Global Information Assurance Certification Paper

Securing NT4 Workstations in an Educational Computer Lab Environment

Eric S. Nooden

March 22, 2001

Introduction

Coming from a small liberal arts college, IT security and function is not high on the budget or priority list and due to staffing constraints, staff must take on multiple rolls. Very little time is given daily to ensuring equipment is secure and operational. Typically the students have more time than you when it comes to finding security holes and IT has to take a reactive stance to almost everything. Therefore security is limited to only being a speed bump in the scheme of things and security failures are inevitable.

More and more students are bringing their own computers to college but there are still quite a few who need access to computers to do their homework and email. Computer labs can be a hassle for IT departments that don't have dedicated staff; additionally, security software can become quite expensive for larger lab environments and can cause more problems than it is worth. With an NT4 server and a few inexpensive third party software packages you can stabilize and reasonably secure a lab using NT4 Workstations so that you can focus your attention to other equally time consuming efforts such as teaching users to update their own virus definitions.

The items used to control a lab are: NT4 Server, NT4 Workstations, Norton AntiVirus Enterprise Edition (v 7.5), and Norton Ghost and the remainder of the software is provided to you by Microsoft for "free".

Procedures:

I. Setup
   - A. Installation of the OS
   - B. Installation of extra software
   - C. Physical Security

II. Deployment
   - A. Server Setup
   - B. System Policies
   - C. Anti-Virus

III. Maintenance
   - A. Keeping an Eye on Things
   - B. Re-imaging a Downed Computer
   - C. Security Scans

I. Setup

A. Installation of the OS

To facilitate installation/upgrade of your lab workstations you should determine how many different models of computers you have (it helps to have standardized on the NICs) so that you will know how many images

and storage space you will need. Install the workstation OS as normal, with the exception for set up options…select "custom" and remove all the extras that you do not want (i.e. games, messaging, Paint, etc.). Also install the latest service pack…SP6a is the most current with SP7 not to far from release.

Ensure that the Guest account is disabled…you should never have to use it.

After loading the initial operating system and before loading the additional software (i.e. MS Word, Word Perfect, Network software, etc.) you will need to execute the first step to securing the workstation. Using the command "cacls", which stands for **C**hange **A**ccess **C**ontrol **L**ist**S**, we will ultimately remove the "everyone" permission from all of the files and folders thus preventing undesired access to our system (type cacls at the command prompt to get a full explanation of the command).

****DO NOT** run cacls after you have installed all of the software and are ready to release the computer to the students. It will remove permissions necessary for the various programs to function properly (Word, file saving, Netscape are a few that I have noticed having problems) and will more than likely cause you to have to reformat the computer and start from scratch.

Go to the command prompt and run each command separately and in order:

cacls c:*.* /T /E /C /G system:f
cacls c:*.* /T /E /C /G administrators:f
cacls c:*.* /T /E /C /R everyone

Note that running cacls does not protect the workstations registry ACL and you must edit those permissions by hand.

B. Installation of extra software

Install the remainder of your lab software at this time. Custom setup should be selected if offered and any non-essential components be removed…remember, the students are there to do work and not play games.

Add any security patches that may apply to your workstation.

Most word processors have an option for auto-recover files locations, temporary file locations and default save locations…these should all be set

before system policies take effect. It is a good idea to make the location of these files in a folder on the desktop so that the user can readily access the file should an error occur.

Once you are happy with your setup and almost ready to create an image for rollout, the last thing you need to do is alter the registry so that unauthorized users do not add additional software (i.e. instant messenger software and games). The key necessary to protect is the *HKEY_Local_Machine\Software* and by using the Regedit32 tool to remove the "Everyone" permission from the key and your workstation can be successfully protected. Note that you will want to ensure that the "Replace Permissions on Existing Subkeys" is not checked off else you will encounter problems later on.

Ensure that you have a shared drive on your server and that you have set up the network boot disk so that you can now make an image of the hard drive to be placed on the server. Follow the directions set up by the software that you have chosen to create your image(s).

C. Physical Security

One of the most essential aspects to securing you lab is to physically secure the computers; ultimately you can re-install the software in the event that someone gets past your security measures…that is, if the computers are still there.

Once the computer is on the lab floor, an Administrator BIOS Password should be setup. Enter the BIOS setup program at the beginning of the boot cycle, go to Security and turn on the Administrator Password feature. When setting the password, make sure that you remember the password. If for some reason you forget the password or it is maliciously changed, there is a jumper on the motherboard that will allow you to reset/defeat the BIOS password.

While in the BIOS, disable the boot option for all other devices except the hard drive. This will prevent malicious users from booting from a floppy and having their way with the computer (i.e. reformatting the computer).

A major reason for disabling the boot option from the floppy is that the hard drive can be read after it has been booted from a floppy. A typical DOS boot disk cannot see the hard drive and its contents but if the user has a program such as NTFSDOS (http://www.sysinternals.com/) they will be able to use this to see the entire contents of the hard drive. Once NTFSDOS is used, the hacker can copy the SAM and crack them using password crack utilities, L0pht Crack being a good example of a program that will crack passwords. (http://www.securitysoftwaretech.com/).

II. Deployment

A. Server Setup

Before the workstation is brought out into the lab, you should have your server set up so that once a machine in installed it will fall under immediate control via system policies (see the following section for setting up System Policy). Via User Manager for Domains, you should set up the user account and permissions (i.e. access to specific printer shares) and ensure that the Guest account is disabled. Although using one user account for all of your lab workstations may seem like creating a glorified Guest account, you are making it possible to limit who can log on as opposed to letting anyone connect to the server.

The server side of the anti-virus that you've selected should also be in place before deployment so that once a workstation is deployed; the client can be pushed out to it. Even though you have System Policies in place, your workstation can still be infected.

Once your workstation is setup and in the lab, you will need to log on as local administrator and join the domain in which your lab server exists. Once the domain has been established, you can then log on via the lab user account and at that point, the system policies will be loaded and your workstation protected.

B. System Policies

An excellent paper has been written concerning System Policies and it is located in the SANS Information Security Reading Room (http://www.sans.org/infosecFAQ/win/SPE.htm). You should review this document to get a good idea on how to implement policies. I use "Windows NT User Administration" and "Zero Administration for Windows" both from O'Reilly for reference.

One item that is touched upon in the SPE paper but not expanded upon is the .ADM files located in the */Winnt/Inf* directory. Included in the standard server setup is three .AMD files: Common, Windows, and Winnt. Microsoft also make available thru its web site, .ADM files for other software packages such as Office98, Office2000, and Internet Explorer. These files can be added to the */Winnt/Inf* directory and loaded into the System Policy Editor thus adding extra control. Another benefit to the .ADM files is that they are fully customizable and you can even create your own .ADM file. (Note: A search at the Microsoft sight using ADM as a keyword yielded numerous references to Microsoft software that have .ADM files associated with them).

C. Anti-Virus

Symantec Corporate edition allows for the pushing of clients and virus definitions. Once installed, workstations can be monitored for virus activity and if new workstations come on line, clients can be pushed to them in minutes. From the System Consol, you can set and lock the setting for each client thus ensuring that your virus protection is maintained. Daily or weekly virus updates can be scheduled so that you are always up to date. Virus scans can also be scheduled.

III. Maintenance

A. Keeping an Eye on Things

Auditing should be set on the workstation so that you can monitor the event logs for any unauthorized activity. When Norton System Center is installed on the server, the workstation clients can be monitored for virus activity in-addition to pushing new clients out to re-imaged machines.

B. Re-imaging a Downed Computer

In the event that a disk failure has occurred or the naughty student has managed to get by your security, having an image of the hard drive is a handy and time saving thing to have. Overall cost for the software and licenses is reasonable. Typical restoration time is about 15 minutes as opposed to several hours if everything has to be hand loaded. Once the image has been applied, you will need to change the IP address and the name of the computer since you will cause conflicts with the original workstation that the image was taken.

*Note that when an image is applied to a workstation, you will need to change the SID before your first logon to the server, if you do not, problems can occur.

C. Security Scans

Periodic scans of your lab and server are a good idea to ensure that your students haven't gotten one up on you. WebTrends offers a free security scanner (http://www.webtrends.com/products/wsa/default.htm) for educational institutions. Nmapnt, the ported version of Nmap, (http://www.eeye.com/html/Research/Tools/nmapnt.html) is now available for NT/2000 and will allow you to scan your workstations for open ports.

Conclusion:

I have had an NT4 Workstation lab in operation for over two years now and have not had any major problems occur; I have had students try…Trojans and such, but to date they have not breached the security. As I have learned and became aware of new tricks and patches, I have applied them. By employing such things as System Policies, Antivirus, Physical Security and taking the time to run system scans, you can create a lab environment that is secure, easy to manage, and flexible enough for students to use…with minimal complaint.

References:

Internet Sources:

Conners, Matthew. "System Policies and the System Policy Editor (SPE) for Microsoft Windows." SANS Information Security Reading Room. 12 February 2001. http://www.sans.org/infosecFAQ/win/SPE.htm (21 March 2001).

Microsoft, "Take Security to the Next Level with System Policies", April 1999, URL: http://msdn.microsoft.com/library/periodic/period99/security.htm (21 March 2001).

Microsoft, "Using the /E Option with CACLS.EXE", 22 February, 1999, http://support.microsoft.com/support/kb/articles/Q131/7/80.asp (21 March 2001).

Sysinternals Freeware, "NTFSDOS", 14 October 1999. http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml (21 March 2001)

Books:

Kurtz, G., McClure, S. and Scambray, J., Hacking Exposed: Network Security Secrets and Solutions, Osbourne/McGraw-Hill, 1999.

Meggitt, Ashley J. and Ritchey, Timothy D., Windows NT User Administration, O'Reilly & Associates, 1997.

Zacker, Craig, Zero Administration for Windows, O'Reilly & Associates, 1999.

Software:

EEye Digital Security, NmapNT
http://www.eeye.com/html/Research/Tools/nmapnt.html (21 March 2001)

SecuritySoftwareTech, L0pht Crack
http://www.securitysoftwaretech.com/ (21 March 2001)

Symantec, "Norton AntiVirus Corporate Edition 7.5"
http://enterprisesecurity.symantec.com/ (21 March 2001)

Sysinternals Freeware, NTFSDOS
http://www.sysinternals.com/ (21 March 2001)

WebTrends Security Analyzer
http://www.webtrends.com/products/wsa/default.htm (21 March 2001)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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 London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS