Notes de recherche-action en Infosec

Outils de recherche

- Note 1 : recherche d'informations d'identification divulguées à l'aide du service Onion sur mobile
- CloudBunny, a tool to capture the origin server that uses a WAF as a proxy or protection. use Shodan, Censys and Zoomeye. https://github.com/Warflop/CloudBunny

Certif SSL et Nom de Domain

- **SSL**

```
$ echo | openssl s_client -servername monsite.org -connect monsite.org:443
2>/dev/null | openssl x509 -noout -dates
```

- **Nom de Domaine**

```
$ whois monsite.org | grep 'Expiry'
```

Cookies

```
curl -qsIL https://opencommons.simplon.co  | grep Cookie
```

Reverse

- Radare, Reverse Engineering Framework with focus on UNIX philosophy and full API bindings. https://rada.re/r/ also works as well on Anrdoid with Termux
- Note 1 : obtenir des hexadécimaux pour les chaînes de noms de fonction api à des fins de shellcoding

Anonymser des fichiers

- Note n°1 : Fihiers images, vidéo ou son
- mat2 is a metadata removal tool https://0xacab.org/jvoisin/mat2

MITM

Bluetooth

- Note n°1 : BtleJuice Framework

Formations

Jeu

- Note 1 : Over The Wire

Pratiques

Bdd de MdP

- Récupérer la base de mots de passe fuités de Have I been pwned pour vérifier en local que les sésames stockés dans son gestionnaire de mots de passe n'y figurent pas

ref :
https://www.ghacks.net/2019/01/18/check-all-keepass-passwords-against-the-have-i-been-pwned-database-locally/

USB, card flash SD

- f3 - Fight Flash Fraud https://fight-flash-fraud.readthedocs.io/en/stable/introduction.html

Biblio

- You broke the Internet https://youbroketheinternet.org

```
sudo strace -p 1205 # See syscalls of PID 1205. Processes don't have to be a black box, you can use strace (on Linux) to view the system calls made by a process, which may give some clue as to why it's misbehaving, where it is saving a file, etc.
```