



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Todd Anderson

Basic steps to hardening a standalone Windows 2000 installation

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 deleted².

More information can be found on EFS can be found at

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

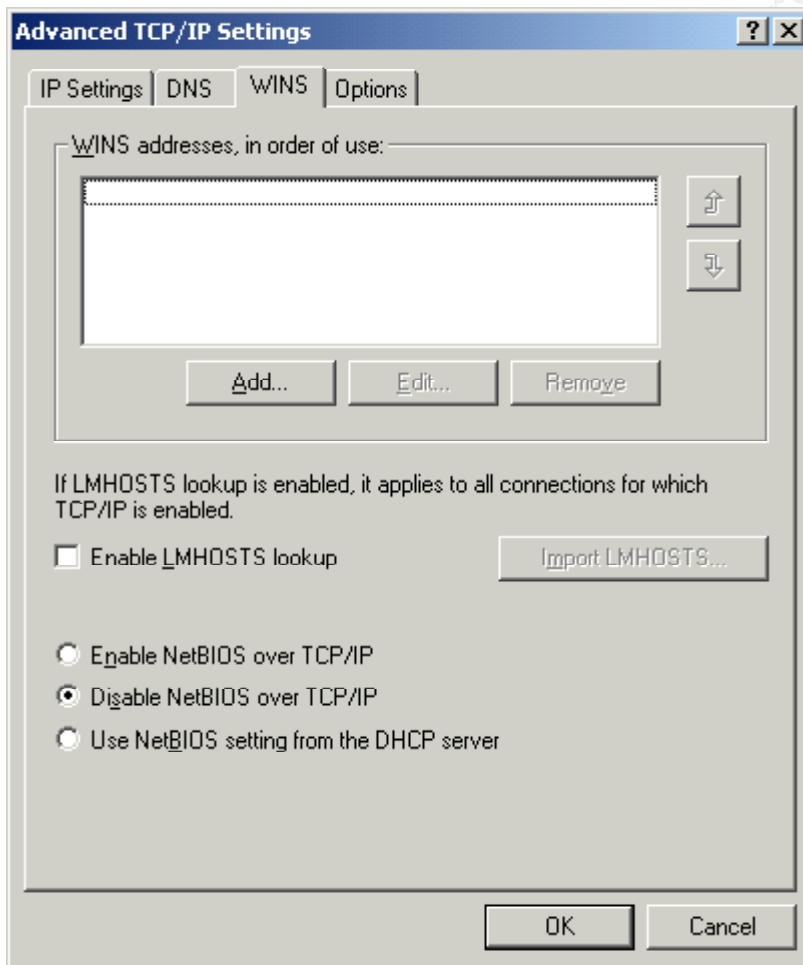
and

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

Protocol Configuration

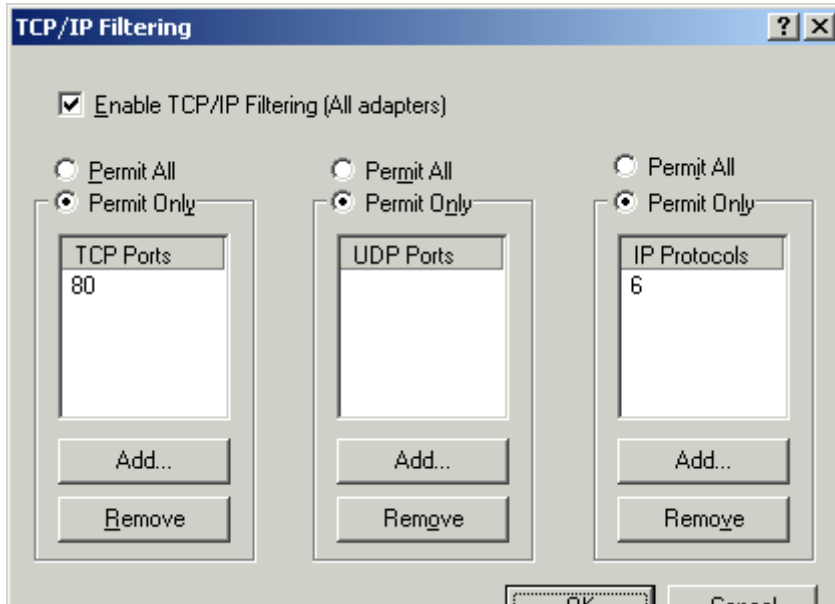
The next option during setup is the configuration of protocols. Use only what you need to get the job done. If you don't need Client for Microsoft Networks or File and Print Sharing for Microsoft Networks, it is best not to install them. If you need to have the Microsoft client installed or file and 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 options³. 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 protocol⁴ as defined in the IP protocol header and TCP port 80 is http. This configuration would allow incoming connections to a web server. These settings will prevent remote administration capabilities if not configured correctly, creating a Denial of Service on yourself.



Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event