Encryptie

In dit labo gaan we dieper in op het onderwerp encryptie en decryptie.

Wat ga je leren in dit labo?

- Burpsuite gebruiken voor Base64 decoding te doen
- Caesar Cypher toepassen
- GPG gebruiken voor encryptie en decryptie van files en berichten.

Voorbereiding

- Lees het deel over base64 encoding in het onderdeel base64 encoding in de syllabus op gitbook.

  https://app.gitbook.com/@apwt/s/g-pro-software-security/hashing/base64-encoding

- Lees het deel over asymmetrische encryptie in het onderdeel GPG in de syllabus op gitbook.

  https://app.gitbook.com/@apwt/s/g-pro-software-security/hashing/encryptie-tools#assymmetrische-encryptie

Stappenplan

1. Download op open het eastere.gg bestand van de beveiligde ftp van de juice shop (zie labo 1)

   Daar vind je een geheime boodschap dat geëncodeerd is in Base64. Decodeer eerst dit bericht en vul het hier onder in.

   ```
   Original bericht -> L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
    Gedecodeerd bericht -> /gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt
   ```

   ▶ Eerste tip

2. Nu je dit bericht gedecodeerd hebt lijkt het nog altijd niet leesbaar te zijn.

   Er is een een caesar cipher gebruikt. We weten wel niet hoeveel de letters opgeschoven worden (we noemen dit de shift).

3. Je kan hiervoor een caesar cipher webtool voor gebruiken. Zorg er zeker voor dat je

   `TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)`

   hebt aanstaan.

4. Vul het geheime bericht hier in het tekstveld in:

   ```
   /the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
   ```

   en wat was de shift van de caesar cipher

   13

5. Maak een bestand `wiebenik.txt` aan met als inhoud voor en achternaam in.

6. Open je terminal en gebruik `gpg` om dit bestand te encrypteren met **symmetrische encryptie**. Gebruik het paswoord `labo_2425`. Je krijgt nu een bestand `wiebenik.txt.gpg`

7. Dit is een geëncrypteerd bestand. Probeer dit bestand eens uit te lezen met notepad of een andere editor, wat merk je op?

   ```
    De inhoud van dit bestand is compleet onleesbaar geworden, hier kan je niets meer uit opmaken zonder de
    decryptie eerst uit te voeren.
   dit is de inhoud:
   Ȼ
   ▯ ▯▯Ûœ8þO qJâÒP▯ =▯▯▯ð0$çÓ‘o½\U▯.‰Z      ▯°▯ìaŸ²ý!Dý▯▯AÏLµEPý=▯▯,œ|g▯âüù£ÁÉz▯ß¾WÛ¾óoþ]L†Ë¸▯▯›ÓÞ|¥õš
   ```

8. Download het geëncrypteerd bestand awesome.jpg.gpg. Decrypteer dit bestand gebruikmakende van `gpg` met het paswoord `labo_2425`.

9. Open dit bestand... And feel awesome! 🦄

10. Ga naar de online pgp tool op https://smartninja-pgp.appspot.com/#

11. Genereer zelf een PGP keypair voor jezelf. Kies RSA als algoritme en een keysize van 1024bit. Zorg ervoor dat de sleutel nooit vervalt. Kies een passphrase en zorg ervoor dat je deze onthoudt.

12. Probeer een bericht te encrypteren met mijn publieke sleutel. Je mag hier zelf kiezen wat je stuurt. Mijn publieke sleutel kan je hier vinden.

12. Plaats het geëncrypteerde bericht in een bestand genaamd `encrypted_message.txt`.

13. Probeer met je eigen public key zelf een bericht naar jezelf te encrypteren en daarna vervolgens te decrypteren.

14. Als extra kan je eens een bericht naar jezelf proberen te sturen met je eigen publieke sleutel. Of je probeert eens samen met iemand anders geheime berichten naar elkaar te sturen.

15. Print deze pagina af als PDF en slaag deze op als `naam_voornaam_labo_encryptie.pdf`

    Zip alle bestanden die je in dit labo hebt aangemaakt en stuur deze in via digitap. Deze bestanden zijn:

    - wiebenik.txt.gpg
    - encrypted_message.txt
    - awesome.jpg
    - naam_voornaam_labo_encryptie.pdf