Password cracking

In the GitHub repo, you will find a file called: “challenge1.zip” – This is an encrypted zip-file, that you need to find the password for.
The password is very weak (between 4 or 6 characters) so it should be fairly easy to brute-force.
Use “fcrackzip” (or any other tool that you like (and makes sense)) to brute-force the password.
When you’ve got the password, you can unzip the content, which is the next challenge (and the information for that challenge).

PGP / GPG email

Encrypt everything!!

A lot of people send messages and e-mails unprotected. This is a very bad idea (in case you were not aware.) Therefor it would be a good idea to start securing the e-mail that you send.

1) Setup PGP, so that you can encrypt your e-mails, by following this guild:
   Windows: https://ssd.eff.org/en/module/how-use-pgp-windows
   Linux: https://ssd.eff.org/en/module/how-use-pgp-linux
   Mac OS: https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
2) Send an encrypted e-mail to someone that uses PGP, and tell them how awesome this is!!

TLS certificates

When we are browsing the web, it is always a good idea to use a secure connection. For this to happen, the server that we connect to, needs to have a TLS certificate, so that we can establish an encrypted connection between the two endpoints.

Not that long ago, the only way to get a SSL/TLS certificate, was to create one yourself – But, since no one was verifying that homemade certificate, the user would get some “nasty” messages on their screen, which would make them feel not so happy. So, what you would do instead, was to pay a lot of money to have a company to verify that this is a trusted certificate.

Luckily, those days are coming to an end. “Let’s encrypt” provides a service where they can generate a trusted TLS certificate for you, for free!! https://letsencrypt.org

1) Install an apache server on your Ubuntu VM.
2) Use “Let’s encrypt” to create a TLS certificate and add it to your apache server.