



# 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).<sup>1</sup> 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<sup>2</sup>.

More information can be found on EFS can be found at

[http://www.infosecurymag.com/articles/february01/features\\_applied\\_crypto.shtml](http://www.infosecurymag.com/articles/february01/features_applied_crypto.shtml)

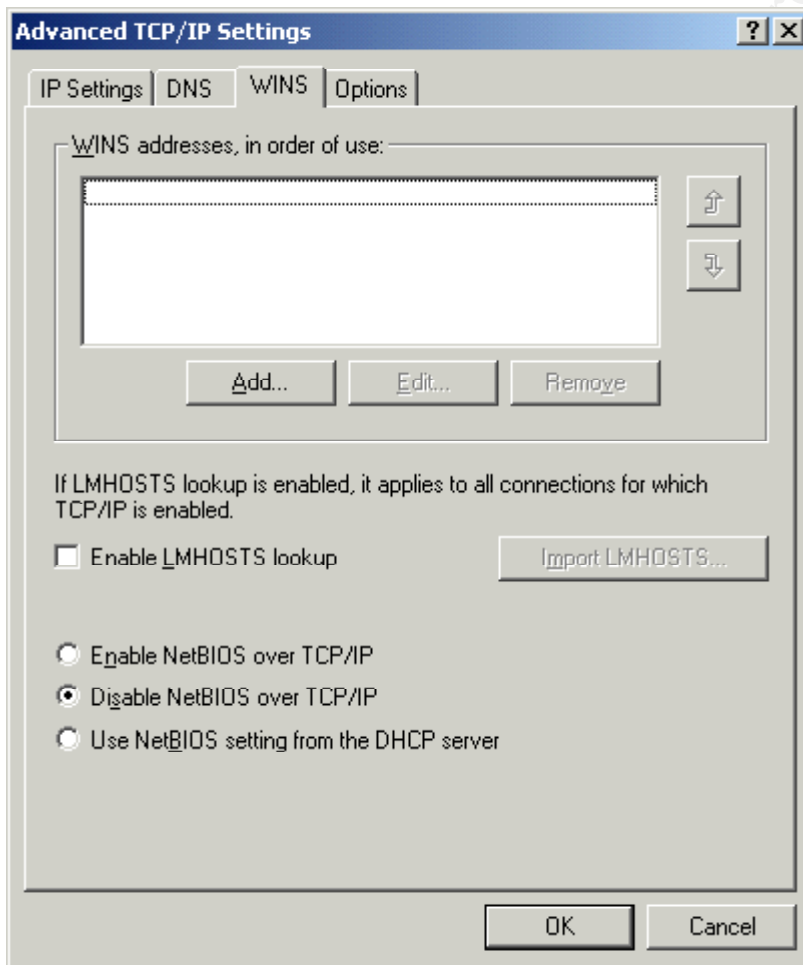
and

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

## Protocol Configuration

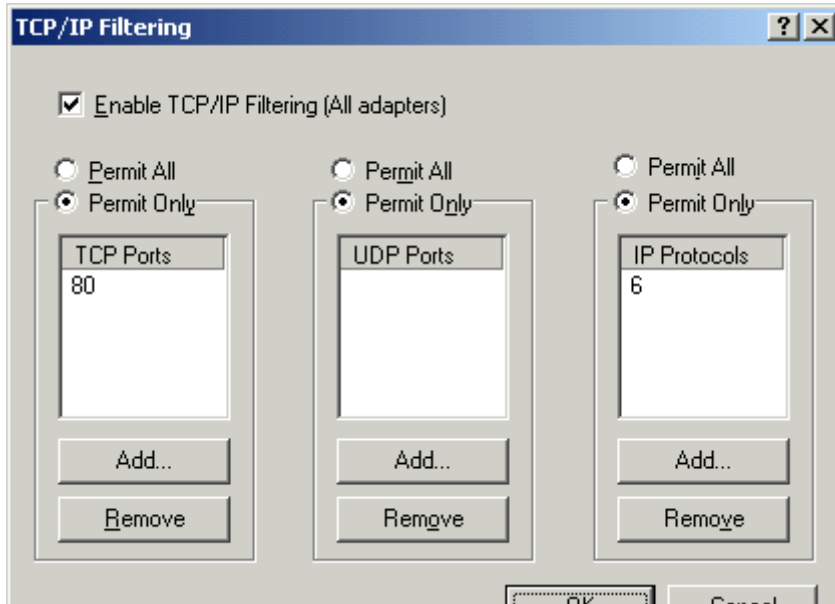
The next option during setup is the configuration of protocols. Use only what you need to get the job done. If you don't need Client for Microsoft Networks or File and Print Sharing for Microsoft Networks, it is best not to install them. If you need to have the Microsoft client installed or file and 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 options<sup>3</sup>. 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<sup>4</sup> 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 Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event