Global Information Assurance Certification Paper

SANS

GSEC Practical Requirements (v.1.3)

Locking Down NT

A PROJECT PLAN SUBMITTED TO

SANS

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

SANS Fundamental Certification

BY

John Brewer

COLORADO SPRINGS, COLORADO

APRIL 2002

CONTENTS

INTRODUCTION

This paper is intended to identify the need to fully lock down a Microsoft NT System that is connected to the Internet or any other network. Techniques used to lock down a system start at the File and Folder permissions, extend to Protocols, and include unneeded services, but they do not stop there. In addition, users, specifically privileged users must be trained on what to access and what not to access while using the privileged user account. In addition, one other thing comes into play-social engineering. The information you pass over the network can be used against you to gain entry into your system. I belong to an organization where four personnel fulfill the combined roles of administrators and network security.

WHAT HAPPENED TO ME

The senior individual, determined to train the other three of us (which included myself) to effectively lock down a system from any potential hacker and maintain that system set strenuous goals for each of us. Using four Windows NT systems on separate domains connected through a star network via a hub using TCP-IP as the only protocol to play a modified form of Capture the Flag Game, a game where two or more teams attempt to capture each others flag by entering into the other teams' territory in pursuit of the destined flag. (CTF, Internet). Similar to ZDNet's Contest version of Capture the Flag where images were the target, ZDNet's eWeek has announced a capture-the-flag challenge to crackers called Openhack, inviting all comers to compromise a system set up for demonstration purposes and win cash prizes "ranging from $500 for defacing the Web server to $1500 for compromising the e-mail server, to $2500 for cracking into the database server," the organizers say (ZDNet, Internet), our version a file would be hidden on an adversaries computer system and an attempt to hide a file on the advocates computer system. The first to hack an opponents computer system, find the file and read the contents would be ordained the winner. Each system's software suite would include Windows NT Server, Internet Information Server 4.0 running Web services and a File Transfer Protocol (FTP) server, and a Telnet server. All four users would have a telnet account on each machine. Each of us were assigned a system and told to lock down that system in any manner we chose and hide a file from the senior user on the machine assigned. The goal: keep the senior user from finding the file on each independent system before one of the other users found the file on his system. The prize: a steak dinner. I thought to myself, "This could not be that hard."

My first attempt was to convert the file system to NTFS and set permissions.

> NTFS file permissions are used to control the access that a user, group, or application has to files. This includes everything from reading a file to modifying and executing the file. Multiple permissions can be assigned to a single user account. They can be assigned to the user account directly or to a group the user account is a member of. When multiple permissions are assigned to a user account, unexpected things can happen. To prevent any heartache we are going to discuss the rules and regulations for assigning multiple NTFS permissions to a

single user or group. This will include how file and folder permissions work together, and how denying a specific permission can affect a users' allowed access. First of all, NTFS permissions are cumulative. This means that a user's effective permissions are the result of combining the user's assigned permissions and the permissions assigned to any groups that the user is a member of. For instance, if a user is assigned Read access to a specific file, and a group that the user account is a member of has the Write permissions assigned, the user is allowed the Read and Write NTFS permission to that file. (NTFS Permissions, Internet)

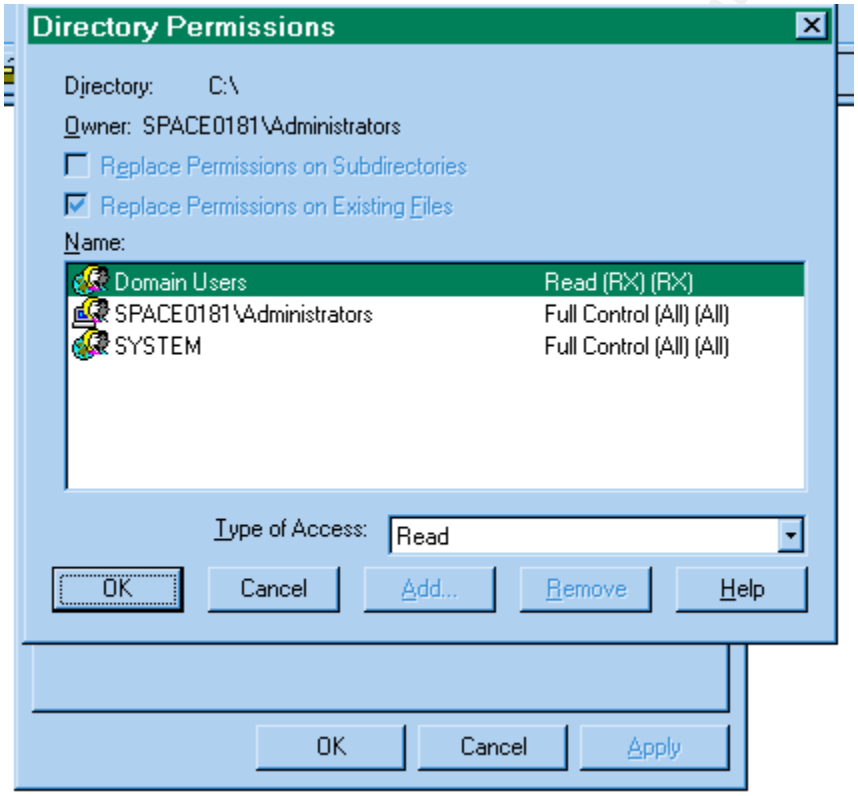

Figure 1

I removed the Everyone group from all drives. I set full access for Administrators and read only permissions for Domain Users on all directories. I created four predefined user accounts, and a group called "Red_Team" and placed the four created accounts in the group. I assigned read permissions for the "Red_Team" to the Inetpub\wwwroot directory. At this point, I added a Windows NT Workstation to my domain and locked it down with NTFS, and set permissions for Admisitrators to full control and removed all other groups. I then created a directory called GuestUsers on the workstation, added Red_Team to the permissions for Read and shared the directory as GuestUsers with Read/Write access for the Red_Team. I created individual user accounts and assigned Read/Write permissions to these folders. I setup FTP to allow the "Red_Team" Read/Write access for their individual user directory, but not FTP Root. I pointed the root directory to the GuestUsers share on the workstation. I copied cmd.exe into the root directory and it inherited the read permissions from the folder. In each user directory, I

created a text file, which contained the text, “If you can’t win by playing fair cheat”. I thought I was set.

At this point, I set back and waited. The senior user kept asking if I had searched for the file on his system and of course, I had not. He then asked me to check his Telnet connection on his system by logging into the account set up for me. Each day he asked if I had logged in and since I had not insisted, I did again. After being asked, several times I decided to log into his system via telnet to make sure it worked and attempt to look for the file. I logged into his Telnet server with the user account agreed upon and was able to log straight in. My default directory was a user directory created for me with no permissions, and files. In addition, I was unable to run any command-line commands. After attempting every command I could think of and getting 'command' is not recognized as an internal or external command, operable program or batch file each time I attempted, I logged out and did not attempt again. At this point, he also stopped asking me to log into his system.

The next day, the senior user inquired if I had any luck finding the file. I answered no and asked if he had any luck on my system. He replied, “If you can’t win by playing fair cheat”. My mouth dropped open and with disbelief, I asked how he did it. However, of course he would not tell.

My next task was to figure out how he got in, correct the problem, and change the content of the file to be found. I could not figure how he got in so I use the information below from the IIS.Resource.com website to lock my system down again.

Locking down an NT Server

- Turn off NTFS 8.3 Name Generation
- OS/2 Subsystem removed and POSIX Subsystem removed
- Hide last logon user name
- Use the C2Config tool to hide the last logon user
- Set password length.
- Remove Shutdown button from logon dialog
- Only admins can assign printers/drive letters
- Run SYSKEY Utility
- Rename Administrator account
- Allow network-only lockout for the Administrator account
- passprop /adminlockout
- Set a very strong password for Admin account
- Prevent unauthenticated access to the registry
- Restrict Anonymous Network Access
- Change "Access this computer from the network" from Everyone to Authenticated Users
- Unbind NetBIOS from TCP/IP
- Audit for Success/Failed Logon/Logoff

- Configure Event Viewer Logs to 10 Megs
- Configure TCP/IP Filtering
    1. Permit only TCP ports 80 and 443 (if you have SSL)
    2. Permit no UDP ports
    3. Permit only IP Protocol 6 (TCP)
- Move and ACL Critical Files
    1. cmd.exe
    2. wscript.exe
    3. cscript.exe
    4. net.exe
    5. ftp.exe
    6. telnet.exe
- Set appropriate virtual directory permissions/Web application space
- Set appropriate IIS Log file ACLs
- Logging enabled
- Disable or remove all sample applicationsTechnology

    Location
    IIS
    c:\inetpub\iissamples
    IIS SDK
    c:\inetpub\iissamples\sdk
    Admin Scripts
    c:\Winnt\System32\Inetsrv\AdminScripts
    Data access
    c:\Program Files\Common Files\System\msadc\Samples
- Remove the IISADMPWD virtual directory
- Disable or remove unneeded COM Components

    Be aware that some programs may require components you are disabling. For example, Site Server 3.0 uses the File System Object.
- Remove Unused Script Mappings
- Disable RDS support - There is a known Denial of Service attack when using RDS,

you should either remove the capability or restrict its usage using ACLs. Remove the following registry keys and any subkeys:

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesW3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

- Disable calling the command shell with #exec
- Install MDAC 2.1.
- Re-install NT SP5 (Locking Down NT Server, Internet)

After locking the system down, I changed the file to read, "If you get this one I guess the steak dinner is yours" and informed the senior user I was ready.

He came into work the next day and to my surprise said, "The steak is mine." I was now puzzled and decided to find out what he had done.

WHAT I LEARNED FROM IT ALL

I started my research with Microsoft Technet and after some searches ended up at the www.osp.nl infobase site. This site is full of information on hacking UniX and Windows systems. What really got my attention was the section on how Windows NT passes a hash over the network of the current user if the user logs into a remote system. The hash can then be cracked and used to log into the initial system.

> The standard SMB protocol now used by LanManager and Windows/NT does not send password information directly across the network. Instead, it uses a challenge response mechanism. When a user logs on to a client computer, he/she enters the password. The client computer calculates the password hash value and remembers it for future use. Whenever a client connects to an SMB server, the server generates an 8-byte random value, which it sends to the client. The client uses the remembered 16-byte hash value together with five null bytes to create three 56-bit DES keys (16 bytes hash + 5 bytes null == 21 bytes * 8 == 168 bits == 3 * 56-bit DES key). The 8-byte random challenge is DES-encrypted with each of the three DES keys thereby generating a 24-byte response. This response is returned to the server. The server pulls the user's hash values from its password database and performs the same calculation. If the server's 24-byte answer is the same as the client's 24-byte response the logon to the server is allowed. (Sniffing passwords from the network, Internet)

After seeing this information, I realized I had made three very big mistakes. First, I allowed the senior person to use social engineering to coax me into giving him my current password. Social Engineering is where an individual uses psychological tricks on users of

a computer system to gather information needed to gain access to the system. Many macro viruses sent via e-mail use this method of attracting users. An irresistible subject line requesting a user read e-mail that kicks off a micro virus. (SANS Institute) By the senior user's repeated requests to log into his system, he was able to gain information he needed to gain access to my system. The only way to minimize the problem of Social Engineering is to train your people and provide policy and guidance on what to do if approached by an individual requesting sensitive or usable information. To paraphrase the words of my boss, "Face it, you messed up, you trusted me."

> The first thing that absolutely needs to be accomplished is training, training, and more training. Users and all staff members must be aware that if anyone asks them for their passwords, or any other sensitive information, proceed with the greatest amount of caution possible. People must know that asking a question does not make them inferior or unintelligent and questioning a person's corporate ranking should be rewarded. Put the procedures into written policies and ensure that every user, manager and human being fully understands the methods listed in the policy. Assign a person to train new- hires on their start date so as not to leave that potential weak link available for even a day. When you show that person how to use their phone, explain to them your company policy on Social Engineering. (SANS Institute, Internet)

Next, I was using the administrator account as my primary account and trying to access other systems over the network. This was probably what hurt me the most. Since I was logged on as the administrator, each and every time I accessed another machine on the network, or even over the Internet, my hash was passed to that machine by Microsoft, which contained an encrypted version of my administrator password. At this point, I basically gave the senior the keys to my car.

Last and third, I logged into the senior user's system using Telnet therefore giving him a copy of my administrator credentials in the hash sent during login. All he had to do was to use a software package like L0phtcrack to recover my password from the network logs.

> The Lanman password hash is used by NT for authenticating users locally and over the network (MS service packs are now out that allow a different method in both cases). L0phtcrack can brute-force these hashes (taken from network logs or progams like pwdump) and recover the plaintext password. l0phtcrack 1.5 also breaks the new NT style password hashes. (L0phtcrack, Internet)

There is of course no way to get around sending your hash out to other systems, but by using a user with limited permissions on the system will decrease the amount of power a hacker will have once they get in. All the senior user had to do at this point was sniff my hash off of the network and use Pwdump to crack it. He could then log into my system as administrator and go anywhere I could go to include the workstation shares and see the hidden file.

This little game is what encouraged me to enroll in the SANS certification process. Not only is it important to lock down the systems with permissions, shutting down extra services and filtering ports, it is also important to create guidelines to operate by. One good example is for all administrators to have a normal user account and to utilize it whenever doing normal day-to-day work not requiring privileged use.

After completing the fundamental section of SANS, I firmly believe there are many steps to locking down a system. I also believe it is an ongoing process that never ends.

The first and most important step would be to install a good firewall that has a logging feature. This way you can process the logs to view anyone who has accessed your network. I say this because I have installed a Broadguard Router and Firewall and it logs whoever goes out of the network but not who comes in, as quoted from PracticallyNetworked, "I found the BG to be lacking on these features. You cannot really view any logs via the admin interface. And although the real-time Access Monitor can show you what kind of traffic the BG is currently handling, you cannot get any historical or cumulative view, either via the Admin interface or via Syslog or SNMP logging. There's no logging of admin access, startup, shutdown, or other similar events either" (PracticallyNetworked -2, Internet), as compared to the Linksys Router and Firewall which includes logging, Log viewer software and even the installation of Zonealarm. PracticallyNetworked also says "The logging mechanism added in V1.35 is performed via a standard SNMP Trap message that is sent to the configured machine on UDP port 162. If you are not happy with the Windows logviewer.exe application that you can get from Linksys, you can use any SNMP Trap application to view and archive logs. (PracticallyNetworked -2, Internet)

Whether you use a Firewall or not Zonealarm is a great addition to your arsenal of tools. Zonealarm will allow you to customize for you local network and acknowledge what software enters or leaves your network. Zonealarm's user-friendly interface will prompt each time an application attempts to gain access to the local network in addition to accessing or being accessed from the Internet. A selection will be allowed to allow, deny or permanently allow or deny access for the specific application. Information obtained from ZoneLabs state, "ZoneAlarm Pro provides world-class protection against worms, Trojan horses, and spyware. New Ad Blocking and Cookie Control protect your privacy. With ZoneAlarm Pro, whenever you're connected to the Internet, you're protected." They go on to say,

> Any personal computer connected to the Internet is a potential target. Hackers randomly barrage Internet connected PCs with "pings" or "port scans", probing to find unprotected PCs. Once found, a hacker can compromise your PC with a dangerous Internet threat - Trojan horse, spyware or malicious worm. ZoneAlarm Pro's TrueVector® technology combines a personal firewall with Program Control to protect your PC from intrusions and hostile attacks. ZoneAlarm Pro's firewall barricades your PC with immediate and complete port blocking. And, then runs in Stealth Mode to make your PC invisible on the Internet - if you can't be seen, you

> can't be attacked. Unlike other personal firewalls, ZoneAlarm Pro includes Program Control to protect against known and unknown Internet threats. Program Control monitors all outbound traffic to prevent rogue programs from transferring your valuable data to a hacker. With ZoneAlarm Pro, you're in control with the ability to specify which programs, known or unknown, can be trusted to access the Internet. (ZoneLab, Internet)

After setting up a firewall, a good look should be taken at blocking ports from port scans and access from external networks, unused services should be disabled. Services are applications that run in the background of Windows NT and execute even while no user is logged on. An individual could potentially access a system with no user logged on and cause a disruption to a service. Creating a portal or backdoor into a system or allowing execution of malicious code. Such entry could go unnoticed for an undetermined amount of time.

Not to be overlooked is the addition of some type of anti-virus software. Every system no matter what the purpose should run software that can detect and inoculate viruses from its system. Many professional software venders provide a solution to this problem, but it is more of a game than a profession. I compare this to the days of the Commodore 64 with its copy-protected software, which deterred the normal user from duplicating software for the purpose of either backup or distribution. For a long, time this worked fine. Until individuals and soon to be companies discovered the law stated one backup could be maintained of any software purchased. Enter the copy software; copy software was developed to allow users to easily copy copy-protected software for backup purposes. Now the race was on. Every time a new type of copy-protection method was developed, the copy companies were off on a venture to defeat it. Today it is the same with anti-virus software and the virus creators. Each is competing to develop a product that can defeat the other. A good example of an anti-virus solution to protect the whole network is the AVStripper by OSITOS. A description provided by the OSITIS web site is as follows:

> AVStripper installs as a network bridge and scans all passing traffic for viruses. Installation is a simple matter of inserting AVStripper between your firewall and your network. The product needs no configuration of client computers, proxy servers or firewalls and scales for enterprises of any size.
> AVStripper provides protection for customers with networks ranging from 25 clients to enterprise level. Installed at the Internet gateway, AVStripper provides a perimeter of defense, scanning seven protocols including; HTTP, FTP, SMTP, News, IMAP, POP3 and SOCKS. All pattern files and engine updates are completed automatically every three hours. AVStripper protects the network at the gateway rather than relying on desktop protection. While users can disable desktop protection or forget to update their pattern files or scan engine, AVStripper is always up to date and scans all incoming and outgoing traffic – preventing viruses from entering the network in the first place. If a virus does enter the network, AVStripper reduces liability and integrity concerns by preventing

users from sending the viruses to your partners or customers.
A key concern with malicious code is that it can be used for several purposes. There are three basic types of attacks: Intrusion, destruction and denial of service. All three of these attacks can and often are carried out with viruses. Intrusion is done with back-door viruses like BackOrifice or NetBus. Destruction happens with viruses such as CodeRed or Sircam. Denial of service is accomplished with viruses like Melissa or Nimda. Without the AVStripper gateway antivirus solution, a firewall alone will not protect your company against these attacks.

Last but for sure not least is the need for Policy and Guidance. I never even thought about the danger of logging over a network while logged in as administrator or being convince by my senior to log into his system could in turn have an effect on my system. I took pride in locking down my system, setting permissions on files and folders, disabling ports, running Zonealarm and critically allowing and/or disallowing services or applications to access the local network or the Internet. The thing I did not think of was I would be the weak link in the chain and actually gives the key to my system away through my NT Hash. I now realize the importance of setting policy and guidelines for all users, privileged and normal to follow and adhere to. Microsoft's Technet suggests and provides some good advice on maintaining security within a network. First, they say to keep pace with changes that might require new security measures. For example, e-commerce will require encryption of private information sent over the Internet. Next, they say to identify and assess threats to the security of online systems. For example, if you open your intranet to access by others, their user IDs and passwords are assets that will be made vulnerable to the threat of exposure on the Internet. Then prioritize threats according to potential exposure and recovery costs. For example, if you allow customers to purchase services from your Web site, determine what assets would be exposed and what the cost would be to secure them. In the continuously developing and emerging online environment, accurate threat assessment is vital to achieving cost-effective security for information shared over the Web between you and others, as well as among your business partners and customers. (Microsoft Technet, June 2001)

After being "Hacked", either socially of physically by my senior I have taken a complete new look at security. The importance of a security system that starts at placing a hardware firewall at the outer parameters of a network, and adding layers by disabling unneeded applications and services, blocking ports that are not used, installing antivirus software, and setting rules for all users to follow will be forever imbedded in my mind. The words of my boss, "Face it, you messed up, you trusted me" will always be a phrase I will live by when faced with providing any information to friend or foe.

SELECTED BIBLIOGRAPHY

CTF Capture the Flag
Internet: http://www.captured.com/threewave/

ZDNET Contest Capture the Flag
Internet: http://www.theregister.co.uk/content/1/11625.html

NTFS Permissions
Internet: http://www.windowsitlibrary.com/Content/592/toc.html

Locking down an NT Server,
Internet: http://www.iis-resources.com/Build_Docs/lockdown.html

Sniffing passwords from the network
Internet: http://www.osp.nl/infobase/ntpass.html#sniff1

SANS Institute
Internet: http://rr.sans.org/social/social.php

L0phtcrack 1.5 Lanman / NT password hash cracker
Internet: http://www.insecure.org/sploits/l0phtcrack.lanman.problems.html

Broadguard Review
Internet: http://www.practicallynetworked.com/reviews/soho_broadguard.asp

Linksys Review Internet:
http://www.practicallynetworked.com/support/linksys_router_help_pg4.htm#logging

ZoneAlarm Home Page
Internat: http://www.zonelabs.com

Virus Protection for Your Entire Network
Internet: http://www.ositis.com/english/products/avstripper/pd_avstripper_en.asp

Microsoft Technet, June 2001 Appendix B. Site Planning Security