ynov CAMPUS

HACKY' NOV

HACKY' NOV

WRITEUP

Web

PerfectLab

Billy Desquiens

Table des matières

1. Recherches sur le site web :

Quand nous nous connectons sur le site web du challenge nous obtenons cette page web :

Le lien qui affiche « Accéder à votre compte » affiche cette page :

Ces deux pages sont codées exclusivement en HTML et JS, aucune fonction majeure n'attire l'attention. La présence d'un commentaire ,un chiffre à 4 digits est à souligner.

Le seul élément en commun et plutôt flagrant sur cette page est l'image de fond.

Il y a en réalité quelque chose de dissimuler dans cette image (sans le savoir il faut effectuer des tests ou demander un indice pour s'en rendre compte).

2. Steganographie :

Une fois l'image téléchargée, on veut tester de récupérer un éventuel (et dans notre cas réel) message caché dans l'image.

On va donc utiliser l'outil steghide pour essayer de ressortir le message caché du fichier labo.jpg.

```
└─$ steghide extract -sf labo.jpg
Entrez la passphrase:
steghide: impossible d'extraire des donn◆es avec cette passphrase!

┌──(tialoc㉿ptbd)-[~/Téléchargements]
└─$
```

Une passphrase est demandée, on va donc utiliser l'outil stegcrack avec le dictionnaire rockyou pour tenter de récupérer le message caché.

```
┌──(tialoc㉿ptbd)-[~/Téléchargements]
└─$ stegcracker labo.jpg /usr/share/wordlists/rockyou.txt                    1 ×
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'labo.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: nintendo
Tried 1807 passwords
Your file has been written to: labo.jpg.out
nintendo
```

Réussite ! La passphrase était « nintendo ».

Regardons le message caché.

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAqkvSQFHEWSUCO9koIWqps7olV+61iev+Ot0FW4DXAFVYtmQjl3Zl
Kpx3TZQCppApwndmzQR5oKz3ZP3KYcDEvK6QCEuA9bqiEWVNVYbMJY9vJ98FgsDMzp/Rje
nh4HegR7Q7sW0P5gVAg0yVVsiq8oEDYbZEXD4pIJwF6vrzmZya0JQUFaTVld3tjE5suxAE
zLCTMmy5oQ+fWK1FmXa1PYrc47Vn7dy7C8XNEjf5Hwatq4ow+9YWSK6XLKB0e6LH2s9IgY
Vobd6q8vyjuRC/RTBduDqsRj9Ji1zFBPJv04nrWIrigC3y/yBvofjBoYftA+YuTu9ttx7t
9MT4QDg5+QAAA8DSRw1N0kcNTQAAAAdzc2gtcnNhAAABAQCqS9JAUcRZJQI72Sghaqmzui
VX7rWJ6/463QVbgNcAVVi2ZCOXdmUqnHdNlAKmkCnCd2bNBHmgrPdk/cphwMS8rpAIS4D1
uqIRZU1Vhswlj28n3wWCwMzOn9GN6eHgd6BHtDuxbQ/mBUCDTJVWyKrygQNhtkRcPikgnA
Xq+vOZnJrQlBQVpNWV3e2MTmy7EATMsJMybLmhD59YrUWZdrU9itzjtWft3LsLxc0SN/kf
Bq2rijD71hZIrpcsoHR7osfaz0iBhWht3qry/KO5EL9FMF24OqxGP0mLXMUE8m/TietYiu
KALfL/IG+h+MGhh+0D5i5O7223Hu30xPhAODn5AAAAAwEAAQAAAQBp/TjFiV6QMQV75EMi
0TT/xEo7uTlJtxSK5EbSVZT7AyNsmVTBjxGV/L4QDZ+8tRsYiqHz1eYxR5XOSFqujoCkAm
1ojD2eMuNtukPwiC4E7om7IgZXA9I0g6m0Dq3ju/CI0DcazYtImVo2nfKQieJDfmJxbTSM
yK9mOVVBk6ELqDSvpkuXEa1UUnEVZP88H4WfyXeYspiPYKmADX6Eqe2jOpiCZJ4aQ+i2Vl
yHNYdSQ/XEQNw/ORLf50Lq9fl5p6gZxMPvqhXgAoHN4sfOG83GK9jHShZWiMcuD2TxMcLZ
kKimEtsMJXSnvSDrExw7rPU/aqHTMXOT3pSCG8ahlfI1AAAAgE9aSE52of6V+7JNU0S1Zc
DTgJLnVeScOt7bqa/s2eVqS50Kz/MF9AzUren2XmC9Ln7gOfxSPbzoQ2zpDHrCuOaexgJg
uHSRI4f9CPeionvVavn8WtUHQ22TF9jinSG7nthHs5EpnwAiIGD5mfw8OpiB31v4dpobFX
yU9lBIYO+FAAAAgQDi8iqh94Aogz0oTCEoK/3YVDfpXt8aHi+/nbci7Fmld5IQ/0bbnCwj
pLnkatYxoo0kZ6oIHfr0gBcgmGx4OI3SG0F56k0HocfeFknYY33ZFeku4dc7GcMVXLyiqy
TRJnlsmsJbnUrMlShbsYeOHWyZ/hAFsZ1knhmsI7pRzgC+qwAAAIEAwBkJu3C5TnvwFiu4
4MKedGZzqKoMJ+5QvvUxLao0cEZ08P2y8wemPfpHi85wOuG7tLuXGfw33lbylqe6oELzAd
o1tbWKWSPArer/iqcFxfGpIs4caQ4Dc5XYu6MWA/povlCOLrystIsosgxLuV60pWh8lUtZ
/SonUM/3cla/mesAAAALcm9vdEBkb2NrZXI=
```

Le message dissimulé dans l'image est une clé SSH pour se connecter comme demandé au serveur.

Il faut maintenant trouver avec quel compte se connecter.

3. Connexion SSH :

Le port d'écoute se trouve en commentaire sur la page « login.html ».

Pour utiliser la clé SSH, il faut trouver pour quel utilisateur elle a donc été générée. Les deux possibilités sont :

- Jacques Pastel
- Admin

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'labo.jpg.out' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "labo.jpg.out": bad permissions
```

Avant tout test on voit qu'il faut restreindre les droits de la clé SSH (avec « chmod 700 » par exemple)

Après avoir tester plusieurs usernames possibles, on s'aperçoit que c'est avec le user « admin » que la clé fonctionne :

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ whoami
admin
$
```

En effectuant un « ls » sur le serveur distant, nous nous apercevons que le fichier « results » est présent.

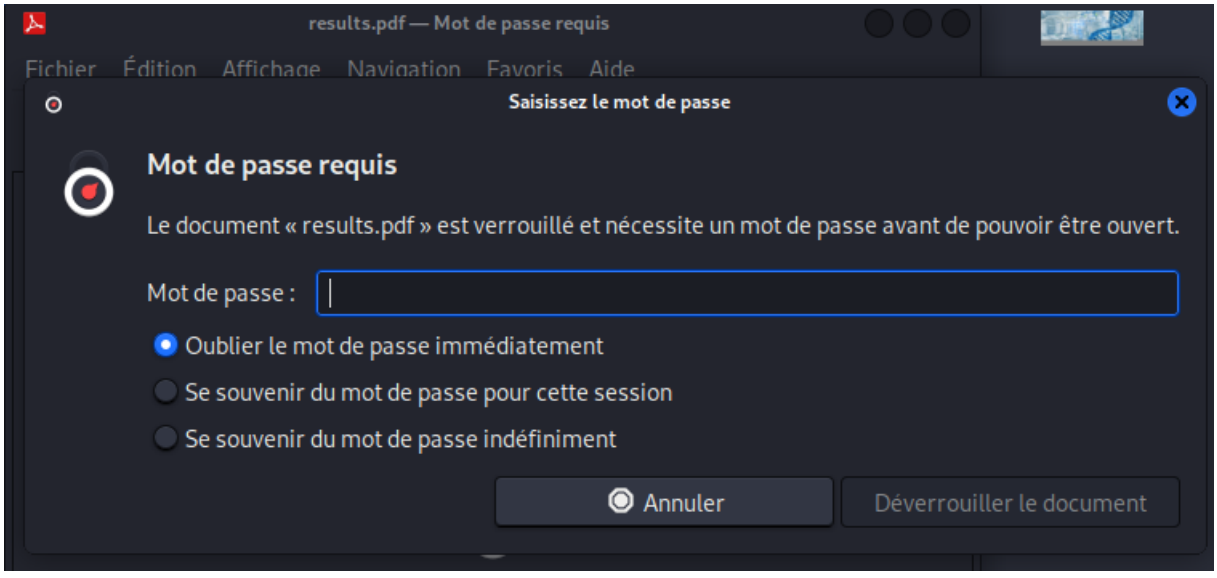
```
$ ls
results.pdf
$
```

Etant un pdf, on ne peut pas l'exploiter avec les commandes cat et more, il faut donc le télécharger en local en utilisant scp :

```
└─$ scp -i labo.jpg.out -P 2223 admin@192.168.1.242:/home/admin/results.pdf ./
results.pdf
```

4. Ouverture du fichier

En tentant d'ouvrir le fichier, on s'aperçoit que celui-ci est protégé par un mot de passe.



Une idée serait d'essayer de craquer ce mot de passe par brute force ou avec un dictionnaire cependant, si c'était possible, le mot de passe serait craqué une fois l'évènement terminé.

Si on se rappelle le site web est un site d'un laboratoire, et les laboratoires de tests biologiques ne sont pas réputés pour la robustesse de leurs mots de passe ni par le moyen de les communiquer.

En effet, dans les différentes salles de l'évènement, il y a des coupons de résultats de PerfectLab, ces coupons ressemblent à ceci :


PERFECT LAB

COUPON RENDU RESULTATS

Perfect Lab – Aix en Provence
Laboratoire de biologie médicale
www.perfect-lab.com
Horaires : du lundi au vendredi de 07h30 à 19h00
Tél : 0123456789

Né le 07/08/1939
M HEWITT Thomas
Tél : 0701211811
Date 1ère analyse : 12/12/2021
Mot de passe : THE07081939678912122021

A partir du :
Pour le respect de la confidentialité, les résultats de vos analyses ne seront disponibles que sur présentation de ce coupon.
Sauf cas particuliers, aucun résultat biologique ne sera transmis par téléphone.

Si on s'y attarde on peut deviner la composition du mot de passe :

- La première lettre du prénom
- Les deux premières lettres du nom de famille
- La date de naissance (sans les slashs)
- Les quatre derniers digits du numéro de téléphone
- La date de la première consultation (sans les slashs)

Si nous suivons la logique avec les informations personnelles visibles sur le site nous obtenons :

JPA14111975678924122021

Gagné, nous avons accès au fichier, un (faux) résultat de test PCR :

Perfect Lab – Aix en Provence
LABORATOIRE DE BIOLOGIE MEDICALE
www.perfect-lab.com

Dr Mah Boulh

Dossier N° : **PELA2202135816** du **13-02-2022**
Enregistré le 13-02-2022
Compte-rendu-complet / Edition du du 13-02-2022 à 23h42
Prescripteur : COVID SANS PRESCRIPTION

M. Jacques PASTEL
14 AVENUE DE LA FOUDRE
RESIDENCE LA COUPE
13090 AIX EN PROVENCE

Résultats d'analyses de :
M. Jacques PASTEL
Nom de naissance : PASTEL
Né(e) le 14-11-1975
Prélèvement du 13-02-2022

Résultats | Références | Antécedents

BACTERIOLOGIE

RECHERCHE D'ARN DU SARS-CoV-2 par RT-PCR
KIT NOVEL CORONAVIRUS (2019-NCOV) - SANSURE

Prélèvement [AC] : Nasopharyngé

Résultat: [AC] : NEGATIF: absence d'ARN du coronavirus SARS-CoV-2 (cibles: gène ORF1ab et gène N).
Absence d'inhibiteurs de la PCR.
Résultat à interpréter selon la symptomatologie (notamment la présence de toux et d'éternuements), la date de début des signes cliniques éventuels, le statut immunitaire individuel et les conditions environnementales.
En cas de forte suspicion clinique, un prélèvement de contrôle serait souhaitable.
En fonction de la date d'apparition des premiers symptômes, une analyse sérologique peut être conseillée afin d'augmenter la sensibilité du diagnostic

Dans le pied de page, nous retrouver le flag tant recherché :

HACKYNOV{PELA2202135816}