Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Access: Making Passwords a Legitimate Corporate Defense

Being forced to select a new password can be a frustrating experience for users. By the time they've memorized their latest secure (or favorite, but insecure) password, "The System" forces them to change it again. Users don't necessarily care about security issues; they just want to get their work done. It's your role to ensure that system and application passwords are secure from both internal and external attacks. Making that easy for users is critical. All this causes you to lose sleep at night. This paper outlines ...

Copyright SANS Institute

Author Retains Full Rights

AD

Securing Access: Making Passwords a Legitimate Corporate Defense

Submitted by: David H Sherrod
GIAC UserID: dsherro001
SANS Security Essentials
GSEC Practical Assignment Version 1.2f (Amended August 13, 2001)
Original Submission
Conference Course Certification (Chicago SANS Conference, November 5-10, 2001)

Introduction:

Being forced to select a new password can be a frustrating experience for users. By the time they've memorized their latest secure (or favorite, but insecure) password, "The System" forces them to change it again. Users don't necessarily care about security issues; they just want to get their work done. It's your role to ensure that system and application passwords are secure from both internal and external attacks. Making that easy for users is critical. All this causes you to lose sleep at night.

This paper outlines four easy steps to secure access to your systems using strong passwords, even those selected by users. Briefly, these are:

- Have a password policy and standards, and supporting procedures.
- Educate your users.
- Utilize your help desk personnel.
- Perform audits.

This paper does not present further methods of securing the network around passwords. For examples of these, see Jason Mortensen's excellent paper, "Password Protection: Is This the Best We Can Do?[i]"

After reading this paper, you will have the information you need, with a reasonable plan of "attack," to secure critical company information while enabling secure access for your users.

Make it a Policy:

To being at the beginning, it is necessary to create a policy for the company concerning securing access through the use of passwords. Many systems, particularly operating systems and corporate off-the-shelf applications, require the use of a password. Unfortunately, few of these systems, by default, require the user to construct a strong password. Actually educating the users with respect to password selection is addressed in the next section. Before such education can begin, however, a corporate policy must exist as the foundation upon which to base the education and other important activities that serve to secure access.

A good "policy" has four aspects to it[ii]. First, there's the policy itself. Second, standards must be specified (although they may vary from department to department). Third, procedures for implementing the policy need to be outlined. Finally, ways to handle the ever-present exception should be addressed.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A Policy is a high level statement that makes reference to one or more Standards statements.[iii]

A policy that addresses passwords should include high-level statements that the entire company is expected to follow, regardless of departmental or operating system differences. These statements should change infrequently over time. Some example items suggested for inclusion in the policy are:

- All accounts with administrative access to an operating system or application must have their password reset a minimum of once every 3 months.
- All user accounts must have their password reset a minimum of once every 6 months.
- Passwords must not be shared for any user account.
- Passwords may not be transmitted electronically (i.e., via e-mail or fax machine).
- Passwords must conform to the minimum corporate password Standard.
- The company will periodically audit user passwords to ensure compliance with this policy and all applicable standards. Such auditing will be performed in such a manner that no person will have access to an individual employee's password.

The last policy point is important. Many programs exist (most notably LC3[iv]) which enable administrators to test the strength of a password file with or without gaining visibility to the actual passwords. Due to legal considerations, it is strongly recommended that no employee be allowed such visibility, that the policy clearly state so, and that those with permitted access to any such auditing program use it in the presence of another person, with both documenting the activity and results.

Standards outline specifications and will be different from department to department[v]***.***

A standard outlines more specific information for different parts of the company. There should be a minimum corporate password standard, and it should include statements such as:

- A password cannot be a word found in any published dictionary (regardless of language of publication).
- Passwords should not be or include family names, pet names, job titles, system or machine names.
- Passwords may not be the same as userIDs used to access a system or application.

The minimum corporate password standard contains statements more likely to change as technology changes. When creating your minimum standard, you should include the least common denominator for password construction as well. For example, if you have an older Unix OS, all printable characters are available to your users when selecting a password (this is good), however, only the first 8 characters of that password are actually stored by the OS (this is unfortunate). If your minimum corporate standard requires 10 character passwords, you will immediately have an exception, and great frustration from your systems administrators as well as your users. Set yourself up for

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

success by knowing the password capabilities of your systems and applications before crafting this standard.

Some standard operating system restrictions include[vi]:

- Novell: Use of all printable characters, case is NOT significant, password length up to 256 characters.
- UNIX: Use of all printable characters, case IS significant, password length up to 8 characters.
- VMS: Use of all printable characters, case is NOT significant, password length up to 32 characters.
- Windows NT: Use of all printable characters, case IS significant, password length up to 14 characters. (Beware, however, of a security "hole" relating to default LAN Manager authentication[vii].)

Standards may then be crafted for individual applications, operating systems (OS), and departments. If an application or OS allows for more diversity in creation of a password, raise the bar for your users (and potential internal or external hackers) by requiring through an application or OS standard that the password include more varied characters.

A Procedure is a set of instructions based on OS, application, user, etc[viii].

Many procedures should be written to show how the company abides by and enforces the password policy. These procedures should include, at a minimum:

- How users initially set passwords for any application and/or OS they access.
- How users change passwords within any application and/or OS the access.
- How users can request that their passwords be changed (by help desk, manager, or other auditable third party).
- How the help desk (or other appropriate party) will convey new and/or changed passwords to users.
- How auditing of passwords will be handled to ensure that the policy and applicable standards are being followed.

Exceptions must be accounted for.

Executives are typically the worst when it comes to password policies. They frequently want to be *exceptions to the rule*, having set passwords that expire never, or, at best, infrequently. Unfortunately they usually have access to some of the most desired information within your company. Depending on your position and their demeanor, it may be a career-ending move to require that they adhere to the policy. Your best bet is to document possible exceptions, incorporating as many of the requirements of the policy as possible. For example, requiring the strongest passwords for executives, but showing them how to easily create one (see the next section on User Education), may be your most prudent move.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Other exceptions may exist if your least common denominator is being brought extremely low by one or two systems. Raising that bar for all other systems, but providing an exception for these few (usually older) systems, will provide greater security across the entire corporation. Keep exceptions to a minimum (if you have too many, revisit your policy, standards, and procedures), but recognize that they do and will exist!

An example of a password policy that includes both a policy statement as described above, and standards and procedures (listed as guidelines) is available online from the SANS Institute at http://www.sans.org/newlook/resources/policies/Password_Policy.pdf.

User Education Pays:
When the construction of a password is left to the mind of the user, they invariably will choose the path of least resistance when it comes time to recall that password. In mid-2001 researchers in Britain (at the bequest of the Internet domain name registry CentralNic) determined[ix] that there are four types of people when it comes to choosing passwords:

1. Family-oriented users. These users select their own name, their nickname, or the names of their partners, children, or pets for the password. They represented nearly half of the study's participants.
2. Fan users. These users select the names of sport stars, cartoon characters, or pop icons. They represented nearly 1/3 of the participants.
3. "Self-Obsessed" users. Selecting passwords like "sexy," "stud," and "goddess," these users represented 11 percent of the participants.
4. "Cryptic" users. Your gold standard, these users selected strong passwords utilizing mixed case characters, numbers and punctuation. Unfortunately they only represented 9 percent of the participants.

The main reason people create weak passwords is because nobody ever explained to them how easy it is to craft strong passwords. Policies and Standards that require a combination of mixed-case characters, numbers, punctuation, and possibly control (non-printable) characters often confuse users. If they do "follow the rules," they often create a greater security risk by writing down their new "secure" password and storing it under their keyboards, mouse pads, or phones (if they hide it at all!).

It is important, therefore, to educate users about the password policy, related standards, and procedures, using language and examples they can easily relate to. Showing the user strong examples that are easily created and remembered is critical to the success of your password policy. Here's an example that has proven successful at several companies:

First, have the user select a short phrase. It can be from a favorite song, movie, or book, anything they'll remember. For an example, use "Choosing a strong password is *Easy*." Ask them to use only the first letter of each word in the phrase. In the example this yields "CaspiE." This is definitely not a dictionary word. Point out the use of different capitalization to provide emphasis in the phrase.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Second, have the user select a single-digit number. Suggest they use the last digit of the year they were born, or of their home phone number, or zip code.

Finally, have them select a non-alphanumeric character from the keyboard. It's useful to display to them (in a presentation or employee manual) the characters you're talking about. For ease, you might just show the characters that appear above the numbers on a standard keyboard.

Now show them how to put these together. One possible example is: **Cas3piE#** Ensure that whatever examples you chose to show adhere to the policy, standards, and procedures that are in place. Avoid the exception during user education!

Ensure that you also educate employees about the procedure for resetting a password at this time as well. Most employees will still have concerns that they'll forget the "Easy and Strong" passwords they're forced to create every X months. You can help put their mind at ease by explaining that password resets are to be expected, and that someone (their help desk) will be available to assist them if and when necessary.

Your user training and new employee manual should also explain why strong passwords are important, and why the policy and standards are so specific. An often cited example[x] on the web includes instructions in question and answer form, including (with others):

- What is a password, exactly?
- What is password security?
- Why is password security important?
- Why can't I tell anyone my password?
- Why can't I write down my password?
- How can I tell if my password can be guessed?

Helping The Help Desk Help You:
The first users you should educate are the help desk staff. They are typically responsible for two key activities that will serve as the best examples for users.

First is creation of initial passwords. When a new employee joins the company, their userID/password combination should NOT be "jsmith/jsmith," "jsmith/password," or "jsmith/jsmith1." It should be "jsmith/Cas3piE#" or some similarly strong combination that adheres to the policy, standards, and procedures.

Second is resetting of passwords. Again, resetting a password to "password," "today," or "userID" is not helpful to your goal of securing access.

A quick word about resetting passwords is appropriate here. During the SANS Security Essentials conference (Chicago) in November 2001, Eric Cole presented a great procedure to follow when resetting passwords. The help desk is contacted requesting a password change. Unless you work for a small company (or have help desk employees

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

with lengthy tenure), chances are the employee answering the phone cannot *absolutely identify* the employee who has contacted them. Fortunately, most companies have a voice mail system, and most of those require a password for access to saved messages. The help desk can utilize this system to allow employees easy access to changing their password, while keeping changed passwords reasonably secure. Imagine overhearing part of a "change my password" conversation:

> *Forgetful User*: Please change my password, as I've forgotten it and can't get in to do my important work.
> *Help Desk Employee*: Okay, Mr. Smith. I can do that for you. What I will do is change your password, and then call you back. Please let your phone ring through to voice-mail. I will leave your new password on voice-mail for you.
> *Forgetful User*: Can't you just give it to me over the phone?
> *Help Desk Employee*: I'm sorry, Mr. Smith, but company policy requires that I give you your password securely. The easiest way to do that is to leave your new password on your voice-mail. I can call your voice-mail immediately with the new password.

Obviously, you will need a help desk that can handle the occasionally irate customer. If you've done your education correctly, your users will already know the drill. The benefit to this procedure is that your "unidentified" user must *know* something that only the user *should* know, their voice-mail password. This works even if the employee is working from home, assuming (usually a safe assumption) that they can access voice-mail remotely. In the event someone unauthorized is requesting the change, the genuine user would receive unexpected voice-mail from the Help Desk and would (if educated to do so) alert them or your Security department to a problem.

Auditors Make The Best Friends:

There is no way to ensure that your policy, standards, or procedures are being followed if you don't audit them periodically. The easiest way to audit the password policy and standards is to execute an automated program against the files in which passwords are stored. LC3 (previously l0phtcrack) is an easy (too easy) to use program that can perform this function for you on many operating systems. Executing it periodically can help you monitor adherence to "the rules." (See the Quick Legal Consideration before implementing this particular device!)

Another idea is to utilize a program such as Password Policy Enforcer[xi] (available from TP Information Systems Pty Ltd). This program checks new passwords when they're created to ensure that they adhere to the policy and standards of a company. Messages are presented to users that craft non-compliant passwords that can help direct them to an acceptable selection. Software such as this may reduce calls to the help desk.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Auditing your procedures is equally, if not more, important. Create new users and review the default assigned passwords. Do they change with each user, or is the same "strong" password used every time?

Request a password reset. Better yet, have your CEO do so[xii]. Is the procedure being followed as documented? Does the new password adhere to the policy and standards?

If you're using LC3 or similar software, audit the software audit procedure. Are two employees running the software together? Can they see the passwords as they are "cracked?" Do they have access to the software when audits are not being executed?

Having an excellent policy, high standards, and easy procedures are laudable goals. If they're not being followed, however, you may as well change your own password to "password." Auditing both policy/standards AND procedures is the only way you can be confident that your goal of securing access is being reached. It is recommended that these audits take place regularly, and at least once a year an unscheduled audit should be performed.

A Quick Legal Consideration:

During a discussion of the LC3 software at the November 5-10 SANS Security Essentials conference in Chicago, Eric Cole presented a scenario wherein he was an expert security witness for a company. The case was determined baseless, however, when the defense attorney asked the system administrator if he audited passwords. The system administrator did, using LC3 or a similar program, which showed the passwords as they were "hacked." The defense attorney then made the case that the company couldn't *prove* his client perpetrated the offense because others within the company had access to the client's password and could easily have used the client's userID and password to commit the crime.

For this reason, it is recommended that you protect yourself and your company by clearly indicating through policy that at no time should passwords be shared. The policy should also indicate that when auditing occurs, passwords shall not be made visible. LC3 gives administrators the option to know whether or not a password was cracked without knowing the password itself[xiii]. Documented procedures should support these policy statements in word, and regular audits of the procedures should demonstrate that the policy and standards are being followed.

Summary:
Securing access through the use of passwords is a viable protection against both internal and external hackers, if done correctly. The keys to making it work are simple:

- Have a password policy, standards, and procedures in place that clearly define the expectations of users in creating a secure environment. Prepare for exceptions, they will occur.
- Educate users concerning the policy, standards, and procedures. Using straightforward language and good examples helps the users comply with "the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

rules" with minimal complaint. Remember, chances are no one has ever shown them how easy it can be!

- Utilize your help desk personnel as allies. Bring them into the process early because they're going to get all the calls when users can't comply with password policies and standards. They're also responsible for adhering to key procedures.
- Perform regular and unscheduled audits to ensure that the policy, standards, AND procedures are being followed as outlined.

By following these steps, you will have secured access for your users, while securing access to the information critical to company operation. You'll also sleep a little easier.

Endnotes:

---

[i] Mortensen, Jason, "Password Protection: Is This the Best We Can Do?", 20 Aug. 2001. URL: http://rr.sans.org/authentic/pass_protect.php (5 Dec. 2001)
[ii] Scarabello, Claudio, "Security Policies: The Why, What, Who and How", TruSecure Corporation presentation, 5 Dec. 2001. URL: http://www.trusecure.com/webinar after free registration. (5 Dec. 2001). Select the presentation "How to Develop Effective Security Procedures" (A direct link is impossible for unregistered users, however, registration is free.)
[iii] Ibid.
[iv] For an excellent write-up of the LC3 (formally l0phtcrack) application, see http://rr.sans.org/authentic/l0phtcrack30.php.
[v] Scarabello, Claudio, "Security Policies: The Why, What, Who and How", TruSecure Corporation presentation, 5 Dec. 2001. URL: http://www.trusecure.com/webinar (5 Dec. 2001).
[vi] Cons, Lionel, "CERN Security Handbook Version 1.2" 12 Dec. 1996, URL: http://consult.cern.ch/writeup/security/security_3.html (3 Jan. 2002)
[vii] LAN Manager authentication allows for 14-character passwords, but stores them in 2 7-character chunks. Information about this security hole, and how to address it, is available online. Microsoft Corporation, "How to Disable LM Authentication on Windows NT" 8 Aug 2001, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706 (14 Jan. 2002)
[viii] Scarabello, Claudio, "Security Policies: The Why, What, Who and How", TruSecure Corporation presentation, 5 Dec. 2001. URL: http://www.trusecure.com/webinar (5 Dec. 2001).
[ix] McAuliffe, Wendy, "Computer Passwords reveal workers' secrets" 29 Jun. 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2781327,00.html. (3 Jan. 2002)
[x] Luce, Kathleen, "A guide to Unix account passwords and password security", 11 Nov. 1999. URL: http://www.acs.calpoly.edu/policies/passwords.html (3 Jan. 2002)
[xi] Further information, and an evaluation copy of the program, is available online at http://www.tpis.com.au/products/ppe/default.htm.
[xii] Cole, Eric. Based on the discussion at the SANS Security Essentials conference, in Chicago, November 5-10, 2001.
[xiii] "@stake LC3", URL: http://www.atstake.com/research/lc3/whatsnew.html (5 Jan. 2001)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced