The Writeup for 5020 Password protected ZIP

Introduction

The mission is to crack a password protected ZIP archive.

Writeup

Vulnerability

This is a password protected ZIP file. All password protected security mechanism is vulnerable to brute-force and dictionary attacks.

Exploit

I plan to use `fcrackzip`, which is a ZIP file password crack tools. Following command will crack this ZIP file to show the password is `close`.

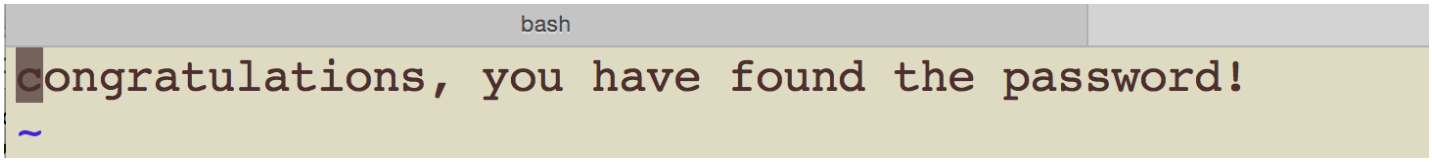
```
hacking-lab.com$ fcrackzip -b -D -p /usr/share/wordlists/rockyou.txt -u ./Geheim.z
ip

PASSWORD FOUND!!!!: pw == close
```

Among the parameters, `-b` means brute-force attack and `-D -p` means dictionary attack with password file `rockyou.txt`. Finally, `-u` means trying to decrypt ZIP file by `unzip`.

The content of the extracted file `Geheim.txt` is
`congratulations, you have found the password!`

The snapshot is followed.



Mitigation

The first comment is that the password should follow best practice. For example, at least 8-16 characters, with no meaningful mixture combination of lower and upper alphabet, numbers and special characters.

Another security issue in ZIP file is that PKZIP Stream Cipher is vulnerable to a know plaintext attack[1,2].

Password protected ZIP file is not a good way to provide confidentiality of documents. In my opinion, zip and encryption with AES-256 is better.

Conclusion

Short password is easy to be cracked by brute-force and dictionary attacks.

reference

1. Biham, Eli and Paul Kocher. “A Known Plaintext Attack on the PKZIP StreamCipher.” FastSoftwareEncryption2, ProceedingsoftheLeuven Workshop, LNCS 1008, December 1994.
2. Stay, Michael. "ZIP attacks with reduced known plaintext." Fast software encryption. Springer Berlin Heidelberg, 2002.