**Cracking Password-Protected Zipped Files using John the Ripper.**

**Objective:**

To understand the process of password-protecting zipped files and using John the Ripper to crack the password.

**Tools Used:**

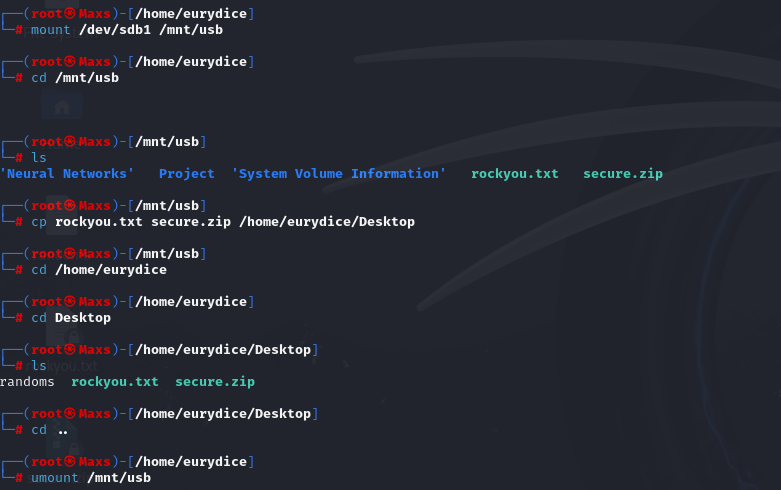
A Kali virtual machine (VM)

John the Ripper

A wordlist for password cracking i.e. rockyou.txt

**Steps**

1. I downloaded the password protected zip file as well as the wordlist and transferred them to my VM via usb

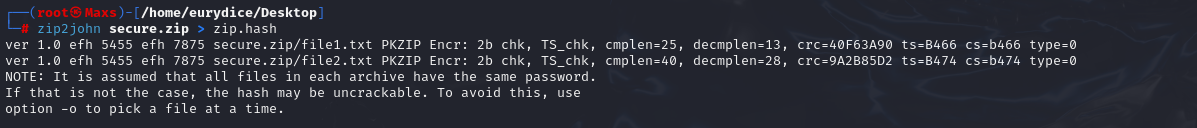


1. Verified that John the Ripper was already running on my machine.

A black background with white text

Description automatically generated

1. I used the zip2hash utility to get the zip file’s password hash so that it can be cracked by John The Ripper.

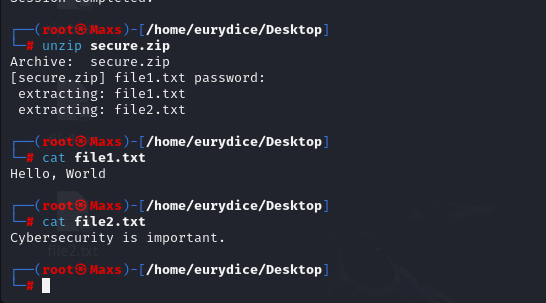


1. I ran the password cracking process by passing the rockyou.txt file as the wordlist argument and the secure.zip as the file whose password we are attempting to crack.

A screen shot of a computer

Description automatically generated

1. The process was completed successfully, and the password of the zip file was found to be ‘hippo’. I attempted to unzip the file with the newly discovered password.



**Analysis of the cracked password**.

The password in question is ‘hippo’ which is a very weak password. In terms of length, the password is short considering strong passwords are considered at least 8 or 12 characters long. Additionally, the password is only made up of lowercase letters hence does not pass the complexity requirements. Strong passwords are required to be a mixture of lowercase letters, uppercase letters, numbers, and special characters. The word ‘hippo’ is also a very common dictionary name which makes it easily guessable and prone to attacks such as dictionary attacks.

**Importance of strong passwords.**

Strong passwords are essential to safeguard your accounts and information against unauthorized access. While most passwords can be cracked, strong passwords make it difficult for the attackers to guess or crack your password due to the complexity. This is also because strong passwords have the benefit of being unique and uncommon, longer passwords also increase the number of combinations that an attacker has to try while attempting to crack your password.

**Guide on Creating Strong Passwords**

* Passwords must be long and complex. They should include a mixture of lowercase and uppercase letters, numbers and special characters.
* They should also not contain any personal information such as birth dates, pet names, SSNs, home addresses etc.
* Users should avoid using variations of the same passwords across different accounts or repeating old passwords.
* Passwords should be updated regularly.

**Advanced File Protection Techniques.**

* Encryption – Using advanced encryption techniques to protect data in transit or at rest.
* Access Control – Implementing access control mechanisms to ensure that only the authorized parties have access to and can modify the files.
* Data Loss Prevention – Configure DLPs to prevent data exfiltration.