GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

My Gate is Locked is Yours:
A Look at Implementing a Strong Password Policy

Peter Garancis
February 25, 2004
GIAC Security Essentials (GSEC)
Practical Assignment Option One

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The target audience is for everyone so they can better understand the importance of implementing a strong password policy. The paper explains the concepts behind how easy it is to crack weak passwords, various methods of password cracking attacks, discusses ways to educate end users on selecting a strong password, and last how implement and enforce a strong password policy. Then last it the paper make recommendation on how to increase your security using stronger authentication methods for windows, account lockout, and password audit trails.

Introduction

The fear of being hacked is always a threat, but many may believe the threat to them is very low and it will not happen to them. Thinking this will only increase your chance of becoming another victim. If you don't believe you will be hacked then you probably won't take the proper measures to prevent it from happening. The Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 12 March 2001.[i]

- 85% (primarily large corporations and government agencies) detected computer security breaches within the last twelve months
- 64% acknowledged financial losses due to computer breaches

These statistics show that everyone is at risk of a potential security breach and measures must be taken to avoid the worst. Just because you are not a top secret government lab does not mean you are not a target. Hackers or unauthorized intruders will try to breach the security of any company, no matter how big or small. They will hack a network for any number of reasons including fun, profit, or malicious intent and always at your expense. A hacker will hack you just to see if they can, they don't always need a rhyme or reason. Once they compromised a server the only way to be 100% sure the system does not have a backdoor or root toolkit is to reload the operation system from scratch. A server rebuild costs a company productivity, time, and money.

Companies invest capital and resources into implementing firewalls, Intruder Detection Systems, hardened servers, and physical security, to increase network security. No matter how much one invests in securing a network, one must not overlook any weak points. You may create the illusion that you have an impenetrable network just relying in hardware. Security hardware alone does not protect a network from a hacker it also requires additional steps including taking the time to educate the user. Companies need to spend more time educating the user on security and not rely on the hardware alone to protect the network. By *NOT* taking the time to train people on security, it will only make it easer for your network to be hacked!

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

One of the easiest ways to increase security it to educated the user and make sure they are aware of how important it is to have a password that is hard to crack. According to the Computerworld's Top 10 Security Mistakes, poor password selection comes in at number five. Ken Hill, vice president of IT at General Dynamics Corp., recently attended a demonstration with about 20 of his top engineers and some anti-hacking experts from NASA. Within 30 minutes, the NASA folks broke 60% of the engineers' passwords.[ii] By allowing easy to guess passwords you create a weak spot in your network security, internally and externally. If you don't mind the high possibility that employees cannot work due to a hacked system, data being erased forever, and network resources grinding to a halt, then you do not have to worry about one of the easiest ways to strengthen your security. By implementing a strong password policy and enforcing it.

My Fortress is Unlocked, but Keep Out

A firewall is used to restrict access to some or all network resources. However, to access services such as e-mail, database access, file transfers, or web access, to and from the internet then ports on the firewall must be opened. The more ports that are opened the less secure the network becomes. To restrict unauthorized access to these services some type of authentication method is needed. In layman terms, think of the firewall as the walls around your fortress (the network) and the open ports are the gates that let services through the firewall. To stop unwanted visitors you need a guard to check credentials of users who login. A login server acts as the guard who prevents unauthorized access through the gates. This guard is actually an authentication method who asks for the user to identify themselves with a username and password before they can enter the network.

There is one problem with our guard. He is not the sharpest tool in the shed because the login server (a.k.a. guard) will allow the any person to pass, if they show the correct user name and password. No matter how many times they try! To prevent anyone from cracking the username and password, you must implement and enforce a strong password security policy. Configuring the login server to prevent unlimited failed login attempts, telling your guard to be on the lookout for suspicious activity, is only part of a strong password security policy.

Just because you are behind a firewall does not mean you are secure, especially if users can remotely logon to you network. Remember the attack can come from the inside by an internal threat, thus totally by passing the firewall. Also any network that has remote access capability can be cracked even if the firewall is properly configured. If you can remotely login to your network so can a hacker. The life of a hacker becomes easier if you allow the end user selects an easy to guess password.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I'm in Control: When I Get Around to It

You may ask yourself, if you need to worry if an account is cracked that has limited access rights? Yes, you do! A compromised account will give access to parts of the network and is a foothold on the system. The hacker may initially have limited access to your network and he/she will eventually find a way to escalate their privileges to take control. Compromising a system does not always start with gaining administrator privileges because it can be an escalation process that may take days or weeks to accomplish. Our hacker is trying ultimately for the grand prize of administrator rights. Once the hacker gains administrator access then it is game over for you. At this point they will have full control of your servers allowing them to do whatever they want, including grinding resources to a halt.

It is All too Hard, Not Really

It seems that most people do not understand the need to have a strong password. Many look at passwords as an inconvenience, especially if the company policy made it too hard to remember. Many may ask- Why do we need a password policy? Are they not just a big hassle? We trust everyone in our company, we don't we have to worry! Having a good password policy is too much work? Who would hack this network? Our network is secure we have a firewall to protect us! *Does this sound too familiar to you?* What you need to make everyone understand is that once you are hacked everyone will be inconvenienced except the hacker who had an easy way in to the network.

If you want a more secure network start with educating the end users and helping them understand how easy it is to crack a weak password. A password is considered weak if it is six characters or less, uses only alphabetic characters, and can be easily guessed such as word in the dictionary. Allowing an easy to guess password is only asking for trouble. Today's computing power and password cracking software can crack a six lower case letter password (308 million character combinations) on average of ten seconds. A well-known cracking tool such as "LoftCrack"(or LC4) would take about 48 hours to scan the entire password file of a company, according to Sutton.[iii] These password cracking tools are available to download for free and are easy to get. Allowing weak passwords is an acceptable practice in many firms and makes it easy for a hacker to compromise your security.

So Many Ways, So Many Choices

There are many types and flavors of password cracking programs available on the Internet. New programs and methods are constantly being developed to better crack passwords or to exploit the weaknesses in the hardware and software. What once took days or weeks to accomplish can be done in a few seconds.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There are three standard methods used with password cracking programs: dictionary or wordlist, brute-force, and hybrid attacks. You can consider that there is a forth method used to crack passwords called specialized attack which is a custom written program to crack specific hashes or encryption flaws.

Dictionary or Wordlist Attack

A dictionary or word list attack works by using a text file of words that will be used by such programs as John the Ripper to go through every word in the list against each user login. These attacks can be specialized if the attacker researches the company before launching the attack using something called social engineering. They will collect information about the company through various means. Once they figure out information about the company the attacker then will add in addition to the complete dictionary a specific wordlists such as a common password list. For instance if the attacker was going after a hospital they may load a medical dictionary in addition to the standard dictionary. Word lists are abundant and easy to download, check under the website www.phreak.org for a large list of various wordlist under http://www.phreak.org/html/wordlists.shtml.

This type of attack is the fastest because according to Oxford there are 615,100 words in the 1989 Oxford dictionary and in comparison it will only take around ten second to go through 308 million alphanumeric characters. If you do the math, you can see a dictionary attack take a very, very short time. According to the CERT statistics based on a password cracking incident that happened on an Internet site in 1998. The cracker had collected 186,126 user records, and had successfully guessed 47,642 of the passwords, which accounts for 25% of the passwords.[iv] The survey, conducted by UK domain registry CentralNic, revealed that nearly half of the workers polled use their own name or a nickname and a third used a favorite sports team or celebrity for their passwords.[v] Dictionary attacks on average get 25% of the passwords and take seconds to perform. These statistics show that most users will select a password that happens to be a word in the dictionary and thus easy to crack. Any attacker using this method will crack at least one password which is enough to gain access to the network. Having a password policy will prevent this from happening. Lesson learned do NOT use a word in any language as a password!

Hybrid Attack

The hybrid attack incorporates the fact that some people may strengthen their password by slightly altering it to make it harder to guess. To make the password stronger you would modify a word in the dictionary by adding a number(s) at the end, capitalizing a letter, replacing a letter with a common character, spelling a word backwards, and so on. Some common examples of altered password are:

- password becomes password12
- Jamie becomes JAM13 (i=one, e=three)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Plane becomes enalp

Password crackers anticipate this behavior and have special scripts that go through a wordlist and alter the words to anticipate the changes. The hybrid method will take longer to crack a password but still considerably shorter than going through every possible character combination. For instance the word "so" can become: so, So, SO, sO, s0 (0=Zero), and S0 on. As you can see this will take a little longer to crack but considerably shorter than using every single possible character combination (1111, 1112, 1113 and so on). Lesson learned don't fall for the common mistakes. I will discuss commons mistakes in detail later.

What a Brute You Are…Brute Force Attack

A brute force attack is essential going through every letter, number, and special character combination to crack the password. This type of attack can take a very long time to crack if the password is over seven characters long. A password that is eight characters long with at least one upper case, one lower case, and one number could take a brute force attack up to 6,354 hours to crack, if there are no flaws in the hash algorithm. The longer and more complex the password the long it will take to crack, which is great for security.

Using Brute Force Attack Time Estimator provided by Mandylion Research Labs shows the time it would take a password cracking program such as LC4 by @stake to compromise a random string of characters.[vi] The chart below shows the times it would take to crack a various lengths of random combination of a string of characters. Remember, if you used a word from the dictionary the time to crack would take a matter of seconds if the attacker employed a dictionary or wordlist attack. If the attacker is forced to use a brute force attack it is going to take longer to crack a password.

Brute Force Time Calculator Results						
Purely Random Combo of Chars.	Lower Case Only (a-z)	Lower Case Only (a-z)	Alpha & Numeric (a-z,A-Z,0-9)	Alpha, Numeric, & Special (i.e. @,!&)	Alpha & Numeric (a-z,A-Z,0-9)	Alpha, Numeric, & Special (i.e. @,!&)
Number of Characters	6	8	6	6	8	8
Total Combination	308 Million	208 Billion	56 Billion	680 Billion	218 Trillion	6 Quadrillion
Time To Crack	**0.01 Hours**	**6.0 Hours**	**1.65 Hours**	**20 Hours**	**6,354 Hours**	**177,407 Hours**

As you can see from the chart a password that is at least 8 characters long using all three types of characters would take 177, 407 hours long. Now you may ask yourself what is wrong with a six character combination, well if you used something called distributed computing, where one would utilize two or more computers to process the information, thus reducing the time to crack the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

password. For example if you used ten computers to run against a six character long password it would cut the time from 20 hours to only two hours to crack. Lesson learned use at least 8 character passwords which also has at least once, upper case, lower case, number, and special character. All passwords can eventually be cracked, just make the password not worth to the time to crack.

I Made This Just For You

The Security and Cryptography Laboratory (LASEC) has developed a specialized method geared at cracking Windows hashes in a matter of seconds. The "faster time-memory trade-off technique" method used was able to accelerate password cracking for Windows and is about 6,000 times faster than a brute force attack. Their system is able to crack 99,9% of alphanumeric passwords (mixed case letters and numbers) in 5 seconds (average on 1000 passwords).[vii][iv]

To under stand how this method works you need to learn the basics about how a password is stored on the server. Passwords are stored in files on the hardware device and are converted into encrypted string of characters called a hash. To accomplish this plain text is run through an algorithm thus creating a hard to decode string of characters. If you take the word "Andrea" and run it through the algorithm it would be converted to the following "093d215dfa460b35aad3b435b51404ee5bed09cd516a9c87226f086d230daf2b." As you can see the hash is hard to decipher back into plain text and then to crack the password you must use a program. Most of the password cracking programs do not try to crack the hash but go after the assumption that then end user will use a password that is in the dictionary. There are specialized attacks that are design to go after flaws or exploits in the hash algorithm.

This specialized password cracking method was created to exploit specific operating system flaw in the Windows LanMan hash. Listed below is a sample of statistics taken from "Advanced Instant NT Password Cracker" by Luca Wullschleger and Claude Hochreutiner**.** The small sample of statistics taken from the LASEC web site shows the average time to crack a password was a matter of seconds.

LanMan and NTHash	Password found	Cracking time
cfd20448dfbf3bb2aad3b435b51404ee	65535	9 s
aadb435b51404eeaad3b435b51404ee 30b7d29ab8f3a34c8c57228d0c3dbe6d	empty password	0 s
6b82181883af465baad3b435b51404ee a2bd4962ce41b917cd0f4dcba8255821	esinj79	6 s
af552bbb1d60add7aad3b435b51404ee a67ae759d3cec1eb8293699075786812	Lancel	0 s
7cc48b08335cd858aad3b435b51404ee	BLABLA	2 s
d5bdda88bdbbdb68aad3b435b51404ee	Myslbek	0 s

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

31da1a63d02e321e2e2fa0b946339b80		
e7e1618d0b24262caad3b435b51404ee 9ad035293e636a2ac375532ebeefc7a6	Terho	3 s
bf86088af93019927a4ddb65bb70d7d2 541fdc8265a6906a6656a373599a3736	**ZBYAYDU<u>notfound</u>**	**90 s****
093d215dfa460b35aad3b435b51404ee 5bed09cd516a9c87226f086d230daf2b	Andrea	8 s
A404c47b54be9a777c3113b4a1a5e3a0	INTRAM57	4 s

Notice that there is one password from this list that was only partially cracked which is listed as ZBYAYDU**<u>notfound</u>**. Only the first half of the password was cracked and the "notfound" possibly means that part of the hash has a special character such as a #, $, or &. This means that they are using a strong password that is harder to crack even when exploiting a flaw. Lesson learned, use a password that uses a special character!

Password Cracking Tools

There are a number of cracking programs available that can be used to recover or crack passwords for any operating system to a specific application such as MS Office. The tools can be used for good if someone forgets an administrator password or for bad intention if you want to break into a system. Some of the most well known tools are LC4 formally called L0phtCrack and John the Ripper. An extensive list of password tools can be found at Russian Password Crackers Web site at http://www.password-crackers.com/crack.html. This site shows you the number of password cracking programs available for the hacking underworld and administrator. These tools are abundant, most are free, and easy to use, so beware of what can be cracked.

All Too Common a Mistake

Some users think they are smart about picking a password and pick something that only they know this could be a favorite author, sports team, movie actor, or any place. They may also try to be tricky and alter the word or replace a character with another. The word they alter has already been incorporated into a word list, thus making the password easy to crack. All these methods below have been anticipated and incorporated into hybrid attacks.

Common categories used for passwords.

- Personal information – first or last name, social security number, birthday, nickname, or pet's name.
- Any word in the dictionary including foreign dictionaries
- Slang words or profanities
- Sport's Team, movies, places, or famous people.
- Fictional places or characters (i.e. Frodo or starwars)
- Commonly passwords: root, admin, public, private, 1234, asdf, and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

password

Methods used to modify a word:

- Numbers added to the front or back of the password: toad123 or 007bond
- Capitalizing one or more letters dictionary word: Password or Airplane
- A double word: zoomzoom
- A world spelled backwards: boat = toab

Replacement methods used in hybrid attacks:

- "0" zero for an "o"
- "1" for an "I" or "L"
- "!" for "I" or "L"
- "2" for a "S"
- "3" for an "E"
- "4" or "@" for an "A"
- "ph" for a "F"

Examples of these method: p@ssw0rd (password) or adm1n1strat0r (administrator).

Any altered word you might think of as uncommon password is probably on some wordlist just waiting to be used. There are many specialized wordlists or scripts abundant to use to anticipate the common mistakes mentioned above. Be smart and create a password that is not easy to crack.

Let's Make You Stronger (Passwords)

As you can see, cracking a weak password can be accomplished in a very short time with the right tool. There are a few easy recommendations to follow too considerably lessen the chance of having a system compromised due to a weak password. First you must start with making a strong password policy that must be enforced company wide. To do so you must understand what constitutes a strong or complex password? According to Microsoft a complex password is defined as:

> You should set password policy to require complex passwords, which contain a combination of uppercase and lowercase letters, numbers, and symbols, and are typically a minimum of six characters long or more for all accounts, including administrative accounts, such as local administrator, domain administrator, and enterprise administrator.[viii]

Microsoft has a good definition, until you factor in the LanMan hash flaw which

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

reduces the cracking time by around a factor of 10. LanMan is enabled by default for backward compatibility with Windows 95/98 machines and should be disabled if you do not have the older operating system running on your network.

I use a slightly different recommendation for a strong password which has the following criteria:

- The password must be ***at least* 8** characters long and administrator passwords should *at least 10* characters long
- The password should contain the following types of characters:
  - Lower case letters (a-z)
  - Upper case letters (A-Z),
  - Numbers (0-9)
  - Special Characters (!@#$%^&*()_+-=<>?,./{}[]|\)
- The password will NOT be written down
- The password cannot contain any consecutive characters of your username
- The password should be something you can remember
- The password should be changed about every 90 days
- The password cannot be changed to any of your four previous passwords
- Never use a password that has been listed somewhere or given to you by someone

Picking a long password can be hard to remember when using the recommendations above. There are methods one can use that allow one to easily remember that a password that meets the above criteria. For instance which password is easier to remember: W2!a#f@sx or GO2~1bigRED. When selecting a password think of something you can remember without choosing a word in that is a dictionary. Below are a few of my favorite methods that I have come across used to create a strong password. Anyone of these methods will allow you to create a strong password that you will not need to write down to remember.

Pass-Phrase and Modified Pass-Phrase Method

One method is think - pass-phrase (special sentence) that you can remember. Then use the strong password criteria above and make sure to include a capital letter, number, and special character. If you want to be crafty alter some of words around or add additional special characters.

Simple Pass-Phrase:
Phrase: My car is fast
Password "My#1carisFAST"

Medium Pass-Phrase
Phrase: Pa will be 82.
Password: "Pa!Willbe82." or "PawWilB8-two!"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Complex Pass-Phrase
Phrase: Matt is to rad!
Password: “maTT’z2rad!” or “Matis2RAD!”

The Sentence Method

Think of a sentence or unique phrase that has only meaning to you and is easy to remember. Then take the first letter of each word and make a password out it, don’t forget to add a number, capital, and special characters.

Sentence	Dive the Great Barrier Reef in 2020!
Password	*dtGBRi2020*
Sentence	Saturday is a rugby day! Hurrah!
Password	siard!H1

Words and Numbers Method

Think of two or more words unrelated words and at least one upper case, at least one number (0-9), and at least one special character (@,#,$,%,…). Next take the words, number and special character and make a password out of them.

Two Words: car, swim,

Number: 21

Special characters: “{“

Password: swim{CAR21

Words: Note, Sky
Number 79

Special Characters: “+”

Password: +79noteskY

Words: house, frog

Number: 57

Special Characters: “<”,”>”

Password: frog<57HOUSE>

Bigger Bolder and Better

Making a strong password one can remember is not too hard, as seen from the samples above. One may argue that these passwords are not true strong passwords because they are not a string of randomly generated characters. Possible, yet they are not in the dictionary, at least eight characters, contain all types of characters, and are not easily guessed. So they are considered strong

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

passwords.

Once users start using strong password your systems are far safer. Educating them on how to create a bigger and better password will eliminate another weak point into your network. It will considerable slow down the attacker from gaining access to the network. However having strong passwords is only half of the battle. You need to ensure that a password cannot get cracked is the next step taken in securing your network. A strong password means it will only take longer to crack.

My Fortress has Faulty Locks

A password is encrypted using algorithm that will convert the plain text into a string of encrypted characters call a hash. All modern operating systems use some type of password file encryption. Windows currently uses three hashing function known as LanMan, NTLM, and NTLMv2. LanMan is a weak and older hashing method that is easy to crack and *is still enabled on Windows 2000/XP for backward compatibility.* Any windows LanMan hash can be cracked to an average 13.6 seconds according Swiss researchers using a large lookup table.[ix] Let's look and see why LanMan is not good to leave enabled.

LanMan Weaknesses:

- Converts all lower case characters to upper case thus reducing the time to crack a password by a factor of 10.
- All passwords are broken into two-seven character hashes. This means you have to crack two separate 7 character hashes instead of one 14 character hash.
- It does not use a random element called a salt that will make the hash different on each machine. All passwords will have the same hash on every machine under windows.

Can I Upgrade to First Class, for FREE

Windows has corrected some of the flaws by developing NTLM and NTLMv2 which introduces a better encryption method. NTLM is an improvement and addresses some of the flaws however, it is still considered fairly weak. In addition, the NTLM response is nearly always sent in conjunction with the LanMan response. The weaknesses in that algorithm can be exploited to obtain the case-insensitive password, and trial-and-error used to find the case-sensitive password employed by the NTLM response. [x] If there are no Windows 9x/ME systems on your network then you can disable LanMan and only use NTLM or NTLMv2 to authenticate. If possible it is best to only use NTLMv2 for authentication and listed below is how to do it correctly.

Disable LanMan for Windows 2000

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- From **Start** select **Settings > Control Panel > Administrative Tools > Local Security Policy**
- From the left window select **Security settings > Local Policies > Security Options**.
- Double Click **LAN Manager Authentication Level**.

- In the **LAN Manager Authentication Level** window
- Select **Send NTLMv2 response only** from the **Local policy setting** drop down box.

Do as I Say or Else...

Password policies that are not enforced and make users understand the need for strong passwords will only result in people select easy to guess passwords such as a word in the dictionary. Just because you created a policy does not mean it is enforced. You must create a security policy that all will be comfortable using and actually follow. Setting up a complex password scheme, not educating the user, and then expecting them to remember a purely random string of ten characters, is not practical. One can only guess what would happen next, they write the password next to their keyboard on a post-it note which rates as number one for the top 10 security mistakes. The best advice I can give is create a security policy that can be enforced and allow the users to select a password they can remember using one of the methods I suggested. Last make sure you educate the users on the policy and why it is needed.

Who's Been Knocking on My Door for the Last Five Weeks

Having strong password policy and enforcing it is not enough to prevent someone gaining access to your network, it will just slow the attacker down. You need to be aware of who has been in and out of your network. Especially for the continuous failed login attempts, this is a sign of someone may be attempting to crack the users password. An audit trail will allow you to monitor suspicious activity. Password audit trails need to be enabled and the logs *must be* looked at on a regular basis. If you enforce a strong password and don't watch your gates someone will eventually get past the guard. You need to track all who try to come through your gates. By default password auditing is not enabled in Windows 2000. To add another level of protection you need to enable an audit trail, which is listed below.

Enable Auditing for Windows 2000

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- From **Start** select **Settings > Control Panel > Administrative Tools > Local Security Policy**
- From the left window select **Security settings > Local Policies > Audit Policy**.
- Select and edit each of the following below from Audit Policy

Audit Policy	Audit Success	Audit Failure
Audit account logon events	Yes	Yes
Audit account management	Yes	Yes
Audit directory service access	No	Yes
Audit logon events	Yes	Yes
Audit object access	No	Yes
Audit policy change	Yes	Yes
Audit privilege	No	Yes
Audit process tracking	No	Yes
Audit system events	No	Yes

More information on setting up account lock policies can be found at Microsoft.

http://www.microsoft.com/technet/treeview/default.asp?

Look under TechNet Home > Products & Technologies > Windows Server 2003 > Maintain > Operate > Account Passwords and Policies

Three Strikes and Your OUT!

Remember our not so sharp guard, if you do not instruct him to turn away someone after so many failed attempts then one can try as many time as they like to get pass him. To prevent this you can enable something called account lock-out so the guard will prevent entry after too many failed attempts. This is another crucial security recommendation that need to be implemented. This will stop password cracking programs from hammering away at accounts until the program finds a correct password. Account lock-out will disable the account after so many failed attempts and then re-enable it after so many minutes. Resetting the locked out accounts is crucial to prevent administrator nightmares. This will prevent the administrator having to reset accounts if the users account is accidentally or intentionally locked out. A hacker could intentionally lock out all the user accounts when running a cracking program. Remember a password cracking program will hit the accounts until it gets through, with account lock out you slow them down even more. This is the name of the game slow the password cracker down so much it will take too long to crack the password. Below are the steps needed to set up account lock out.

Setting account lock-out for Windows 2000

- From **Start** select **Settings > Control Panel > Administrative Tools >**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Local Security Policy

- From the left window select **Security settings > Account Policies > Account Lockout Policy**.
- Select and edit each of the account lock-out policies listed below

Remember that you need to set the account lockout duration, account lockout threshold, and reset account lockout counter to the security level that meet your needs. The more security you need the high these setting should be set. The above example show the account will be locked for ten minutes after three failed attempts. In addition the lock out counter will reset after 10 minutes, meaning if you have two failed attempts in less than 10 minutes the next failed attempts will lock the account out. One needs to wait the whole ten minutes before they get three more attempts. You can set the password policy dependant on user rights and/or systems using the **Group Policy Objects** in Active Directory.

Conclusion

Following the recommendations above is an easy way to increase the security of the network but implementing and enforcing a strong password policy. Of course this requires some extra work and training however this definitely out weights the risk of lost productivity. The overall long-term benefits and low cost to implement the policy will considerably lessen the chance of being compromised. This will secure another weak link is closed and it will help reduce the chance of someone hacking into your systems. If you ignoring the recommendation it will just make it easier for a hacker to gain unauthorized access to the network. Remember if users can login so can a hacker. Once they are in it is only a matter of time before they fully compromise your network.

Once a system is compromised it will take time, effort, and money to ensure the system is secure again. Think of the worst case scenarios when you have been hacked can you afford days of lost productivity or having to valuable data permanently lost. A compromised system is always at your expense. So implementing a strong password policy, enforcing it, and having an audit trail is well worth the effort. Don't leave your gates wide open and prevent unauthorized access to your resources. All passwords can be cracked. Just make certain it will take too long time for someone to crack a password thus giving you time to catch the incidents in the audit trail. If you don't watch what goes on you might not even know someone is attempting to get in until it is too late. Thus following these recommendations above should feel a lot safer because at least you know gate now has a stronger lock and a watchful guard.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

i The Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 12 March 2001, http://www.gocsi.com/prelea_.htm

ii by Alan S. Horowitz , Top 10 Security Mistakes, COMPUTERWORLD, July 09, 2001

iii Jay Lyman, Survey: Security Password Picks Are Easy Prey**,** NewsFactor Network, June 26, 2001

iv CERT Coordination Center, "Password Cracking Activity.", The 1998 incident was reported as CERT Incident IN-98-03

v By Jay Lyman, Survey: Security Password Picks Are Easy Prey, NewsFactor Network, June 26, 2001

vi Mandylion Research Labs, "Brute Force Attack Time Estimator", http://www.mandylionlabs.com/index15.htm

vii Luca Wullschleger and Claude Hochreutiner, "Advanced Instant NT Password Cracker", the Laboratoire de cryptographie, EPFL - http://lasecpc13.epfl.ch/ntcrack

viii Microsoft, www.microosft.com

ix Robert Lemos, Windows passwords broken in seconds, CNET News.com, CNET News.com July 23, 2003

x Eric Glass, "The NTLM Authentication Protocol", http://davenport.sourceforge.net/ntlm.html.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.