Cracking Password-Protected Zipped Files using John the Ripper.

Objective:

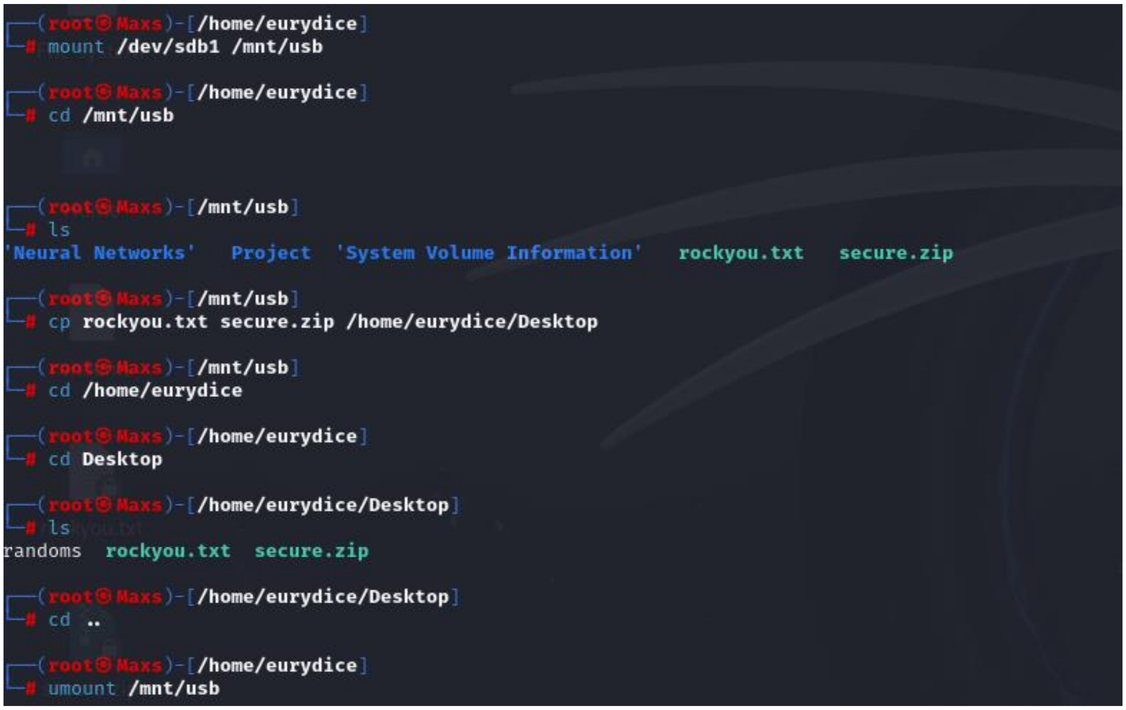
To understand the process of password-protecting zipped files and using John the Ripper to crack the password.

Tools Used:

A Kali virtual machine (VM)
John the Ripper
A wordlist for password cracking i.e. rockyou.txt

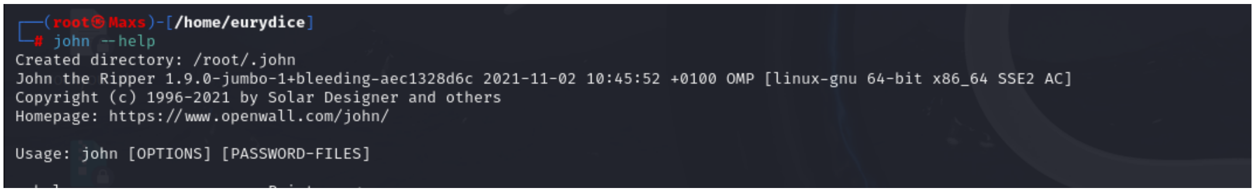
Steps

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



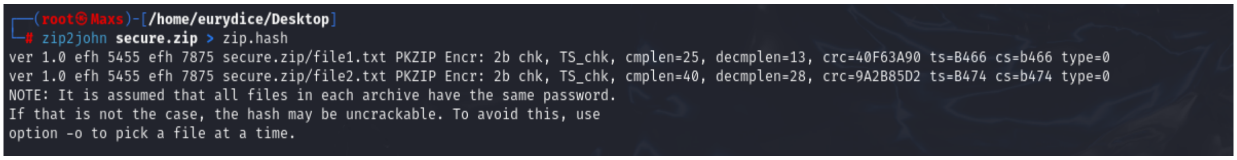
```
┌──(root㉿Maxs)-[/home/eurydice]
└─# mount /dev/sdb1 /mnt/usb

┌──(root㉿Maxs)-[/home/eurydice]
└─# cd /mnt/usb


┌──(root㉿Maxs)-[/mnt/usb]
└─# ls
'Neural Networks'   Project  'System Volume Information'   rockyou.txt   secure.zip

┌──(root㉿Maxs)-[/mnt/usb]
└─# cp rockyou.txt secure.zip /home/eurydice/Desktop

┌──(root㉿Maxs)-[/mnt/usb]
└─# cd /home/eurydice

┌──(root㉿Maxs)-[/home/eurydice]
└─# cd Desktop

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# ls
randoms  rockyou.txt  secure.zip

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# cd ..

┌──(root㉿Maxs)-[/home/eurydice]
└─# umount /mnt/usb
```

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



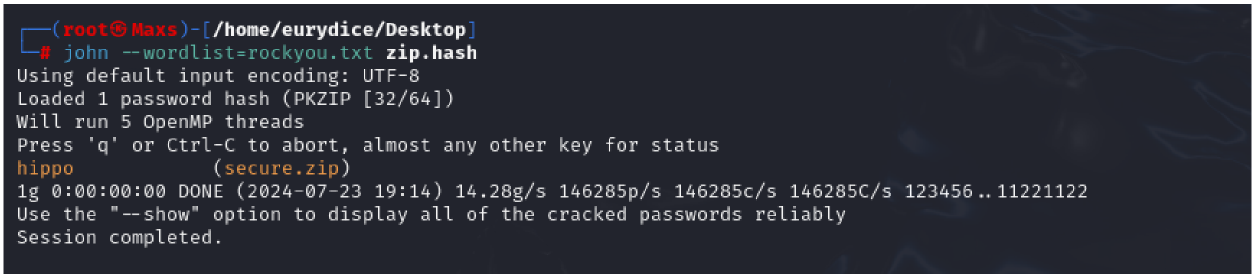
```
┌──(root㉿Maxs)-[/home/eurydice]
└─# john --help
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
```

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



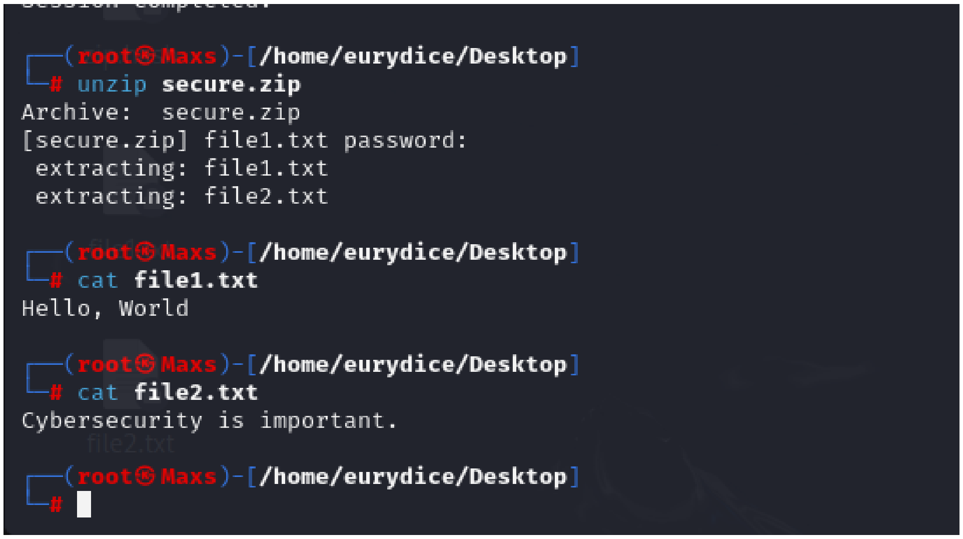
```
┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# zip2john secure.zip > zip.hash
ver 1.0 efh 5455 efh 7875 secure.zip/file1.txt PKZIP Encr: 2b chk, TS_chk, cmplen=25, decmplen=13, crc=40F63A90 ts=B466 cs=b466 type=0
ver 1.0 efh 5455 efh 7875 secure.zip/file2.txt PKZIP Encr: 2b chk, TS_chk, cmplen=40, decmplen=28, crc=9A2B85D2 ts=B474 cs=b474 type=0
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

4. 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.



```
┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# john --wordlist=rockyou.txt zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hippo            (secure.zip)
1g 0:00:00:00 DONE (2024-07-23 19:14) 14.28g/s 146285p/s 146285c/s 146285C/s 123456..11221122
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

5. 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.



```
Session completed.

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# unzip secure.zip
Archive:  secure.zip
[secure.zip] file1.txt password:
 extracting: file1.txt
 extracting: file2.txt

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# cat file1.txt
Hello, World

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# cat file2.txt
Cybersecurity is important.

┌──(root㉿Maxs)-[/home/eurydice/Desktop]
└─# 
```

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.