

Exercices SSI : Script Kiddie

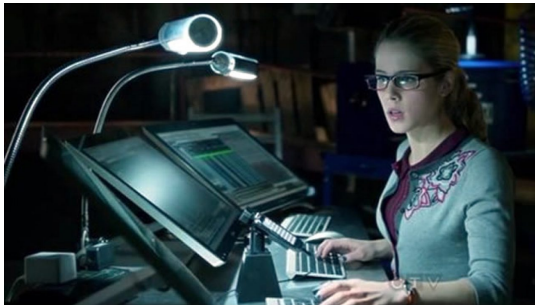
Éric BERTHOMIER
eric.berthomier@free.fr

9 février 2021



Version 1.4 - Version Stagiaire

Vous voici devenu un véritable hacker offrant vos services moyennant quelques centimes de ₿(Bitcoins)



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots
- Google est son ami



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots
- Google est son ami
- English is more powerful on Internet than french or other language



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots
- Google est son ami
- English is more powerful on Internet than french or other language
- Utilise les outils qui sont à sa disposition



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots
- Google est son ami
- English is more powerful on Internet than french or other language
- Utilise les outils qui sont à sa disposition



Voici les caractéristiques d'un hacker :

- Recherche la nature même des éléments
- Comprendre, analyser, réfléchir sont ses maîtres mots
- Google est son ami
- English is more powerful on Internet than french or other language
- Utilise les outils qui sont à sa disposition

"The quieter you become, the more you are able to hear . . . "



Les challenges

- Fichier Excel avec cellules protégées
- Absent mais présent ...
- Un accès WiFi gracieux
- Marre de ces gouvernements ! Créons un second WikiLeaks
- Chiffrement... Oui mais de quelle qualité ?
- De l'argent pas cher ...



Fichier Excel avec cellules protégées

Un ami vient vous voir, la personne qu'il remplace a protégé les feuilles d'un fichier Excel avec un mot de passe et il doit absolument modifier le fichier.



Fichier Excel avec cellules protégées

Un ami vient vous voir, la personne qu'il remplace a protégé les feuilles d'un fichier Excel avec un mot de passe et il doit absolument modifier le fichier.

Vos outils

- Windows 10
- Le fichier Excel :
`http://cours.ericberthomier.fr/xls/classeurprotege.xlsx`



Absent mais présent ...

Un client ne supporte pas le flicage effectué par sa société au travers de Skype Entreprise. En effet, lorsqu'il n'est pas derrière son clavier, Skype passe en statut "Absent".



Absent mais présent ...

Un client ne supporte pas le flicage effectué par sa société au travers de Skype Entreprise. En effet, lorsqu'il n'est pas derrière son clavier, Skype passe en statut "Absent".

Son PC

- Pas de compte "Administrateur"
- Windows 10
- Libre Office
- Les paramètres d'inactivité de Skype semblent les mêmes que ceux de l'économiseur d'écran...



Absent mais présent ...

Un client ne supporte pas le flicage effectué par sa société au travers de Skype Entreprise. En effet, lorsqu'il n'est pas derrière son clavier, Skype passe en statut "Absent".

Son PC

- Pas de compte "Administrateur"
- Windows 10
- Libre Office
- Les paramètres d'inactivité de Skype semblent les mêmes que ceux de l'économiseur d'écran...

Trouver une solution à votre client ...



Absent mais présent ...

Un client ne supporte pas le flicage effectué par sa société au travers de Skype Entreprise. En effet, lorsqu'il n'est pas derrière son clavier, Skype passe en statut "Absent".

Son PC

- Pas de compte "Administrateur"
- Windows 10
- Libre Office
- Les paramètres d'inactivité de Skype semblent les mêmes que ceux de l'économiseur d'écran...

Trouver une solution à votre client ...

Pour les plus hardis sans Libre Office ...



Un accès Wifi gracieux ...

Votre voisin vient vous demander de faire un petit nettoyage de son PC car il trouve qu'il est lent. Comme ce dernier ne vous renvoie pas pas véritablement l'ascenseur et que vous êtes sur la ligne de mire de Hadopi, vous vous dîtes qu'il serait intéressant d'avoir la clé Wifi de sa Box.



Un accès Wifi gracieux ...

Votre voisin vient vous demander de faire un petit nettoyage de son PC car il trouve qu'il est lent. Comme ce dernier ne vous renvoie pas véritablement l'ascenseur et que vous êtes sur la ligne de mire de Hadopi, vous vous dîtes qu'il serait intéressant d'avoir la clé Wifi de sa Box.

Son PC

- Windows 10
- Se connecte en Wifi à la maison



Un accès Wifi gracieux ...

Votre voisin vient vous demander de faire un petit nettoyage de son PC car il trouve qu'il est lent. Comme ce dernier ne vous renvoie pas véritablement l'ascenseur et que vous êtes sur la ligne de mire de Hadopi, vous vous dîtes qu'il serait intéressant d'avoir la clé Wifi de sa Box.

Son PC

- Windows 10
- Se connecte en Wifi à la maison

Trouver la ou les clés Wifi ...



Marre de ces gouvernements ! Créons un second WikiLeaks

Exaspéré par la politique, vous vous mettez en chasse de documents confidentiels sur le Net ...



Marre de ces gouvernements ! Créons un second WikiLeaks

Exaspéré par la politique, vous vous mettez en chasse de documents confidentiels sur le Net ...

Vos outils

- Google

Ne pas ouvrir les documents !



Chiffrement ... Oui mais de quelle qualité ?

La Justice vous confie le disque dur d'une personne suspectée de détenir des éléments en lien avec une activité terroriste. Hélas, le disque dur est crypté par BitLocker.



Chiffrement ... Oui mais de quelle qualité ?

La Justice vous confie le disque dur d'une personne suspectée de détenir des éléments en lien avec une activité terroriste. Hélas, le disque dur est crypté par BitLocker.

Vos outils

- Linux
- Le disque dur crypté



Chiffrement ... Oui mais de quelle qualité ?

La Justice vous confie le disque dur d'une personne suspectée de détenir des éléments en lien avec une activité terroriste. Hélas, le disque dur est crypté par BitLocker.

Vos outils

- Linux
- Le disque dur crypté

Protéger la preuve !



De l'argent pas cher ...

Votre ami Webmaster cherche une solution pour faire de l'argent mais sans utiliser de la publicité sur son site. Il vous indique avoir entendu parler des éléments suivants :

- Javascript - Exécution sur le poste de l'utilisateur
- Minage

