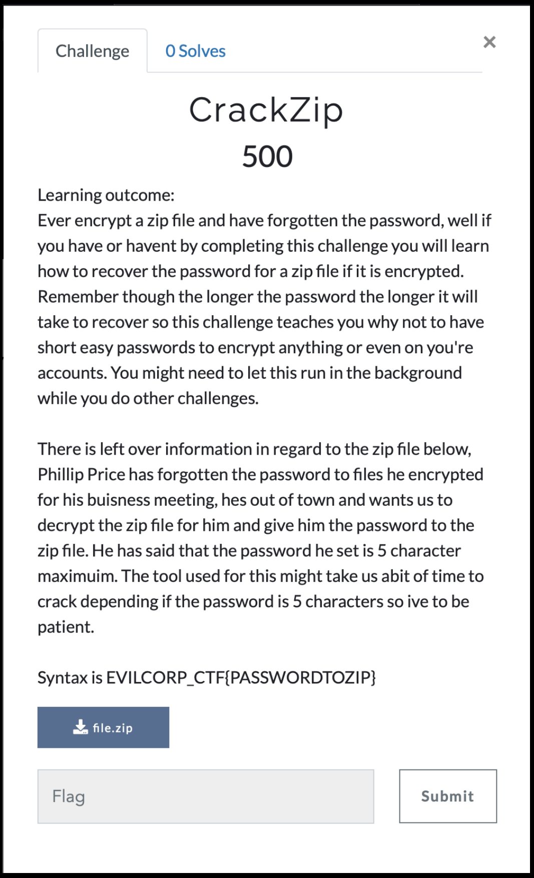
MR. ROBOT

1. In this challenge there is a zip file which is encrypted with a password and the password needs to be found for the answer to the challenge.



CrackZip

500

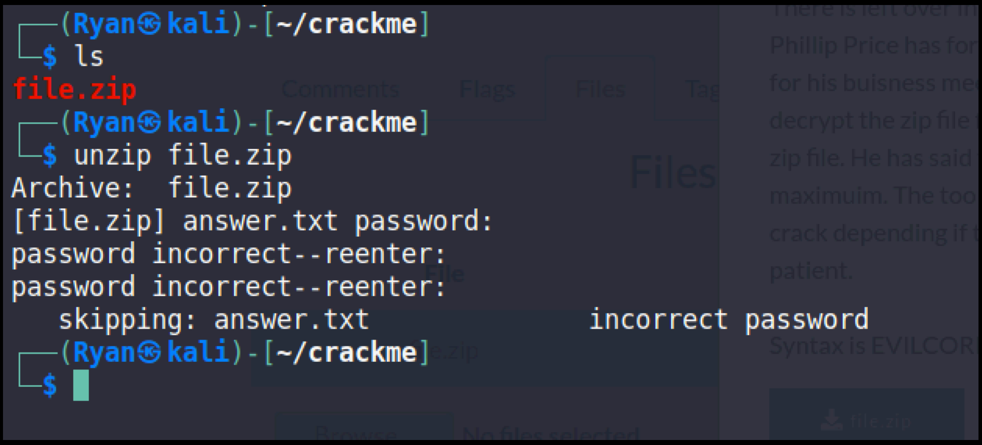
Learning outcome:
Ever encrypt a zip file and have forgotten the password, well if you have or havent by completing this challenge you will learn how to recover the password for a zip file if it is encrypted. Remember though the longer the password the longer it will take to recover so this challenge teaches you why not to have short easy passwords to encrypt anything or even on you're accounts. You might need to let this run in the background while you do other challenges.

There is left over information in regard to the zip file below, Phillip Price has forgotten the password to files he encrypted for his buisness meeting, hes out of town and wants us to decrypt the zip file for him and give him the password to the zip file. He has said that the password he set is 5 character maximuim. The tool used for this might take us abit of time to crack depending if the password is 5 characters so ive to be patient.

Syntax is EVILCORP_CTF{PASSWORDTOZIP}

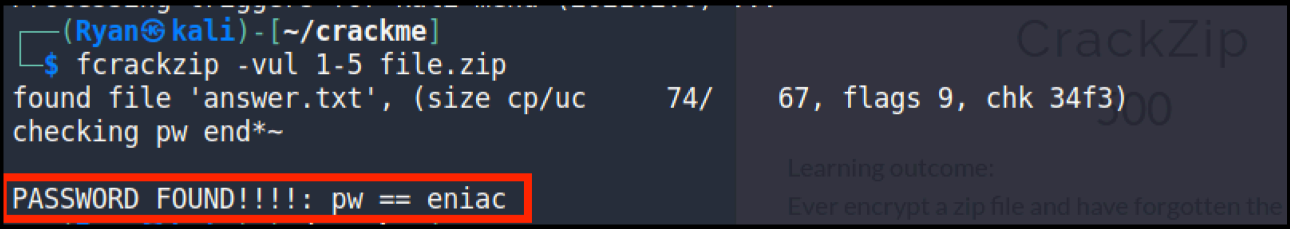
2. Download the Zipfile onto the system your using. The following commands will be explained:
   LS - Listing the directory that the zip file is saved in
   unzip file.zip - try to unzip the file but as you can see there is a password.

So as you can see the file is encrypted with a password and in order to unzip the file the password needs to be found



```
┌──(Ryan㉿kali)-[~/crackme]
└─$ ls
file.zip
┌──(Ryan㉿kali)-[~/crackme]
└─$ unzip file.zip
Archive:  file.zip
[file.zip] answer.txt password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: answer.txt              incorrect password
┌──(Ryan㉿kali)-[~/crackme]
└─$ 
```

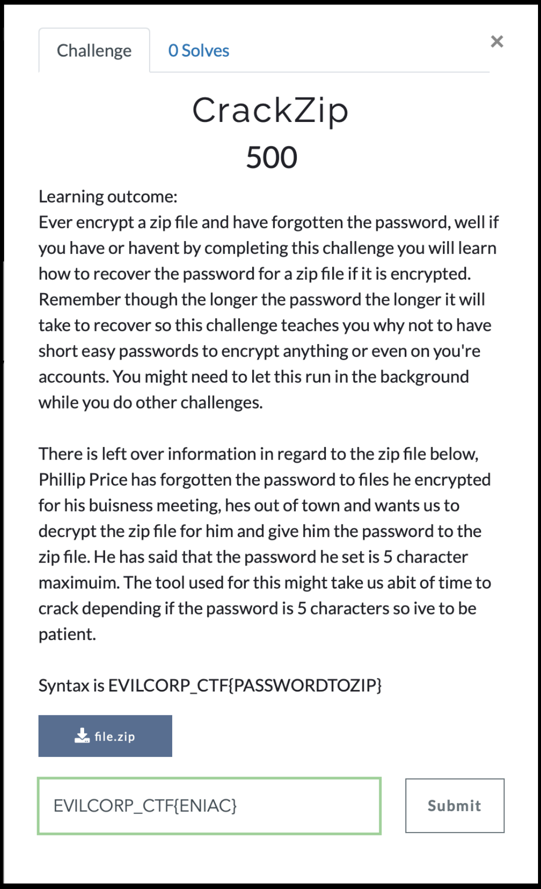
3. Using fcrackzip the password can be brute forced. The command used was fcrackzip -vul 1-5 file.zip. The following command will brute force any password that has a length that is 1-5 characters long, the challenge description gives the hint that this password is 5 characters in length max. Remember that this challenge takes time for example on the machine that ran this it took 15 minutes, so don’t worry if its taking a long time the password eniac will be found eventually.



```
┌──(Ryan㉿kali)-[~/crackme]
└─$ fcrackzip -vul 1-5 file.zip
found file 'answer.txt', (size cp/uc     74/    67, flags 9, chk 34f3)
checking pw end*~

PASSWORD FOUND!!!!: pw == eniac
```

3. So after finding there password being ENIAC, put this in the flag to complete the challenge which is EVILCORP_CTF{ENIAC}



CrackZip

500

Learning outcome:
Ever encrypt a zip file and have forgotten the password, well if you have or havent by completing this challenge you will learn how to recover the password for a zip file if it is encrypted. Remember though the longer the password the longer it will take to recover so this challenge teaches you why not to have short easy passwords to encrypt anything or even on you're accounts. You might need to let this run in the background while you do other challenges.

There is left over information in regard to the zip file below, Phillip Price has forgotten the password to files he encrypted for his buisness meeting, hes out of town and wants us to decrypt the zip file for him and give him the password to the zip file. He has said that the password he set is 5 character maximuim. The tool used for this might take us abit of time to crack depending if the password is 5 characters so ive to be patient.

Syntax is EVILCORP_CTF{PASSWORDTOZIP}

EVILCORP_CTF{ENIAC}