



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

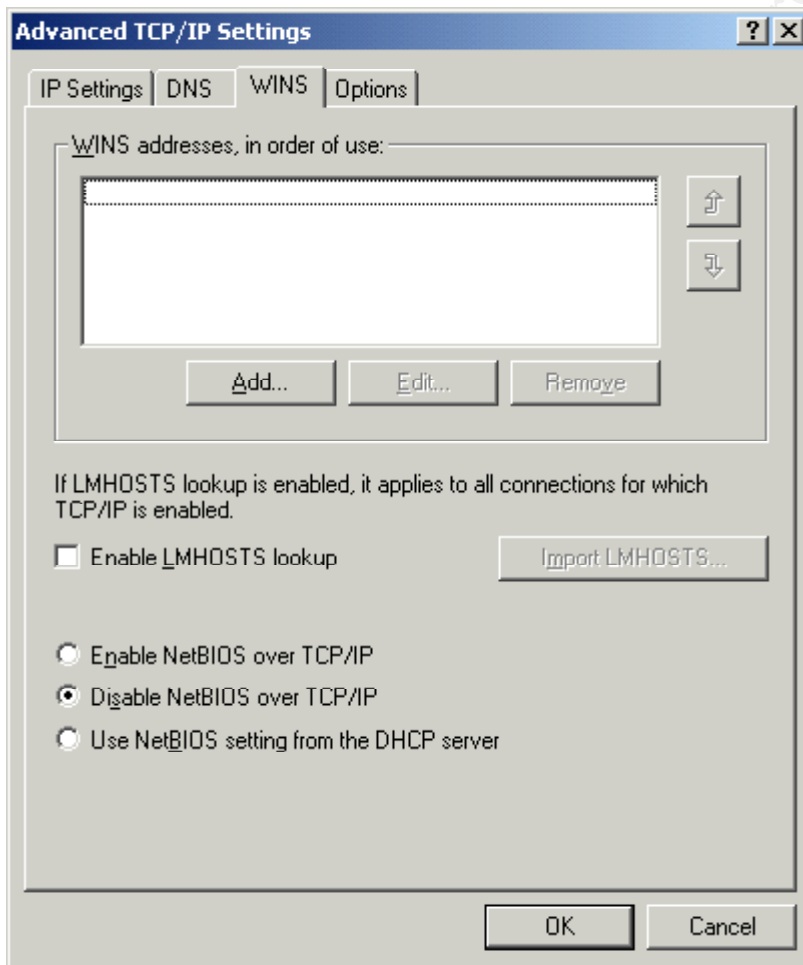
and

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

Protocol Configuration

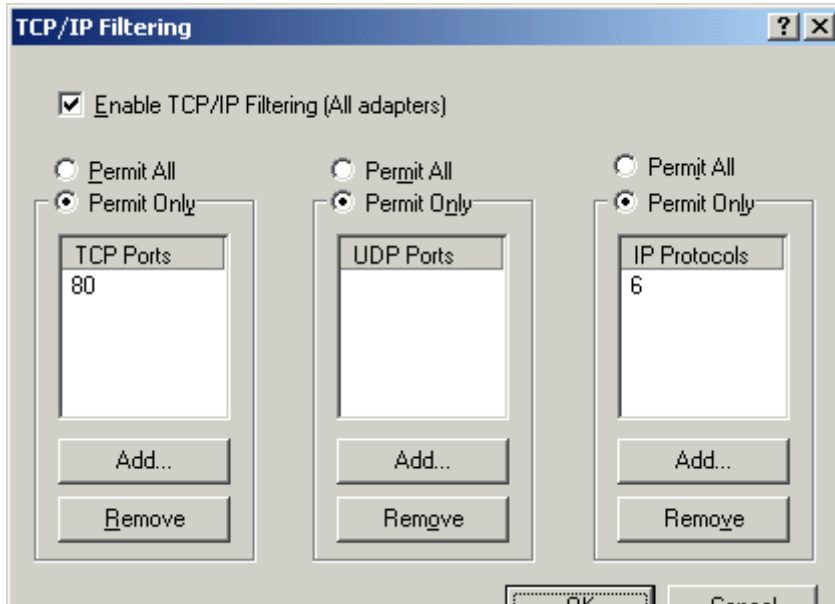
The next option during setup is the configuration of protocols. Use only what you need to get the job done. If you don't need Client for Microsoft Networks or File and Print Sharing for Microsoft Networks, it is best not to install them. If you need to have the Microsoft client installed or file and 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.



© SANS Institute 2000 - 2005
SANS full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Annapolis Junction SEC401	Annapolis Junction, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Kingdom Of Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - SEC401	Ankara, Turkey	Aug 08, 2018 - Oct 03, 2018	Mentor
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session AW - SEC401	Raleigh, NC	Aug 22, 2018 - Aug 29, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201809,	Sep 11, 2018 - Oct 18, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event