CSE331 Fall'21: Project 1

PassWord123

Radu Sion
Soroush Meghdadizanjani

Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end-users. However, it is a well know problem in security that human chosen passwords are inherently insecure. There have been studies [1] which suggest that most users end up choosing their passwords from a small domain. This enables adversaries to attempt to login to accounts by trying all possible password combinations, using a technique known as "dictionary attack".

One of the most popular tools to launch a dictionary attack is *John the Ripper*. John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. Security researchers and enthusiasts have been using this tool for several years to audit leaked passwords. For this project, your aim is to get familiarized with this tool and use it to study password based authentication in different forms.

1 Ethics Statement

We will be covering topics involving personal and public privacy and security, and security of many systems that are widely deployed and potentially critical. Throughout this course, and its projects, we will investigate methods, tools and techniques whose use may negatively impact the rights, property and lives of others. As security professionals, we rely upon the ethical use of all the technologies available to us to perform research. However, it is easy to use such tools in an unethical manner. Unethical use includes the circumvention of existing security or privacy measurements for any purpose, or the dissemeniation, promotion, or exploitation of vulnerabilities of these services. DO NOT conduct any action that could be perceived as unethical behaviour or a misuse of the technology provided to you. You are expected to abide by the Code of Ethics and Professional Conducts linked to on the course website.

2 Setup

You need to install John the Ripper tool on your OS to get started with this project. You can easily find the detailed steps online to install the tool on your OS, but a good starting point would be the

official website `https://www.openwall.com/john/`.

There are two versions available for the tool, a minimal version which comes included with most software repositories (on linux), and the jumbo version (v1.9.0) which is the full fledged tool with a lot more powerful options. It is highly recommended that you install the jumbo version, as the minimal version may limit your experiments. *Note: You do not need the PRO version for this project.*

2.1 Learn about the tool

Refer to the man pages and other documents available for JtR (John the Ripper) and answer the following questions.

- What are the various hashing algorithms that JtR can crack?
- What are the various types of attacks you can do using JtR? Assuming that your main objective is to crack passwords, what are the different techniques to do so?

3 Password protected ZIP files

The first part of this project is to crack open the zip file provided to you. The **passwords.zip** file contains the password dump which you will need for the next part of the project. However, this zip file has been encrypted using a key that will not be shared with you.

You will need to figure out how to use *John the Ripper* to crack open this file by extracting the encryption key used. Document all the steps on how you used the tool to find the encryption key, and provide screenshots to show that you were able to decode the key using the tool.

3.1 Learning outcome

Answer the following questions:

- How long did it take for you to figure out the encryption key for the zip file?
- If this file contained more sensitive information, what could the owner do to protect their files from attackers?
- What would be your recommendation for users who want to share sensitive information in ZIP files without having to share the password with anyone? Only the intended recipient should be able to decode the file without knowing the key the sender used.

4 Cracking Password databases

Once you have extracted the contents from the zip folder, you will find 3 text files containing password dumps. These password dumps were part of a DEFCON password cracking challenge quite a few years ago, and lists usernames and their password hashes.

For the purposes of this project, assume that the attacker (you) has obtained this password dump from a social networking website and intends to compromize as many user accounts as possible. Your goal is then to leverage the tools at your disposal and obtain the passwords of as many users as you can.

Document every step you took to decode the files and provide screenshots to show the process.

4.1 Tricks of the trade

There are some techniques which you can use to make your password cracking process a bit easier.

- Each of the three files provided to you use different hashing algorithms. Before you can successfully decode all the hashes, figure out which hashing algorithm is used for each file.
- Based on our discussions in class, can you figure out what makes human selected passwords more vulnerable? Can you devise a technique to identify the most vulnerable passwords in the dataset easily?
- Understand how different Password Cracking techniques work and use them efficiently for each type of hashing algorithm.

4.2 Learning Outcome

Answer the following questions:

- What were the hashing algorithms used in each file? What did you learn about the difficulty of cracking them, and which techniques work best for each?
- Do you have any interesting observations from the password dumps? How do you think most users choose their passwords? Did you notice any common patterns in users' passwords?

5 Cracking User Accounts

Password based authentication is not only limited to social media websites or just on Internet, but also our own personal computers. When you create a user account on your computer, it saves the username and the subsequent password somewhere locally which it then uses later for user authentication.

Assuming an attacker is able to gain physical access to your computer, how would they be able to retrieve your username and passwords?

5.1 Password Storage

Figure out how do Windows and Linux store username and passwords locally on the system. You need to find out what cryptographic hash function do they use, what format is it stored in, and how does attacker gain access to the location where the passwords are stored.

List out all these information for Windows and Linux systems.

5.2 Attacking a Linux User

Assume that you are provided with a system for shared usage (like computer labs in university), and it provides *sudo* privileges to all users. Demonstrate how an adversary can take advantage of this *privilege* to login as another user on the system.

For this part, you will need to install an Ubuntu 18.04 VM. You can use VirtualBox to create your VM and you can retrieve official desktop image from `https://releases.ubuntu.com/18.04/`.

Then you need to create multiple user accounts on that VM with sudo privileges. Create at least 3 user accounts for the purpose of this exploit. Now, using what you have learnt from the previous exercises, demonstrate how the attacker will be able to obtain the stored credentials of all users.

As a security professional, what would be your recommendation to the system administrator on how privileges should be managed on a shared computer?

References

[1] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, pp. 5–14, 1990.