Global Information Assurance Certification Paper

Hardening Windows 2000 Advanced Server for Internet Participation

Andy Brock
02/22/2001

The following paper was written to satisfy the practical requirement for the SANS GIAC Windows NT Security Administrator certification.

Introduction

The base installation of Windows 2000 Advanced Server provides a great deal of functionality and ease of use. Unfortunately when configuring a machine to interact with the Internet the more functionality an operating system allows also means a wider array of possible exploits for a malicious user. This paper describes a method for 'hardening' a base install of Windows 2000 Advanced Server for safer inter-operability with the Internet as a stand-alone machine.

The assumptions made for this document are:

- Windows 2000 Advanced Server has been installed and no further modifications have been made
- The machine is intended to function as a public part of a larger network, such as a web server or an FTP server.

1.0 Post-Installation

Network Connectivity

The machine should be configured to run as a stand-alone server; this means it is NOT a member of a Windows domain. Domain membership opens additional points of entry into the machine; it also provides for additional targets in the case your machine is compromised.

The machine should also have a static IP address. Running with a dynamic (DHCP) address not only can lead to name resolution difficulties but also adds reliance upon another machine, a DHCP server that could itself be susceptible to attack, leaving your machine unable to obtain an IP address.

Operating System Partitions

Provide a dedicated partition for all operating system files (normally C:) and a separate partition for additional applications and associated data. This is to prevent applications from (accidentally or maliciously) getting access to system files. Both partitions must be formatted as NTFS; the NTFS file system provides access control and auditing capabilities for files and directories. If Windows 2000 was installed on a FAT partition, convert to NTFS with the following command:

```
convert [drive:] /fs:ntfs
```

Operating System Updates

Upgrade to the latest service pack. Service packs are released to upgrade the functionality of the operating system and to fix bugs from previous releases. However, be sure to research all service packs before installation. For current fixes to Windows 2000, check the Microsoft site for the latest service pack. Reference the Microsoft Knowledge Base Article "How to Obtain the Latest Windows 2000 Service Pack" ID: Q260910

2.0 Account Policy

Employ the following policies to strengthen the logon security and user rights access to the Windows 2000 operating system.

Default Userids

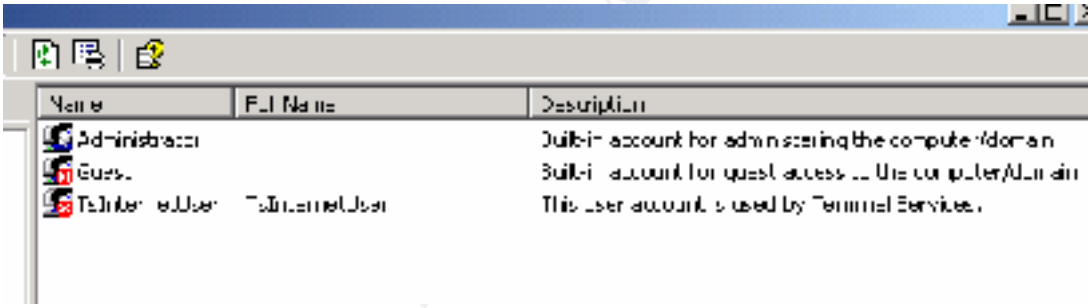
There are three userids created by the Windows 2000 system: Administrator, Guest and TSInternetUser. To modify them access the 'Local Users and Groups' snap-in from Administrative Tools >> Computer Management >> Local Users and Groups.

- Administrator
  Every Windows 2000 system has an initial account named 'Administrator'; the account should be renamed. This is to provide additional protection of Windows superuser account; if it is not readily identifiable then additional reconnaissance must be performed to discover it. In addition, a good practice is to create a personal, non-administrative account for everyday use while using the newly-renamed Administrator account only when necessary.

- Guest

The Guest account is disabled by default. When users attempt to logon to the machine with no credentials, they are granted whatever access is allowed to the Guest account. This account should be disabled to prevent users from accessing any services possible left open to Guest.

- TSInternetUser
  This account is used for Terminal Services. Terminal Services allows you to remotely execute application on the Windows 2000 server from a variety of network connections. This account should be disabled since Terminal Services will not be used.



Passwords

Access the Microsoft Management Console (MMC) 'Local Security Policy' snap-in from Administrative Tools >> Local Security Settings >> Account Policies to perform the following steps.

Password Policy

The following settings should be configured to strengthen the default password policy.

- Enforce password history: 5 passwords remembered. This ensures that passwords are not frequently reused.

- Maximum password age: 91 days. This requires users to change passwords at least every 91 days; if the password hasn't been changed, the account is locked out. This works in conjunction with the password reminder; users are reminded to change passwords after 30 days have passed, but accounts are not actually locked out until after 91 days.

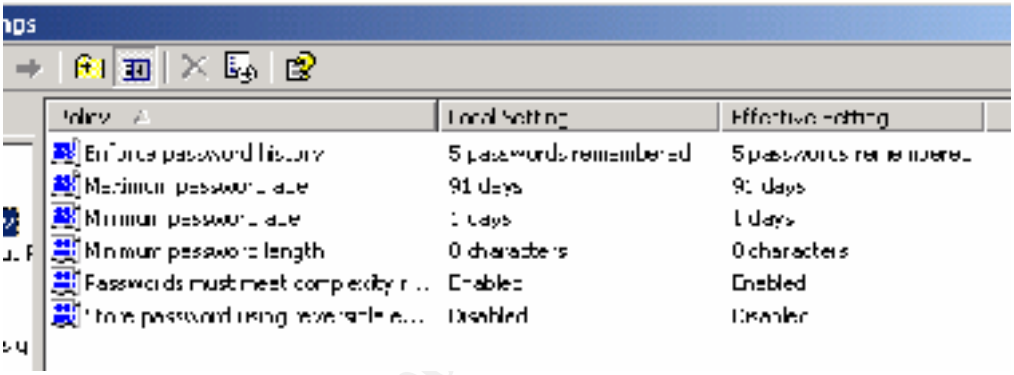
- Minimum password age: 1 day. This is to prevent the changing of passwords many times at once to bypass the password history check and arrive back at the original password.

- Minimum password length: 8 characters. Longer passwords are exponentially safer from brute force attacks than shorter ones.

- Passwords must meet complexity requirements: enabled. This requires passwords to have a mixture of upper and lower case letters and symbols or numbers.

- Store passwords using reversible encryption: disabled. Otherwise, decrypted passwords may be revealed to anyone with Administrator authority.

- Prompt user to change password before expiration: 61 days. This local policy security option, in conjunction with the password expiration local policy will promote an environment where passwords are changed every 30 days while minimizing the need for administratively resetting locked out passwords.



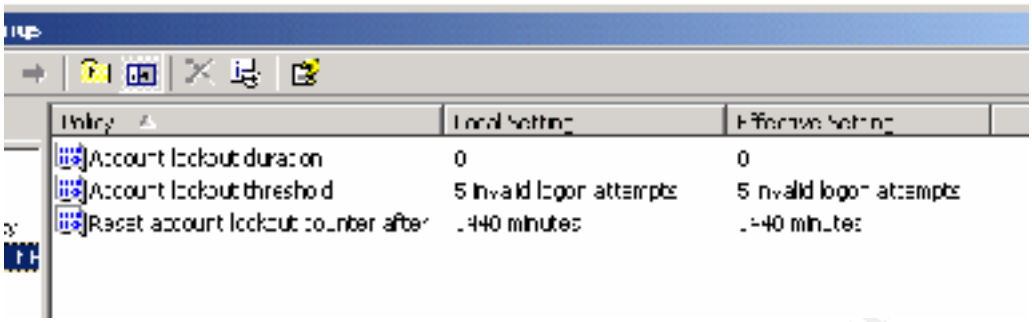
Password Lockout Policy

The following settings should be configured to enable the account lockout policy. This feature limits the ability of an unauthorized user performing "brute force" attacks against user account passwords.

- Account lockout threshold: 3 invalid logon attempts. Users are locked out after 3 bad logon attempts.

- Account lockout duration: 0. With this setting account lockout is forever; the Administrator must unlock accounts that have been locked out.

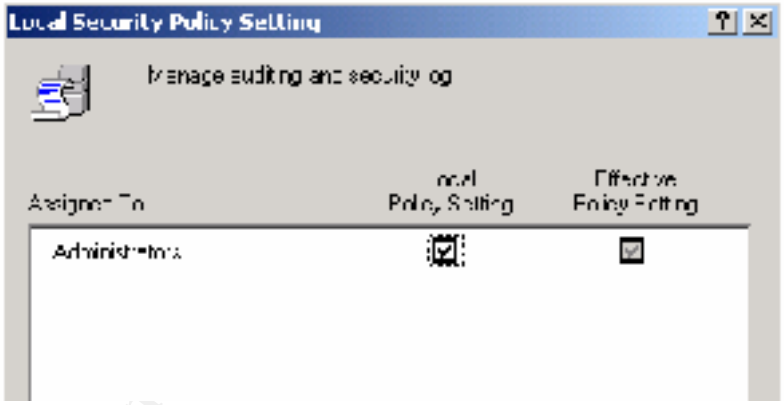
- Reset account lockout counter after: 1440 minutes. The account lockout threshold maximum is 3 bad logon attempts in a period of 1 day. This setting permits users to accidentally mis-type a password, but not hold them responsible for more than 1 day.



User Rights
Access the MMC 'Local Security Policy' snap-in to perform the following modifications:

- Shut down the system: This right should be given to the Administrators group and Power Users groups only.

- Manage auditing and security log: This right should be given to the Administrators group only. This right must be explicitly granted for managing the audit policy and security log; restricting this right to the Administrators group prevents unauthorized manipulation of Windows 2000 security logging.



3.0 File and Directory Permissions

By default, file and directory permissions on Operating System Resources (OSRs) are lax, giving the user Everyone access to virtually the entire system.

- No longer assign permissions with the Everyone group; instead use the group "Authenticated Users", as this prevents Null Session Users (users that gain access to the machine without providing credentials)

The following table lists the critical Windows 2000 system files and directories that must be protected to prevent unauthorized changes that could damage the entire operating system. Apply the following permissions by right-clicking on the file/directory, choosing "Properties" and selecting the "Security" tab.

Note: In most installations, %SystemRoot% is C:\WinNT

File and Directory OSRs	Users	Access
\	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%\system	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%\system32	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%\system32\config	Administrators System Authenticated Users	Full Control Full Control List
\%System Root%\system32\drivers	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%\system32\spool	Administrators System Authenticated Users	Full Control Full Control Read
\%System Root%\repair	Administrators	Full Control
\boot.ini	Administrators System	Full Control
\ntdetect.com	Administrators System	Full Control
\ntldr	Administrators System	Full Control
\autoexec.bat	Administrators System Authenticated Users	Full Control Full Control Read
\config.sys	Administrators System Authenticated Users	Full Control Full Control Read

4.0 Audit Policy

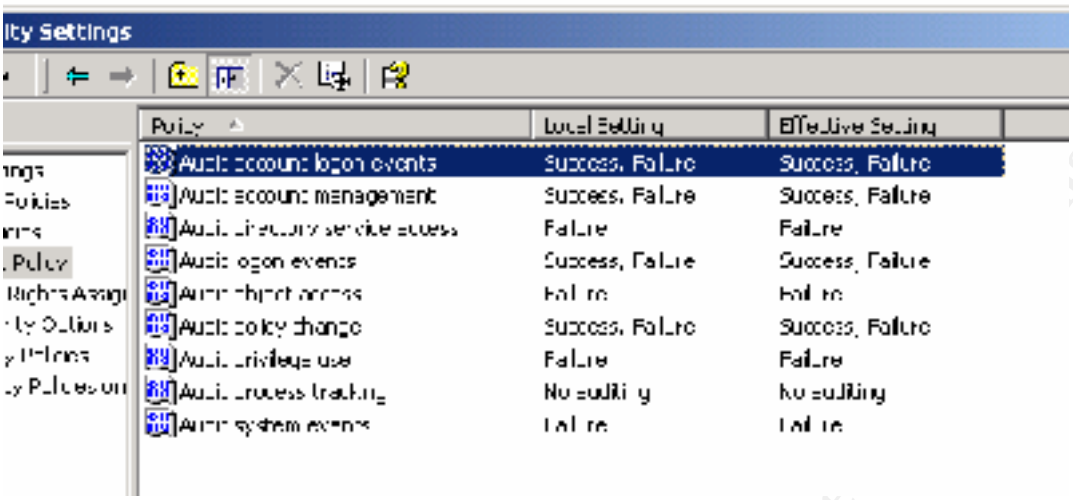
Operating system auditing is used to track selected activities of users; audited events are written to the Security Log, which can be accessed through the Event Viewer. The audit policy is the choosing of which activities the system is going to audit. The following chat explains each

activity and the recommended setting for a system in a high-risk environment such as the Internet.

Audit Policy Event	Description*	Audit Settings
Account Logon Events	These events describe both successful and unsuccessful logon attempts to a domain controller.	Success and Failure
Account Management	These events describe high-level changes to the user accounts database, such as User Created or Group Membership Change.	Success and Failure
Directory Service Access	These events describe both successful and unsuccessful accesses to objects within Active Directory	Failure
Logon Events	These events describe a single logon or logoff attempt, whether successful or unsuccessful.	Success and Failure
Object Access	These events describe both successful and unsuccessful accesses to protected objects.	Failure
Policy Change	These events describe high-level changes to the security policy database, such as assignment of privileges or logon capabilities.	Success and Failure
Privilege Use	These events describe both successful and unsuccessful attempts to use privileges. These special privileges are audited only at assignment time, not at time of use.	Failure
Process Tracking	These events provide detailed subject-tracking information. This includes information such as program activation, handle duplication, and indirect object access.	Logging not required
System Events	These events indicate something affecting the security of the entire system or audit log occurred.	Failure

*Descriptions taken from the MSDN Online Library (Reference [11])

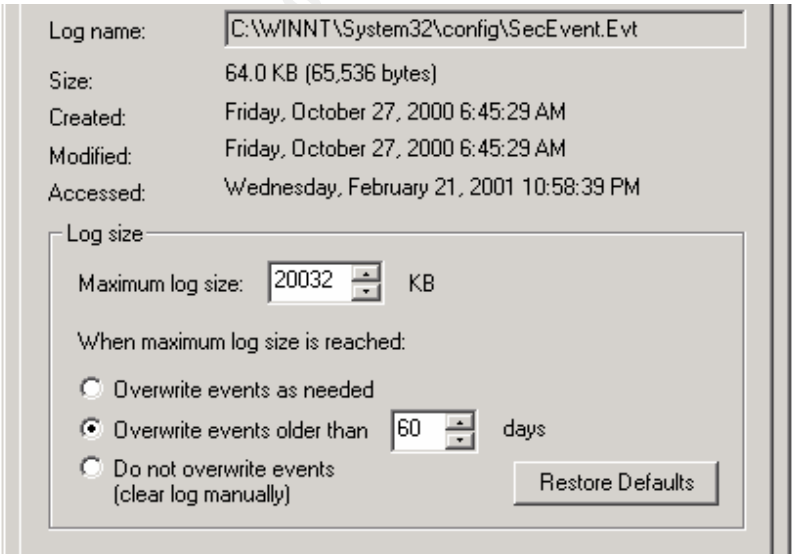
There are no events audited by default. Enable auditing by opening the Microsoft Management Console (MMC) 'Local Security Policy' snap-in, choose Local Policy >> Audit Policy and configuring each audit event type accordingly.



Event Log Settings

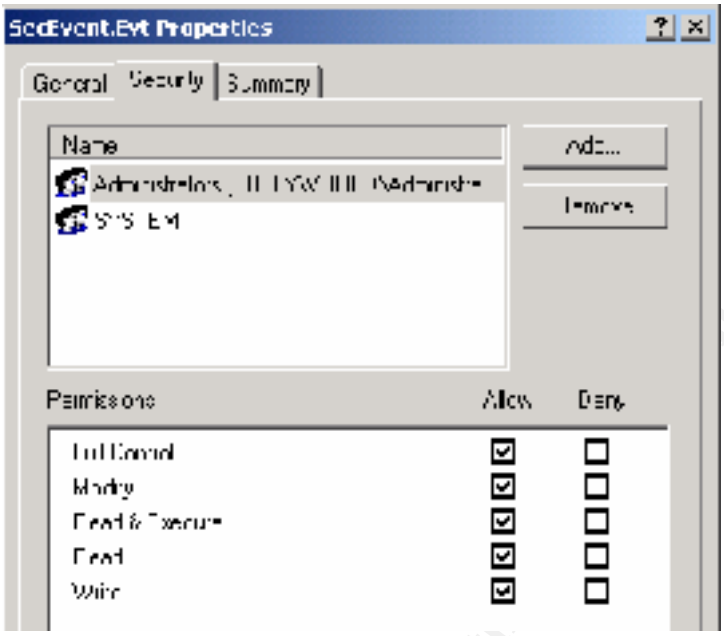
After auditing enablement, configure the Security Log for the retention of events generated from the audit policy. Open the Event Viewer, located in Administrative Tools, right-click on "Security Log" and choose "Properties". Note that the other two logs (Application and System Logs) can be configured in this same manner.

- Maximum Security Log File Size: 20032 KB. A sufficient size of the security log must be set in order to maintain the logs
- Overwrite events older than 60 days. Logs should be retained, for a current unauthorized activity could have related forensic information logged at a previous time.



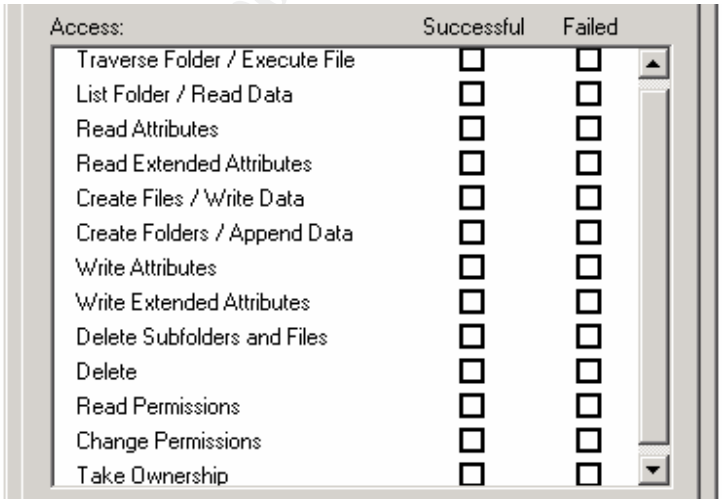
Event Log Access

The information in the Event Viewer is stored in three files (each associated with the Application, System, and Security logs) located in the \%System Root%\System32\config directory. Access to them, especially the Security Log file (SecEvent.Evt) should be restricted to the Administrators and the System groups; these logs contain information that may assist a hacker to compromise the system.

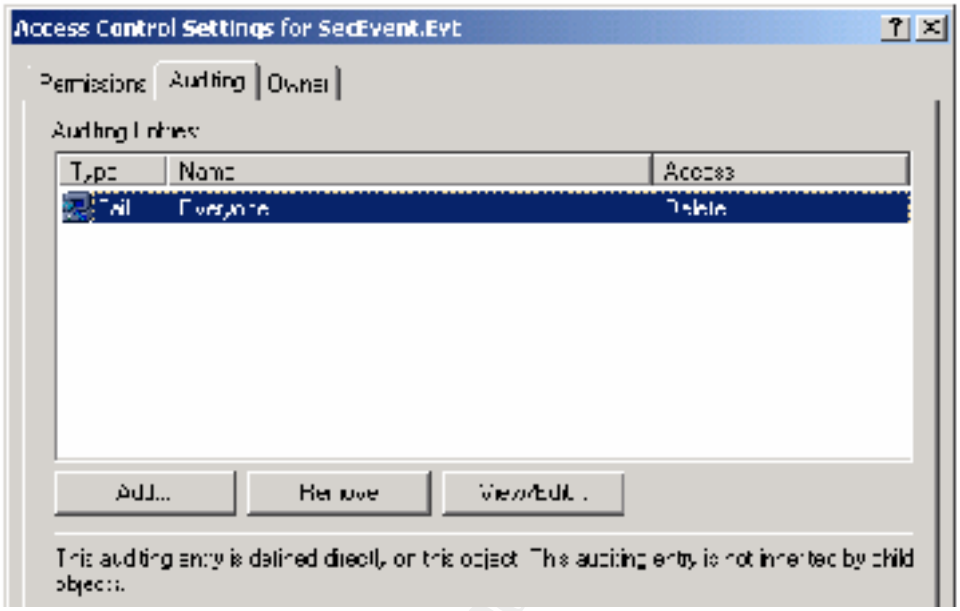


Object Access Auditing

The auditing of files is configured similarly to permissions: After enabling Object Access auditing, choose the object (a file or folder) then select the users and groups whose actions you want to audit. Choose the actions you want to audit, such as attempts to delete the selected object. The following chart describes all of the auditable characteristics of an object. Both successful and failed attempts can be audited.



Security Log Auditing
For additional Security Log protection, configure auditing on the SecEvent.Evt file so that unauthorized actions can be logged. Click the "Advanced" button on the above panel and go to the "Audit" tab.



System Utilities Auditing

Windows 2000 comes with powerful executables that can perform sensitive activities; activities that should be reserved for Administrators only. The following table lists several of these tools that should be audited upon their successful or unsuccessful execution.

\%System Root%\regedit.exe	Allows access to the Windows Registry
\%System Root%\system32\at.exe	Lists scheduled commands or schedules commands and programs to run on a computer at a specified time and date
\%System Root%\system32\ntbackup.exe	Perform Windows 2000 backup functions from the command line or a batch file.
\%System Root%\system32\runas.exe	Allows a user to run specific programs with different permissions than the user's current logon provides.
\%System Root%\system32\regedt.32.exe	Allows access to the Windows Registry
\%System Root%\system32\secedit.exe	Used to create and apply templates and analyze system security.

\%System Root%\system32\syskey.exe	Adds additional encryption to the Accounts database *(non-reversible)*

5.0 Network Application Security

When building a machine that is to be connected to the Internet, only services the machine needs to fulfill its function should be enabled. By disabling unnecessary services, you can reduce the possible exposure to attack by providing malicious users with fewer targets to exploit.

The following is a port scan of a base Windows 2000 Advanced Server installation using the popular tool Nmap:

```
----------------------
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host xx.xx.xx (xx.xx.xx.xx) appears to be up ... good.
Initiating TCP connect() scan against xx.xx.xx (xx.xx.xx.xx)
Adding TCP port 445 (state open).
Adding TCP port 3389 (state open).
Adding TCP port 13 (state open).
Adding TCP port 9 (state open).
Adding TCP port 53 (state open).
Adding TCP port 139 (state open).
Adding TCP port 19 (state open).
Adding TCP port 1030 (state open).
Adding TCP port 7 (state open).
Adding TCP port 42 (state open).
Adding TCP port 135 (state open).
Adding TCP port 17 (state open).
Adding TCP port 1025 (state open).
The TCP connect scan took 2 seconds to scan 1541 ports.
Initiating FIN,NULL, UDP, or Xmas stealth scan against xx.xx.xx(xx.xx.xx.xx)
The UDP or stealth FIN/NULL/XMAS scan took 10 seconds to scan 1541 ports.
For OSScan assuming that port 7 is open and port 1 is closed and neither are
firewalled
Interesting ports on xx.xx.xx(xx.xx.xx.xx) :
(The 3049 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
7/udp      open        echo
9/tcp      open        discard
9/udp      open        discard
13/tcp     open        daytime
13/udp     open        daytime
17/tcp     open        qotd
17/udp     open        qotd
19/tcp     open        chargen
19/udp     open        chargen
42/tcp     open        nameserver
42/udp     open        nameserver
53/tcp     open        domain
53/udp     open        domain
67/udp     open        bootps
68/udp     open        bootpc
135/tcp    open        loc-srv
135/udp    open        loc-srv
```

```
137/udp    open         netbios-ns
138/udp    open         netbios-dgm
139/tcp    open         netbios-ssn
161/udp    open         snmp
445/tcp    open         microsoft-ds
445/udp    open         microsoft-ds
500/udp    open         isakmp
1025/tcp   open         listen
1030/tcp   open         iad1
1032/udp   open         iad3
1645/udp   open         radius
1646/udp   open         radacct
1812/udp   open         radius
1813/udp   open         radacct
3389/tcp   open         msrdp

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

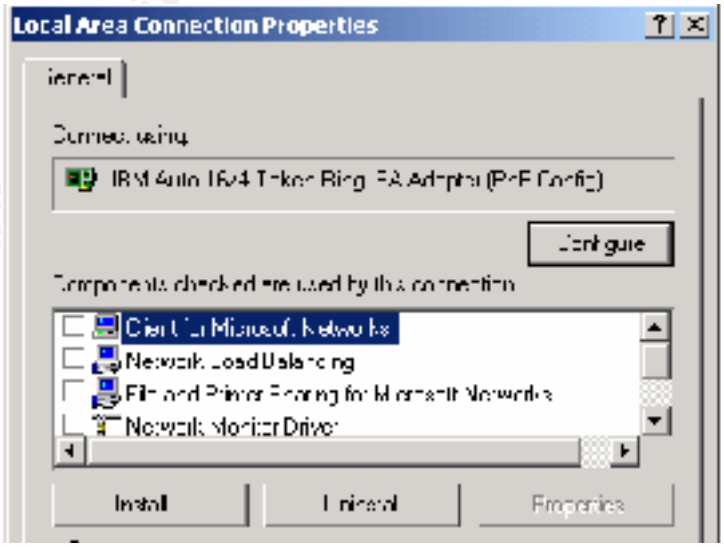
All of these services are by default enabled. The vast majority of these services are not required and should be disabled.

Note: A listing of common Windows services and their associated port assignments can be found here: http://microsoft.com/windows2000/library/resources/reskit/samplechapters/cnfc/cnfc_por_simw.asp

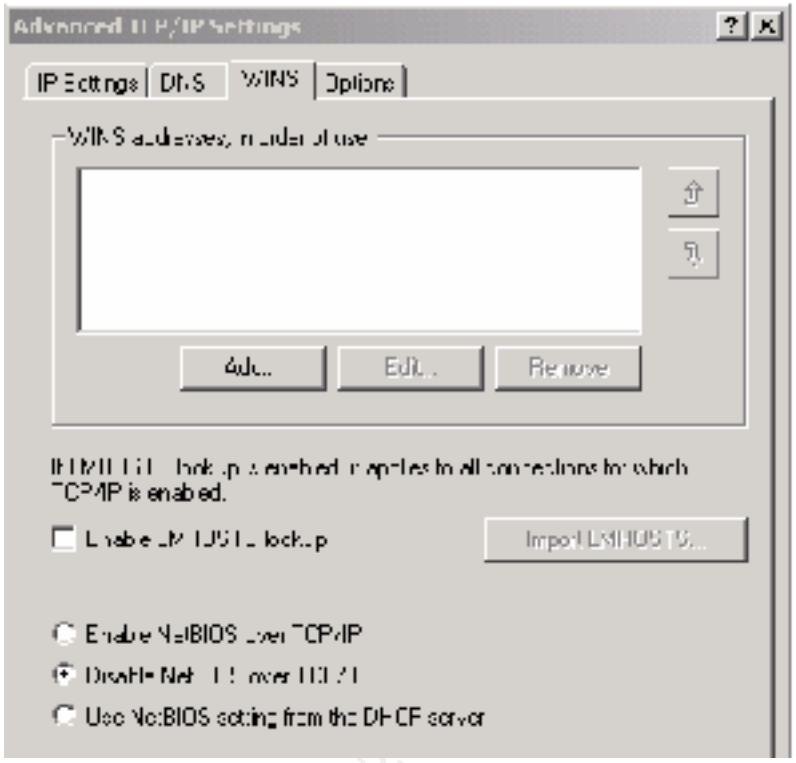
Perform the following steps to disable unneeded networking services:

1. From the Start Menu, choose Settings >> Network and Dial-up Connections. Right click on the proper connection and choose "Properties". As illustrated in the following graphic, disable the following Microsoft Networking components:

- Client for Microsoft Networks - this component allows your machine to access other resources on a Microsoft network
- File and Printer Sharing for Microsoft Networks - this component allows other computers to access resources on your computer using a Microsoft network



2. Next from the component list select “Internet Protocol (TCP/IP)”, click “Advanced”, select the “WINS” tab. On the resulting screen select the radio button “Disable NetBIOS over TCP/IP”.



3. Disable all of the unneeded services. Go to Administrative >> Services. For the following services, stop them and set them to manual to prevent restart upon a reboot. As a baseline measurement, Microsoft’s IIS generally does not require these services.

- Alerter
- Clipbook Server
- Computer Browser
- DHCP Client
- DHCP Server
- DNS Server
- Net Logon
- Network DDE
- Network DDE DSDM
- Print Spooler
- SNMP
- Terminal Services
- WINS
- Internet Authentication Service
- TCP/IP NetBIOS Helper Service
- Simple TCP/IP Services

After performing these fixes, a new scan of the machine reveals far fewer available services:

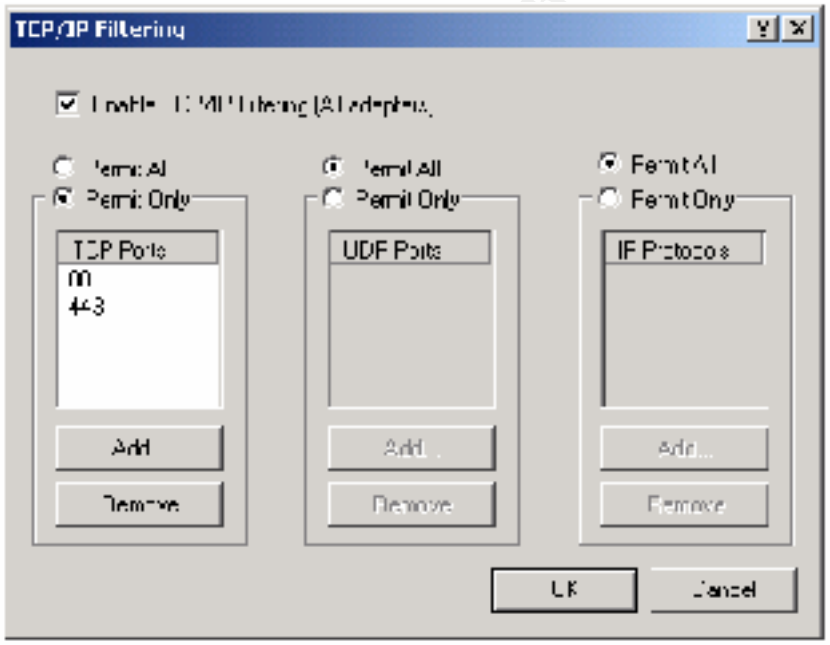
```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host xx.xx.xx(xx.xx.xx.xx) appears to be up ... Good.
Initiating TCP connect() scan against xx.xx.xx(xx.xx.xx.xx)
Adding TCP port 135 (state open).
Adding TCP port 1025 (state open).
The TCP connect scan took 2 seconds to scan 1541 ports.
Initiating FIN,NULL, UDP, or Xmas stealth scan against xx.xx.xx(xx.xx.xx.xx)
The UDP or stealth FIN/NULL/XMAS scan took 5 seconds to scan 1541 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither
are firewalled
Interesting ports on xx.xx.xx(xx.xx.xx.xx):
(The 3072 ports scanned but not shown below are in state: closed)
```

```
Port        State       Service
135/tcp     open        loc-srv
135/udp     open        loc-srv
500/udp     open        isakmp
1025/tcp    open        listen

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
-----------------------------------------------
```

- Apply the 'Minimalist Philosophy': systems should only run services or daemons that are absolutely necessary for the function and maintenance of the machine.

Port Filtering
A built-in security feature of the Windows 2000 operating system is port filtering. Set the proper TCP port, UDP port or IP protocol to allow at Network and Dial-up Connections >> Connection Name Properties >> Internet Protocol (TCP/IP) Properties >> Advanced >> Options >> TCP/IP filtering. This function will apply inbound filters for the chosen interface, so care must be taken not to inhibit functionality by disabling the wrong traffic.



A different approach to filtering traffic is to implement a firewall, either host-based or network-based. A firewall will block any access attempt to unauthorized ports so that only traffic destined for proper ports are allowed. Two well-known host-based firewalls are ZoneAlarm (http://www.zonelabs.com) and BlackICE (http://www.networkice.com).

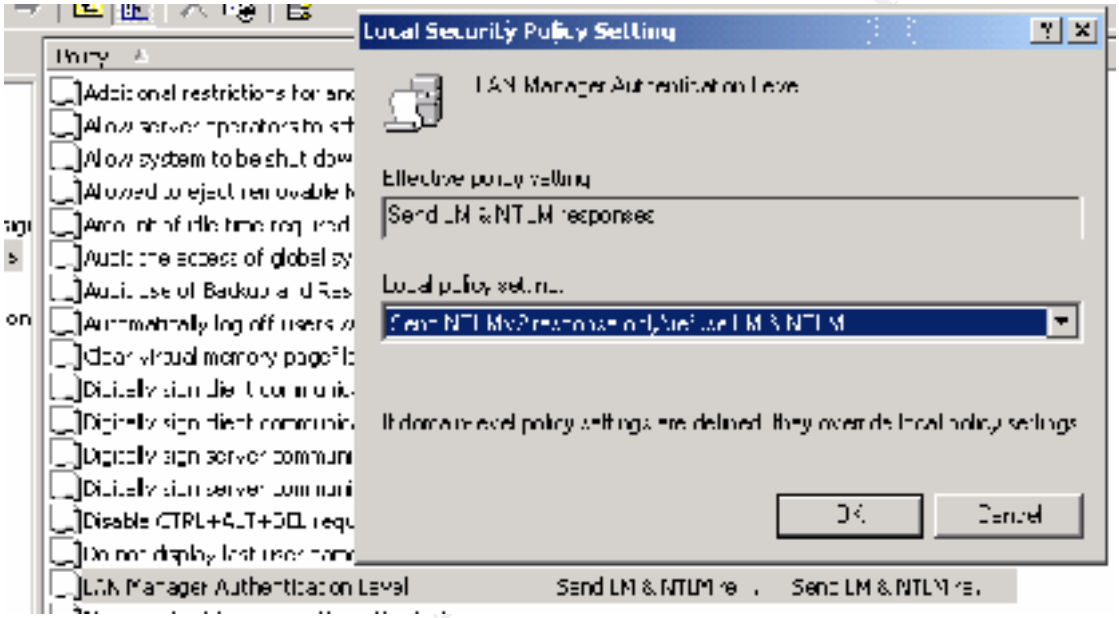
6.0 Security Settings

Additional security features of the Windows 2000 platform can be activated via the Microsoft Management Console (MMC) 'Local Security Policy' snap-in and through the creation and manipulation of registry keys within the Windows registry.

Security Options
The MMC 'Local Security Policy' snap-in to perform the following steps.

- Disable LanMan/NTLM authentication: By disabling the weaker challenge/response protocols in favor of the stronger NTLMv2 protocol, passwords are much more adverse to brute force attacks (e.g. L0phtcrack).

Policy:	Lan Manager Authentication Level
Local Policy Setting:	Send NTLMv2 responses only/refuse LM & NTLM



- Display Legal Use Notice (1 of 2): This setting enables a dialog box to appear before a user logs into the Windows 2000 machine and provides the dialog box with a title. This could be necessary for alerting unauthorized users that they should not be accessing the machine and can be held liable for damages.

Policy:	Message title for users attempting to log on
Local Policy Setting:	Warning!

- Display Legal Use Notice (2 of 2): This setting provides the text for the Business Use Notice dialog box.

Policy:	Message text for users attempting to log on
Local Policy Setting:	Unauthorized use of this machine is prohibited.

- Hide last logon user name: This setting prevents an unauthorized user from obtaining a valid account name at a logon prompt.

Policy:	Do not display last user name in logon screen

Local Policy Setting:	Enabled

- Clear the Windows 2000 pagefile at shutdown: Some applications may store sensitive, unencrypted information in the paging file, which may be susceptible to attack.

Policy:	Clear virtual memory pagefile when system shuts down
Local Policy Setting:	Enabled

Registry Options
Use the Registry Editor (Regedt32.exe) to perform the following steps.
Warning: Improper modification of the registry can cause serious problems that may result in the need to reinstall the operating system. Perform ONLY the modifications described.

- Disable automatic administrative shares: Because all default installations have these shares, it is best to disable them so as to reduce the number of known targets for a malicious user. These hidden shares with their associated paths are:

  C$, D$ The root of each partition
  ADMIN$ %System Root%
  IPC$ Temporary connections between servers
  PRINT$ %System Root%\System32\Spool\Drivers

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\LanmanServer\Parameters
Name:	AutoShareServer
Type:	REG_DWORD
Value:	0

- Crash on Audit Fail: With the current audit policy of retaining audit logs for 60 days, there is a possibility that the maximum log size is reached before then. If that happens then additional events are not logged. For a machine in a high-risk environment, this is not desired; Windows 2000 has a feature that will cause the machine to shut down if logging can no longer occur. If the following key does not exist, then create it.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Value:	1

If the machine shuts down as a result of this setting, the registry value will be set to '2' upon restart, meaning that only an Administrator can logon. Once the Administrator backs up and clears the filled log, they must reset the CrashOnAuditFail value to '1'.

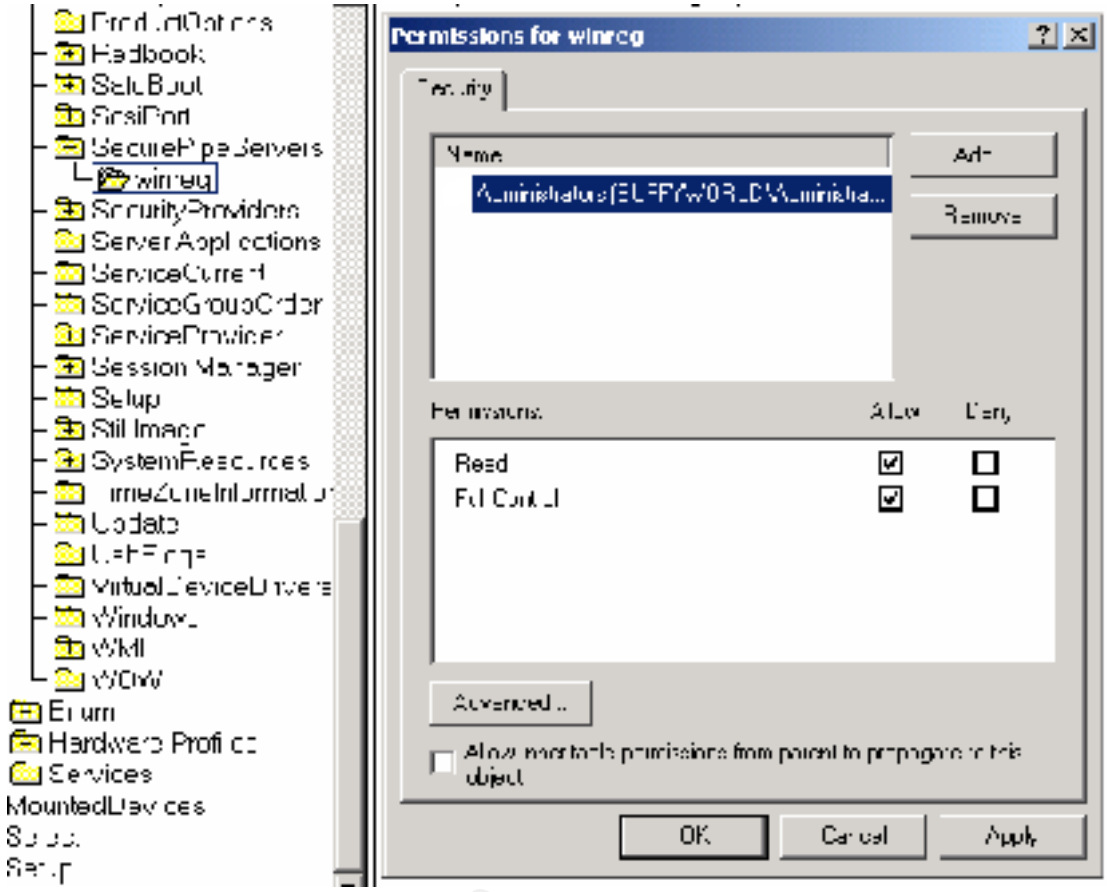
- Syn Flood Attack Protection: Even with closing down all unneeded network ports, there is still methods of attack against those ports that are still open. One such attack is a Syn Flood:

a Denial of Service (DoS) attack in which a Syn packet is sent to the target machine, ostensibly to begin the TCP "3-way handshake" and causing the target machine to set aside an amount of machine resources for a specific amount of time to handle the connection. However, the handshake never completes, instead the source machine send hundreds more Syn packets forcing the target to set aside more and more resources until the machine has no resources left, causing an unstable state and possibly even a crash. By setting the following key, the time machine resources are reserved for the completion of the 3-way handshake is reduced.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	SynAttackProtect
Type:	REG_DWORD
Value:	2

- Limit remote registry access: Modifying the following key will prevent remote access into the Windows registry. Remote access must be limited so unauthorized users cannot manipulate the registry, such as adding registry entries that execute programs at boot time. Ensure that only the Administrators group and System group has Security Permission:Full Control over this key.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\SecurePipeServers
Name:	Winreg



- Limit Scheduler list access: The Scheduler service in Windows 2000 allows for commands to be executed at a defined time. Commands executed with the Scheduler run under the System account and have complete authority over the operating system. By default, only Administrators and Power Users have the ability to schedule jobs, but if an unauthorized user can list the scheduled jobs, they might possibly replace one of the jobs with a Trojan that can run malicious code with no limitations. Modifying the permissions of the following registry prevent unauthorized users to view scheduled jobs. Ensure that only the Administrators group and System group has Security Permission:Full Control over this key.

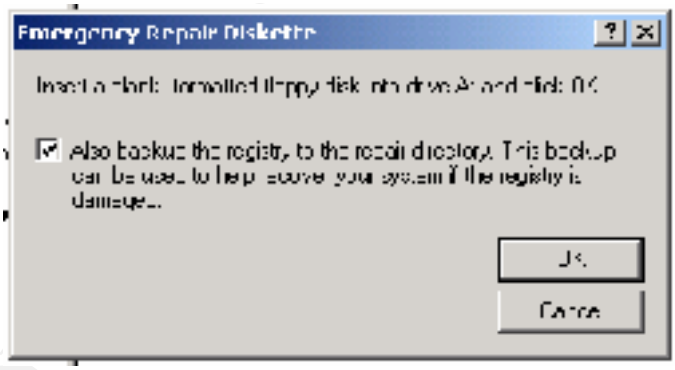
Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services
Name:	Schedule

8.0 Emergency Repair Disk

Once system configuration is complete, it is wise to make an Emergency Repair Disk (ERD). The ERD contains information about the registry, system files, partition boot sector, and the startup environment; it can be used to repair your machine if the system will not start or if system files have been damaged or erased.

To create an ERD, insert a blank 3½" floppy disk into the server and go to the Start Menu >> Programs >> Accessories >> System Tools >> Backup.

Choose the "Emergency Repair Disk" Option. The resulting screen should present an option to backup the registry. Select this option.



The files created by this process are:
Emergency Repair Disk:

- setup.log
- config.nt
- autoexec.nt

\%System Root%\repair\RegBack directory:

- default
- NTUSER.DAT
- SAM
- SECURITY

software
system
UsrClass.dat

- Verify that the permissions set on the RegBack directory are Full Control for Administrators *only* as a copy of the Accounts database is stored there and is a prime target for malicious users.
- Lock the ERD away in a secure place.

If the need arises to repair your operating system, you must have the original Windows 2000 installation cd.
1) Insert the cd and boot to the Windows 2000 Setup program
2) Follow the prompts until Setup asks if you want to repair or recover.
3) Choose the Emergency Repair Process.
4) Choose a "Fast Repair" and insert the ERD when prompted. Files will be copied back to the hard disk from both the Windows 2000 Server cd and the \%System Root%\repair\RegBack directory.
5) Follow the prompts until told to reboot.
6) If the repair process completes properly and the machine reboots, then the repair was a success.

9.0 Continuing Protection

All of the configurations to this point have strengthened Windows 2000 a piece at a time into a secure system. The next step is to add monitoring software for real-time protection of the operating system.

AntiVirus Monitoring
It should be considered *mandatory* for any machine running any Windows operating system to be scanned and protected by an antivirus product. Modern antivirus software not only scan for virii but other malicious code as well, such as BackOrifice. Two popular products are Norton AntiVirus (http://www.symantec.com) and McAfee AntiVirus (http://www.mcafee.com).

Host-Based Intrusion Detection
Programs are available for real-time analysis of Event Log entries, automating the task of searching through them looking for suspicious entries. These programs can also allow for storage of the Event Log data on a remote machine, freeing hard drive space and eliminating the danger of log tampering.

Startup Programs
There are a number of registry keys and files that can automatically (and silently) launch programs when the machine boots. The following operating system locations should be checked at regular intervals for unauthorized and/or suspicious entries.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce\
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
%systemroot%\win.ini
%systemroot%\Profiles\All Users\Start Menu\Programs\Startup
%systemroot%\Profiles\Administrator\Start Menu\Programs\Startup

- For greater protection of these keys, assign the Administrators group and System group Security Permission:Full Control over each.

A tool that provides a graphical listing of these locations and simplifies the verification procedure is called Autoruns. It can be downloaded at
http://www.sysinternals.com/files/autoruns.zip

Mailing Lists
Stay informed of the latest security developments. This allows you to quickly react to the constantly arising exploits of Windows 2000 and networking in general. Several prominent lists are :
Microsoft (http://www.microsoft.com/security)
NTBugtraq (http://www.ntbugtraq.com)
Security Focus (http://www.securityfocus.com)

References

[1] Fossen, Jason. *Windows NT Security: Step by Step*. The SANS Institute GIAC Training, 2000

[2] Fossen, Jason. *Internet Information Server for Windows 2000 Parts 1 and 2*. The SANS Institute GIAC Training, 2000

[3] Farrington, Dean. "Windows NT Web Server Auditing" SANS GIAC website, 2000

[4] "How to Disable LM Authentication on Windows NT" Microsoft Knowledge Base Article ID: Q147706

[5] "How to Obtain the Latest Windows 2000 Service Pack" Microsoft Knowledge Base Article ID: Q260910

[6] "How to Clear the Windows NT Paging File at Shutdown" Microsoft Knowledge Base Article ID: Q182086

[7] "How to Restrict Access to NT Registry from a Remote Computer" Microsoft Knowledge Base Article ID: Q153183

[8] "Exploring Terminal Services" http://www.microsoft.com/windows2000/guide/server/features/terminalsvcs.asp

[9] Page, Jeremy. "Securing Windows 2000: First Steps Ars Technica" http://arstehnica.com/tweak/win2k/security/begin-1.html

[10] "Windows 2000 Installation Security Checklist" htttp://www.labmice.net/articles/securingwin2000.htm

[11] "Auditing Security Events" MSDN Online Library http://msdn.microsoft.com/library/default.asp?URL=/library/winresource/dnwinnt/s8328.htm

[12] "Security Considerations for Network Attacks" Microsoft TechNet, http://www.microsoft.com/TechNet/security/dosrv.asp

[13] "Windows NT Security Step by Step Version 2.15" The SANS Institute, 1999

[14] Saddique, Mohammed "Server Security for a Domino Server" SANS GIAC website, 2000

Last Updated: July 20th, 2017

Upcoming Training

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**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**