Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Basic Steps to Hardening a Standalone Windows 2000 Installation

There are many tools in Windows 2000 (at least relative to Windows NT) that make the job of securing the operating system easier. It is important to learn these tools. New exploits will require responses; these tools will help you respond.

Copyright SANS Institute
Author Retains Full Rights

AD

Basic steps to hardening a standalone Windows 2000 installation
Todd Anderson

The first consideration in a Windows 2000 installation is to define the purpose of the installation. One would set up a home machine very differently from one set up as a web server. Generally, it is a good idea to limit the roles any given machine will play, especially when connecting a machine directly to the internet, where every port you open or service you enable creates a potential security hole.

Installation of Windows 2000

There are a few security options that can be addressed while installing the operating system. If you are not using a script or performing an unattended installation, and have no need of a network connection, disconnect the machine until a strong administrator password has been set, service packs have been installed and necessary hot fixes applied.

File System Security

Be sure to format all partitions as NTFS, including the system partition. Windows 2000 runs best on an NTFS partition. Many of the features of Windows 2000 - resistance to fragmentation, file and folder level access rights, encrypted file systems, distributed file systems - can only be leveraged using the NTFS file system.

NTFS includes the use of encrypted file systems (EFS).[1] EFS is a capability, integrated into Windows 2000, which allows users to transparently encrypt files. Those needing to store sensitive data on a Windows 2000 machine should consider using EFS to add an extra layer of defense to protect their data.

The decision to implement EFS, however, should not be taken lightly, especially on a standalone machine. When encrypting files it is important to use a strong password and even more important not to forget it. If a user encrypts a folder and that user's account is deleted, the folder cannot be unencrypted because the user's key will no longer exist. Normally, the administrator could reset the user's password and then login to recover the encrypted files. This will not work if the account has been deleted[2].

More information can be found on EFS can be found at

http://www.infosecuritymag.com/articles/february01/features_applied_crypto.shtml

and

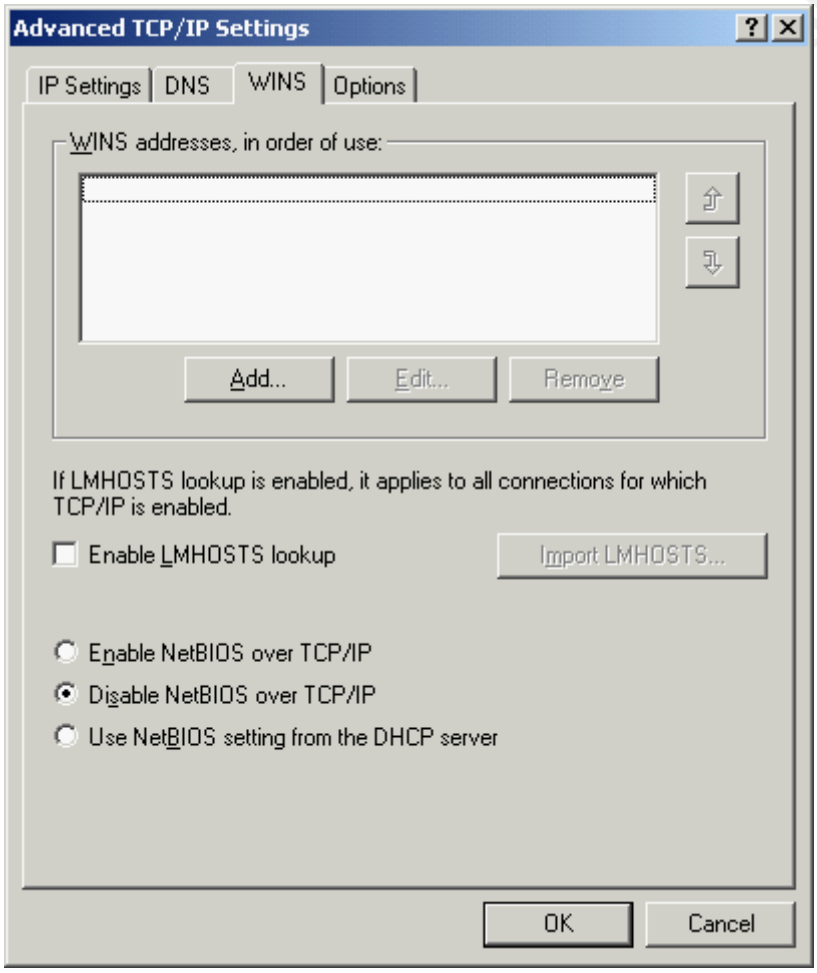
http://www.microsoft.com/windows2000/library/planning/security/efssteps.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Protocol Configuration

The next option during setup is the configuration of protocols. Use only what you need to get the job done. If you don't need Client for Microsoft Networks or File and Print Sharing for Microsoft Networks, it is best not to install them. If you need to have the Microsoft client installed or file and print sharing enabled, you will need more than a hardened workstation to protect you data, you will need a secure network infrastructure, including a firewall.

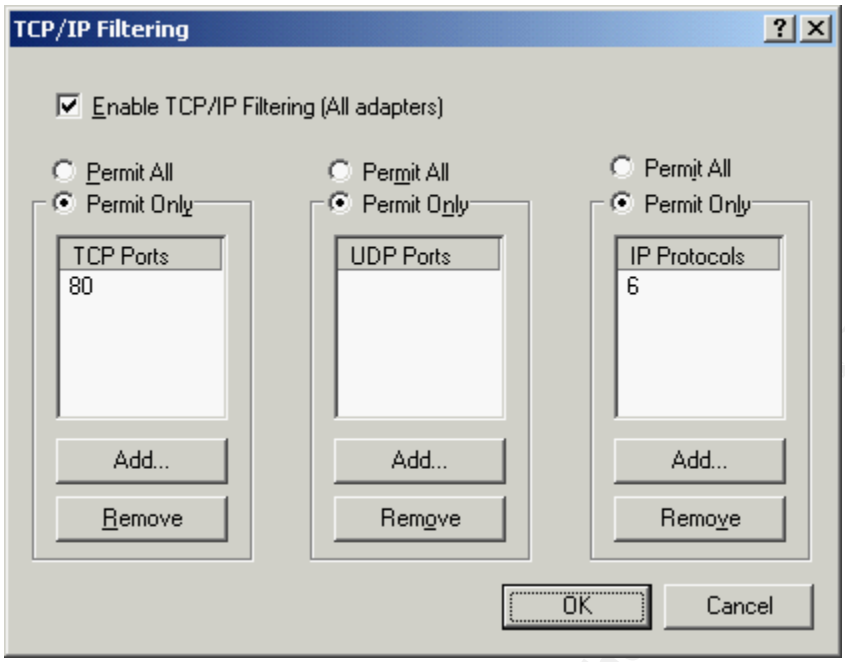
Configure the advanced TCP/IP options[3]. On the WINS tab, uncheck "Enable LMHOSTS lookup" and check Disable NetBIOS over TCP/IP.



On the TCP/IP options tab, select TCP/IP filtering. By enabling filtering you can prevent many incoming connections while, at the same time, allowing outgoing and established connections to work normally. If your machine is a single purpose machine, configure the protocols you want to allow in. In the example below TCP is IP protocol[4] as defined in the IP protocol header and TCP port 80 is http. This configuration would allow

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

incoming connections to a web server. These settings will prevent remote administration capabilities if not configured correctly, creating a Denial of Service on yourself.



This should not be the only line of defense. Defense in Depth is the goal. Make your box more work than it is worth to break into.

Whether you are configuring a home machine or a web server, a virus scanner and some type of firewall are essential tools. It is important to regularly update virus definition files. Keep your OS patches current. Many patches fix known exploits and vulnerabilities.

Post Windows 2000 Installation

After Windows reboots, there is plenty more to configure. As with Windows NT, in order to properly configure or harden your system, you must at some point edit the registry (obligatory note to back up registry first). However, many of the registry changes that need to be made can be done with security policies.

Security Configuration Tools

Many services can be configured using the System Security Toolbox[5]. These security snap-ins can assist configuring and hardening your Windows 2000 machine. On a local or standalone machine the group policy snap-in or gpedit.msc allows you to view or edit the policy on the machine.

Using the Security Configuration and Analysis tool and the Security Template tool, which are snap-ins in the Microsoft Management Console (MMC), you can centrally

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

manage the local computer policy and avoid making many of the direct registry modification that were required when hardening Windows NT.

As described in other GSEC papers[6, 7], the templates allow you to configure make templates for many of the Windows settings. The settings allow you to manage account and local policies, restrict groups, control registry and file system access, and manage system services. Security templates are stored as text based .inf files in SystemRoot\Security\Templates by default. The template files can either be edited manually using a text editor such as notepad or using the Security Template tool. You must be an administrator to create save or implement security policies.

With the system policy you can create a template for the security policy of the machine. Creating a template is beneficial. First, it creates a file that can be easily transferred to another machine where the same configuration is desirable. Second, by creating a security template, you create an auditing tool. By analyzing the current configurations against the configuration of the template, you can determine if the computer policy has been altered.

Many of the settings in these policies are undefined, even in the high security policies. Taking the time to go through these and create a good template is worth the time and effort. Each section of the policy template has settings that are important. There are too many to go over here in detail, but a good resource is the Windows 2000 Security Handbook[3]

To use the security configuration tools, create a custom Microsoft Management Console (mmc from the command line). Add the Security Configuration and Analysis tool, and the Security Template tool. Follow these steps:

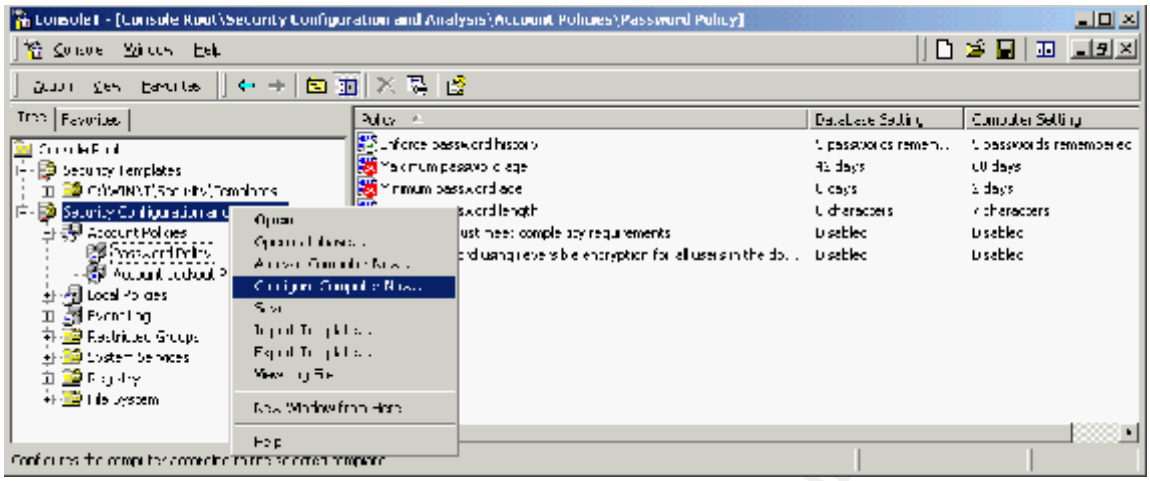
Create a template or use a pre-configured template from one of the Security Templates.

Create a new database
Right click on the Security Configuration and Analysis snap-in and select **Open Database…**. Type in the name of the database you are going to create. Next you need to choose the template file (*.inf).

At this point you have two options you can either analyze or apply the policy file. If you choose to analyze the computer you can then view and edit the results. Discrepancies between the system and the template are highlighted with a red flag. Consistencies are highlighted with a green check mark. The security setting is not specified in the database if there is no flag or check mark.

Once the configuration is defined as you like it you can apply the policy using the **Configure Computer Now…** option of Security Configuration and Analysis tool.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



It may seem easier to just edit the local security settings in the Administrative Tools section of the Control Panel or by using gpedit.msc. While this is true for a single machine, if you have to edit multiple machines and desire to check them occasionally to make sure that settings have not been modified, use a policy.

These tasks can be automated even further through the use of the secedit.exe command. Secedit.exe is a command line version of the security configuration and analysis snap-in.

secedit /configure [/**DB** *filename*] [/**CFG** *filename*] [/**overwrite**][/**areas** *area1 area2*...] [/**log** *logpath*] [/**verbose**] [/**quiet**]

Configure the machine with the least amount of privilege to serve its function. This includes logons, services, and protocols. Audit the machine, using event logging to monitor the system. It may be worth using Tripwire to check file integrity for critical machines.

There are many tools in Windows 2000 (at least relative to Windows NT) that make the job of securing the operating system easier. It is important to learn these tools. New exploits will require responses; these tools will help you respond.

Security Configuration Tool Set

[1] "Step by step guide to Encrypting File System (EFS)" 7 March, 2000 URL: http://www.microsoft.com/windows2000/library/planning/security/efssteps.asp

[2] Bragg, Roberta "Applied Cryptography, Hardening EFS" February 20001 Information Security Magazine URL: http://www.infosecuritymag.com/articles/february01/features_applied_crypto.shtml

[3] Cox, Philip. Windows 2000 Security Handbook. Berkeley: Osborne / McGraw Hill, 2001. Chapter 10

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[4] Stevens, W. Richard. TCP/IP Illustrated Volume 1. Reading: Addison Wesley, 1994. 10

[5] "Step-by-Step Guide to Using the Security Configuration Tool Set" 16 February, 2000 http://www.microsoft.com/windows2000/library/planning/security/secconfsteps.asp

GSEC Papers

[6] Brill, Jeffrey "Windows 2000 Template Security Implications" May 2, 2000 URL: http://www.sans.org/infosecFAQ/win2000/template.htm

[7] Scannella, Carlo "Implementing Password Controls and Account Policies Using Windows 2000" February 15, 2000 URL: http://www.sans.org/infosecFAQ/win2000/group_policy.htm

© SANS Institute 2003, Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced