ELCOMSOFT
PROACTIVE SOFTWARE

PROACTIVE IS BETTER THAN REACTIVE

TESTING PASSWORD SAFETY – A KEY TO SECURING A CORPORATE NETWORK

Copyright (c) 2007 ElcomSoft Co.Ltd.

CONTENTS

INTRODUCTION

Information protection gets much attention these days. Many have realized that their data is a treasure, which not only should be treated properly, but should be protected as well.

Preventing and minimizing risks is much better than suffering consequences. This plain rule is also true for informational security of any enterprise.

So a few dollars spent on defending against security threats now can reap millions in avoiding future losses due to hacking of your enterprise network. Fighting to recover from the aftermath of a severe confidential information leak can cost a great deal of money and could even ruin your business.

Average corporate network security is generally at the level of its weakest link. In many cases, it takes only one weak password to cause a breach in the security system of the whole enterprise.

This article is about the risks of using weak passwords within a corporate network and ways to minimize these risks.

NOT ALL PASSWORDS ARE CREATED EQUAL

Password protection is the most common method of identity verification used by Windows operating systems. Though many other methods exist on the market, for example, smart-cards or biometry, the majority of work stations continue using the "login-password" combination.

Some companies require that their user passwords meet basic requirements. This is called "Password policy" (policy of managing passwords), and is a part of general security policy. Password policy is used to determine basic parameters, such as length, structure and validity period for user passwords.

But, as a general rule, most organizations do not have an elaborate password policy and it is not well enforced, allowing users to ignore it. Thus, the complexity of passwords may vary considerably.

Many companies have been strongly influenced by regulating legislative acts like, Sarbanes-Oxley (USA), HIPAA (USA), J-SOX (Japan), LSF (France), to impose certain rules for creating passwords. These rules pertain to such things as password length or password structure. Despite these measures, it doesn't mean that passwords are really safe and will survive an attack.

The majority of popular passwords are nothing but words, derived from the mother tongue of a user. Sometimes words, used as passwords, can be found in a user's daily life: birth year, pet name, phone number, credit card number etc. Possessing such information acts in an intruder's favor making the victim a sitting duck.

Changing a password doesn't really improve the situation. A new password can be a slightly modified previous password or is created by the same principle (for example, John1 becomes Mary2). This is the way most users solve the problem of regular password-changing, prescribed by security policy.

Moreover, having intruded a victim's computer once, an experienced intruder may become its invisible master for a long period of time with the help of spyware, remote access utilities and other means.

HOW TO FIND A WEAK PASSWORD?

There are currently several basic methods of finding passwords with the help of software:

1. Brute force attack
2. Mask attack
3. Dictionary search
4. Rainbow table attack

Let's review some of these methods in detail, because it's crucial for understanding the characteristics of a weak password.

Brute force attack

Brute force attack is simple: in search for a password a program tries every possible combination of symbols. The search may be restricted to a certain length, symbol type (letters, digits or other) or symbols, which should be first to be tried.

Time needed for extracting a password with brute force depends on password length, set of symbols, performance of a PC and on password protected file type.

Of course, a correct password may be found quickly and a program won't have to try all the possible combinations. But trying a password can take years, if run on an average PC, right? Let's see.

Password speed search for Windows logon is 10 million combinations per second. LM-hash maximum password length is 7 symbols (password length is limited to 14 and password is split in two) with no regard to lowercase and uppercase letters. If a password contains 7 symbols, then brute force attack will succeed in 2 hours.

NTML-hash requires more time – about 4 days – to find a 7 symbol password, because lower case letters are used. If a password contains 8 symbols, then it's "hacking" will require about 8 months. Attacking more complex passwords, such as those which also include punctuation symbols, by brute force takes years.

Password length is an appropriate protection from brute force attack.

Mask attack

If you possess some information about a password, for example, you know its length or some of the symbols, then you may try to recover a password with the help of mask attack by limiting the search range.

For example, if you know that a password starts with a name “john” or ends with a date “1977”, you may use search templates – “john???” and “????1977”. Unknown symbols, known as ‘wildcards’, are designated with question marks in the pattern.

Mask attack makes sense because a program has to try fewer combinations, allowing a password to be found in less time. To protect yourself from intrusion, avoid using words and combinations which can be easily derived from other sources.

Dictionary search

Another method is dictionary search. Users tend resort to common words for creating passwords. Generally, these are English words like “open”, “access” or “password”. In comparison with chaotic combinations of letters and digits such passwords are easier to remember. Ready-made dictionaries may be found on the Internet or created manually. In many cases a dictionary containing the most popular passwords, like admin, 1234, abc123, passwords, 12/3/75/, asdf, qwerty, aaa, is enough.

Before attempting an intrusion a hacker may study user information. Any personal data is useful: names, family names, dates of birth, pet names etc. Some data can be extracted from public sources, such as blogs. Other personal information can be found out directly from a user under any pretence.

The advantage of this kind of attack is speed. The list of common words generally used in passwords is limited. It never contains more than a hundred thousand words. Trying a hundred thousand combinations is an easy task for a modern PC.

To protect yourself from this kind of attack avoid creating passwords consisting of simple words or combinations, or some data which may be obtained by someone studying your identity in detail.

Rainbow table attack

A method employing rainbow tables (rainbow attack) is used to eliminate the problem. The basis of this method is using pre-computations of password variants for a certain set of symbols.

The idea of replacing resource-intensive computations with a search by a lookup table, that was prepared beforehand, is not new. Lookup tables are used when data is easier extracted from the memory rather than created. The main drawback of a lookup table is its size: not every enterprise can afford storing terabytes of data. That's why rainbow tables, or optimized lookup tables came into being. The size of a rainbow table is much less than that of a regular lookup table.

The size of a table may be determined at generation step: the bigger a table, the higher the probability of finding a password, and vice versa. Thus, in a comparatively short period of time it is possible to get tables, with the help of which you can quickly find a password from a certain range.

In comparison, with simple lookup tables the probability of password recovery is slightly lower than 100%, but still the technique is worth trying. For example, rainbow attack based on a table for 7 alphanumeric symbols (built within a week) allows recovering any password consisting of seven alphanumeric symbols within a few minutes. Brute force attack would take up more than 24 hours.

The probability of recovering a password by use of rainbow table attack is lower when compared to traditional methods. It is possible to reduce the risk of rainbow attack by using longer passwords.

WHICH PASSWORDS ARE WEAK?

By taking into account these possible kinds of attack we can conclude which passwords are weak. The following list gives general guidelines to avoid in selecting passwords because they produce weak passwords that are vulnerable to attack.

1. All passwords used in software by default;
2. Popular passwords (qwerty, 123, password, p@$$\/\/0rd, abc123, monkey etc);
3. Repeated combinations of symbols (aabbcc, 123123, aaaa etc);
4. Inversion of common words (drowssap, nimda etc);
5. Passwords coinciding with user name or it's variation;
6. Short passwords having up to 7 symbols, which can be found with brute force attack or rainbow table attack;
7. Passwords, consisting from common words or word combinations, thus quickly discovered with a dictionary search;
8. Passwords, based on personal data or user characteristics; modified version of older passwords, which can be easily found with dictionary search or mask attack;
9. Passwords, which can be found with relatively popular rainbow tables;
10. Passwords, stored in various Windows system files or cached in memory (such passwords may be safe, but improper system settings may give them away in a trice).

There are many other criteria indicating password weakness. In fact all of them cannot be taken into account by corporate password policy. Thus, the best way to discover weak passwords is by auditing the whole system regularly.

WEAK PASSWORDS – GRAVE DANGER

DO WE OFTEN USE WEAK PASSWORDS?

According to research on informational security of large enterprises carried out by consulting group Deloitte Touche[1], 14% of companies have faced the problem of using weak passwords within the past 12 months. In 9% of cases these were the default passwords, in 7% of cases these were simple passwords, easily found out by intruders.

Summarizing the data of the research, it's reasonable to say that 30% of all enterprises face the problem of using weak passwords. Gross negligence of the simplest security rules and password policy amounts into 16% of cases.

According to research data by Bruce Schneier[2], 3.8% of users resort to simple curt passwords, which can be easily found in a dictionary. 12% of users also use simple word passwords, but they add a special symbol in the end. 28% of users use only lowercase letters and digits, which makes password vulnerable to brute force attack.

These statistics show some of the risks induced by using weak passwords. The range of real danger may vary.

POTENTIAL PROBLEMS INDUCED BY WEAK PASSWORDS

Let's review possible dangers in detail. There are two types of dangers:

1. **External danger.** Attack comes from without. A password is found as the result of direct hacker attack.
2. **Internal danger.** Gaining unauthorized access to confidential information as the result of finding out another user's password by an unscrupulous employee or insider.

In the first case a password becomes the source of a direct hack, a hack starting point. Getting invisible access to a resource within an infrastructure of target-enterprise may help develop the attack. If the intruder gains access to unauthorized information by using spyware (for example, programs logging access keys or confidential information entered by authorized users) or social engineering software, he has an additional advantage.

We should understand that attacks are not for fun or idle curiosity. Hackers are interested in having access to valuable company resources. These resources are the target. Finding a weak password is only the first step in exploiting the target network.

[1] «2007 Global Security Survey», Deloitte Touche,
[2] «MySpace Passwords Aren't So Dumb», Bruce Schneier, 2006

The situation can be even more perilous if company security is threatened by an insider. The insider may have considerable computing resources at his or her command. Company computers may be used to attack password protected resources. The insider is good at all possible attacks: brute force, mask attack, dictionary search or methods on the basis of user personal data (dates of birth, names, family names etc). The insider is not prevented from accessing a target-computer physically, which may help him or her break through even the safest password protection.

Material losses caused by hack, unauthorized access to confidential information and financial fraud, may amount to large sums of money, depending on the scale and type of enterprise.

Let's adduce more facts to illustrate the situation. According to a survey among representatives of 370 American companies carried out by Computer Security Institute , average losses induced by a single violation of security totals $345K in 2007. The figures have doubled since the last year.

For some business fields, like finance or insurance, reputation losses are crucial. A single scandal concerned with leaks of clients' personal data may set a company on the verge of bankruptcy. The most frightening fact is, unlike virus attack, password hack may not be revealed quickly. Thus an intruder may have access to confidential data, strategic or financial information for a long period of time. Hack and leakage are often discovered after the information has been extracted and the threat cannot be eliminated.

Password change regulations in force in many companies are useless when confronted with experienced hackers who get a new password from a pre-installed key logger.

To minimize risks associated with weak passwords, passwords should be audited regularly. The next chapter discusses ways of auditing a system.

[3] «Computer Crime and Security Survey», Computer Security Institute (CSI), 2007

DISCLOSING WEAK PASSWORDS

As it was said before, corporate password policy, regulating password length or password structure is not enough to secure access to company data. These measures do not protect company passwords from being quickly hacked by dictionary search or template search (for example, complex passwords usually comprise from letters in the beginning, followed by digits and uppercase letters in the tail).

Moreover, regular change of passwords, imposed by corporate security policy of large enterprises, makes users simplify and shorten passwords, use permanent patterns or their slight modifications.

It is possible to minimize the risks mentioned above. The preventive key is regularly auditing passwords which are used on the corporate network.

How does it work? It's as easy as ABC. Imagine you are an intruder and try to do an intruder's job, try to find passwords from users' accounts.

This is easily done with the help of specialized software, widely used by security departments of huge corporations and special services of different countries.

Routinely launching password audit software will help discover and remove weak links in the security chain of an enterprise. Furthermore it will help to find out which users are well-disciplined and which users need an extra lesson in password security basics.

WHAT'S THE BEST SOFTWARE TO USE?

Auditing company passwords can be carried out by various software products. The market abounds in this type of software: starting with self-made and free solutions and ending with specially designed commercial solutions. When choosing a product, keep in mind its features and usability.

The most important features are modeling different types of attack, support of remote network, different languages and platforms.

One of the most functional and easy to use solutions is Proactive Password Auditor by ElcomSoft. It'll be introduced further.

PASSWORD AUDITING WITH PROACTIVE PASSWORD AUDITOR

Proactive Password Auditor (PPA) solves the task of auditing passwords quickly and efficiently. PPA supports different types of possible attacks: dictionary search, brute force attack and rainbow table attack.

This product was designed to test password security in Windows NT, Windows 2000, Windows XP, Windows 2003 Server, Windows Vista and the newest Windows Server 2008.

PPA was designed for corporate use. This product allows system administrators to identify user accounts with weak passwords.
The nature of hashing doesn't allow restoring an original password from the hash (either LM-hash or NTLM-hash). But a password can be restored with brute force attack, dictionary search, trying all possible combinations within a set range or by a certain list of words. Thus, to find a password you need to:

- collect password hashes;
- find passwords corresponding with the hashes.

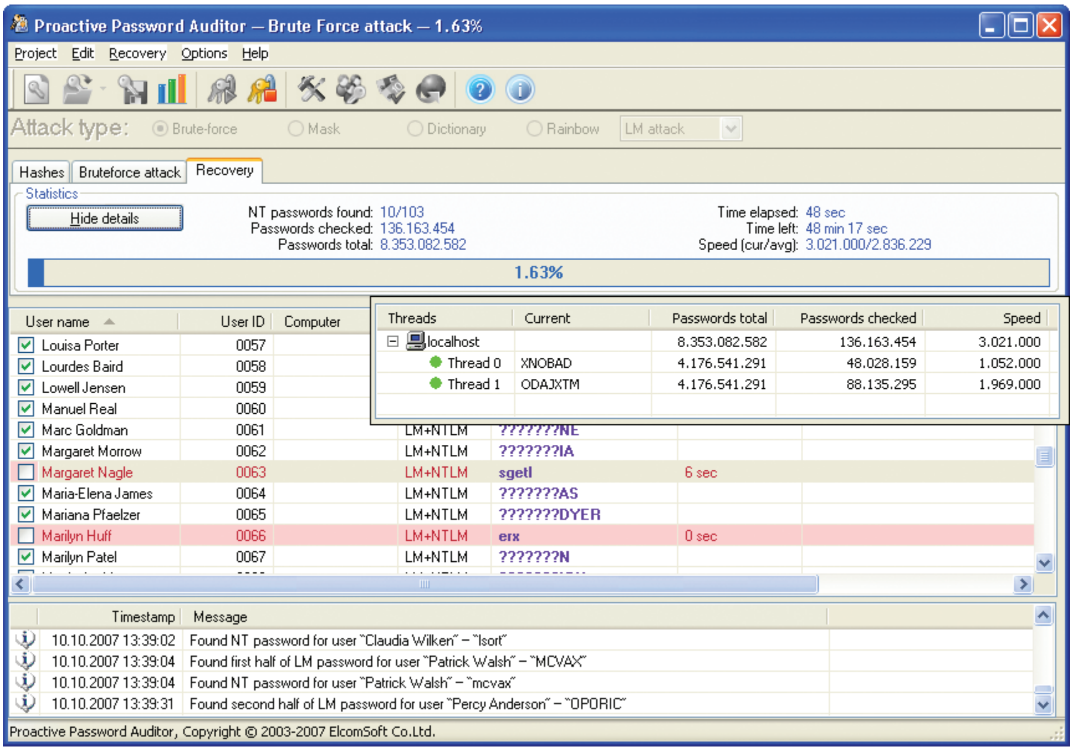
To get password hashes with PPA you may do one of the following:

- read a local PC's memory;
- read remote PCs' memory (with Active Directory support);
- read a local PC's registry;
- use dump files obtained by utilities like pwdump;
- load hashes created with the help of Elcomsoft System Recovery.

Proactive Password Auditor allows carrying out a password audit within a limited period of time. This product uses unique algorithms while optimizing search speed. After completing the audit you should remember that replacing weak passwords is just not enough. What if new passwords turn out to be even weaker? Think over a corporate password policy and its efficiency in the first place. If regular PPA auditing continues to hack too many passwords, then the policy should be reconsidered.

In addition to direct use, PPA can be also used by a system administrator to recover the password of any user (to restore access to encrypted EFS data, saved Internet passwords etc) with brute force attack, dictionary search and rainbow table attack.

You can download Proactive Password Auditor trial here.



Proactive Password Auditor — Brute Force attack — 1.63%

Attack type: ● Brute-force ○ Mask ○ Dictionary ○ Rainbow LM attack

Statistics

NT passwords found: 10/103
Passwords checked: 136.163.454
Passwords total: 8.353.082.582

Time elapsed: 48 sec
Time left: 48 min 17 sec
Speed (cur/avg): 3.021.000/2.836.229

1.63%

Threads	Current	Passwords total	Passwords checked	Speed
⊟ localhost		8.353.082.582	136.163.454	3.021.000
● Thread 0	XNOBAD	4.176.541.291	48.028.159	1.052.000
● Thread 1	ODAJXTM	4.176.541.291	88.135.295	1.969.000

	User name	User ID	Computer			
☑	Louisa Porter	0057				
☑	Lourdes Baird	0058				
☑	Lowell Jensen	0059				
☑	Manuel Real	0060				
☑	Marc Goldman	0061		LM+NTLM	???????NE	
☑	Margaret Morrow	0062		LM+NTLM	???????IA	
☐	Margaret Nagle	0063		LM+NTLM	sgetl	6 sec
☑	Maria-Elena James	0064		LM+NTLM	???????AS	
☑	Mariana Pfaelzer	0065		LM+NTLM	??????DYER	
☐	Marilyn Huff	0066		LM+NTLM	erx	0 sec
☑	Marilyn Patel	0067		LM+NTLM	???????N	

Timestamp	Message
10.10.2007 13:39:02	Found NT password for user "Claudia Wilken" – "lsort"
10.10.2007 13:39:04	Found first half of LM password for user "Patrick Walsh" – "MCVAX"
10.10.2007 13:39:04	Found NT password for user "Patrick Walsh" – "mcvax"
10.10.2007 13:39:31	Found second half of LM password for user "Percy Anderson" – "OPORIC"

Proactive Password Auditor, Copyright © 2003-2007 ElcomSoft Co.Ltd.

Picture 1. Proactive Password Auditor audits user passwords.

ABOUT ELCOMSOFT

Founded in 1990 in Moscow, Russia, ElcomSoft is a leader in the password/system recovery and forensics market. Thanks to one-of-a-kind technologies, ElcomSoft's products have garnered wide recognition both in Russia and abroad.

ElcomSoft's clients include many well known international companies from the following sectors:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

ElcomSoft is a Microsoft Gold Certified Partner, Intel Software Partner, as well as a member of the Russian Cryptology Association, the Computer Security Institute (CSI), and the Association of Shareware Professionals (ASP).

ElcomSoft is an acknowledged expert in the password/system recovery and forensics market. The company's technological achievements and opinion leadership is quoted in many authoritative publications. For example: "Microsoft Encyclopedia of Security", "The art of deception" (Kevin Mitnick), "IT Auditing: Using Controls to Protect Information Assets" (Chris Davis), "Hacking exposed" (Stuart McClure).

Visit our website to find out more.

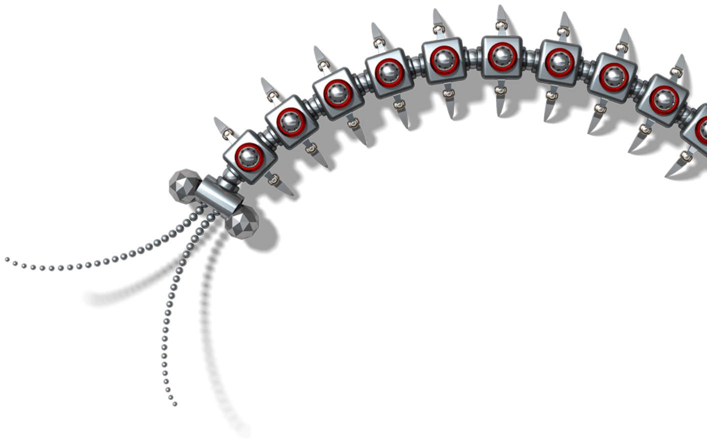
ADDRESS:
Elcomsoft
Zvezdny bulvar 21, office 541
129085 Moscow, Russian Federation

FAX:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

WEBSITES:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr

intel
Software
Partner

Microsoft
GOLD CERTIFIED
Partner



Copyright (c) 2007 ElcomSoft Co.Ltd.
All right reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Intel and Intel logo are registered trademarks of Intel Corporation. Elcomsoft and Elcomsoft logo are trademarks or registered trademarks of ElcomSoft Co.Ltd. Other names may be trademarks of their respective owners.