Global Information Assurance Certification Paper

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 deleted[2].

More information can be found on EFS can be found at

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

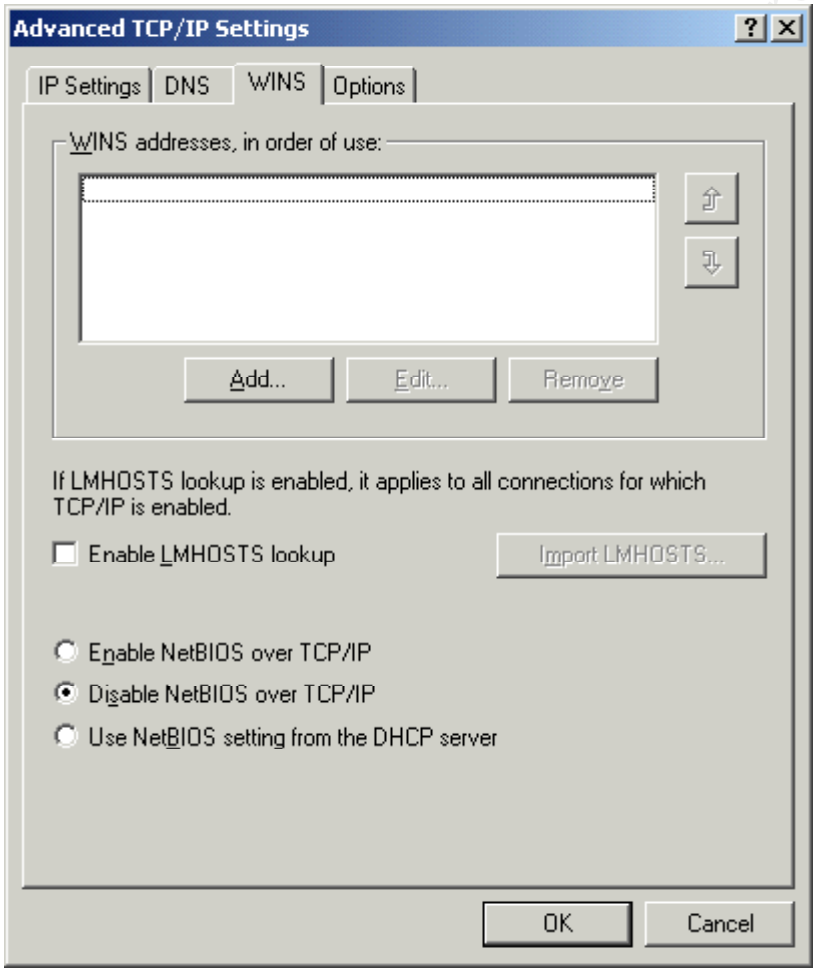
and

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

Protocol Configuration

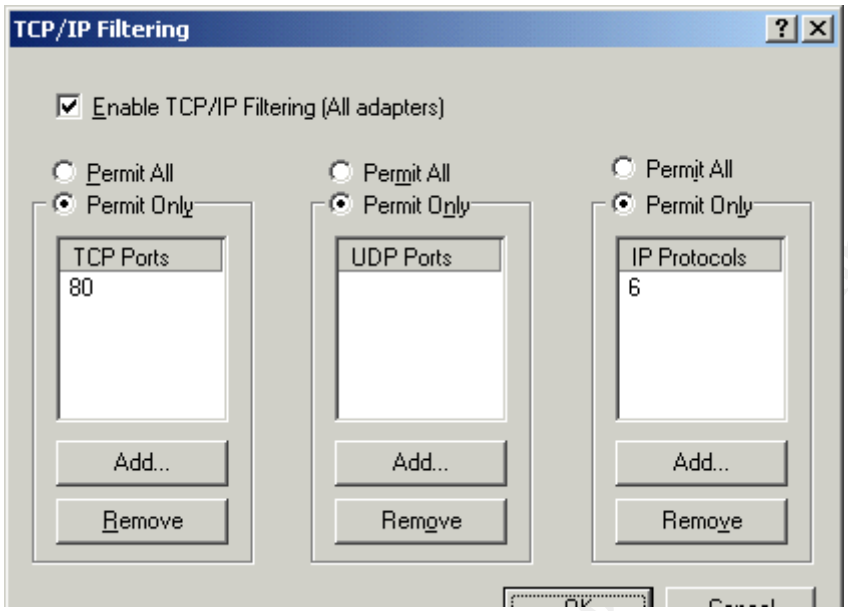
The next option during setup is the configuration of protocols. Use only what you need to get the job done. If you don't need Client for Microsoft Networks or File and Print Sharing for Microsoft Networks, it is best not to install them. If you need to have the Microsoft client installed or file and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



Last Updated: February 24th, 2018

Upcoming Training

SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
Mentor Session - AW SEC401	Melbourne, FL	Mar 01, 2018 - May 10, 2018	Mentor
SANS London March 2018	London, United Kingdom	Mar 05, 2018 - Mar 10, 2018	Live Event
Mentor Session - SEC401	Vancouver, BC	Mar 06, 2018 - May 15, 2018	Mentor
Mentor Session - SEC401	Grand Rapids, MI	Mar 09, 2018 - Apr 13, 2018	Mentor
SANS Secure Osaka 2018	Osaka, Japan	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Paris March 2018	Paris, France	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TX	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, Germany	Mar 19, 2018 - Mar 24, 2018	Live Event
Mentor Session - SEC401	Studio City, CA	Mar 20, 2018 - May 01, 2018	Mentor
Mentor Session - AW SEC401	Mayfield Village, OH	Mar 21, 2018 - May 23, 2018	Mentor
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS 2018 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 03, 2018 - Apr 08, 2018	vLive
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201804,	Apr 09, 2018 - May 16, 2018	vLive
Community SANS Charleston SEC401	Charleston, SC	Apr 09, 2018 - Apr 14, 2018	Community SANS
SANS Zurich 2018	Zurich, Switzerland	Apr 16, 2018 - Apr 21, 2018	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Apr 16, 2018 - Apr 21, 2018	Community SANS
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
Mentor Session - AW SEC401	Memphis, TN	Apr 17, 2018 - May 17, 2018	Mentor
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, IL	May 01, 2018 - May 08, 2018	Live Event
Community SANS Houston SEC401	Houston, TX	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event