Lab : Password Cracking

CSE3801 : Introduction to Cyber Operations

Introduction to Password Cracking

In class, we learned how the operating system stores passwords as hashes. Although cryptographic hashing is a one-way function, poorly chosen passwords, weak salting, and restrictive password policies can often lead to an attacker *cracking* the hash by calculating and comparing hashes against potential passwords.

Password Audit

A private company asked you to audit their password policies as a network penetration tester. After meeting with the CISO, he tells you his business has been under attack, and they believe weak passwords have enabled the attack. He permits you to audit his password policy. You ask for any documentation regarding the password policy and are provided with the emails below, and a list of hashed passwords. He asks if you can crack them.

```
From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: August 30, 2019 at 11:30 AM EDT
To: IT Managers

Team,

Our executives are having a terrible time remembering their passwords.
Ask them to use their favorite animal with a capital letter for
the first letter. I have attached a list of animals to this email.

<<attachment: Animals.txt>>

Bob Smith | CISSP
EvilCorp, North Atlantic Division
```

From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: August 30, 2019 at 1:30 PM EDT
To: IT Managers

Team,

Hackers have cracked our executive’s passwords. We think they are using a dictionary of animal names. Have the executives replace every letter e with a number 3. This should prevent the attack.

Bob Smith | CISSP
EvilCorp, North Atlantic Division

From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: August 30, 2019 at 4:30 PM EDT
To: IT Managers

Team,

It seems the attackers have figured out our latest strategy. Have the executives just concatenate two animals together as their password. This should make it much more complex and harder to attack. So Advark+Bear=AdvarkBear. No way they are guessing these passwords.

Bob Smith | CISSP
EvilCorp, North Atlantic Division

From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: August 31, 2019 at 3:30 PM EDT
To: IT Managers

Team,

It seems that didn’t work well either. Instead, have the executives alternate upper and lower case letters. So Advark should become AdVaRk. This will definitely fool the attackers.

Bob Smith | CISSP
EvilCorp, North Atlantic Division

```
From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: September 1, 2019 at 7:30 AM EDT
To: IT Managers

Team,

I just came from a meeting at the CISO’s office on the C-suite. He advised us
to use three letters from one animal concatenated with three letters from
another. Something like Advark+Bear=AdvBea.

Bob Smith | CISSP
EvilCorp, North Atlantic Division
```

```
From: Administrator <admin@evilcorp>
Subject: Password Policy
Date: September 2, 2019 at 2:30 PM EDT
To: IT Managers

Team,

One of our admins came up with the idea of having the executives use only
animals greater than seven letters and then append two numbers as their
password. Something like Elephant99.

Bob Smith | CISSP
EvilCorp, North Atlantic Division
```

John The Ripper Toolkit

John the Ripper (JTR) is a fast password cracker, currently available for many flavors of Unix, macOS, Windows, DOS, BeOS, and OpenVMS. [1] We will use it today to examine weak password schemes.

To run John, you need to supply it with a file of hashes (here shadow) and optionally specify a cracking mode or a list of potential passwords (foo.txt) to check. On your lab workstations, you will need to provide it the full path to execute.

```
john -wordlist=foo.txt shadow.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Press ’q’ or Ctrl-C to abort, almost any other key for status
letmein         (root)
```

Hints

1. It will probably benefit you to create your new dictionary files. You are welcome to write scripts to automate building your new dictionaries. For example, this would produce a new file containing passwords where the letter a has been replaced with a 4.

```
f = open(’Animals.txt’)
f2= open(’L33t-Animals.txt’,’w’)
for line in f.readlines():
    if ’a’ in line:
        newline=line.replace(’a’,’4’)
        f2.write(newline)
f.close()
f2.close()
```

2. Password salts are used to introduce complexity into password cracking. Is there anything you notice about salts in the data set given to you by the CISO?

Lab Deliverables

1. Your lab report containing an overview, methodology, and results sections. You must discuss what passwords you were able to crack, why and offer insight on how the CISO could safeguard passwords better in the future. Consider salting, hashing algorithms, and policies in your response.

2. A list of the passwords your team cracked.

Extra Credit (+10)

The group with the most cracked passwords. - To be eligible for this, your group must submit your cracked passwords via Canvas within before the end of class.

References

[1] Openwall *John the Ripper* (https://www.openwall.com/john/), 2019.