Global Information Assurance Certification Paper

Narrowing the Path to your NT Servers in the Wide-open Highway of Higher Education Networks: A look at Securing NT Services in an Open Network Environment

Steven A. Boren, Jr.

GSEC Practical Assignment Version 1.2d

Network security is receiving much needed attention lately. Hackers and crackers with a widely varying knowledge base are constantly breaking into networks and computer systems if for no other reason than to brag to their cohorts. In order to provide an open environment for students and faculty to perform their research, many universities maintain campus networks that are relatively open and do not block network traffic either to or from the Internet making it extremely easy for this kind of malicious activity to take place.

Working for a relatively small research center or department in a large public university presents many obstacles when it comes to securing the Windows NT-based network that is provided for users. The University as a whole has a very large IT organization that provides central services for students, faculty, and staff but when it comes to providing services to individual departments there are voids that are best filled by hiring departmental staff and setting up departmental servers.

The research center of which I have been a part for over three years is made up of over 150 users who require many computer related services that are supported both locally and remotely. We provide local email, web services, file server and print services, backup services as well as remote access via dialup and the campus wide area network. All of this is done with a small staff that must balance an already heavy workload and take on the responsibilities of making sure the network services are secure and constantly available with little to no help from the campus networking staff.

Although not an easy task, there are many steps that can be taken to minimize the threats to a network while still maintaining the needed open environment required by the students and faculty in higher education.

Security Policy:

If there is a centralized Information Technology department in your university, there will most likely be some sort of policy in effect that sets general guidelines for the campus. The University of Colorado at Denver offers a comprehensive Information Security Handbook that can be used as a model. It is imperative that if an administrator is going to run port scans on their subnet and run password crackers, as will be discussed below, that these topics be

discussed in the security policy in order to inform users and other systems administrators of the implications. If these topics are not covered in the campus wide security policy, perhaps a departmental addendum is necessary so that departmental users know what to expect and to warn administrators that such activities may be authorized.

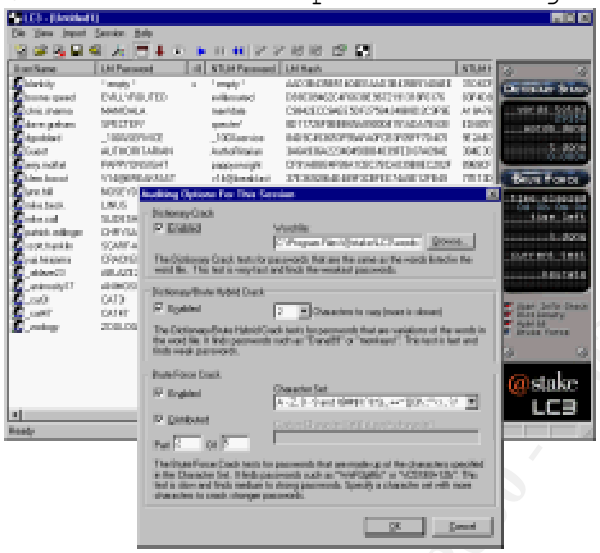
Virus Detection:
As systems administrators are well aware, it is not possible to keep all viruses off their users' systems. Antivirus software is no longer an option it is a necessity. If an administrator only has to deal with a small number of servers and systems he or she might be well served with "single user" antivirus packages. For departments that have many servers and computers, the best protection from viruses is delivered when a centrally managed network based Virus detection package is purchased. These packages, such and Computer Associates InoculateIT and McAfee Active Virus Defense are installed on the servers as well as all the workstations in your department. They have a logging system so that you have a record of any viruses detected on your network and they have the ability to update the virus definitions to all systems from the management console.

Passwords and Password Monitoring:
A system is only as secure as its weakest password. When preparing your security policy, it is necessary to include several points on use and makeup of passwords. First it must be stressed that passwords are not to be shared. Additionally, the complexity that will be required of the systems passwords should be set up in the security policy. Most passwords can be made up of four groups of characters consisting of lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters such as !#$%()^*&~. Windows NT can be set to require that each password be of a minimum length as well as contain at minimum characters from more than one, two, or three of the listed groups. In order to promote better password security, a password should be made up of at least three of the different character groups.

In order to monitor the passwords that users choose, a password cracking application should be utilized. A widely available Windows password-cracking application is l0phtcrack or LC3, as it is now known since it was recently acquired by @stake, Inc. You should regularly run

password-cracking software against your domain passwords. When doing so, set the software package to break only passwords that are less secure than your required level of complexity so that the check will complete in a timely manner and to maintain the secrecy of the passwords that are properly secure. The level of password security is something that is easily set in the options of LC3 as seen in figure 1. However given enough time, any passwords can be cracked using unchecked brute force.

Figure 1.
@stake LC3 and Options dialog box

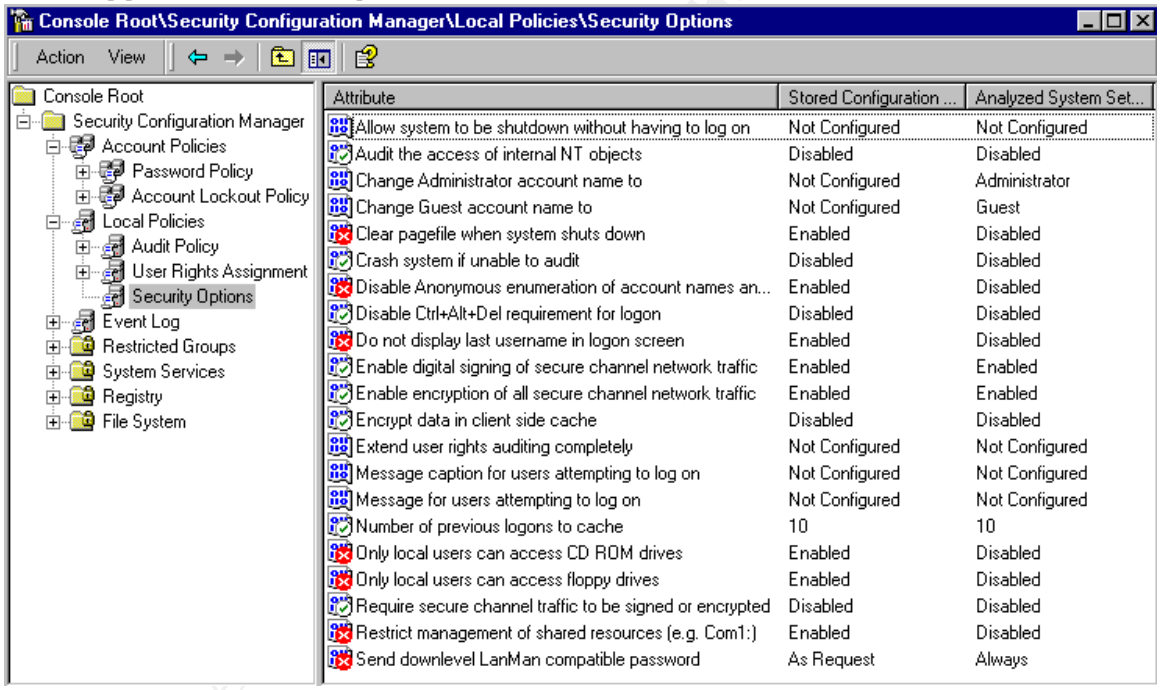


Hardening and Updating Systems:

Although it is possible to configure Windows NT as a very secure operating system, the default installation leaves much vulnerability which should be addressed. The process of disabling unneeded components of the operating system and applying Service Packs and hotfixes to eliminate known bugs and vulnerabilities is called hardening a system. Microsoft provides guides as well as tools that can be used with both Windows NT and Windows 2000 to harden the system. Many of the customizations that need attention can only be adjusted in the registry so the SCE or Security Configuration Editor by Microsoft offers an easily used graphical user interface to update these settings. The SCE is available from Microsoft's FTP site at ftp://ftp.microsoft.com. Setting the password policy for your domain (figure 2) or comparing your current settings to the Microsoft suggested settings (figure 3) are just a few of the many capabilities of the Microsoft SCE.

Figure 2.
Microsoft SCE Application editing Password Policy

Figure 3.
Microsoft SCE Application comparing current configuration to suggested configuration



Additionally, there are several references that cover the topic of system hardening. One is freely available from Microsoft and others published by SANS.org and by O'Reilly & Associates, Inc. are much more detailed.

Vulnerabilities are being discovered at an alarming rate. Once a system is set up and hardened, it is necessary to apply Service Packs and hotfixes as they become available. Microsoft and others offer mailing lists, generally free of

charge, that send email notification when a vulnerability is found or an update is available.

Keeping up to date with Security:
In order to keep current on your system patches and hotfixes, there are several mailing lists to which you should subscribe. Microsoft Windows administrators should definitely join the Microsoft Security Notification Service. This service is offered free of charge by Microsoft and notifies the subscribers of any new security vulnerabilities that are found. This is a very active mailing list and when a vulnerability is detected that affects any installed systems you should quickly evaluate the hotfix and apply it if needed.

There are many mailing lists and web sites available that provide a wealth of information to those interested in security issues. The SANS.org Security Alert Consensus is available both at http://www.sans.org/newlook/digests/SAC.htm and as a mailing list that can be personalized to users particular needs. The Security Alert Consensus provides a wealth of information on recently discovered Operating System and application vulnerabilities. SANS.org also provides a Weekly SANS Newsbites digest available both at http://www.sans.org/newlook/digests/newsbites.htm and as a mailing list that highlights security related issues that occurred over the last week. The Software Engineering Institute at Carnegie Mellon University houses the Federally Funded CERT Coordination Center. The CERT/CC provides a great deal of research on Internet security as well as publishing security-based alerts. The CERT/CC web site available at http://www.cert.org and its alerts contain a great deal of security information.

Host Firewall software:
Since universities may not be as compelled to set up firewalls, blocking traffic in and out of the campus network, the burden of doing so generally falls to the individual departments. Without the support of the campus wide network staff, personal or host firewall software might end up being the best option to protect workstations and servers. It's rather obvious why administrators would want to have some type of firewall software on their servers. Windows servers that are currently being installed have increasingly fast processors, large amounts of RAM, and many gigabytes of hard drive storage. If

hackers can gain access to these large resources, they can use it for their own gain or enjoyment.
There are now several companies that are offering Server Host firewall applications. Network-1 Security Solutions, Inc. has a program called CyberwallPLUS and Network Ice Corporation offers its ICEpac Security Suite. Both of these programs offer centrally manageable host firewall applications for servers and workstations alike. For administrators who have all user files stored on the server it might not be readily obvious why personal firewall software would need to be installed on workstations. After all, if a workstation were compromised the applications would be relatively easy to reinstall. The problem with a compromised workstation is not the potential to destroy local data but more likely the potential to gain access to the more valuable network resources or to use the workstation to mount attacks on a third party. More and more hackers are gaining control of workstations with Internet access and they are using them as a stepping-stone to attack other systems in order to better hide their own identities.

Intrusion Detection and Port Scanning applications:
Once a system or network of systems has been set up and made to be as secure as it can be, it is necessary to monitor the systems on a regular basis to make sure that its secured status is not compromised. In addition to the commercially available software packages there are several applications available as shareware or freeware. In many cases these are the same applications that hackers use to determine the vulnerabilities in systems. Programs such as Nmap, a freely downloadable network port scanner available at http://www.insecure.org/nmap/index.html, is widely known for its network and port scanning capabilities. Both network administrators and hackers use Nmap to evaluate and determine vulnerabilities in network systems.

Although securing a network with a firewall system and all available network security procedures would be the preferred method, it is not always that the environment provides a way to do so. In the case of Higher Education and its research demands that require a more open and available networking environment, it is easy to see why campus network personnel find it difficult to provide a perimeter network firewall. This being the case, it does not excuse the need for local security on a departmental basis. The more roadblocks that are set up on a network to

thwart would-be hackers, the better the experience is going to be for all the legitimate users connecting their systems to the internet.

References

@stake, Inc. "LC3 – The Password Auditing and Recovery Application." 2001. URL: http://www.atstake.com/research/lc3/index.html

Carnegie Mellon University, Software Engineering Institute. "CERT Coordination Center." 29 MAY 2001. URL: http://www.cert.org

University of Colorado at Denver. "CU-Denver Security Handbook." 2 Jan 1997. URL: http://thunder1.cudenver.edu//admin/securtoc.html

Computer Associates International, Inc. "InoculateIT Workgroup/Advanced Edition Product Description." 9 April 2001. URL: http://www3.ca.com/Files/ProductDescriptionBrochure/inoculateit_workgroup_pd.pdf

Insecure.org. "Nmap – The Network Mapper." 10 Mar 2001. URL: http://www.insecure.org/nmap/index.html

McAfee.com. "McAfee Active Virus Defense Brochure." URL: http://a1472.g.akamai.net/f/1472/1207/15m/download.mcafee.com/products/biz/services/avd/avd_Brochure_1-2.pdf

Microsoft, Inc. "MS Security Configuration Manager for Windows NT 4" 12 Jan 2000. URL: http://www.microsoft.com/technet/winnt/winntas/technote/scmnt4.asp

Microsoft, Inc. "Product Security Notification." December 2000. URL: http://www.microsoft.com/technet/security/notify.asp

Microsoft, Inc. "Security Tools and Checklists" 23 May 2001. URL: http://www.microsoft.com/technet/security/tools.asp

References Continued

Network-1 Security Solutions, Inc. "CyberwallPLUS Firewalls – Access control, Intrusion Detection." 2001. URL: http://www.network-1.com/products/index.html

Network ICE Corporation. "ICEpac Security Suite." URL: http://www.networkice.com/products/icepac_suite.html

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. Sebastopol: O'Reilly & Associates, Inc., January 2001.

SANS Institute Publications. "Windows NT Security Step-by-Step." 5 March 1998, updated monthly. URL: http://www.sans.org/newlook/publications/ntstep.htm