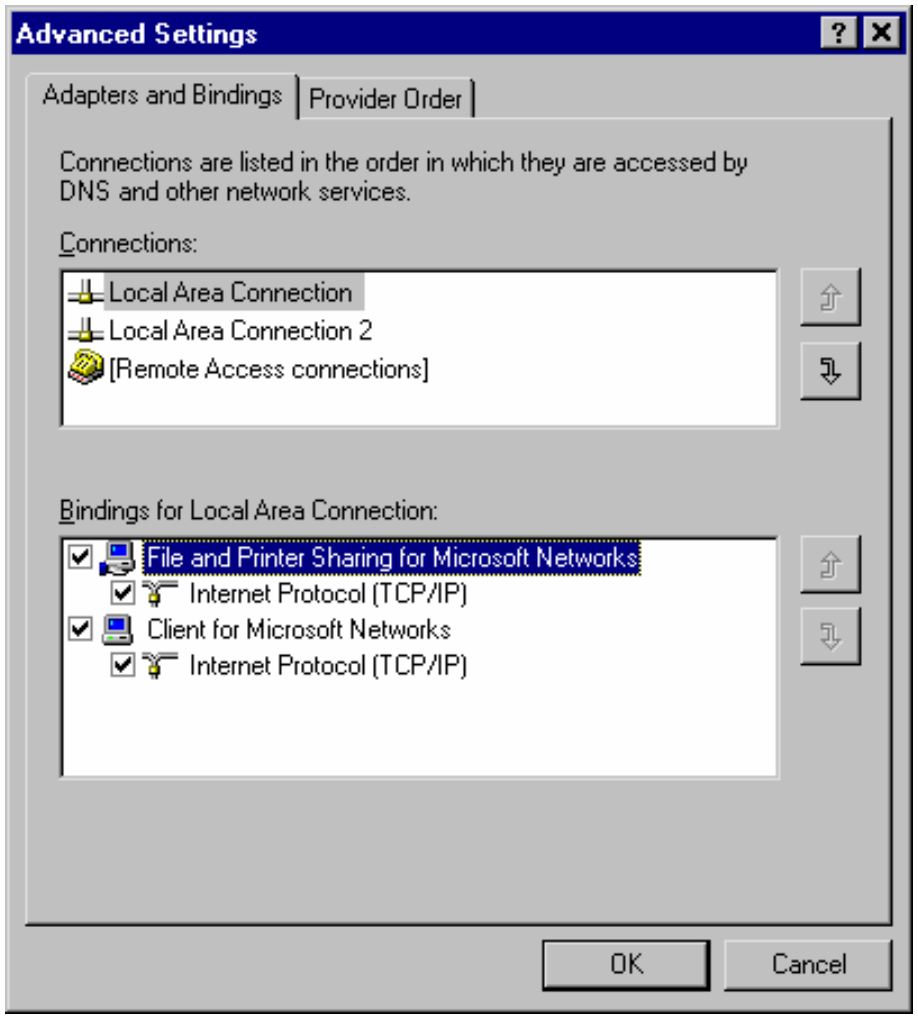
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled (for high security)
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled (for medium-high security)
Secure channel: Digitally sign secure channel data (when possible)	Enabled (for medium security)
Secure channel: Require strong (Windows 2000 or later) session key	Enabled (for ultra-high security
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	This should be consistent with your policy
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Do Not Allow
Unsigned non-driver installation behavior	Do Not Allow

Directory Permissions

- The root (C:\) should be tightened down
- Default installation of Win2K will give the Everyone group full control of the top level of this directory
  - Give “Everyone” group has Read-only access
- CAUTION: This has a high likelihood to break some software, so ensure you test it in your environment before propagating it out

Unbinding Services

- Network and Dial-Up Connections | Advanced | Advanced Settings selection
- A reboot is NOT required to set this feature



Unbinding Microsoft Networking

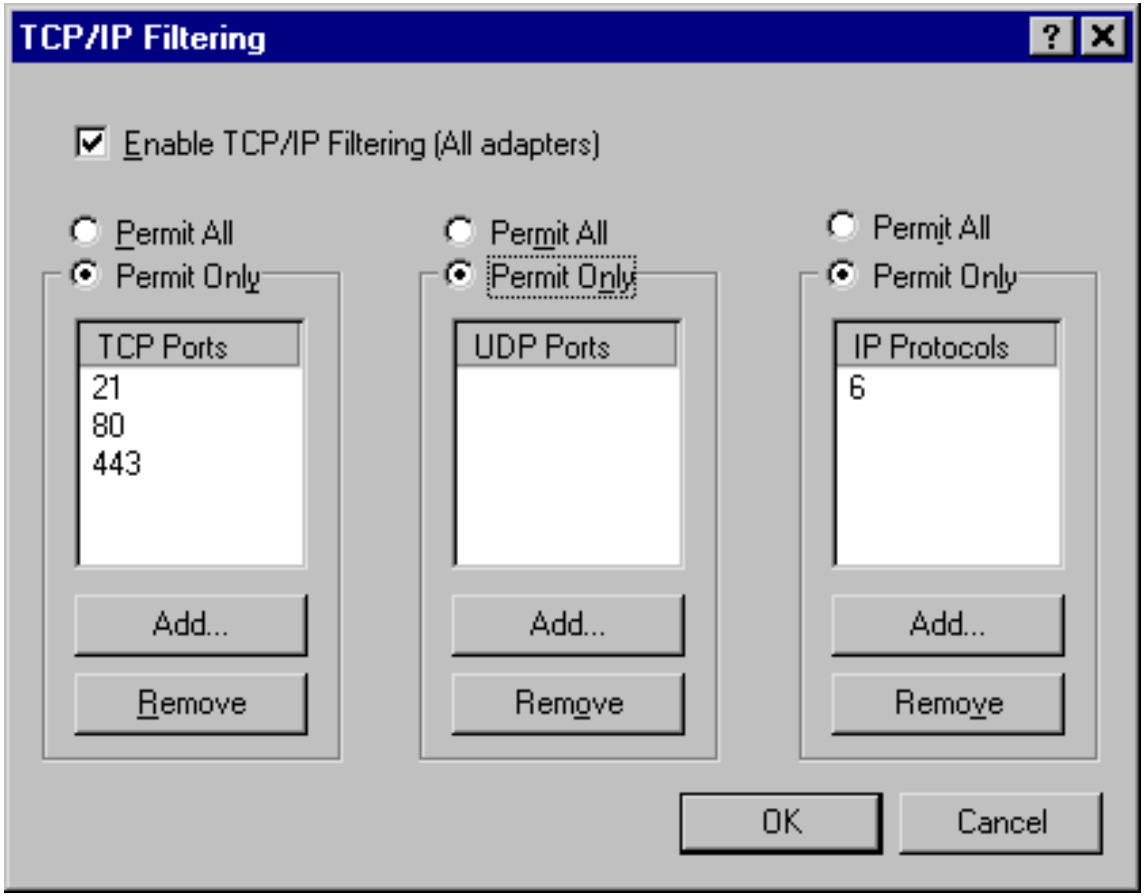
- Unbinding “File and Printer Sharing for Microsoft Networks”
  - Prevents remote machines from connecting to CIFS/SMB services on this machine
  - Tcp 139 will still be listening on this NIC, but will not return any information to the remote machine
  - If “Client for Microsoft Networks” is still enabled, the host itself will still be able to perform SMB connections to remote hosts even though it won’t accept any incoming requests

Filtering

- Two methods to accomplish this task
  - IPSec filters
  - TCP/IP Filtering
- TCP/IP Filtering is the same method that WinNT provided
- IPSec is more granular, but harder to setup
  - Can be implemented in Group Policy, where TCP/IP filtering is only locally configurable.

Filtering with TCP/IP Filtering

- Internet Protocol (TCP/IP) | Properties | Advanced | Options | TCP/IP Filtering | Properties on the interface you are configuring



Important “Features”

- TCP/IP Filtering has some very important “features” that you should be aware of:
- It does not affect any sessions initiated by the system
- It will still allow ICMP in
- By disallowing UDP, you will block the ability of your client to receive DNS query replies
  - This is because the filtering is not stateful, and thus the return UDP packet is blocked. You'd have to open up all inbound ports over which you think you'd receive DNS traffic (i.e., all UDP)
  - I have not found a workaround

IPSec filters

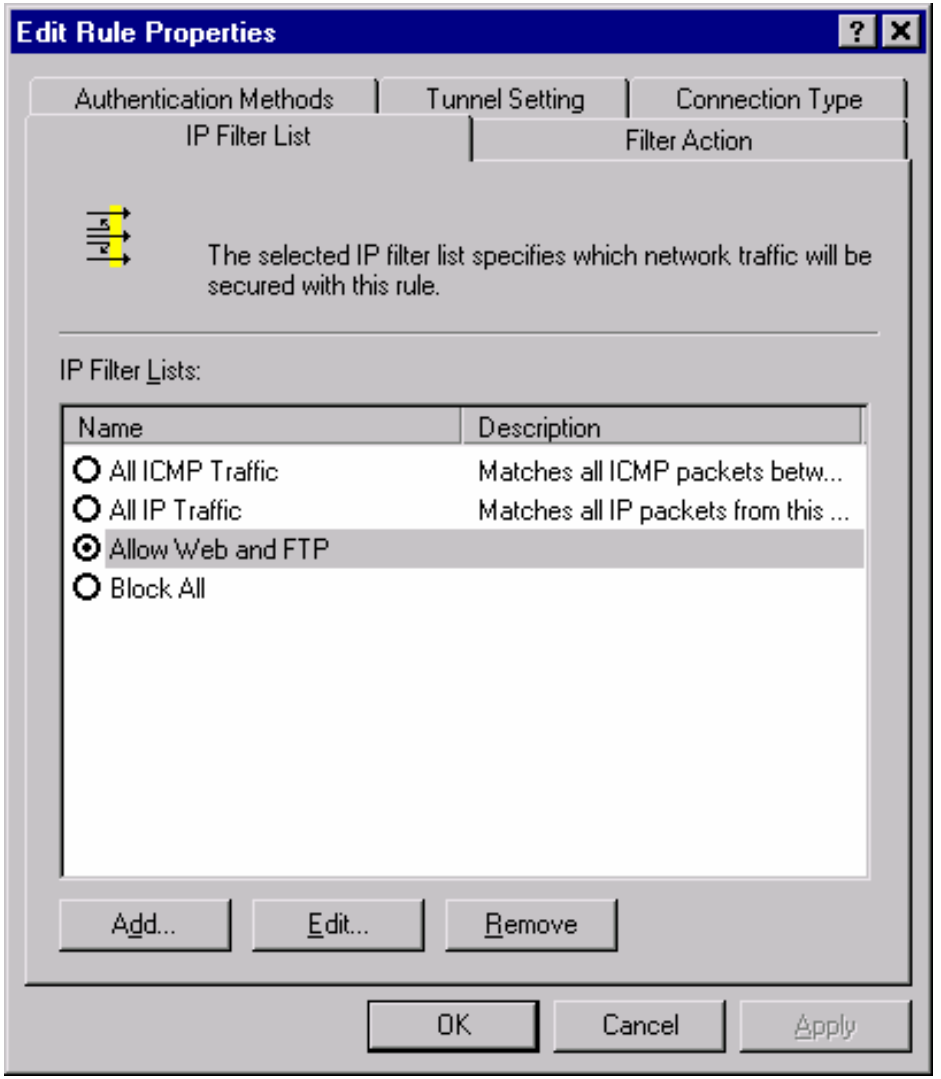
- Manage IPSec policies from the Local Security Policy or the individual IPSec Policy snap-in, and are activated via the Local or Group policy
- Three key configurations that we will need to set are:
  - IPSec filter lists
  - IPSec filter actions
  - IPSec policy rules

IPSec Filter Steps

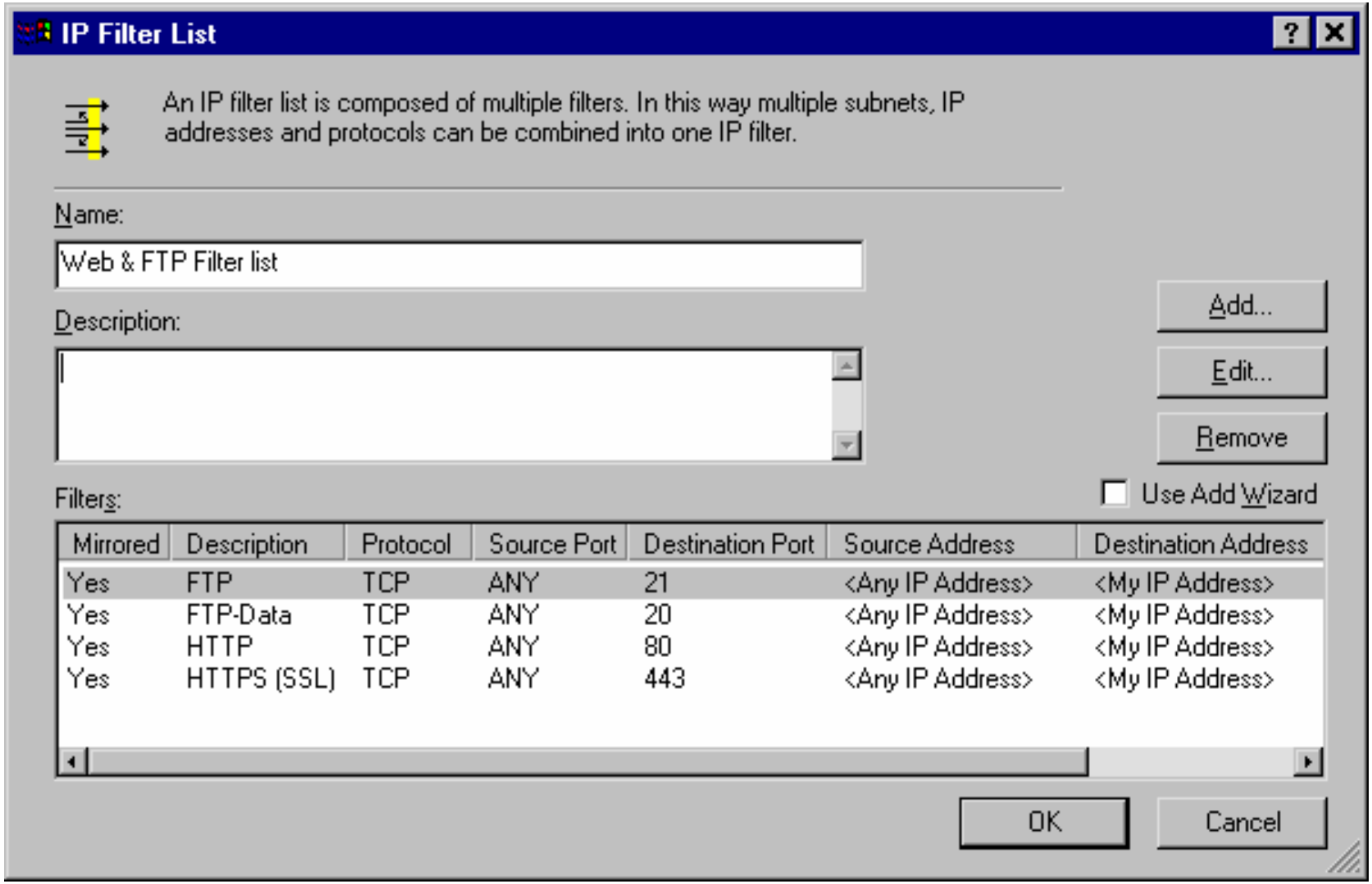
- First you will create an IPSec policy
  - We will call it “Web & FTP”
- Then add an IPSec filter list that will hold the IPSec filter actions we want applied
  - We are creating a filtering policy that will contain a list of filter actions that will be applied to network traffic entering and leaving the system
- When you create your filter, you will also need to add the 'All IP Traffic' filter list to the policy and set to 'Block'. That way everything is now being blocked except what you allow

Filtering TCP/IP Connections with IPSec

- Another option in the hardening process is to setup the IP Security Filters on a system to help secure it
- Can be set at LSDOU level with IP Security Policy



IPSec Filter List



IPSec Filter List Explanation

- The figure shows the IPSec filter actions that are associated with the IPSec filter list that was created
- The filter allows traffic from any IP address with a destination of the web server with a destination port of HTTP (port 80), HTTPS (443), FTP (port 21), and FTP-DATA (port 20)
- The mirror rule to the FTP-DATA allows PASV FTP
- By default, all filters are “mirrored,” which means that packets with source and destination addresses reversed will also match the filter

Traffic Not Filtered By IPSec

- IP Broadcast addresses
  - Can't secure to multiple receivers
- Multicast addresses
  - From 224.0.0.0 through 239.255.255.255, same reason
- RSVP - IP protocol type 46
  - Allows RSVP to signal Quality of Service (QOS) requests for application traffic that may then be IPSec protected
- Kerberos- UDP source or dest port 88
- IKE - UDP dest port 500
  - Required to allow IKE to negotiate parameters for IPSec security

Blocking RSVP and Kerberos

- By default Win2K allows Kerberos (88) and IKE (500), regardless of the IPSec filters rules established
- After SP1, you can change this behavior. You need to create the NoDefualtExempt key in the IPSec service:
  - Key: HKLM\System\CurrentControlSet\services\ipsec
  - Data: NoDefaultExempt
  - Value: 1 (REG_DWORD)
- A value of “1” will block RSVP and Kerberos. Thus leaving only IKE, Multicast, and Broadcast exempt
  - Note: See Microsoft KB article Q254728 for more details.

Tightening TCP/IP

- HKLM\System\CCS\Services\Tcpip\Parameters:
  - SynAttackProtect: a semi-dynamic way to reduce the time the system will wait for SYN-ACKs
  - TcpMaxHalfOpen: This determines the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate
  - TcpMaxHalfOpenRetried: Number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent before SYN-ATTACK protection begins to operate
  - PerformRouterDiscovery: Win2K will try to perform router discovery (RFC 1256). This is on a per-interface basis
  - EnableICMPRedirect: Controls whether Windows 2000 will alter its route table in response to ICMP redirect message
  - KeepAliveTime: How often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet

Time Synch: Win32Time

- Installed by default on Win2K
- Sync with NTP servers: NT5DS and NTP
  - NT5DS: used AD for sync
    - Need external server for forest root PDC
  - NTP: specify an NTP server
- Uses SNTP
  - No error checking or filtering
- HKLM\SYS\CCS\Services\W32Time

More Time Sync

- Net Time
  - Allows for setting at the command line
  - **`net time /?`**
- Mixed domains
  - With no AD, use NT's Win32Time as SNTP server for Win2K
  - With AD, use forest root PDC as main server

Securing the AD

- Rests on multiple factors
- 6 layers of security that we need to worry about:
  - Securing the system
  - Securing the database
  - Securing the replication
  - Securing the normal access methods
  - Securing the objects
  - Auditing

Default AD Permissions

- Everyone group in the Pre-Windows 2000 compatible permissions built-in group
- Read access to all user and group object attributes
- This gives the same access as a WinNT domain for queries

Securing Normal Access

- Blocking access to the ports that can be used to access the AD
  - ldap (389, 636), Global Catalog (3268, 3269), SMB (135, 137-139), and CIFS (445)
  - Use Group Policies to control what actions are allowed on the domain objects
- Auditing the AD
  - You need to ensure that you are auditing critical operations and data, such as changes to policy data or critical files in the WINNT, NTDS, and SYSVOL partitions.

Why AD Security is important

- Bugtraq message on 2/21/2001: Win2k directory services weakness
- The important part …
  - In Active directory there is one Configuration Container for the whole forest. So every domain controller has its own copy of Configuration Container and is able to change it and replicate changes to other domain controllers
- If you have large organization, every DC is then (almost) equally vulnerable; if a hacker beaks into one, he gets all.

Tidying Up

- Now that the majority of work is done, there is still some tidying up to do
- Install ServicePacks and Hotfixes
- Removing unneeded Sub Systems
  - Remove the OS2 and Posix registry values from the HKLM\System\CurrentControlSet\Services\Session Manager\SubSystems registry key
  - Delete the associated files (os2*, posix*, and psx*) in %systemroot%\System32.

Tidying Up

- Change Permissions on Binaries
  - Make a separate group that does not have the Administrators group in it, then re-permission
    - Change the ACLs on the following tools to “remove” LocalSystem and the Administrators group, and add new group
  - arp.exe, ipconfig.exe, Nbtstat.exe, at.exe, net.exe, Netstat.exe, atsvc.exe, nslookup.exe, ping.exe, cacls.exe, posix.exe, Qbasic.exe, Cmd.exe, rcp.exe, rdisk.exe, debug.exe, regedit.exe, Regedt32.exe, edit.com, rexec.exe, route.exe, edlin.exe, rsh.exe, Runonce.exe, finger.exe, secfixup.exe, Syskey.exe, ftp.exe, telnet.exe, Tracert.exe, xcopy.exe, tftp.exe, command.com, clipsrv.exe, dialer.exe, hypertrm.exe, attrib.exe, ping.exe, sysedit.exe, cscript.exe, wscript.exe

Tidying Up

- Cleaning Up Anonymous Registry Access
  - Allowed Paths | Machine key
  - Evaluate all, the only real option that you should allow in there by default is the System\CurrentControlSet\Control\ProductOptions
- Use the EFS to encrypt sensitive files
- Configure the system to boot immediately
- Configure system dumps
- Run an integrity checking software (i.e. Tripwire) over the final system to get a baseline for later detection

Test Security Settings

- Once you have the system(s) configured, you will want to test them to see what you can get at from the outside
- You will need:
  - Port Scanner (Nmap): You will need some type of UDP and TCP port scanner
  - EPDump: You will use this tool to help you determine which RPC services have which ports open
  - Netstat: You will use this tool on the local host to identify its open ports
  - Fport: A great overall tool from www.foundstone.com
- Once you have the tools, then scan the system to see what is open

Win2K may still fall short

- Unless you are hardening a single host, there is a high likelihood that you will be using some type of service that will be relying in some manner on Microsoft networking (either NetBIOS, SMB/CIFS, or RPC)
- This means that you can't use Win2K to protect itself, you will have to use other security measures to isolate those systems from people that you do not intend to access those Microsoft services
- A simple Screening Router will accomplish the task just fine, but you may choose to have a more full-featured firewall

Papers and Filters @ SystemExperts

- HardenW2K12.pdf: Hardening Windows 2000 version 1.2
- home_Low.ipsec: IPSec filters to block inbound connections to NetBIOS/SMB ports
- home_User.inf: IPSec filters to set Local Security Policy for a home user configuration
- secureWebServer.ipsec: IPSec filters to only allow inbound http by default. Additional filters defined for https, smtp, NetBIOS, ICMP
- Web_Secure.inf: IPSec filters to set Local Security Policy for a web server configuration. Note that this Web Server template was partially created on a Windows 2000 Professional System, so Power Users (or related SID) may be present in rulesets, instead of Server Operators
- hardenWin2K.zip: Zip file of the directory contents