Global Information Assurance Certification Paper

Jeffrey C. Benfield
June 8, 2001
SANS Security Essentials GSEC Practical Assignment Version 1.2e

The Enemy Within An Assessment of Security in a Community College

Introduction

This paper will present an audit of the security practices at a Community College in North Carolina and some of the security problems that are inherent in an organization of this type. Most of the issues I will site are not unique to a college environment, in fact I think they are quite common, but they do seem to be more prevalent in this environment. I will discuss the problems I found and the steps that have been or will be taken to correct the issues. I will conclude the paper with a brief analysis.

Background

A Community College has a very mixed user community. In terms of technical skills the user base varies from computer science professors to those who are completely computer illiterate. In political terms the user base varies from professors who are free speech advocates to financial auditors that advocate strict control. There are approximately 160 faculty/staff users and a student user base that varies from a few hundred to over a thousand. From a security standpoint the range of viewpoints and types of users are not compatible. With this in mind, after attending a recent SANS GIAC Security Essentials Course I performed a security audit of the college using the principles set forth in the course.

The physical campus network is composed of approximately 600 PC's and 21 servers connected via 10 MBS Ethernet using a combination of fiber and copper for the physical media. The operating systems used on the network include: MS Windows 9X, Windows NT 4.0, Windows 2000 Professional, and Mac OS 8.X. Network operating systems include: Microsoft Windows NT 4.0, Novell Netware 4.11, and Sun Solaris 2.6. There is a dedicated T-1 connection to the Internet that goes through a Cisco PIX firewall. There is a Microsoft Windows NT based web server that sits outside the firewall. The network is primarily used for file and print sharing, e-mail, Internet access, central administration database access, and distance learning.

Audit

Documentation and Policy Audit

I started the audit by assembling all documentation and policies and procedures that concerned the network and security, both from a physical and a logical perspective.

- *Documentation*: I found very little documentation of the Windows NT network other than the information that can be found in the User Manager applet. I did find some documentation for the Novell and Sun servers dealing with user account creation. I also found extra information with the

Novell NWAdmin applet and the Solaris admin tools applet.

- *Policies and Procedures*: I found the following policies that dealt with network security: *Computer and Network Usage* this policy specifies that a user will have a password and that it is their responsibility to protect the password and that campus computers will only be used for official business*, Accountability for Property* this policy says that all employees are responsible for protecting equipment in their charge*,* and *Copyright, Computer Software* this policy says that employees will not illegally copy or distribute software.

Policy Compliance Check

Policies in place are very limited and checking for compliance was relatively easy.

- *Computer and Network Usage*: I looked in the User Manager applet of Windows NT on the Primary Domain Controller for password information. The settings on the accounts page were minimum password length 5, password never expires, allow immediate changes, do not keep password history, and lockout account after 3 bad attempts. With these settings the NT system does comply with the policy. I checked the Solaris passwd file and found that password aging was set at 60 days I checked admin tools and found that passwords required a minimum of 7 characters and must include 1 numeric. With these settings the Solaris system is in compliance. I checked the Novell system through NWAdmin and found that passwords were not required, there was no aging, uniqueness is not enforced, and bad login attempts are not tracked. With these settings the Novell system is not in compliance.
- *Accountability for Property*: A physical inventory of all fixed assets is performed every year and unoccupied rooms are locked so the school is in compliance with this policy.
- *Copyright, Computer Software*: Metering software is in use so for networked computers so the school is in compliance with the policy. Non-networked computers are the responsibility of the user and compliance is assumed. This is not a true security policy issue per se and so will not be covered any further in this document.

There are many items of specific password security that are not covered by the policy and they will be discussed in the next section of this document. There are inadequacies in the other policies that will be covered later. Unfortunately there are several areas that are not covered by either policy or documentation.

Security Problems Not Covered By Policy

Passwords and Account Sign-On

The policy only mandates that passwords will be used so even in areas that are in compliance the password policy is extremely weak, this is particularly true in the Windows NT area. Specific security weaknesses not covered in policy are as follows:

- *Minimum Password Length*: Current policy does not set a minimum

password length nor does it require that at least one numeric character be used in passwords. The Windows NT system has a minimum password length of five and no tool is used to force strong passwords i.e. those that include non-alpha characters. A five-character password that is all alphas can be at most one of 1.49 e18 possible passwords. This may seem like a lot but with modern password crackers such as lopht crack it would not take very long using brute force on a Pentium IV 1.3 GHz machine to crack any password that met these requirements. If a non-alpha character was required the total possible number of passwords goes to 2.27 e 29 a very significant increase. If minimum length is raised to seven and requires non-alpha, like the Solaris requirement, the total number goes to 3.12 e 35.

- *Maximum Age of Password*: Current policy does not cover maximum age of passwords. Even with strong passwords, such as those that use seven characters and non-alpha, if they are not changed they will eventually be broken.
- *Password Uniqueness*: Without uniqueness being required the user can use the same password over and over and in effect get around any aging requirements that might be set for passwords.
- *Minimum Age of Password*: Even if uniqueness is required, if minimum password aging is not set the user can immediately change the password as often as they want and get around uniqueness requirements.
- *Account Lock Out*: This is not required in policy but is in place in two of the Network Operating Systems. Account lock out and bad attempt counts at least provide minimum intrusion detection for no cost.

Implementing these changes in password policy is difficult in this environment for several reasons but primarily user reluctance. A classic example of this is e-mail account passwords. When a user is given an e-mail account there login is first initial and last name and the password is the same. Users are told they should change their password but since it is Novell based it is not required. As a test I randomly picked 25 e-mail accounts from our campus and tried to get into the accounts using the default password I was successful 17 times, or 68% of my attempts. I discussed it with several of the users and I was told that it would be too difficult to remember the password if they changed it plus “no one would guess the password anyway.” I pointed that a student with a grudge might guess their log in and use it to send offensive mail to a college executive in their name. This argument seems to have worked; I tested the same accounts one week later and was only successful three times.

Another problem with strong password policy implementation here is lack of a single sign-on. This is not a security issue per se but it does lead to security problems. At present users have a separate password for NT, Novell, and Solaris the stronger these three passwords are the more likely they are to write them down. At present a single sign-on product from Novell is being evaluated to alleviate this problem.

I have created a committee of faculty, staff, and IT to come up with a new password policy that is acceptable to the user and provides sufficient security to

protect college data. The recommendations of this committee will be implemented as policy. Specific procedures for account creation and enforcement are being created by each of the system administrators.

Computer and Network Usage

There are several potential security problems not covered by policy in this area:

- *Firewall Settings*: There is no policy in effect for opening or closing holes in the firewall. At present if a user cannot get to something on the Internet and they think it is a firewall problem they contact the firewall administrator and ask him to open a port. The decision of whether or not to open the port is left solely to the discretion of the administrator. Also there is no documentation of the ports that are open on the firewall other than by doing a *write terminal* from the IOS prompt. A committee of IT and college administrators are working on recommendations for a firewall policy. This policy is essential to protect data, the administrator, and to protect the users from the administrator. In a campus environment this policy is difficult because faculty feel that academic freedom gives them the right to use any Internet resource they choose regardless of the consequences. This will be primarily an issue of educating the users on why we have a firewall and what it does.
- *Anti-Virus Software*: Anti-Virus software from Command is loaded on all campus machines but its use is not mandated by policy. When the software is installed it is set to automatically scan all files for viruses but this feature is easily turned off, and frequently is. Nothing addresses opening unexpected attachments. In the past we have had a few infections caused by users blindly opening attachments that had viruses i.e. “Snow White.” When I have asked why a file was blindly opened I was told it was not their responsibility to make sure the file was clean, which under current policy unfortunately is correct. Definition file updates are not mandated by policy. At present the NT administrator puts out the updated def files and they are loaded by log in script commands. However, the administrator is not required to by policy to do this. I am writing a policy on Anti-Virus software and its use and am preparing training classes for the users on the software and viruses in general.
- *Network Configuration*: At present the network is a flat TCP/IP network that uses three subnets interconnected by routers. This is an inefficient arrangement and a dangerous one. To protect the college database and faculty/staff files Virtual Private Networks (VPN) should be setup to segregate student machines from the rest of the network. We have not had any attempts to break into the administrative database which resides on the Solaris box, but students are curious and it is only a matter of time. When I have asked faculty about this I have been told, “our students are adults and they wouldn’t do this.”
- *Intrusion Detection*: Current policy and procedure do not mandate intrusion detection and at present intrusion detection is minimal. The only real detection in use at the moment is account lock out on NT and

Solaris and scripts that look for accounts that do not fit the requirements set in Solaris admin tools. These scripts are locally written and look for accounts with a UID of 0 (root), accounts with no password, and accounts that have no expiration. The scripts are as follows:

Root User Script checks for any login using Root UID of 0
awk -F: '{if ($3 == 0) print $1 }' /etc/passwd
Script for finding accounts that do not have a password
awk -F: '{ if ($2 == "") print $1}' /etc/shadow
Script for finding accounts that do not have a password expiration date
awk -F: '{ if ($5 == "") print $1}' /etc/shadow

To correct the lack of intrusion detection TripWire for Servers 2.4 is being implemented on the Solaris server and all Windows NT servers.

- *Laptops*: There are approximately 60 laptops in use within the organization and there is no policy on configuration, anti-virus software, use, or remote access with these devices. This is a very serious security concern because of the mobile nature of the devices but is difficult to correct because they are primarily used by administrators who believe they know what they are doing and do not need policy to tell them how to do it. I am working with an executive committee to write a policy on laptops.
- *Account Creation*: There is no current policy on account creation or deletion. Accounts are created based on the feeling of the administrator as to what rights and privileges are required for the user. There is also no documentation of what accounts have been created and why. This makes it very difficult to control accounts. We are now in the process of auditing all accounts to make sure they are valid and have only the necessary rights. As an account is audited it is documented. A committee of personnel from the major campus departments is working on recommendations for account configurations for their departments.

Documentation Problems

The lack of documentation is a major concern. As stated previously in the paper there is no documentation of accounts there is also no documentation of the physical network. We have started a project to document accounts but it will be a long process and the IT staff is reluctant to do it because of the work involved. It is very difficult to detect physical changes in the network when you do not have a baseline to start with and compare against. It is also very difficult to implement changes that would enhance security, such as VPN's, without a current network map. I have started a project to map the network prior to implementing VPN's but IT staff and college administration are hesitant because they don't see the benefit of the map. There is no documentation of equipment configuration such as the firewall, printers, web servers, etc. Here again without this documentation a baseline cannot be created and changes to the configuration are difficult if not impossible to find.

Analysis

There are many issues that surfaced during the audit some of which are very serious, but they can be corrected. Some corrections have already been put in place TripWire is loaded on several servers, the firewall has been documented and the policy is awaiting approval, Windows NT account policy has been changed to require a minimum password length of seven and all passwords expire in 60 days, and Novell account policy has been changed to require passwords and 60 day expirations. Other changes will take much longer account documentation, network mapping, and policy writing. Probably the most difficult thing to correct will be user attitudes, this does include IT. Security is important to the survival of the college and some attitudes on what constitutes academic freedom may have to change.
The bottom line is that we have several problems that require immediate attention but they are not equipment or technology issues, they are people issues. We have to change the way we look at security as an institution if we are to protect our students and ourselves. In terms of security, at least at this college, we are probably the biggest enemy we face.

Sources:

Gordon Howell. "Managing Internet Security Understanding the real risks & defences in exposing corporate networks to the internet." October 10, 1998. URL: http://www.ibsc.co.uk/conferences/infosec98/InfoSec98/

Unknown. "Play IT Safe A Practical Guide to IT Security for everyone working in General Practice, NHS Information Authority." January 13, 2000 URL: http://www.standards.nhsia.nhs.uk/library/sdp/safe/home.htm

Maurene Grey and Joyce Graff, Gartner Analysts. "Complacency now the worst enemy." June 04, 2001 URL: http://www.techrepublic.com/article.jhtml?src=search&id=r00120010604ggp01.htm&adSiteNameOverride=bc&adPageNameOverride=Security

Matthew Mercurio. "Get your IT staff involved when creating firewall policies." April 04, 2001 URL: http://www.techrepublic.com/article.jhtml?src=search&id=r00320010404mer02.htm&adSiteNameOverride=bc&adPageNameOverride=Security

Richard Ford. "I'm Protected. Right?" Unknown, URL: http://www.commandsoftware.com/virus/dwelling.html

Cisco Systems. "Increasing Security on IP Networks." April 26, 2001 URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Evi Nemeth, Garth Snyder, Scott Seebass, Trent R. Hein. "UNIX System Administration Handbook." Prentice Hall PTR 1995

Unknown. "Microsoft Windows NT Server Networking Guide." Microsoft Press

1996

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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
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 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
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 Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor