GIAC
CERTIFICATIONS

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 permited 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

Setting up A Secure Windows XP Lab

GIAC Security Essentials Certification (GSEC)
Option b
Date re-submitted 2/11/04
Mark Ross

Abstract:

Working in an Education environment, one of the most challenging and time consuming aspects of our jobs is setting up a secure Windows XP lab. Our 7 labs average from 30 to 40 computers per lab, with hundreds of users per day. The tasks required to setup, maintain, and secure these labs are tremendous. Following, is a guide which may be used as an additional resource in dealing with the setting up and security aspects this task.

Introduction:

Before addressing the issues involved in securing a Windows XP lab, I would like to first explain the types of users we provide service to and what we must provide to them. The labs are set up for use by undergraduate and graduate students pursuing degrees from Elementary Education to Computer Science. All students have access to the same software and computers. Our goal as IT professionals in a higher education environment is to set up and maintain a secure and stable computer oriented environment which will enable all students to excel in their studies. In giving every student a stable working computer environment we must also consider the stability of the network and its computers as a whole. One of the ways we do this is through lab security.

This paper is meant to be a reference guide to assist with the problems in setting up and maintaining a Windows XP lab. Although this paper is directed towards any person or professional in lab set-up, in reference to security concerns. The first portion of this paper Setting up a Secure Workstation can also be used to set up a single Windows XP workstation. The second portion of this paper will deal with preparing the workstation for cloning, and the last discusses physical security features and how we address them. In no form is this paper meant to include all available security measures possible for a Windows XP Lab or workstation. Hopefully this paper will help guide you through the total process from setting up a clean Windows XP workstation, properly deploying an image, and physically securing the machines.

Throughout this paper screen shots will be given from the following:

- Microsoft Windows XP Professional
  - General security policy settings
  - Password security settings.
- Computer/Network use disclaimer

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Setting Up A Secure Workstation:

For the initial setup of Windows XP, I will refer you to another guide written exclusively for setting up and patching the operating system. The guide is called Windows XP: Surviving the First Day and can be viewed at the web address listed in my references. Whether setting up a lab workstation as we are, or setting up an individual workstation the majority of the following steps should be generally the same. In the following I will touch more on subjects covered in the previous paper and also add some new features tailored to a lab environment.

For the following steps I am assuming there is no previously installed operating system on the computer.

Physical Setup of components

The first step is to setup the physical components of the workstation ie. CPU, monitor, keyboard mouse, speakers …etc. For the following steps I am referring to only the workstation which will be later cloned. Before you plug in the power if the workstation has a wireless network card either disable any access points within reach or remove wireless network card. Next check to be sure phone line is not yet plugged into the modem or any other network cable is plugged in. Now plug in the computer and insert the Windows XP CD. Next we will proceed to the setup of the operating system.

Installing a new copy of windows XP

The first thing you will be prompted for is to press any key to boot from cd. If you are not asked this question, shut down the machine and enter the BIOS to change the boot sequence to boot from cd first. Once your computer is booting from the Windows XP cd you may proceed to the following steps.

You will be asked if you want to install windows XP now. Proceed through the questions until you get to the questions pertaining to where you want to set up your operating system. Here you will be given a few options depending on the drive in which you are installing your operating system. If there are multiple partitions we would like to first delete all partitions and start from scratch. Once all partitions are deleted you will be left with one large un-partitioned drive.

At this point we want to create two partitions. The first partition will be for the operating system and the second will be for unprotected storage which I will explain later in the paper. Three partitions will actually be created but we will only create two, the third is created by default. Now we are ready to choose the file system we would like to use on the partitions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The partition in which we will install the operating system is always in our case the larger one. The reason we do this is to allow us to install the operating system and all the applications needed by the students on the single protected partition. Before we proceed to the install we must choose between a few different format options. The file system features offered are Fat and NTFS. In all cases we choose NTFS, this is for many reasons. The first of which is that Fat file systems do not support drives over 32Gig (Microsoft Corp). The second is for security purposes. NTFS offers more control over file access. File access is controlled by user and group permission, for example: "When a user logs in to a Windows NT or 2000 network, the account that is used becomes the key to what that person can access, including NTFS objects." (Kozierok) By using an NTFS file systems we are able to limit access to individual files.

Once the partition and format is chosen Windows will go through its initial format and file system setup process then re-boot.

When the computer re-boots some additional files will be installed and you will proceed through some more basic steps i.e. cd key, regional settings. When you get to the computer name and administrator password stop. This is a very important step. The computer name will be very important in identifying the computer on the network. I will discuss this more in detail later, but be descriptive, this computer could cause network problems later, and a good computer name will help track it down. The administrator password will be discussed in detail later, and may be changed later, but for now just choose a good secure password. Once you have chosen filled in these features proceed through the next steps until you get to choosing network settings.

When you arrive at the Networking setup screen choose the custom settings option, and choose next. As mentioned in the Surviving The First Day paper, deselect file and print sharing, and Client for Microsoft networks, If needed this can be enabled later. The next step will be to set up a user account. You will be prompted to set up a user of this computer. You must set up a local account at this point. Once you input your account name in this box you may proceed. We will later disable or delete this account. For now set up an account and remember this account will have the same permissions as the administrator account.

Once this step is finished you can choose next and the computer will re boot. At this time you may plug in the Ethernet connection to prepare for downloading patches.

When the computer reboots the very first thing to be done is to install patches and updates. Go to www.windowsupdate.com and download and install all available updates. Once this is finished you may proceed to the next section of this paper, User Accounts. This section will help secure local user accounts.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

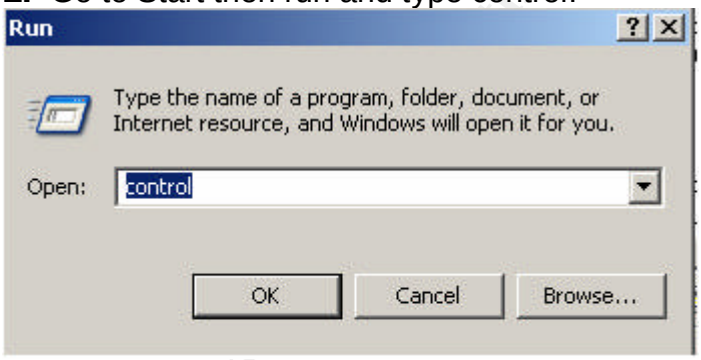
User Accounts

Local user accounts are the first item of discussion. The most dangerous default windows account is the Local administrator account. When setting the password on this account, be wise and choose at least a ten digit password with a strong combination of numbers, symbols, and characters, remember no dictionary words. If you are a home user set up a power user account for your every day use. When setting up a power user account use a different password with at least an eight digit password. Once you have taken care of the administrator account, the next step is to move on to disabling the guest account.

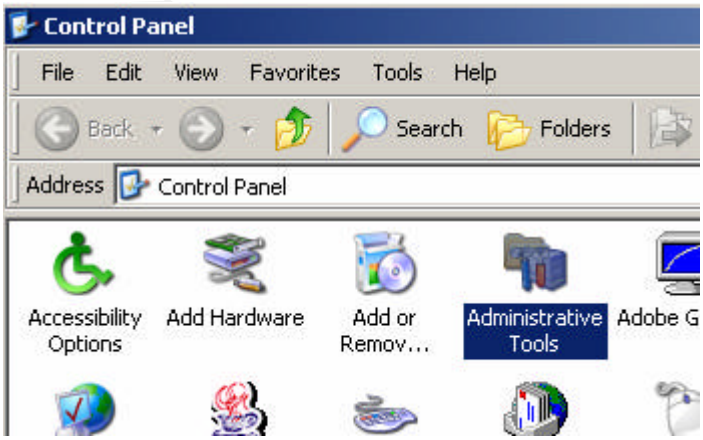
By default Windows XP has an account called Guest; initially this account has a blank password. Follow the steps below to disable this account. For the next few sections of this document we will refer to the following steps as the local security policy settings. The first three steps represent how to get to these settings. The last two are the actual changing of the guest account.

Local Security Policy settings:

1. Go to Start then run and type control.

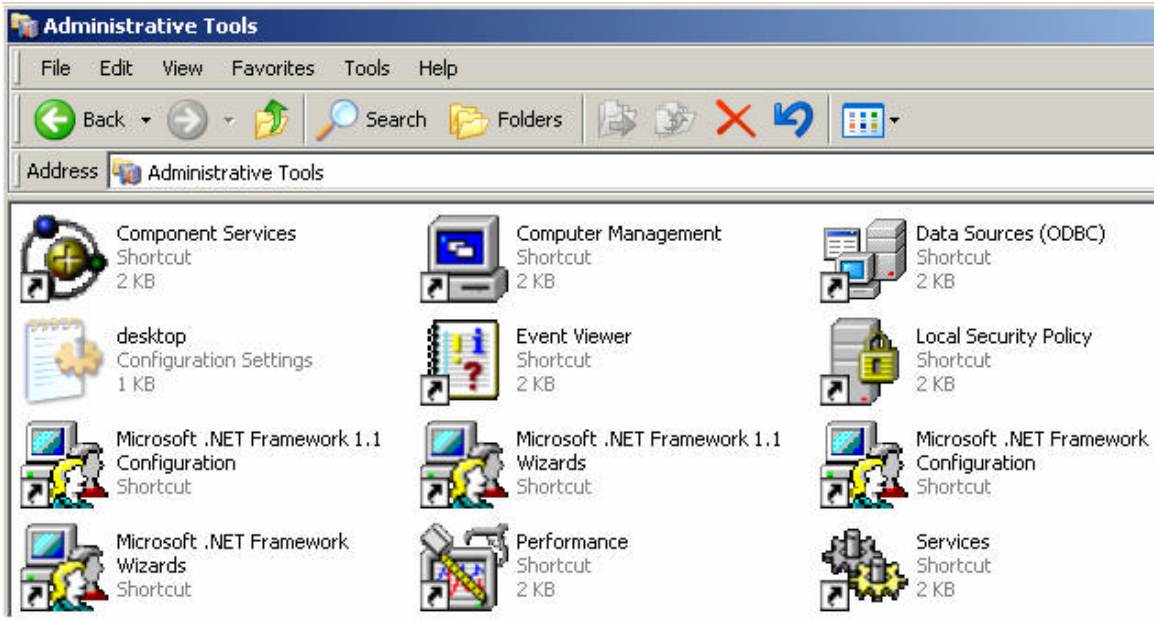


2. Once the control panel opens, find administrative tools and open it.

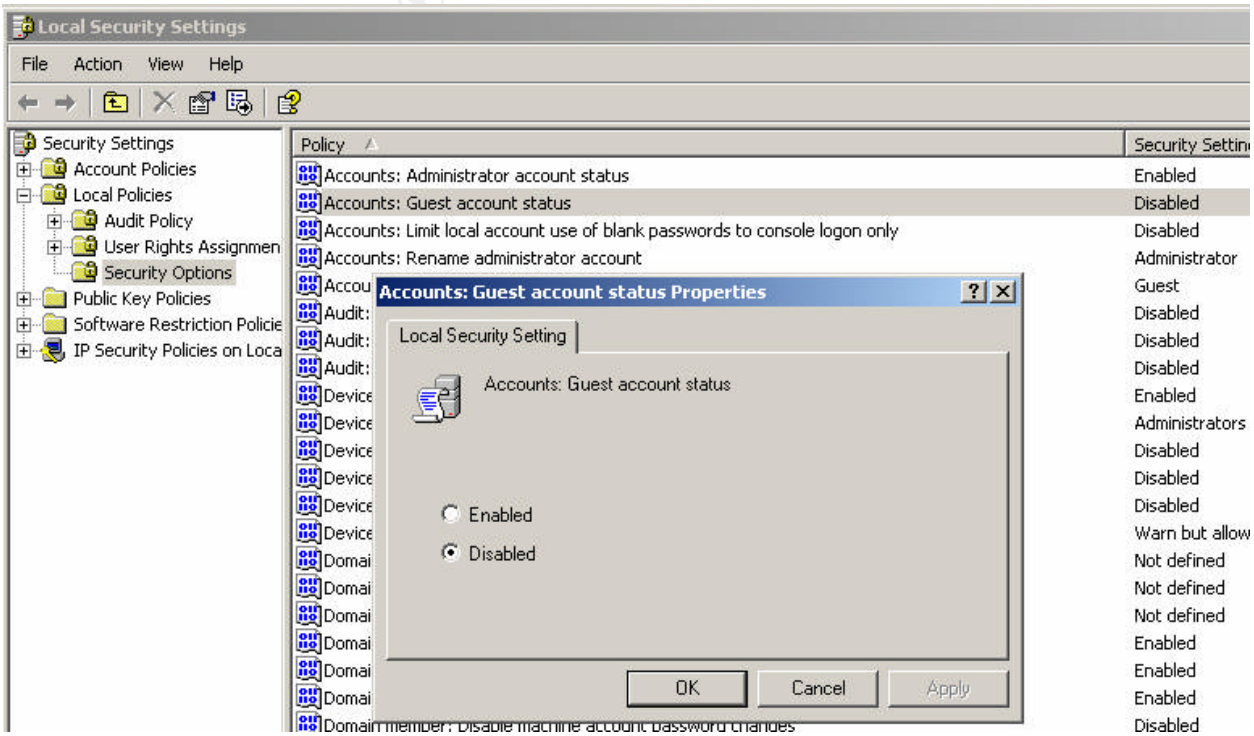


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Choose the Local Security Policy icon. 



4. Once you have the local security policies open, scroll down to Local Policies then to Security Options: Next find the Guest account status. If the account is not disabled, double click it and choose disable.



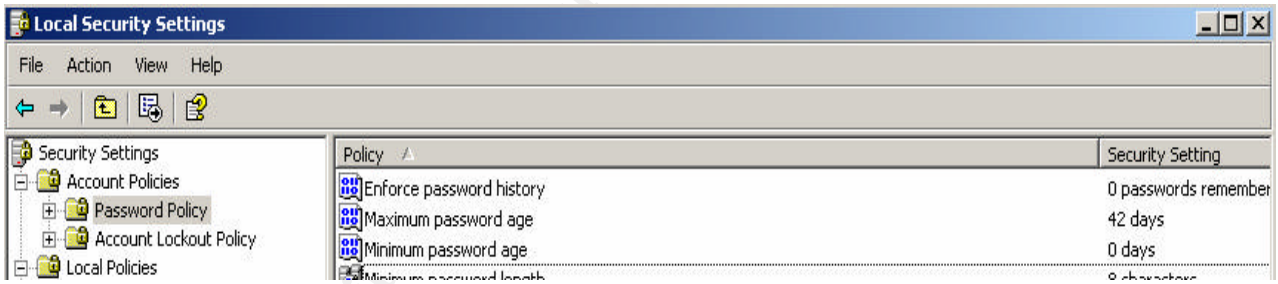
5. Once the guest account is disabled, press the ok button and close all active windows.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Once the Administrator account is properly secured and the Guest account is disabled we will move on to the next changes. Before I show how to make these changes I would like to discuss them. The following are a few measures that can be taken to better maintain accessibility (or the lack of) through security. If the machine or machines to which these changes are being made on are going to be members of a domain, the domains security policies will take precedence for users logging on the domain. Following is a list of the suggested measures, followed by the reasons. Most of these modifications can be done in Local security settings as described earlier.

Set a maximum password age. Microsoft suggests from 30 to 42 days. Simply given, many users, if given the option would rather not be required to use a password, so you enforce the maximum password to require continuous changes. With a maximum password length, a, would be intruder would have a shorter time frame to crack the password. To make these changes, take the following steps. Refer back to Local Security settings policies to re-open the policies window.

1. Once the policies window is open, instead of opening Security options, open password Policy.



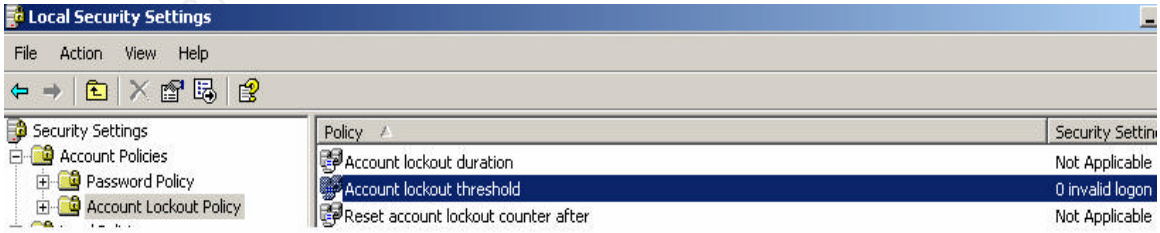
2. Next open the maximum password age properties window by double clicking it. The properties window will open and you can set the maximum. Press ok to finish.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The next step is to *Set minimum password length* to at least 8 digits. Microsoft suggests 7, but passwords are often referred to as your first line of defense so stronger is better. The NSA suggests that " privileged users (such as administrators) have passwords longer than 12 characters". (Bickel, 33) The reasoning behind setting minimum password length requirements is simple. Longer passwords take more time to crack. To set minimum password length, go back to the Password Policy window and change the length just as you changed maximum password age.

Enforce Password History, This setting will not allow users to use one of their old passwords. The standard is usually 10. To set the Enforce Password History option, go back to the Password Policy window and change the length just as you changed maximum password age, and Length.

Limit unsuccessful logon attempts. This setting is usually set at 3 or 4. If a user attempts to logon to the workstation unsuccessfully 3 times there account will be locked. This measure prevents intruders from attempting to guess passwords. To change these settings go back to Local Security settings. Choose Account lockout threshold, and change it as you did in previous sections. In this window you may also be able to change account lockout duration.



When discussing security there are three common issues to be addressed, "Confidentiality, Integrity, and Availability". The issues covered

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

previously may be considered confidentiality issues. “Confidentiality is the need to ensure information is disclosed only to those who are authorized to view it.”(Cole, 257) Account management is one of a list of things that will assist in assuring you are providing access to the proper users. Integrity is also addressed. By maintaining tight access measures you are helping to ensure only users with access to certain information can change that information. The last, availability, is addressed in terms of denial of service attacks. With tight local security settings you can help prevent unauthorized access through malicious code, and unauthorized logins.

There are many more local security settings which can be set to help enforce access security to your Windows XP workstation. For this guide we will stop at these and move on to the next topic.

Patches:

As covered previously patches are one of the most important precautionary measures when installing any OS. “a good security architecture, one that can withstand the threat, has many aspects and dimensions. “if one countermeasure fails, there are more behind it”. (Sans,293) Securing your operating system is in my belief the first means of initial defense. On almost a daily basis security vulnerabilities are surfacing, maintaining up to date patches is the most basic means of protecting yourself against these vulnerabilities. Because this was covered in depth by the previously mentioned paper I will stop at saying regardless of all other measures taken, an un patched machine is more vulnerable to malicious activities. Once the machine is patched you must then plug in the network cable and proceed with the rest of the installations

Other Installations

After all patches are installed the next step is to install all additional software packages and printers i.e. Anti Virus Software, Office, IP printers, rename Computer, Join domain, and any other additional tasks. The antivirus software should be installed first and all current virus definitions downloaded. “Your antivirus protection is only as good as the latest updates.” (Universit of Cambridge) After your AV software is installed and virus definitions are updated, proceed with any other installations or changes.

When renaming the computer use a descriptive name. This will allow your Network Admin to easily track down computers causing network problems. For instance if your network admin is seeing unusually large amounts of traffic moving across the network, he/she can often analyze that traffic and track it back to an IP address which can in-tern be linked to a computer name.

Joining the computer to a domain is the next step, in doing this we address many security concerns. When we join a computer to a domain several things change. Assuming there were no additional local accounts added after installation the only local account left (see footnote) should be an administrator account, most other account properties are maintained at a another level.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Password authentifacation, privileges, and restrictions are authorized at the domain controller. Once the computer is joined to the domain additional local accounts can and often do exist, but only to those who are authorized to have them.

Centurion Guards

A Centurion Guard is a piece of hardware we use to help maintain an operational pc. The centurion guard is a piece of hardware placed on the floppy drive cable between the motherboard and the floppy drive. In an environment like a heavily used lab it is essential to take as many steps to ensure availability to the users. What this technology does is prevents ANY permanent changes made to the system. Without a key any changes made to the protected partition will be disregarded upon reboot. There are advantages and disadvantages to this technology. Listed below are some of those advantages and disadvantages. Some of the disadvantages contradict account/password policies set in the account section, negating previously described local settings on machines with Centurion Guards.

Advantages

- Regardless of group membership no permanent changes can be made without key or software keys.
- Maintenance time spent in labs is reduced.
- Confidentiality issues are reduced by clearing any information saved by previous user
- Problems usually arise due to hardware failure not software.
- Prevents changing of boot devices.

[1]In some cases additional accounts are added for some software, for example a System management server installs a client account

Disadvantages

- Automatic updates inoperable
- Local log files cleared upon reboot
- Virus definitions must be manually updated
- Password history reset upon reboot

Some of the disadvantages described above are addressed when the computers are joined to a domain. For example: all authorized users have network passwords maintained on the domain controller. Password history is no longer maintained with local security policies, instead by the domain controller. Local log files are actually lost, but successful and unsuccessful logon attempts are also logged at the domain level. Automatic Updates and virus definitions are and should still be maintained on a regular basis. This is done using a tool

[1]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

provided by Centurion technologies. This tool enables us to unlock all protected machines at once (as apposed to one at a time with keys), at one administrative console. Once all machines are unlocked we can install updates either manually with disk or through the windows or antivirus update features.

The centurion guards do take away some valuable local security tools, such as log files, cached old passwords, and automatic updates. In an attempt to ensure availability to those who need it, we must sometimes sacrifice some security measures to facilitate that.

Once the computer is set up exactly as you would like all other machines in the lab to be set up, you may proceed to the next step.

Cloning the Lab:

The first step before starting the actual cloning process is to run sysprep. There are two main reasons we want to run sysprep.

- Generate new Security Identifiers
- Generate new Computer names
- Prepare a mini setup

One of the problems with cloning a Windows XP is with Security Identifier duplication, in particular as a member of a workgroup or on a domain(see symantec). One of many ways a computer is identified on a domain is through its security identifier. “The Windows XP networking and security subsystems rely on a unique token known as a Security Identifier (SID). This token is randomly generated at installation time. Each user account, security group, and computer has its own SID.” (Symantec) When pulling an image from one machine (The first machine for this we will call the master) and duplicating that machine on others, you also duplicate the SID. One of the problems with this is when two machines with the same SID is attempting to logon to a domain, only one of them will be allowed and the other will be rejected. Because this is a unique key generated to identify one particular machine on the network these keys need to be regenerated,(Microsoft sysprep) this can be done using sysprep.(As with SID’s Computer names must be regenerated when cloning a machine for duplication. For this we will also use sysprep.

Sysprep is a Microsoft system preparation tool, we will use to generate new SID’s, new computer names, and setup to use one open license windows CD key. To use sysprep follow these directions. Many steps are left out due to the different options available with sysprep. The following are very general directions on the main topics needed in sysprep.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. On the Master computer Create the folder C:\WINDOWS\DEPLOY
2. Insert a Windows XP and find the Support\Tools\Deploy.cab folder.
3. Copy all files out of that folder into your new Deploy folder.
4. Run through sysprep, different applications will require different options to be checked. For this application the important ones are to Generate new security identifiers, generate new computer names, and run through mini setup. Just follow through the onscreen instructions to finish.
5. Once finished the computer will shut down, at this point do not restart the computer, or you will have to re-run sysprep.

At this point go you can use what ever software you have purchased to pull the image and push it back out to the lab. Once the clone is pushed out to the lab computers, you boot the machines and run through the mini setup. Depending on the setup features you chose in sysprep, your lab should be operational when setup is complete. Upon completion of the mini setup we would lock the centurion guards and finish up.

Physical Security Measures

In this section I will to discuss some security measures taken in our labs. These measures are taken for many reasons, Deterrence, notification of policies, theft prevention, and also for the safety of our lab users. The first physical security measure I would like to discuss is deterrence.

Deterrence

Deterrence is shown in many ways and for as many reasons. In all our labs we have posted large signs warning of the watching eye of cameras, The signs benefit in two ways. The first is for legal issues, and the second is for warning purposes. Even if the camera is out of sight if an individual sees the camera signs that will be enough to deter any actions. Lab attendants are placed in most labs; the cameras were put in place mainly for the safety of the lab attendants. We also use the cameras to record lab activity in case something was to go wrong. The lab attendants are another form of deterrence. Just having them there is often enough.

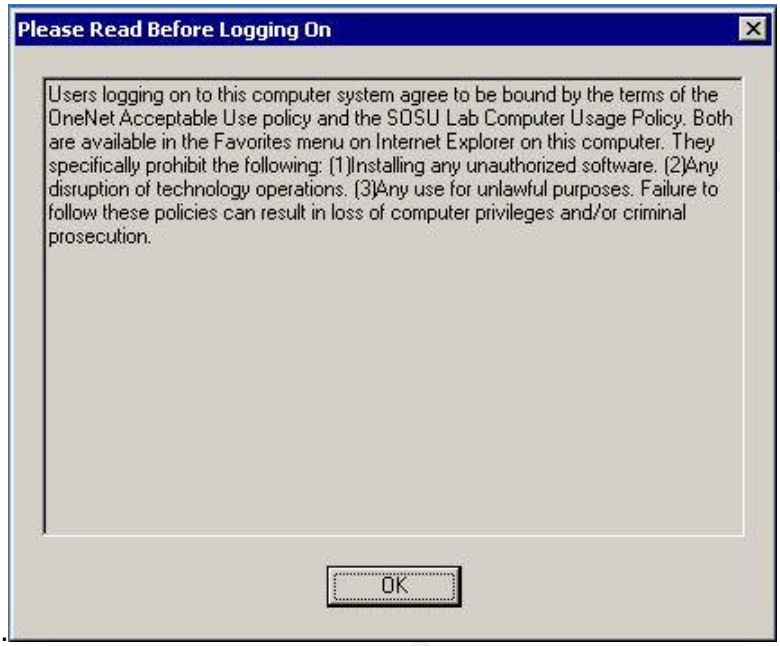
Theft prevention

Theft prevention is taken care of in several ways. As With deterrence the cameras and the lab attendants help with this. In some labs we are unable to employ attendants throughout all open hours, so we use other measures. In this situation we install computers in locked boxes in addition to cameras.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Policy Notification

We address policy notification 3 different ways .The first is through an orientation, when users are first introduced to our facilities they are given pamphlets with policies and instructions of computer/network use. The next way we introduce policies is through classes. In adition to an orientation day, most users must attend a class, in this class we have began teaching policies. The last way we notify our users of poly is through login scripts. This also is a small reminder every time they log on. Following is a screen shot of our policy screen



Conclusion:

In this paper I haven shown: how to secure a workstation through local security settings and update awareness, in preparation to setting up a Windows XP lab. I have shown measures that we take with centurion guards to ensure availability, and also I have shown a few physical security measures which can be taken after the labs completion. Although some of our security measures are unable to be implemented in some environments (Centurion Guards) because of there inherit security problems, most of these features can me used universally. Hopefully these steps will assist others in the task of setting up a secure windows XP lab. For additional readings on some of these covered topics see my recourses.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

- Microsoft, How to Use Sysprep: An Introduction. November 29, 2002http://www.microsoft.com/windowsxp/pro/using/itpro/deploying/introduction.asp

- University Of Cambridge. Securing Windows XP Home Edition for Stand Alone Use. October 2002. http://www-tus.csx.cam.ac.uk/pc_support/WinXP/collegehome.html

- Symantec Corp.Introduction to cloning a Windows NT, XP computer December 19, *2*003 *.http://service1.symantec.com/SUPPORT/ghost.nsf/8f7dc138830563c888256c2200662ecd/92c05c601bf35fb2882567a70080df54?OpenDocument&src=bar_sch_nam*

- Ullrich Johannes. Windows XP: *Surviving the First Day* December 23, 2003. http://www.sans.org/rr/papers/index.php?id=1298

- Bickel, R, Cook, M Haney J, Kerr M, Parkes H. Guide to Securing Microsoft Windows XP. October 30, 2002 http://www.nsa.gov/snac/winxp/index.html

- Norton, Peters, Dave Kearns. Complete Guide to Networking Indiana, October 1999.

- Cole, Erin, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK .Volume 1. *Physical* United States of America, April 2003.

- Install Windows XP Professional *New* Installation. Microsoft Corporation. August 24, 2001. \http://www.microsoft.com/windowsxp/pro/using/howto/gettingstarted/guide/installnew.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Kozierok, Charles M. General NTFS Security Concepts.. The PC Guide. April 17, 2001 http://www.pcguide.com/ref/hdd/file/ntfs/secGen-c.html

© SANS Institute 2004, Author retains full rights.

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