MARCH 2020

Password Cracking

Case Study

LIFARS
your digital world, **secured**

Contents

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

OVERVIEW

For this case study we extract used plaintext passwords from more than 1,500,000 cracked active directory hashes from LIFARS' former pentests.

PASSWORD CRACKING

When we black box penetration test or Red team internal or external systems, we often have hashes. These hashes are subsequently cracked for checked vulnerable password policy. This is a very old a method to get a plaintext password and reuse it for other systems and infrastructure devices.

For external pentests, the most common hash sources are SQLi, path traversal, and IKE aggressive mode handshake.

For internal pentests, hash sources are mostly MItM for authentication of AD, DB and web services, IPMI, and kerberoasting.

The difference of the normal user password selection depends on the type of system and password policy.

Web-based interfaces, where there is less restriction on password policy, choose simpler passwords and much more usable dictionaries.

In the case of a multinational corporation or a worldwide web service, the native language and cultural habits of the user or of the corporation's branch office are important factors.

It could be assumed that all passwords are written in English or Lantin. The following examples show that is not so

Дерпароль
василиса
йцукен21
масяня10
яфйцычсву
фывфывфыв
саша1964
Ńlkjhgfdsajose
ôlkjfdsa123
$äöLkjhgfd
österreich2014
Ómama1922
§§Gruenling

¨üpoiuzt
Üpoiuztre2
&é"'azer
CoÿnnÿecÿT
ńńńńńńńń
ŕŕŕŕŕŕŕŕ
ńlkjhgfdsa
ńlkjhgfdsajose
ß0987654
Čiovo+123
Ákos1217
éTzyden1
äúp2015*

µµµµµµµµ
Ü35Training
¨üpoiuzt
ŁPerot2000
ľščťžýáíé.11
+ľščQWERasdf
miroslav+íáí
1Q2W3E4Rť't
1Q2W3ečr
Gronštolne700
ôôô1111
ôlkjfdsa123

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

In addition to the language used, passwords differ significantly in the cultural context that influences the choice of password.

It has to be said that there are no published statistics or dictionaries of leaked or found entries for each language that could be used as a solid basis for an attack.

This factor derives from the 100/0/0 most common words for a language. These are well documented everywhere for English, but much worse for Arabic, Chinese, or Danish. The use of Latin, a dead language is also no exception.

A closely related factor to the language is also the localized character set used (many times depending on the service used), which, without adequate dictionaries, makes it impossible to search effectively.

Someone who thinks that a dictionary in a language can be generated, for example, by downloading the language mutation from Wikipedia is wrong. The dictionary used by users for passwords is different from the word form used in the common language.

In a corporate environment, entropy of passwords is ensured by at least a preset Active Directory policy. Even if there are brave people who are humiliating, in most cases they are kept and promoted many times just before the pentests :)

This hash cracking methodology is well known and implemented by all red teams and pentesters, for which reason I will not explain it here any further.

Cracked hashes are also used in pentests for escalation of rights, and other information about domain control and other systems.

PASSWORD CRACKING VALUE FOR INTERNAL TESTS

In the case of an internal organization test and successful LDAP or Active directory compromise, we automatically perform password testing for a crack.

Apart from the recommendations for improving the password policy, the output also includes the occurrence of unique and complicated passwords in public dictionaries.

There are many sites that allow cracking passwords by anonymously typing hashes.

If there are complex, unique passwords in dictionaries of such websites, it can be an important Indicator of Compromise (IOC)

This indicates either the use of the same password by users on one of the publicly scared websites or the former compromising organization.

This data can be another source besides the dark web, since the compromised data does not have to be generally traded.

In any case, such a fact requires the attention of a CISO or retraining of the user.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com