TP – Sécurité Informatique – Forensics

LP DA2I – 2018

Enseignant : Margot PRIEM

Bon amusement !

EXERCICE 1 : TROUVER L'ATTAQUANT

Enoncé : Vous recevez une commission rogatoire vous demandant de fournir les logs de vos applications métier suite à une enquête sur l'un de vos salariés.

Vous fournissez donc les fichiers web_application.log et mysql-error.log présent dans le dossier de l'exercice.

Analysez-les et répondez aux questions suivantes

Questions :

- Quel est l'email utilisé par l'attaquant ?

- Quelle est la commande SQL qui a été effectuée ?

Hash de vérification :

Afin de vous assurer que vous avez la bonne réponse, vous pouvez comparer l'empreinte SHA-512 de vos résultats avec celles présentes ci-dessous.

```
echo -n <réponse> | sha512sum
```

Email de l'attaquant :

```
b552c6a4622435a225276bee7dc738b64ac376422178e7e581b38c67431fd4e9d36a
04aa54d5a13da4c163107402a104ee3992cd6b88b7dfb181b83a7488f0d7
```

Commande SQL :

```
df9323ff7a13e889e4dd71de9a9f8762470be343ba7f3c493c3aa4e34b0178575d94
17e1e3924e20bd30f126c301e8e3058bd4f1d3eed085c8478b12181e34c6
```

EXERCICE 2: TOR

Enoncé : En déplacement dans un pays ayant une situation politique sensible, un journaliste doit écrire un article. Certains sites Internet sont régulièrement bloqués afin de maintenir une censure et de filtrer l'information.

Afin de pouvoir consulter ces sites bloqués, il a choisi de configurer un proxy TOR transparent.

N'arrivant toujours pas à accéder à ces sites, il vous demande de vérifier si le problème vient de lui.

Analysez la capture et trouvez les sites bloqués.

Questions :

- Quel est le 1er domaine bloqué ?
- Quel est le deuxième domaine bloqué ?
- Quel est le troisième domaine bloqué ?

Hash de vérification :

1er domaine bloqué :
`08db8ad2e93fbf431c5e9a0dce72baf4de0891a13b837da578c05fc652fb0d19b0be08a02e31a2cbc27707efd5f8473d9b0a58709cfae348b765f073b09ef122`

2eme domaine bloqué :
`5a5de8179e30fee574f0d878bdf28f77870d91f81aa78d99dca3b0ae1272753e45928f11e7fa6ab13aa4ed4fb33a7fc27562a8b38deab47987643ad715ac32fa`

3eme domaine bloqué :
`8fa36e29f52b5b2747e39900c5d344b0bf344038970360dc190e9793b02ebd4286d550f9a41fc20876dc8e3bb0c970d28de299f13eeee24cc529f73ef91dda2f`

Ressources :

- http://marschall-m.net/le-fichier-hosts-resolution-dns-local/
- https://www.wireshark.org/docs/dfref/d/dns.html

EXERCICE 3 : **RAT**

Enoncé : Kévin a été infecté par un malware après avoir téléchargé un antivirus via un email suspicieux.

Déterminez la nature des données exfiltrées.

En trouvant la nature des données exfiltrées, vous trouverez parmi elles un flag qui vous permettra de valider l'exercice.

Questions :

- Quelle est la nature des données exfiltrés ?
- Quel est le flag ?

Hash de vérification :

Type de donnée :
`eb31d04da633dc9f49dfbd66cdb92fbb9b4f9c9be67914c0209b5dd31cc65a136e1c`
`dce7d0db88112e3a759131b9d970cfaac7ee77ccd620c3dd49043f88958e`

Flag :
`809c2993a20d6e951135362c2f9ba9b3324459c4092bbd83ad656fe6b4a2b6414a95`
`40f050732f34543d16bcc8bc937f907187de0aec7991399b671f0f1a4ac7`

Ressources :

- https://www.it-connect.fr/reconstruction-dun-fichier-depuis-un-enregistrement-pcap/