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.

"Password security and the means of achieving it within a Novell environment"

Today, passwords are the primary means of authenticating to most computer systems. As a result, people are forced to remember an abundance of passwords, not only for their employer's directory services, email, and other applications, but also for some web sites they visit. Since they must remember a lot of passwords, it is likely that their password was chosen with simplicity in mind and can be easily guessed or cracked. A step towards maintaining security is breaking users of this habit and enforcing strong passwords....

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

“Password security and the means of achieving it within a Novell environment”
Erik Ball
GSEC v.1.4b
February 3, 2003

Abstract:

Today, passwords are the primary means of authenticating to most computer systems. As a result, people are forced to remember an abundance of passwords, not only for their employer’s directory services, email, and other applications, but also for some web sites they visit. Since they must remember a lot of passwords, it is likely that their password was chosen with simplicity in mind and can be easily guessed or cracked. A step towards maintaining security is breaking users of this habit and enforcing strong passwords. Account security is critical, especially for more privileged accounts, which can provide access to sensitive mission critical data, personal information, such as social security numbers, or financial information, like credit cards numbers or account access. This paper will focus on the need for password security and the various means of implementing and maintaining it within a Novell NDS / eDirectory environment. Securing the accounts in your directory involves a combination enforcing strong passwords, account lockout periods and security policies, in addition to providing the users with training. An additional security add-on called Novell Modular Authentication Services allows for definable password characteristics and multi-factor authentication using smart cards, tokens, or biometrics.

The need for password security and the means of achieving it

Users are generally considered to be the weakest link in the security chain. They do not think about the importance of security, nor the variety of possible security threats. In the eyes of the end user, security is a task that adds an additional layer of complexity to an already perplexing computer environment. While some people may be paranoid and have a high regard for security, the majority of people are too trusting of others and aren’t as security conscious. These people typically don’t believe that they will be targeted, that their level of access could cause any harm, or that they would be held accountable for a security breach. These users must be made aware of the seriousness and severity of security issues. These employees must be convinced that a compromised account is a serious problem that may have a direct impact on them and their coworkers. They must recognize that security problems can be avoided by taking the appropriate action – things that they are easily capable of doing (Weirich). If users are conscious of security, and aware of the potential dangers, then they are more likely to take steps to protect their account.

Unfortunately, a recent report by NTA Monitor confirmed that most users do not think seriously about the security of their accounts. This can be inferred by their lack of concern for the fundamental mechanism that keeps their account secure

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

– a well chosen password. The study showed that people chose passwords that are easy to remember and don't bother changing them. "The 2002 NTA Monitor Password Survey found that 84% of computer users consider memorability as the most important attribute in selecting a password and that 81% of users select a common password where possible…67% of users rarely or never change their password, and further 22% admit that they would only ever change their password if it was forced by a Web site or system/IT department…49% of heavy computer users write their password down, or store them in a file on their PC. This number falls off for lighter users with an average of 31% of all users storing their passwords" (NTA-Monitor). Even though organizations may have layered security, secure configurations, and patched software, there is still a major password security problem present today. In order to protect from unauthorized activity, password security must be enforced, policies must formed, and their employees must be trained.

There are a variety of issues that come from failing to maintain adequate password security. A weak password is more susceptible to guessing, social engineering techniques, and password cracking methods. After a user's password is discovered, the attacker has the ability to disguise their activity using the compromised user's account. Having gained unauthorized access to the system, the perpetrator could steal sensitive or confidential data, make damaging system changes, create backdoors, or perform other malicious activities. This presents a problem because a compromised account is usually detected through a reactionary process that takes place after spotting unusual activity, like login dates and times, or unauthorized and damaging changes. By this time, the damage could have already been done; the attacker might have taken the information that they wanted and covered their tracks before the issue is fully investigated.

When passwords are the only means of authenticating to an account, a strong password is a critical part of protecting it from unauthorized access. This leads to the question of what characteristics differentiate a strong password from a weak one. Weak passwords are generally characterized as having an easily determined sequence or consisting of words that can be found in a dictionary. When someone's password contains a simple sequence, like 'qwerty' or '12345', it is easy to decipher password by watching over their shoulder. On the other hand, when a password contains dictionary words or alphanumeric hybrid words, it can be obtained by making logical guesses or with a password cracker. Out of a desire for simplicity and memorability, users inadvertently create passwords that are easily guessed or discovered through social engineering; their password typically consists of a dictionary word or an alphanumeric combination that is significant to their interests. Some of the guesses that attackers may attempt are: a variation of the username, a family member's name, partner's name, birthdays, sports, celebrities, bands, favorite places, their name, or their pet's name (Kessler). The attacker could gather much of this information through a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

seemingly innocent conversation, a simple investigation, or by snooping around their desk.

Strong passwords should be used to protect an account since they are not easily guessed and are harder to crack. Strong passwords have the following characteristics (SANS Policy Project):

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line

These characteristics help make a password unguessable and hold up to either a dictionary or a hybrid attack. Such attacks are usually limited to the alphabet and numbers, which is 36 characters if case insensitive or 62 characters if case sensitive. An attacker prefers to keep the smallest character set possible, since adding to it exponentially increases the amount of time to crack the password. In general, hackers are trying to obtain as many passwords in the shortest time possible. However, if they are seeking an individual password, they will take the extra time to use a full character set and perform a brute force attack. Although it used to be especially time consuming, the latest computers on the market are making it more of a reality. One countermeasure is using extended ASCII characters in a password; these characters provide additional protection against a brute force attack. Extended ASCII characters are produced by holding down ALT and pressing a two or three digit code on the numeric keypad. One project discovered that certain ASCII characters rendered a password uncrackable using L0phtCrack, as seen in this table (Kleppinger).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Uncrackable Alt-Characters

1= ☺	21= §	143= Å	172= ¼	192= └	212= ╘	232= Φ	252= ⁿ	177= ±	229= å
2= ☻	22= ▬	144= É	173= ¡	193= ┴	213= ╒	233= Θ	253= ²	178= ²	230= æ
3= ♥	23= ↨	145= æ	174= «	194= ┬	214= ╓	234= Ω	254= ■	181= µ	231= ç
4= ♦	24= ↑	146= Æ	175= »	195= ├	215= ╫	235= δ	255= B	182= ¶	233= é
5= ♣	25= ↓	148= ö	176= ░	196= ─	216= ╪	236= ∞	127= ⌂	183= ·	241= ñ
6= ♠	26= →	153= Ö	177= ▒	197= ┼	217= ┘	237= φ	131= ƒ	186= °	246= ö
7= •	27= ←	154= Ü	178= ▓	198= ╞	218= ┌	238= ε	135= ‡	187= »	247= ÷
8= ◘	28= ∟	155= ¢	179= │	199= ╟	219= █	239= ∩	149= •	188= ¼	
9= ○	29= ↔	156= £	180= ┤	200= ╚	220= ▄	240= ≡	160= B	189= ½	
10= ◙	30= ▲	157= ¥	181= ╡	201= ╔	221= ▌	241= ±	161= ¡	191= ¿	
11= ♂	31= ▼	158= ₧	182= ╢	202= ╩	222= ▐	242= ≥	162= ¢	196= Ä	
12= ♀	32= S	159= ƒ	183= ╖	203= ╦	223= ▀	243= ≤	163= £	197= Å	
13= ♪	127= ⌂	164= ñ	184= ╕	204= ╠	224= α	244= ⌠	164= ¤	198= Æ	
14= ♫	128= Ç	165= Ñ	185= ╣	205= =	225= ß	245= ⌡	165= ¥	199= Ç	
15= ☼	129= ü	166= ª	186= ║	206= ╬	226= Γ	246= ÷	166= ¦	201= É	
16= ►	130= é	167= º	187= ╗	207= ╧	227= π	247= ≈	167= §	209= Ñ	
17= ◄	132= ä	168= ¿	188= ╝	208= ╨	228= Σ	248= °	170= ª	214= Ö	
18= ↕	134= å	169= ⌐	189= ╜	209= ╤	229= σ	249= ·	171= «	220= Ü	
19= ‼	135= ç	170= ¬	190= ╛	210= ╥	230= µ	250= ·	172= ¬	223= ß	
20= ¶	142= Ä	171= ½	191= ┐	211= ╙	231= τ	251= √	176= °	228= ä	

It should be noted that L0phtCrack is a tool for cracking Windows SAM databases and cannot be used on NDS or eDirectory. However, as multiple directories are emerging within organizations, Active Directory could be synchronized with eDirectory. As John Enck from Gartner stated, “In the real world, people are deploying multiple directories for their platforms. Because the directory is tied to a platform, you don't have a choice;” furthermore choosing one directory is not realistic, and it doesn't make sense (Fogarty). If the Active Directory SAM database was compromised or stolen, the synchronized account passwords could be obtained with Windows cracking tools. This creates an additional need for password security when multiple directories exist or password synchronization is in place.

Password synchronization is a process that keeps the password the same across various systems within an organization. Single sign on technologies or password synchronization can both reduce and improve security at the same time. This process can reduce security in two ways. The first case is when a single system is insecure and compromising that system will provide the intruder with access to the synchronized password for the other systems. The second case is when users don’t chose strong passwords and their password is discovered; likewise the attacker has access to all the systems that the user has accounts on. However, password synchronization can also improve security. The primary reason is because when a user has a single password to remember, they are less likely to write it down. In addition, they are more likely to abide by strong password policies because there will only be a single complex password to remember. When considering a solution for synchronizing passwords, insecure systems or systems that can be accessed via the internet with insecure protocols

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

should be left with standalone passwords, while the participating systems should require strong passwords that are changed on a frequent basis (M-Tech, p.13).

While there are a number of compelling reasons to have strong passwords, this does no good without a policy that affirms the organizations commitment to password security, and a training program that supports its implementation. The first step should be drafting a strong password policy that is suitable for your organization. The SANS Policy Project resources, located at: http://www.sans.org/resources/policies, can provide a good starting point. The password policy should be clearly defined, well written, and understood by the users, especially if password security was neglected in the past. It must also have the support of upper management. When upper management seeks to be the exception to the rule, it not only sets a bad precedent, but it also leaves some of the organizations most vital resources vulnerable. Often, upper management holds some of the most privileged accounts that have access to the most sensitive information. Management should realize the value of strong passwords and try to instill these same concerns for security in their employees.

Similar password policies should be imposed on the system administrators. Administrators and administrator accounts should uphold a password policy that is stronger than necessary for ordinary users. At the very least, administrator accounts should have extremely strong passwords that have no bearing on the system or the organization. These passwords should be changed on a periodic basis, in addition to whenever any suspicions arise or a system administrator is terminated. A log can be also kept to verify that the passwords are changed on all of an organization's systems during a period of time.

Merely creating a organizational password policy is not enough; it would be unreasonable to create a policy that suddenly shocked the users and left them wondering what to do when their password changes. This could easily develop into a situation where people are choosing passwords that they can't remember or writing them down. Without the proper training to support a password policy, the result could not only be disastrous, but it could also lead to bad habits. A training program should be developed to inform employees about the importance of security, the password policy, and how they are expected to meet these requirements. It could be incorporated into Human Resources' employee orientation program, in addition to using email, newsgroups, and an intranet security site to serve as a refresher for existing employees (Donovan).

Part of the training should demonstrate how to create a complex password from an easy to remember thing or event. Users should learn to follow a logical system for creating strong passwords, in which you take a phrase of information and you use a method to convert it to a password. The phrase of information that you use to create your password should be something instilled in your memory, like a description of event in your life, or something you have or like. Good examples are, "My new car is silver", or "The perfect game of golf". Next,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

this phrase needs to be converted to a symbolic representation of it, which is used for the password. This can be combined with character substitution for non-alphanumeric characters like "@" for "a", "!" for "i", or "$" for "s". For example, when your take your informational phrase a like, "My son Billy was born in 1984", you could translate it to a password like, "M$Bwb!1984". Preserving a mixture of upper and lower letters, as in this example, also increases the strength of the password. Ordinarily, this password would seem cryptic and hard to remember; however, the person that created it should be able to easily recall it and come up with their complex password. With proper training, users will be more likely create and remember passwords that meet the guidelines of the password policy, without becoming frustrated or perplexed with the idea of a strong password.

Although employees may understand and meet the requirements of the password policy, they must also be aware of social engineering techniques. If people are deceived by an attacker, the strength of their password is irrelevant. Social engineering can be defined as, "a hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system" (Palumbo). As part of the training program that goes along with implementing secure passwords, users must be aware of the methodology that an attacker may use to obtain their password. They should know that if anyone asks them for their password, or any other sensitive information, they should act with the greatest amount of caution possible and confirm the identity of the person before proceeding. One form of social engineering is impersonation, such as a phone call pretending to be someone from the IT department, needing your password to perform some kind of repair or account maintenance. Another method is to disguise malicious code in something that may be interesting to the user, like an email with a catchy subject containing a virus, trojan, or keystroke logger to capture your passwords or other sensitive information. Finally, social engineering techniques may help the attacker gain physical access; for example, after smoking with the employees, this person walks in with them. This could present an opportunity to gain access to a computer on the internal network or collect information from a person's desk. In each of these examples, the attacker could have been thwarted if they were forced to prove their identity. Finally, users should know that they cannot write down their passwords, especially on sticky notes, desk blotters, or calendars where someone else could easily find it. If users can relate to examples where social engineering has succeeded, and know how to react in these situations, they are more likely to keep their account secure and their password out of the hands of an attacker.

The final piece in addressing account and password security deals with the user support process. There are going to be occasions when a user forgets their password or gets locked out of their account, especially while adjusting to a stricter password policy. These situations usually generate a call to the helpdesk for assistance, where the identity of the user must be validated to deter against

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

social engineering. If an intruder calls and says, "Hi, this is John Doe from the budget office - can you reset my password for me – I seem to have forgot it and locked myself out of my account", and the support technician unlocks their account or resets their password without first confirming their identity, then the support process has a major security hole. Hacker's social engineering techniques can only be foiled when they are forced to prove their identity with something they know or something they have. To ensure that the new password is left in the right hands, it could be put on their office phone's voice mail, relying on the strength of their numeric voice mail password to keep an intruder away. Another method is to require the person to present in person, or fax, a valid form of ID with their request.

The issue of securing the user support process is further complicated when there are a lot of technicians that are capable of resetting a user's password and there is no means of determining who performed the reset, when they did it, and how they validated the identity of the requestor (M-Tech, p.15). A doctor, who was concerned about HIPPA regulations, recently asked about the security of his email and calendar since he had patient information in his account. After telling him that the security of his account relied on his password since the information was encrypted, he questioned the number of people that were capable of resetting his password to gain momentary access. With this in mind, there needs to be a way of tracking who is resetting passwords. If someone feels that they did not forget their password, rather it was changed to gain access to their account, then a log can help narrow down who is responsible for resetting an individual's password. Finally, whenever a password is reset, it should be valid for a single logon; the support technicians cannot rely on the user to change their password from the default value to something unique. If the person is not forced to change their password immediately, then others may be tempted to try logging into accounts using the default reset password value.

Maintaining Account Security in NDS / eDirectory

Within the framework of NDS /eDirectory, there are some basic means of enforcing account security, through mechanisms like password restrictions, login times, station restrictions, and intruder lockout. Using the right combination of these settings within your environment can provide an acceptable level of security for most accounts.

Password security settings ensure that users create passwords that will adequately protect the account (Figure 1). The password following restrictions can be placed on any user account:

- Allow a user to change their password
- Require a password with a minimum length:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

All accounts should require a password that is at a minimum 6 characters in length, however, 8 characters is recommended. Unfortunately, there is not a built in feature to require alphanumeric passwords, or set other password attributes. Even if you set the minimum length to 8 characters, users could still chose weak passwords that are easily guessed or cracked. To truly enforce strong passwords in NDS, this setting would have to be coupled with a user training program and administrative password cracking to ensure that users to comply with the password policy.

- Force periodic password changes after 'x' days
  Routine password changes should occur at least every 40 to 90 days, depending on the perception of risk and possible ramifications. Periodic password changes can be a double edged sword; if the users perceive it as being too frequent, they may be inclined to pick up bad habits to help remember their password, such as choosing weak or easily guessed passwords (controls to prevent this are only available in add-in packages) or writing down their password. Keeping in mind these dangers, the shorter the life of the password, the less time an attacker has to guess the password or use the account if it is compromised.
- Require unique passwords
  When this is enabled, hashes of previously chosen passwords are kept in NDS to prevent them from being used by that account again. While this will prevent users from rotating back and forth between the same two passwords, it does not prevent them from incrementing their passwords with numbers. If users get into the habit of tagging a 1,2,3,4 onto the end of their password every time it changes, after the password is guessed or cracked once, the attacker can reliably predict upcoming passwords and continue to have access to the account after future password changes. Unfortunately, NDS does not have the capability of enforcing a "minimum difference" rule on its history. This is to prevent people from changing their password from golfer01, to golfer02, golfer03, etc. If users are only changing 1-2 characters they're defeating the whole purpose of a password change; a recommended minimum of 4 characters should change. This should be set on any systems that have this feature.
- Limit and allow 'x' number of grace logins
  These provide a grace period for the user to think of a new password. If you nag people with, "Your password has expired. You have 'x' grace logins. Do you want to change your password now?" then hopefully they will think of a good new password during this time. On the other hand, if they are presented with "Your password has expired, please enter your new password" it is likely they will quickly decide on a new password that does not adequately secure their account, so they can continue with their work.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In addition to the fact that only basic password restrictions exist, there are also two other disadvantages that relate to passwords within a Novell environment. eDirectory is case insensitive; if an attacker is aware of your platform, he or she may know that they can save time by using a smaller character set. "Novell eDirectory versions 8.6.2 and 8.7 supports case insensitive passwords, which could allow a remote attacker to use brute force techniques to gain unauthorized access to the system. (ISS X-Force). This was rated as being a low risk vulnerability. In addition, there is not full support for non-alphanumeric or extended ASCII characters across the Novell environment. I noticed this after changing my password to incorporate extended ASCII characters. After the password change, I could no longer login to GroupWise, which used an LDAP bind to eDirectory. Novell TIDs 10068385, 10076271, 10065014, 2915205, and possibly others TIDs mention issues with special characters in passwords. Spanning a variety of different Novell products, each case reports that logins with special characters would fail. While both of these issues are low risk, they are important to remember when assessing the overall password risk.

NDS also provides alternate means of providing account security beyond passwords restrictions. These include:

- Time Restrictions
  This can be used to ensure that the account is only accessed during normal business hours. This could prevent someone from accessing the account during off hours to steal data or perform unauthorized activities and it also limits the time periods in which an attacker could attempt to guess passwords or use the account.
- Network Address Restrictions
  This can provide a means of adding physical security to the account. If the machine has an IPX address or a static IP address (note: other address types are supported), then the account can only be used at designated workstation. This allows a degree of multi-factor authentication, the individual workstation, which is where you are, and a password, which is what you know. Otherwise, address restrictions can be used to lock down an account without a password, which is used by a public workstation either to print or for some other specific purpose.

Password restrictions should be coupled with intruder lockout to prevent an attacker from excessive guessing or using a password cracker. In eDirectory, intruder lockout can be set at the organizational unit, for all the accounts residing in it. Depending on how many incorrect passwords are entered, the account is locked and cannot be logged into for a specified period of time. The number of incorrect passwords should be chosen in consideration to the number of valid passwords that user may have for other systems. When a user has a number of different passwords for different systems, they have a tendency to substitute passwords. For example, the user may unknowingly enter the wrong password, substitute a password used on a different system, and eventually come back around to the correct password. The user should be able to go through this

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

process at least once before being locked out of their account. The other intruder lockout setting is the lockout period, after which time the account unlocks itself. If it resets in a short period of time, like 15 minutes, users can be instructed to wait and try again later, keeping the load off from the helpdesk. However, this also means the attacker can try to guess passwords on a more frequent basis. If a higher setting is chosen, like 24 hours, the users could be instructed to call the helpdesk to unlock their account. An advantage to this is that the helpdesk could also record the network address of the system that locked the account. This information could be used to track down suspicious activity and collect information on whether this mechanism is hindering users or successfully deterring password guessing. Although legitimate users will occasionally get locked out, it is important to remember that the user support process should still validate the request; otherwise the process may be insecure.

Multi-Factor Authentication using Novell Modular Authentication Services

As part of greater concerns for security, regulations such as HIPAA, and other influences, a need for stronger authentication than what is included with NDS / eDirectory becomes apparent. Multi-factor authentication involves a combination of what you know, which is your password, with another means of authentication. One method is something that you are, which is the field of biometrics that uses techniques such as fingerprint scans, retina scans, voiceprint analysis, etc. Another method is something you have, such as challenge-response lists, one-time pads, smart cards, tokens, etc. Novell Modular Authentication Service, NMAS, is a means of incorporating these features and enhanced password policies into NDS / eDirectory using client and server side components. NMAS also allows for graded authentication, which specifies a combination of passwords, token cards, or biometrics needed to gain access to a specific server volume.

While recognizing that NMAS can incorporate alternate means of authentication, the primary focus on NMAS will relate to its role in enforcing users to comply with the organization's strong password policy. The enhanced password is arguably something that should be included with eDirectory by default. In addition to setting minimum and maximum password length, the maximum number of consecutive or repeated characters can also be imposed. This would prohibit users from having passwords like 'golden123', or 'aaaabbbccd'. Passwords, like the one in the example that contain a many repeated characters are easy to obtain by watching over someone's shoulder. Another option that NMAS can enforce is the placement of numeric or special characters and the minimum and maximum number of them needed in the password (Figure 2). This guideline should go hand in hand with training users to substitute numeric and special characters for similar letters when they create their password. An example would be substituting the password 'Webster's dictionary' for 'W3b$t3r's d!cti0n@ry'. Another option provides the ability to adjust the size of the password history

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(Figure 3). As mentioned before, the minimum number of different characters in a password cannot be used against this history; otherwise, this product could also combat users who try to increment or make minor changes to their passwords. Finally, there is an option to synchronize this enhanced password with the regular NDS password and the simple password. This allows the enhanced password to be the default means of supplying a password for eDirectory and NetWare's Native File Access.

Overall, NDS / eDirectory can provide an adequate means of password security with account lockout periods. However, the password restrictions included by default may not be sufficient for some accounts that have access to sensitive or mission critical information. NMAS can be used as a step towards securing these more privledged accounts, through enhanced passwords that have definable characteristics or multi-factor authentication using smart cards, tokens, or biometrics. In any case, the right settings in eDirectory or the additional features included in NMAS can be combined with a security policy, training program, and security conscious support personnel as a means of tightening account security.

References

Donovan, Craig. "Strong Passwords". 2 June 2000. URL: http://rr.sans.org/policy/password.php (8 Dec 2002).

Fogarty, Susan. "Microsoft vs. Novell misses the point". 26 Mar 2002. URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci811818,00.html (3 Jan 2003).

ISS X-Force. "novell-edirectory-insecure-passwords (9229)". 30 May 2002. URL: http://www.iss.net/security_center/static/9229.php (8 Dec 2002).

Kessler, Gary C. "Passwords — Strengths and Weaknesses". Jan 1996. URL: http://www.garykessler.net/library/password.html (6 Jan 2002).

Kleppinger, Joel. "How to Make Windows 2000 and NT 4 Passwords Uncrackable". Jan 3, 2001. URL: http://www.sysopt.com/articles/win2kpass/ (23 Nov 2002)

M-Tech, Mercury Information Technology. "Password Management Best Practices". 28 Nov. 2002. URL: http://www.psynch.com/docs/best_practices.pdf (9 Dec 2002)

NTA Monitor. "NTA Password Security: NTA Monitor calls on industry to help

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

users address personal IT security". 9 Dec 2002. URL: http://nta-monitor.com/password-survey-press-releasse_tade_final.doc (16 Dec 2002).

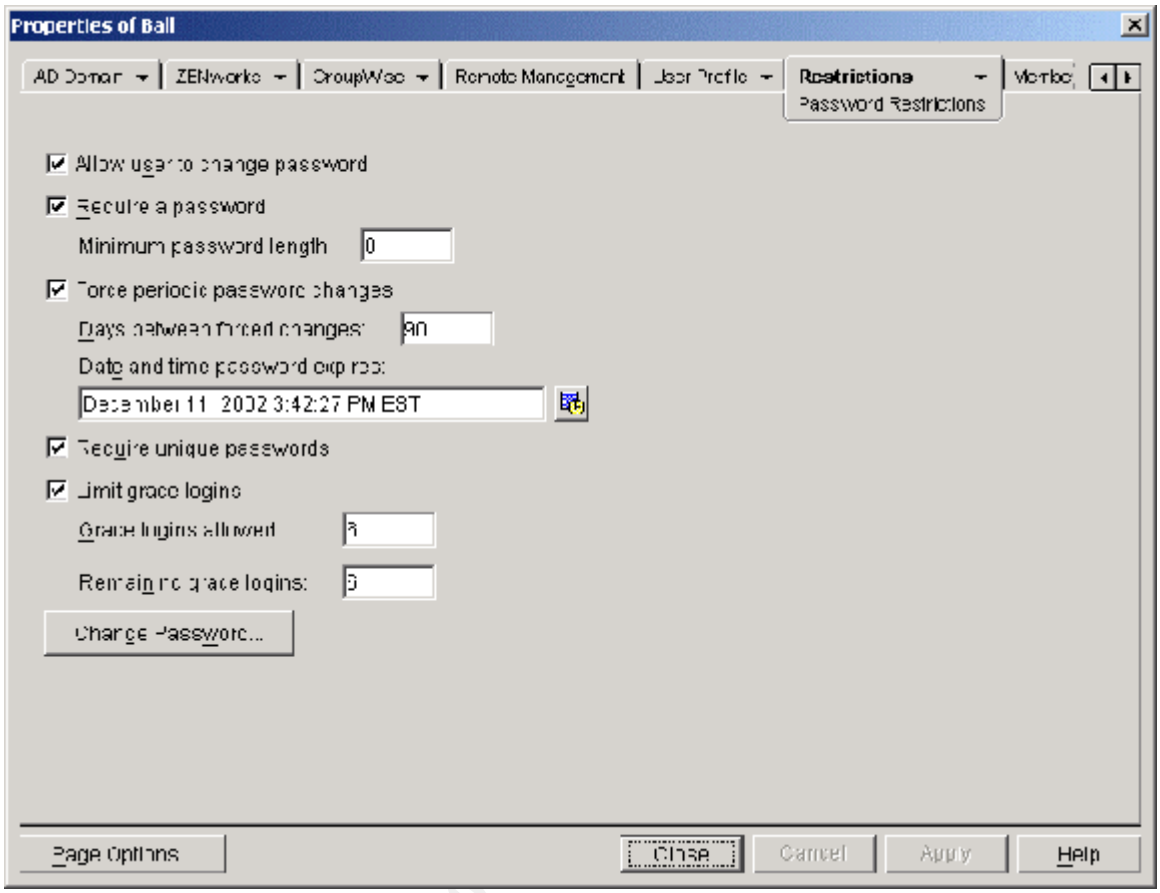
Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done?" 26 Jun 2002. URL: http://rr.sans.org/social/social.php (12 Nov 2002)

SANS Security Policy Project. "Password Policy". URL: http://www.sans.org/newlook/resources/policies/Password_Policy.pdf (23 Nov 2002)

Weirich, Dirk, Sasse, Martina A. "Persuasive Password Security". URL: http://www.cs.ucl.ac.uk/staff/D.Weirich/chi2001.pdf (12 Nov 2002)

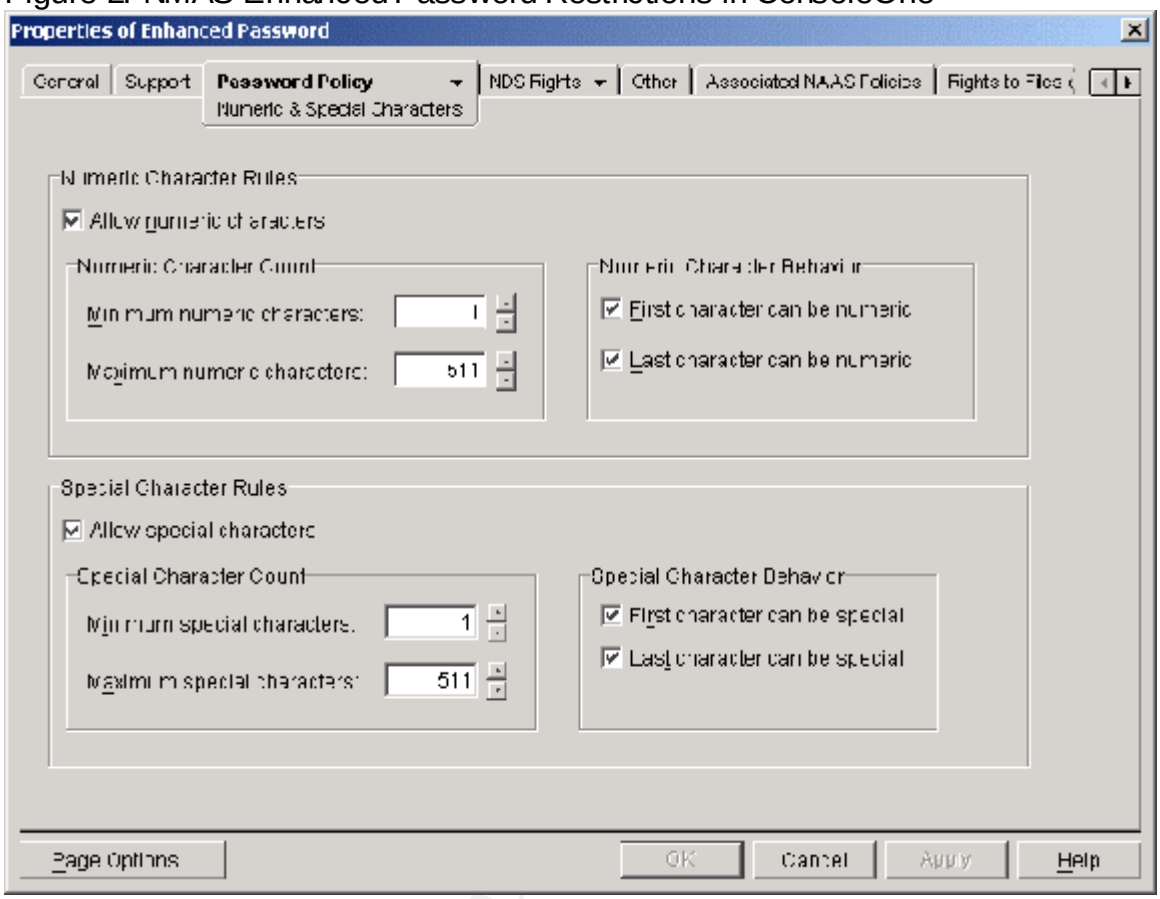
© SANS Institute 2003, Author retains full rights

Figure 1: NDS / eDirectory Password Restrictions in ConsoleOne



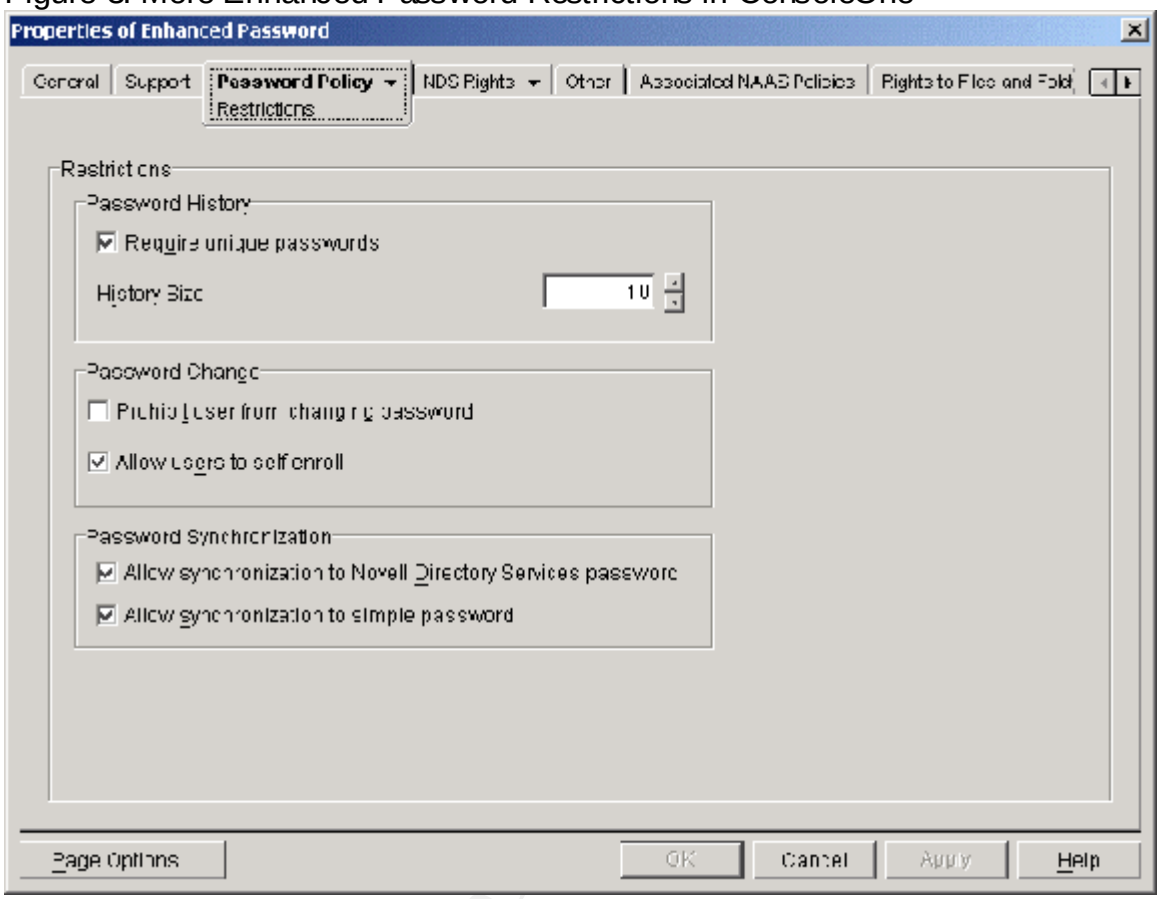
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 2: NMAS Enhanced Password Restrictions in ConsoleOne



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 3: More Enhanced Password Restrictions in ConsoleOne



© SANS Institute 2003, Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced