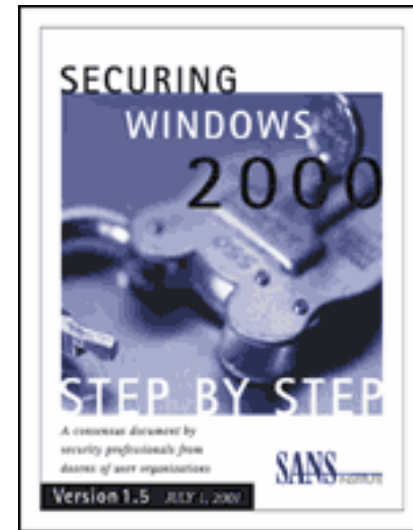


Session Three: Attacks, Incidents, and Hardening Windows 2000



**Don Murdoch, CISSP
MCSE, MCSD**

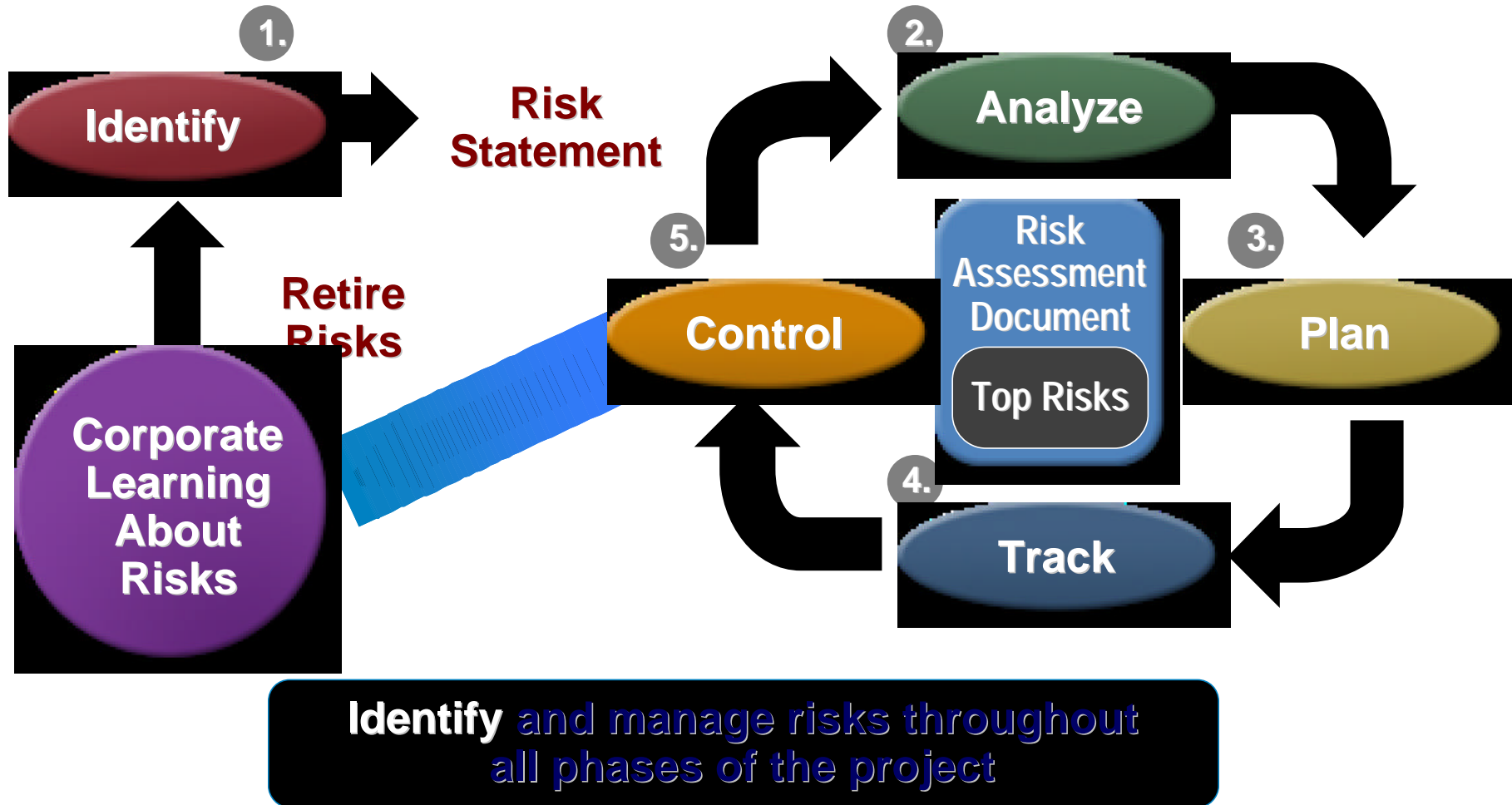
Agenda

- What makes Windows Vulnerable
- Out of the Box Installs
- What are the tools involved
- Operating system features that improve security
- Operating system hardening
- IIS hardening
- Network hardening
- Sources of Guidance

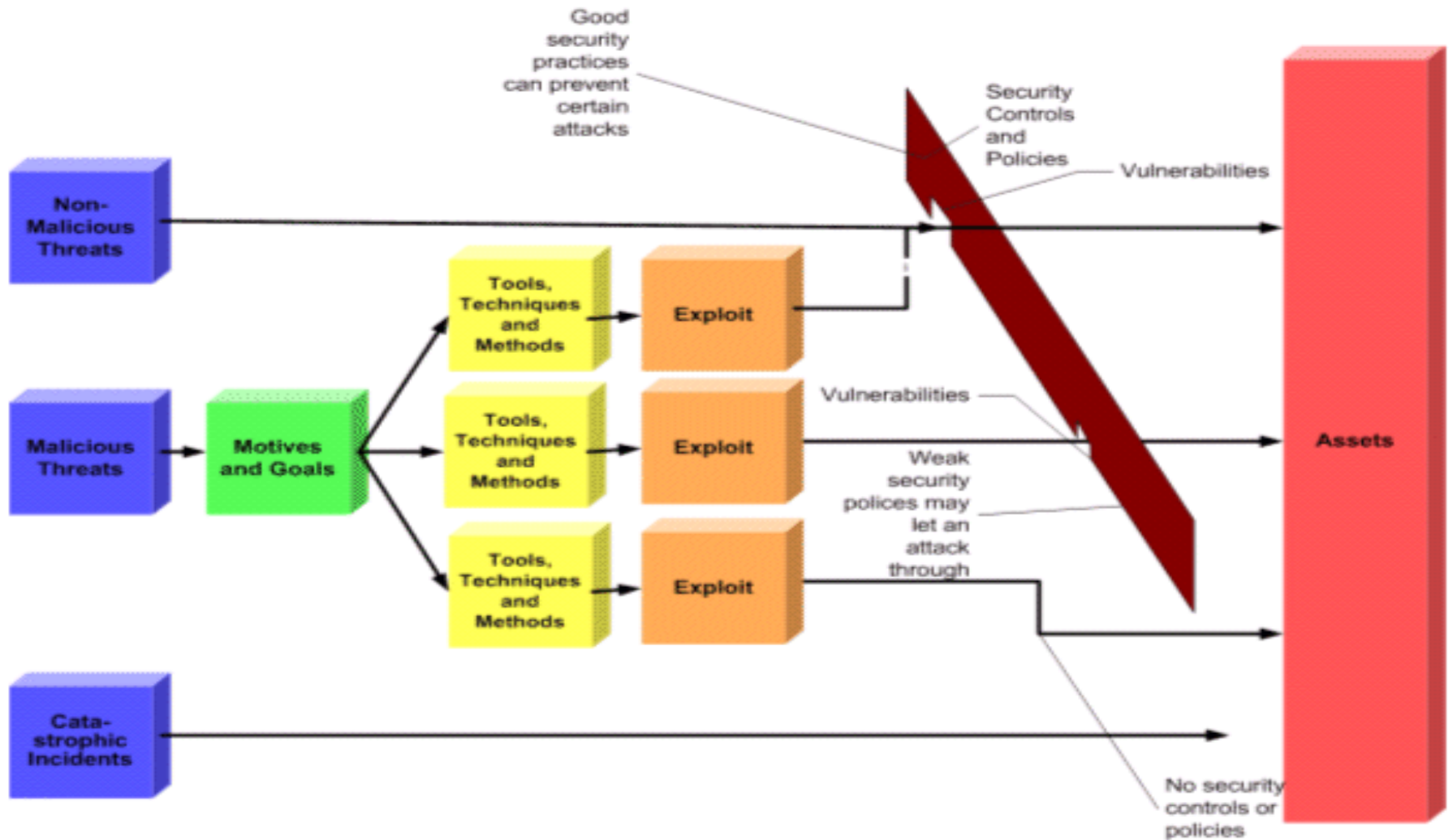
- Credit and Sources
 - *Microsoft Windows 2000 Security Guide*
 - *SANS Securing Windows 2000 Step by Step*
 - *SANS Securing Win2K using the Gold Std Template*

Jog the Memory

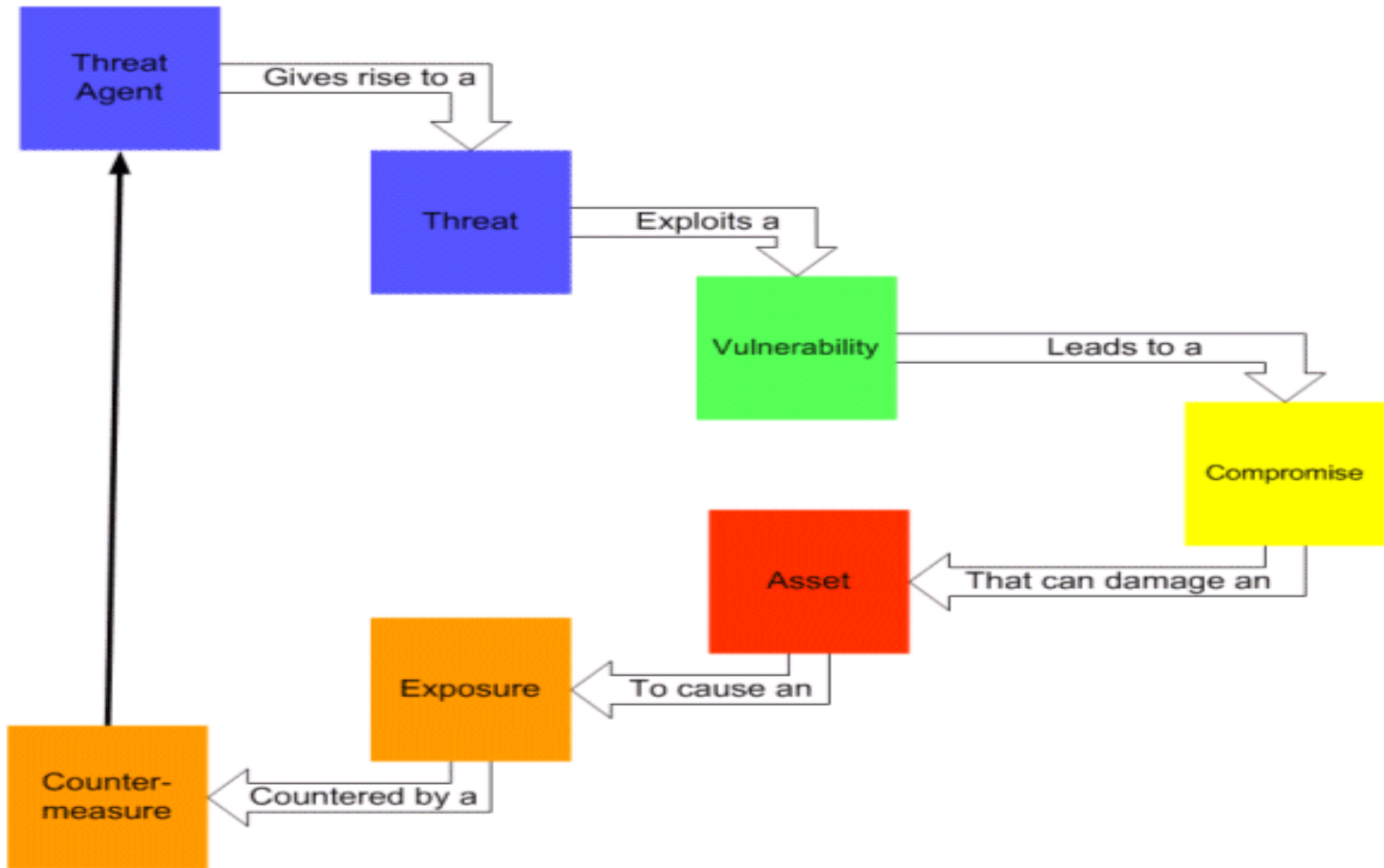
Risk Modeling and Mitigation




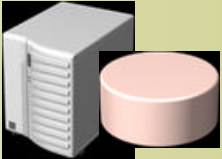




The Ingredients of an Attack (threat plane)



Revisiting the Threat Continuum



Common Indicators of Security Incidents

Area	Examples
<p>Network irregularities</p> 	<ul style="list-style-type: none">• Network performance decreases• Accounts are used at irregular times
<p>System irregularities</p> 	<ul style="list-style-type: none">• Audited events increase significantly• System performance decreases• Computers crash or reboot mysteriously
<p>Direct reporting of events</p>  	<ul style="list-style-type: none">• Users report security incidents• A new virus is published• Intrusion detection software detects an incident
<p>Physical indicators</p> 	<ul style="list-style-type: none">• Hardware is missing• Visible signs exist of physical compromise
<p>Business indicators</p> 	<ul style="list-style-type: none">• Confidential information is published on the Internet or in print• Competitor appears to possess trade secrets

Phases of an Attack

1. Foot printing
2. Scanning
3. Enumeration and Vulnerability Identification
4. Penetration
5. Privilege Escalation
6. Evidence Elimination
7. Stage the Return

Foot Printing

- The process of learning about *you*
- Newsgroup postings
 - Identify items and people of interest
 - Technologies being deployed
- Network information
 - DNS registrations
 - DNS entries
 - IP addresses, ranges and public segment size
 - Email addresses
- Your own website
 - Headers
- News media
- Low and slow scans and probes

Scanning

- Public IP's in use and registered
- Mapping your site – services offered
- DMZ and perimeter configuration
 - Screening routers and ACL's
 - Candidate firewalls and firewall rules
 - Fragmented packets that might penetrate
 - OS and information service fingerprinting based on TCP and IP responses
- Tools
 - Nmap, Nessus, Firewalk, Hpoing2, Whisker

Enumeration and Vulnerability Identification

- Perhaps a little social engineering
- Check out what you have and use
 - Determine its vulnerabilities
 - Look for the least intrusive tool to exploit a vulnerability
 - Various sites list security holes or weaknesses and how to exploit and patch them
- User account and password guessing

Penetration – Going for It!

- The act of actually exploiting a vulnerability
 - Gaining access to the system
 - Preventing legitimate access to the system
 - Redirecting people away from your site
- Breach
 - A breach violates one or more:
 - Confidentiality
 - Integrity
 - Availability

Privilege Escalation

- Break-ins don't always result in supervisory level access (admin or root)
- Privilege escalation may involve
 - Consolidating control
 - Gaining supervisory access
 - Replacing a binary / program for later use
 - Installing a root kit that will hide itself
 - Extracting valuable data

Evidence Elimination

- Removing evidence in log files
- Removing the log files if you can't remove the trace ...
- Removing one's own uploaded tools that were used during penetration

Staging the Return

- Creating a “hole” that may stand out in the open
 - New logical looking account
 - Trojans – Netcat, NetBus, SubSeven, Loki
 - RootKit – over 60 for *nix
 - RootKit – at least 6 for NT/2000
 - Install / Activate a sniffer that can report back
 - Enabling spy ware

SANS Six Steps for Incident Response

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow up

Response

Communicate the attack to



- Security specialists
- Network administrators
- Management

- Legal advisors
- Law enforcement

Team members should

- Available 24 hours a day
- Trained in responding to security incidents
- Competent in their area of responsibility
- Able to analyze situations objectively under pressure
- Strong communicators

SANS Top Ten Vulnerabilities for Windows

- Internet Information Services (IIS)
- Microsoft Data Access Components (MDAC) -- Remote Data Services
- Microsoft SQL Server
- NETBIOS -- Unprotected Windows Networking Shares
- Anonymous Logon -- Null Sessions
- LAN Manager Authentication -- Weak LM Hashing
- General Windows Authentication -- Accounts with No Passwords or Weak Passwords
- Internet Explorer
- Remote Registry Access
- Windows Scripting Host

SANS Top Ten Vulnerabilities for Unix

- Remote Procedure Calls (RPC)
- Apache Web Server
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- R-Services -- Trust Relationships
- Line Printer Daemon (LPD)
- Sendmail exploits and vulnerabilities
- BIND/DNS
- General Unix Authentication -- Accounts with No Passwords or Weak Passwords

Securing New Installations



Plan to:

- Implement secure defaults
- Install only required services and applications
- Secure default accounts and passwords

To secure a new installation, you can:

- Deploy the OS on an isolated network
- Use updated, secure installation media
- Create custom installation scripts
- Create hard drive images by using imaging software
- Deploy the OS or hard drive images by using Remote Installation Services

Steps in Hardening Windows NT/200X/XP (and operating systems in general) (1/2)

- Customize the base install
- Remove and lock down services
- Know and monitor user accounts
- Implement auditing and review the audit logs frequently
- Customize file system permissions
- Customize registry permissions
- Secure directory services
- Use highest possible authentication

Steps in Hardening Windows NT/200X/XP (and operating systems in general) (2/2)

- Apply domain wide group policies
- Apply local policies (especially notebooks)
- Use necessary network protocols only
- Apply service packs as they become available
- Apply patches as necessary, after some testing if at all possible
- Install antiviral software
- Deploy IDS systems if possible
- No physical security? There is no security.

Customize the Installation

- Plan for a portable setup
 - P1: 4 GB NTFS Windows NT/2000
 - Booting and recovery support only
 - Update both maintenance and production over time
 - P2: 8-10GB Windows NT/200X
 - Operating system and applications
 - P3: Remaining disk
 - Applications
 - Data
 - Install the Recovery Console – “winnt32 /cmdcons”
- Unattended setup is mandatory for portability and service control, detailed setup
 - Documented in Resource Kit/Technet/Support sites
 - winnt32 /unattend: <answer file> /s: <install source> [/syspart: <target drive>] [/tempdrive: <target drive>]

Remove Unnecessary Services

- Determine services based on
 - Need
 - Security policies
 - Business requirements
- Disable unnecessary services
- Remove services where possible
- Review necessary privileges
 - Logon
 - Startup type
 - Recovery actions
 - Dependencies list

Services: Customize Base Install (1)

- Executable and Service Descriptive Name
 - Certsvc.exe: Certificate Services (CertSvc)
 - Cisvc.exe: Indexing Service (cisvc)
 - Clipsrv.exe: Clipbook (Clipsrv)
 - Dfssvc.exe: Distributed File System (DFS)
 - Dmadmin.exe Logical Disk Manager Administrative Service (DMAdmin)
 - Dns.exe: DNS Server (DNS)
 - Faxsvc.exe: Fax Service (Fax)
 - Grovel.exe: Single Instance Storage Groveler (Groveler)

Services: Customize Base Install (2)

- Executable and Service Descriptive Name
 - Inetinfo.exe:
 - IIS Admin Service (IISADMIN)
 - FTP Publishing Service (MsFtpSvc)
 - Network News Transfer Protocol (NNTPSvc)
 - Simple Mail Transport Protocol (SMTPSvc)
 - Site Server ILS Service (LdapSvcX)
 - World Wide Web Publishing Service (W3SVC)
 - Ismserv.exe: Intersite Messaging (IsmServ)
 - Lssrv.exe: License Logging Service (LicenseService)
 - Locator.exe: Remote Procedure Call Locator (RPC Locator)

Services: Customize Base Install (3)

- Executable and Service Descriptive Name
 - Lsass.exe
 - IPsec Policy Agent (Policy Agent)
 - Kerberos Key Distribution Center (KDC)
 - Net Logon (Netlogon)
 - NT LM Security Support Provider (NTLMSSP)
 - Security Accounts Manager (SAMSS)
 - Lserver.exe: Terminal Services Licensing (TermServLicense)
 - Mnmsrvc.exe: NetMeeting Remote Desktop Sharing (MnmSrvc)
 - Mqsvc.exe: Message Queuing (Msmq)
 - Msdtc.exe: Distributed Transaction Coordinator (Msdtc)

Services: Customize Base Install (4)

- Executable and Service Descriptive Name
 - Msiexec.exe: Windows Installer (MsiServer)
 - Mstask.exe: Task Scheduler (Schedule)
 - Netdde.exe:
 - Network DDE (NetDDE)
 - Network DDE DSDM (NetDDEdsdm)
 - Nscm.exe: Windows Media Station Service (NsStation)
 - Nslservice.exe: On-line Presentation Broadcast (Nslservice)
 - Nspm.exe: Windows Media Program Service (NsProgram)

Services: Customize Base Install (5)

- Executable and Service Descriptive Name
 - Nspmon.exe: Windows Media Monitor Service (NsMonitor)
 - Nsum.exe Windows Media Unicast Service (NsUnicast)
 - Ntfrs.exe File Replication Service (Ntfrs)
 - Regsvc.exe: Remote Registry Service (RemoteRegistry)
 - Rseng.exe: Remote Storage Engine (Remote Storage Engine)
 - Rsfsa.exe: Remote Storage File (Remote_Storage_File_System_Administration)

Services: Customize Base Install (6)

- Executable and Service Descriptive Name
 - Rsfsa.exe Remote Storage Notification (Remote_Storage_User_Link)
 - Rssub.exe Remote Storage Media (Remote_Storage_Subsystem)
 - Rsvp.exe QoS Admission Control (RSVP)
 - Scardsrv.exe Smart Card (ScardSrv)
 - Smart Card Helper (ScardDriver)
 - Services.exe
 - Alerter (Alerter)
 - Application Management (appmgmt)
 - Computer Browser (Browser)
 - DHCP Client (Dhcp)
 - Distributed Link Tracking Client (TrkWks)
 - Distributed Link Tracking Server (TrkSvr)

Services: Customize Base Install (7)

- Executable and Service Descriptive Name
 - Services.exe (cont'd)
 - DNS Client (DnsCache)
 - Event Log (Eventlog)
 - Logical Disk Manager (DmServer)
 - Messenger (Messenger)
 - Plug and Play (PlugPlay)
 - Protected Storage (ProtectedStorage)
 - RunAs Service (Seclogon)
 - Server (LanManServer)
 - TCP/IP NetBIOS Helper Service (LMHosts)
 - Windows Management Instrumentation Driver
 - Extensions (WMI)
 - Windows Time (W32Time)
 - Workstation (LanmanWorkstation)

Services: Customize Base Install (8)

- Executable and Service Descriptive Name
 - Sfmprint.exe Print Server for Macintosh (MacPrint)
 - Sfmsvc.exe File Server for Macintosh (MacFile)
 - Smlogsvc.exe Performance Logs and Alerts (SysmonLog)
 - Snmp.exe SNMP Service (Snmp)
 - Snmptrap.exe SNMP Trap Service (SnmpTrap)
 - Spoolsv.exe Print Spooler (Spooler)

Services: Customize Base Install (9)

- Executable and Service Descriptive Name
 - Svchost.exe (multithreaded super service)
 - COM+ Event System (EventSystem)
 - Internet Authentication Service (IAS)
 - Internet Connection Sharing (SharedAccess)
 - Network Connections (NetMan)
 - Remote Access Auto Connection Manager (RasAuto)
 - Remote Access Connection Manager (RasMan)
 - Remote Procedure Call (RPCSS)
 - Removable Storage (Ntmssvc)
 - Routing and Remote Access (RemoteAccess)
 - System Event Notification (SENS)
 - Telephony (TapiSrv)

Services: Customize Base Install (10)

- Executable and Service Descriptive Name
 - Tcpsvcs.exe
 - Boot Information Negotiation Layer (BinlSvc)
 - DHCP Server (DhcpServer)
 - Simple TCP/IP Services (SimpTcp)
 - TCP/IP Print Server (LpdSvc)
 - Termsrv.exe Terminal Services (TermService)
 - Tftpd.exe Trivial FTP Daemon (Tftpd)
 - Tlntsrv.exe Telnet (TlntSrv)
 - Ups.exe Uninterruptible Power Supply (UPS)
 - Utilmon.exe Utility Manager (Utilmon)
 - Winmgmt.exe Windows Management Instrumentation (WinMgmt)
 - Wins.exe Windows Internet Name Service (WINS)

Services Related Registry Keys

- Which programs start when the computer starts:
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Which services start when the computer starts
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- Check which services starts the svchost
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Svchost
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Svchost

Without
physical
security,
There is no
security

**Tools, Methods, and
Ways to Get There!**

What makes Windows Vulnerable

- Convenience features
- Openness – on the corporate or home network
- Default to “fail open”
 - Changing with Windows 2003 server
 - Windows XP example – UPNP service ON and advertising
- Size / Complexity
- User weaknesses and lack of education

Out of the Box Installs

- To generic
 - Many services are installed and enabled
 - Don't take into account intended application
- Default Services
 - Web Server: IIS / PWS
 - Networking: NetBIOS, Telnet
- Default Installation
 - Weak NTFS and registry permissions
 - Known accounts/SID's
 - No policies
 - Registry can be read remotely
 - Shares can be easily explored

Tools Involved to Help Secure a System

- CIS Scoring Tool
- SCAT
- Net.exe – command line network usage
- Nbtstat.exe – views NetBIOS info
- Variety of resource kit tools
- Conversion Kits like cygwin
- Sysinternals has great tools
- Scripting (not as powerful as Unix)
 - for /f "tokens=1*" %i in ('fscan -eq -p 80 10.120.1.1-254') do @ping | nc -v -n %i 80 | Find /i "Server"

Know and Monitor User Accounts

- User accounts
 - Rename “administrator” and “guest” via group policy (320053)
 - Administrator can be renamed on a standalone with the Computer Mgmt MMC
 - Create a dummy “administrator” account
 - Secure the password
- Group accounts
 - Backup Operators
 - Server Operators
 - Administrators and Domain Admins
- IIS_Machinename and IWAM_Machinename
- Windows XP
 - HelpDesk

Implement Auditing

- On individual servers and with Group Policy, enable auditing
- Audit nearly everything
- Make the log files LARGE
- Review the audit logs
- Audit logs need to survive the “full backup” cycle at a minimum

Customize File System Permissions

- By default drives are shared for administrative purposes
 - Root partitions or volumes - C\$: hidden share to the C:\ drive
 - Admin\$ which is the system root folder
 - Others - FAX\$, IPC\$, PRINT\$
- Disable administrative shares
 - 318751 for server, 314984 for workstation
- Best accomplished with the SCAT
- Minimum share is “Authenticated Users”
- Always secure with NTFS

Secure Directory Services

- Avoid NTLM V1
 - Windows 2000 Server CD has NTLMV2 client for both Win9X and WinNT
- Migrate to Windows 2000 AD ASAP
 - Disable NTLM and use Kerb5 in Group Policy
- Implement IPSec between DC's

Group Policy

- Settings that Windows 2000 and XP “learn” from the domain and apply
- Automatically refreshed
- Two categories – Computer and User
- Applied under these rules
 - “the last write is right”
 - NT4 -> L -> S -> D -> OU
- Scope
 - Sites
 - Domains
 - Organizational Units

More Group Policy

- Created with Snap In's
- Set baseline policies in the domain wide group policy
- Set exceptions or extra restrictions to computers and users in specific GPO's
 - Kiosk PC's
 - PC's and users close to the public (e.g. receptionist, loading dock)
- Forced refresh with secedit

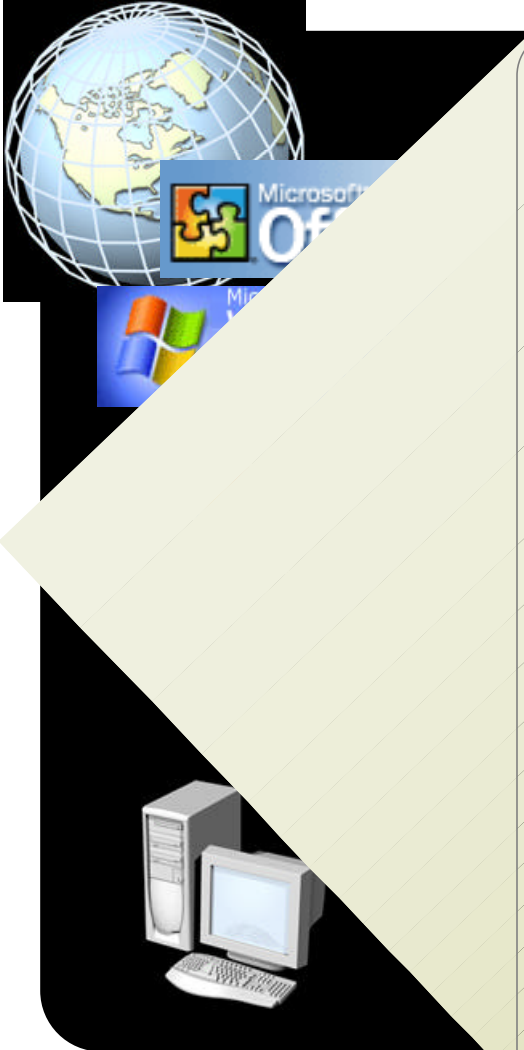
Network Protocols

- Use TCP/IP only unless there is a valid reason not to
- Other protocols include
 - NWLink (IPX/SPX)
 - NetBIOS
 - DLC
 - PPTP
 - AppleTalk

Tools for Operating System Maintenance

Tools	Use for	Detail
Windows Update	Home computers and small offices	<ul style="list-style-type: none">• Scans individual computers for updates• Recommends critical updates to install, and then installs updates
Office Update	Home computers and small offices	<ul style="list-style-type: none">• Scans computers for updates• Recommends and installs updates
HFNetChk	Standalone and networked workstations and servers	<ul style="list-style-type: none">• Scans individual computers or networks for the status of service packs and security updates• Provides multiple reporting formats
Microsoft Baseline Security Analyzer	Standalone and networked workstations and servers	<ul style="list-style-type: none">• Scans individual computers or networks for the status of service packs and security updates• Provides multiple reporting formats• Scans computers for known security vulnerabilities

Windows Update Site



Windows Update scans workstations and installs security updates to:

- Microsoft Internet Explorer 5.01 or later
- Microsoft Windows NT® 4.0, Windows 2000, and Windows XP

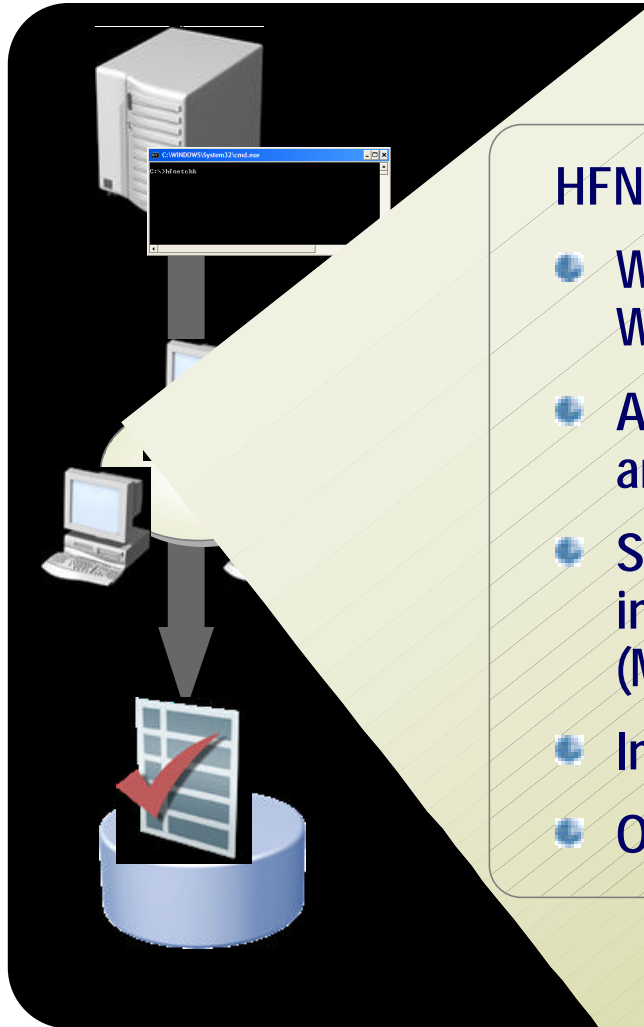
Windows Update also scans for and installs:

- General updates for Windows
- Device driver updates

Office Update scans individual computers and installs security updates to:

- Office 2000
- Office XP

HFNetChk (Network Hotfix Checker)



HFNetChk scans for security updates to:

- Windows NT 4.0 , Windows 2000, and Windows XP
- All Windows services, including IIS 4.0 and 5.0
- SQL Server 7.0 and SQL Server 2000, including Microsoft Data Engine (MSDE)
- Internet Explorer 5.01 and later
- Office XP

Software Update Service (SUS)

- Automatic Update (AU) client
 - Automatically download and install critical updates
 - Security patches, high impact bug fixes and new drivers when no driver is installed for a device
 - Checks Windows Update service or Corporate Update server once a day
 - New! Install at scheduled time after automatic downloads
 - Administrator control of configuration via registry-based policy
- Support for Windows .NET Server, Windows XP and Windows 2000
 - Software Update Services
 - Corporate hosted server supports download and install of critical updates through Automatic Update client
 - Server synchronizes with the public Windows Update service
 - Simple administrative model via IE
 - Updates are not made available to clients until the administrator approves them
 - Runs on Windows .NET Server and Windows 2000 Server

Microsoft Baseline



MBSA scans for security updates to:

- Windows NT 4.0, Windows 2000, and Windows XP
- All Windows services, including IIS 4.0 and 5.0
- SQL Server 7.0 and 2000, including Microsoft Data Engine (MSDE)
- Internet Explorer 5.01 and later
- Office XP

MBSA also scans for known vulnerabilities, including:

- Weak passwords
- Unnecessary services
- Office XP and Internet Explorer configuration
- IIS configuration



NULL shares in the Registry

- Null shares allow some services to access remote resources w/o authentication (and auditing)
- Not a great idea.
- How to Article: [289655](#)

OOB –Enumerating a NULL share

- Establish NULL session
 - Net use \\192.168.1.17\ipc\$ "" /user:""
- Enumerate 'administrator'
 - User2sid \\192.168.1.17 administrator
- Enumerate 'users'
 - Sid2User \\192.168.1.17 #'s (above)
- Countermeasure
 - Change Local Policy
 - Local Policy – Security Options – set “No access without explicit anonymous permissions” to 2.

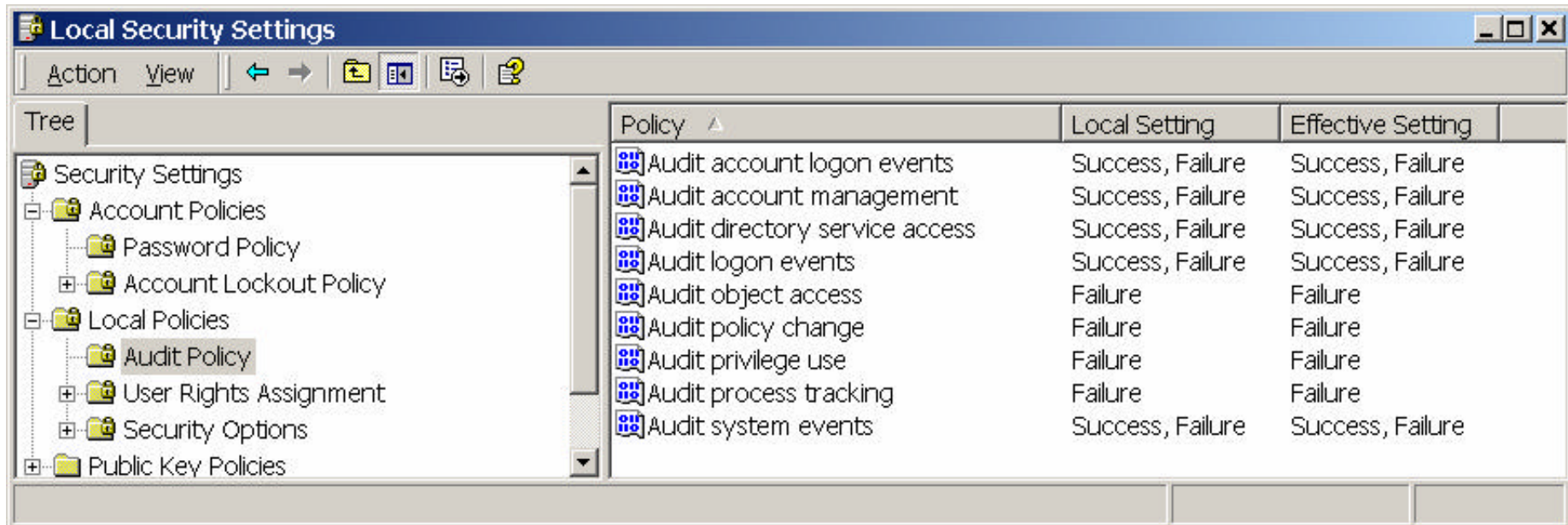
System Policies

Local and Domain Wide

**Applying Security Settings
To the System**

Local Audit Policies

- Audit – enable Success and Failure auditing for most options
- Notes:
 - Set log policy size large enough
 - Set overwrite options on each log



The screenshot shows the 'Local Security Settings' window. The 'Tree' pane on the left is expanded to 'Local Policies' > 'Audit Policy'. The main pane displays a table of audit policies with their current and effective settings.

Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Success, Failure	Success, Failure
Audit logon events	Success, Failure	Success, Failure
Audit object access	Failure	Failure
Audit policy change	Failure	Failure
Audit privilege use	Failure	Failure
Audit process tracking	Failure	Failure
Audit system events	Success, Failure	Success, Failure

Sensible Account Policies

- Password policy – long and complex
- Maintain password history – 8 or more
- Maximum password age – 60 to 90
- Minimum password age – open to debate
- Min password length – AT LEAST 7
- Disable NTLM if at all possible
- Enable complexity
- Disable reversible encryption
- Account lockout
 - Threshold – 3
 - Duration – 90 minutes
 - Reset lockout timer – 30 minutes

Local: User Rights Assessment

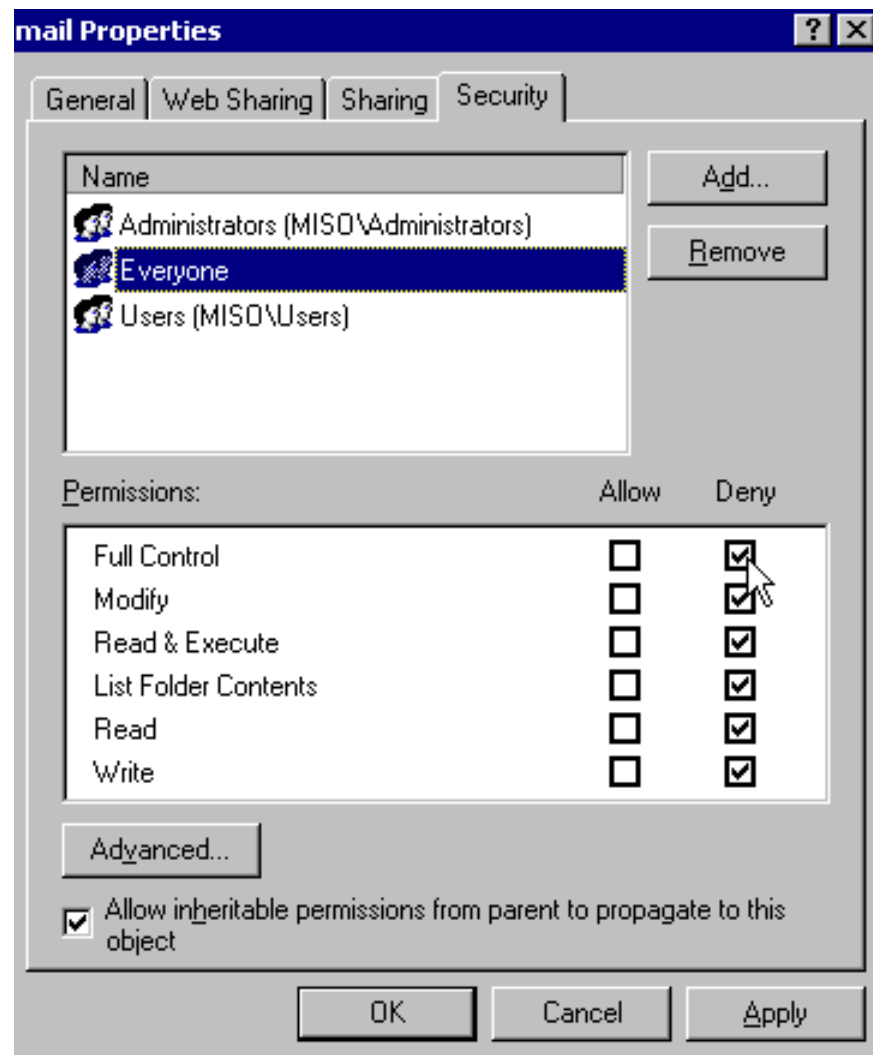
- Access this computer from network: set to "Authenticated Users"
- Act as part of the operating system: LocalSystem
- Backup/Restore files and directories: Admin/SPECIFIC Operators
- Change System Time: Administrators
- Load and unload device drivers: special
- Logon as a service: only service accounts for applications
- Logon locally: Authenticated Users
- The "Deny" Policies
 - This group allows restrictions to specific accounts – Deny overrides

Local: Security Options

- Additional restrictions for anonymous access: set to "Do not allow enumeration of SAM"
- Automatically log off users when logon time expires: Good way to get clean backups over night, can be annoying
- Clear virtual memory pagefile when system shuts down: advised for notebooks; takes extra time
- Disable CTRL+ALT+DEL requirement for logon: never enable this.
- Do not display last user name in logon screen: Enable; the logon name is "half the battle"
- LAN Manager authentication level: NTLM V2!
- Message text for users attempting to log on: YES
- Prevent users from installing printer drivers: if possible

Disable Windows 2000 Client Software

- Vulnerable Apps
 - TFTP
 - FTP
 - Telnet
 - Internet Explorer (frequently patched)
 - Management agents (Compaq)
- Countermeasure
 - Disable by removing access permissions
 - Audit the file
 - WFP will restore the file if you remove it!



Windows 2000 Desirable Components

- IPsec networking between servers and workstations wherever possible
- Group Policy
 - Apply restrictive GPO's at the domain level and loosen at the OU level
 - Enable maximum auditing at the highest level
- Logon Banner
 - Following "wiretap" guidance by the FBI, use a stringent banner that states something like ...
 - **"This system may be used only for authorized purposes. Unauthorized access or modification of information stored on this system may result in criminal prosecution. Accessing this system implies consent to possible monitoring or auditing."**

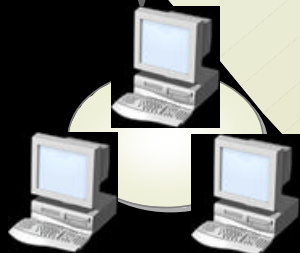
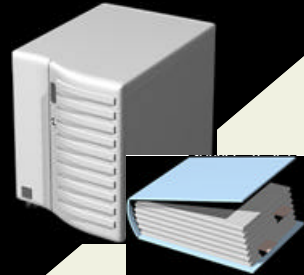
Windows 2000 Operating System Features

- Kerberos

- Secret-key protocol and distributed service, for third-party authentication
- Kerberos KDC is trusted intermediary
- Confidentiality: DES (CBC mode), ...
- Integrity: cryptographic hash algorithms
- Authentication: login password (local)
- Non-Repudiation: knowledge of password

Kerberos Specific Account Policies

- Enable “enforce user logon restrictions”
- Max lifetime for service ticket – 600 min
- Max lifetime for user ticket - 10 hrs
- Maximum lifetime for user ticket renewal – 7 days
- Maximum tolerance for computer clock synchronization – 5 min (no more)



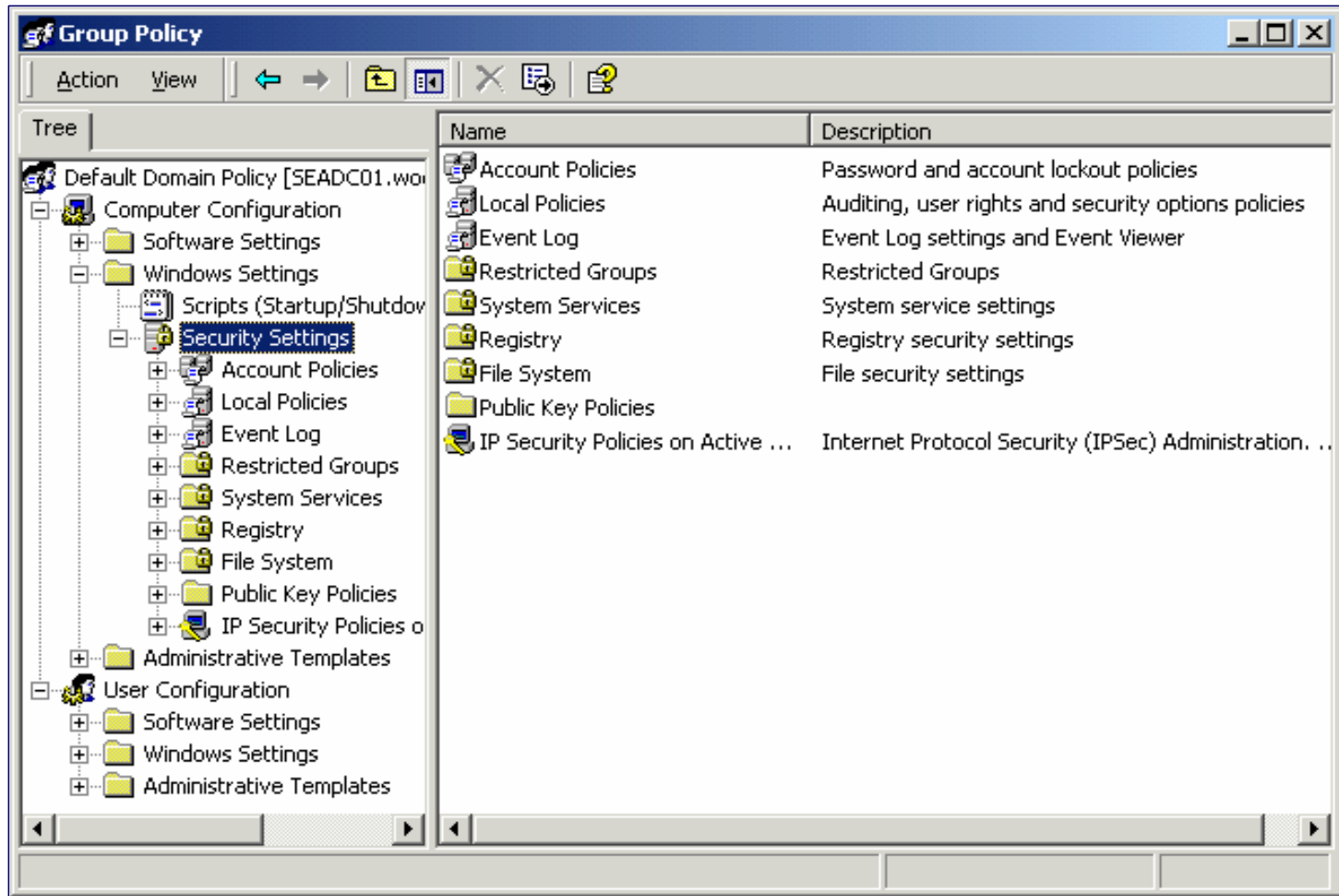
Use Security Templates for Windows 2000 and Windows XP to configure:

- Account policies
- Audit policies
- Security options
- Default service, file, and registry permissions
- Assignments of user rights
- PKI and IPSec policies
- Software restriction policies (Windows XP only)

You can deploy Security Templates by:

- Using Group Policy
- Creating scripts that use the `secdit` command line utility

Demonstration: Applying Security Templates by Using Group Policy



- <http://www.sans.org/rr/win2000/tools.php>

IIS Specifics

- A variety of services should be disabled
 - FTP, SNMP, SMTP, Indexing, Alerter, NetDDE
- Some services should be removed
 - Simple TCP/IP Services, NNTP, FPSE
- A Windows web server should always be installed unattended – IIS needs to be on a non default drive and directory
- Carefully edit HTTP Headers
- Edit ACL's on log files
- Remove IISAdmin site
- Articles: 321141

More IIS Specifics

- Edit the default error pages
- Remove sample scripts
- Remove script mappings
- Review installed ISAPI Filters
- Logon account should be machine local
- Never use IIS on a domain controller
- Never set “write” and “script execute” permissions on the same folder
- Frequently backup the Metabase
- Apply correct logon security

IIS Desirable Components/Capabilities

- SSL over port 443 with proper certificate
- Run IIS Lock Down Tool
- Extract the URL Scan tool from package
 - URLScan examines HTTP requests
 - Allows only static pages by default
- Enable W3C enhanced logging
- Plant IIS behind a firewall

Disable Posix and OS/2

- Windows session manager (SMSS.EXE) may load optional components as needed
- POSIX and OS/2
- POSIX allows for a specific delete file vulnerability when the complete path of the file is known
- MSFT Article: 101270, 320869

TCP/IP and Network Hardening

- Registry Keys (Tcpip\Parameters):
 - *SynAttackProtect*: reduces retransmission retry
 - *TcpMaxHalfOpen*: determines open port threshold
 - *TcpMaxHalfOpenRetried*: controls connections in retry state
 - *EnablePMTUDiscovery*: Attempt to determine the MTU of the sending network
 - *EnableDeadGWDetect*: Use backup gateways if primary is not responsive

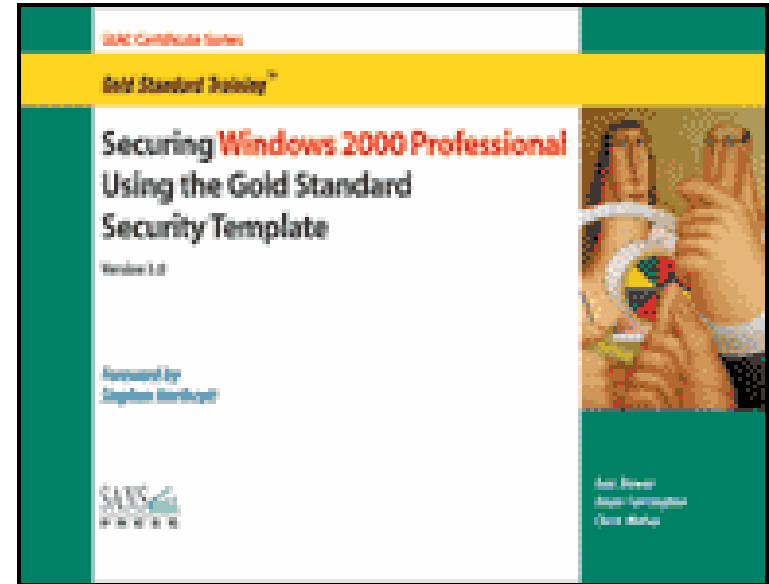
SecAdmin's Sample System

- Multiboot setup
 - P1: 2 GB FAT Windows 2000
 - Booting support only
 - P2: 8-10GB EXT3 Linux / RedHat
 - P3: 8-10GB Windows 2000/XP
- Windows Tools
- Linux Tools

Tools to Learn and Use

- Understand how to monitor the Network
 - Ethereal
 - SuperScanner 3.0
 - Nmap and nmapfe
 - IANA addresses and ports
- Everything SysInternals publishes!
- MBSA, SUS, HfNetChk
- Explore the Resource Kit

Windows 2000 Professional Gold Standard Security Template



Great place to start – but might not be the best fit for everyone.

Starting Place

- Windows 2000 Pro with SP3 installed
- NTFS formatted drives
- Tools to be demonstrated
 - SecEdit
 - Security Template MMC
 - Security Analysis MMC
 - HFNetCheck
 - CIS Scoring tool

Windows 2000 Security Templates

- Templates apply to
 - User rights assignment
 - Groups
 - Registry
 - File system settings
 - System services
 - Local security policy
 - Event Logs

The Gold Standard Template

- Developed by Industry experts
 - SANS
 - National Security Agency
 - Center for Internet Security
- Available from CIS
 - Template and PDF files
 - Level 1 and 2
 - Server and Professional

SCAT MMC Tools

- Microsoft supplied templates
 - Templates are different by OS
 - Setup – applies security settings at Windows installation time (out of the box)
 - Basic
 - Compatible – relax installed settings (?!)
 - High Security
 - Domain Controller
 - Workstation (applies to member server)
 - Gold Standard

Process Steps

- Create console
- Open a new database
- Analyze the computer
- Choose and import the template
- Apply template
- Can be applied with `secedit.exe`

Sample Microsoft Security Resources

- White Paper: Microsoft Security Response Center Security Bulletin Severity Rating System
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/rating.asp>
- "CSI/FBI Computer Crimes and Security Survey 2002," Computer Security Institute:
<http://www.gocsi.com/>
- Security information on Microsoft Products
 - <http://www.microsoft.com/technet/security>
 - <http://www.microsoft.com/security>
- Active Directory
 - <http://www.microsoft.com/ad>
- ISA Server information:
<http://www.microsoft.com/isa>
- Hacking Exposed – Network Security Secrets & Solutions, 3rd Edition; Joel Scambray, Stuart McClure, George Kurtz

Best Practice Resources and Sources

- Best Practices for Enterprise Security
 - <http://www.microsoft.com/technet/security/bpentsec.asp>
- Sources used in this presentaton
 - Tim Mullen's articles on Security Focus
<http://www.securityfocus.com/infocus/1297>
 - Services Lists
 - <http://camica.netfirms.com/services.htm>
 - http://www.pacs-portal.co.uk/startup_pages/startup_full.htm
 - Microsoft Support Base and TechNet
 - SANS GSEC and Gold Template books