Write-up (version en français) machine : Three.

Introduction

La machine **Three** (ip pour cet exercice : 10.129.22.182) est une box de difficulté intermédiaire qui met l'accent sur l'exploitation des services cloud, en particulier AWS. Elle teste plusieurs compétences essentielles en sécurité offensive, notamment :

- La **découverte de structure web** pour identifier des points d'entrée potentiels.
- L'**énumération de buckets**, une étape cruciale pour identifier des fichiers accessibles publiquement.
- L'**accès anonyme** ou en tant qu'invité à certains services.

L'**upload arbitraire de fichiers**, une technique permettant d'exécuter du code malveillant sur le serveur cible.

L'objectif de cette machine est de démontrer l'importance de la sécurisation des infrastructures cloud et des applications personnalisées.

Reconnaissance

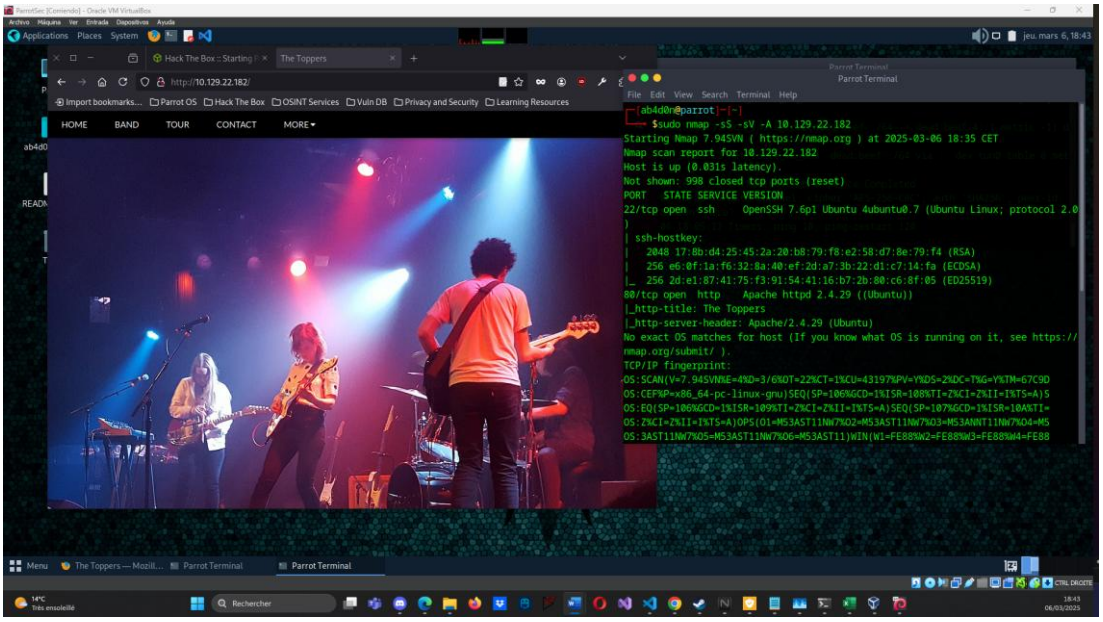
On commence par réaliser un scan avec nmap avec la commande suivante :

```
sudo nmap -sS -sV -A 10.129.22.182
```

On observe deux ports ouverts :

```
22/tcp open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http   Apache httpd 2.4.29 ((Ubuntu))
```

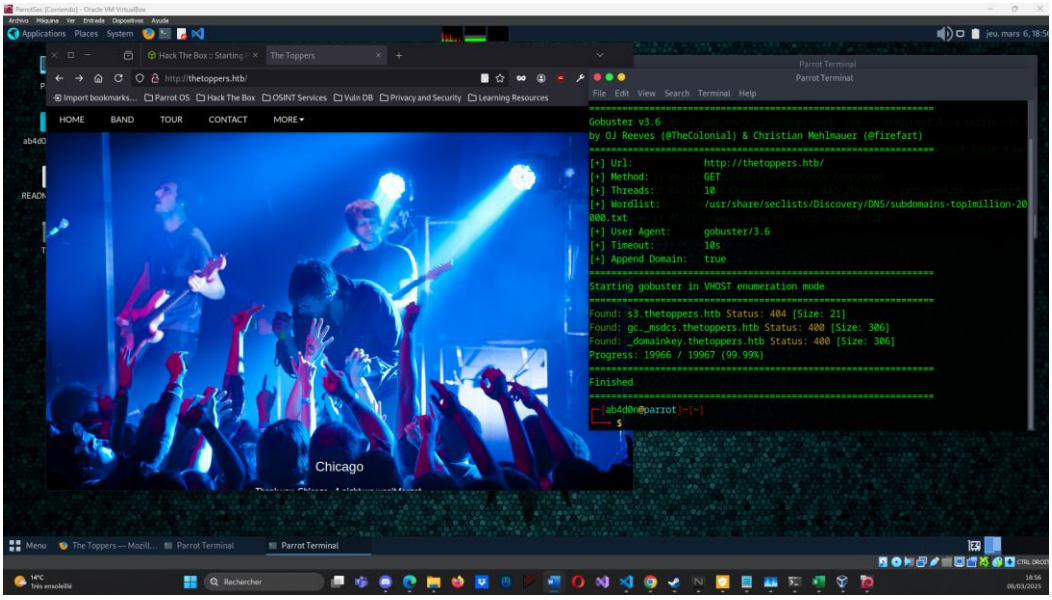
On continue donc notre reconnaissance sur le navigateur web, l'application semble être une plateforme de réservation de billets de concert.



Nous remarquons une adresse e-mail associée au domaine **thetoppers.htb**. Nous ajoutons donc ce domaine au fichier /etc/hosts pour pouvoir y accéder correctement :

```
echo "10.129.22.182 thetoppers.htb" | sudo tee -a /etc/hosts
```

Puis on procède par énumérer les sous-domaines en utilisant des outils comme gobuster :



Notre premier sous-domaine est s3.thetoppers.htb, après une petite recherche sur le web on constate que le service en cours d'exécution dans ce sous-domaine s'agit très certainement de Amazon S3.

Identification des vulnérabilités

Puis encore une fois sur le web on cherche " which command line utility can be used to interact with amazon s3", et on obtient comme réponse awscli qu'en suite on installe depuis notre terminale et finalement nous configurons un profil AWS avec des valeurs arbitraires.

```
sudo apt install awscli
```

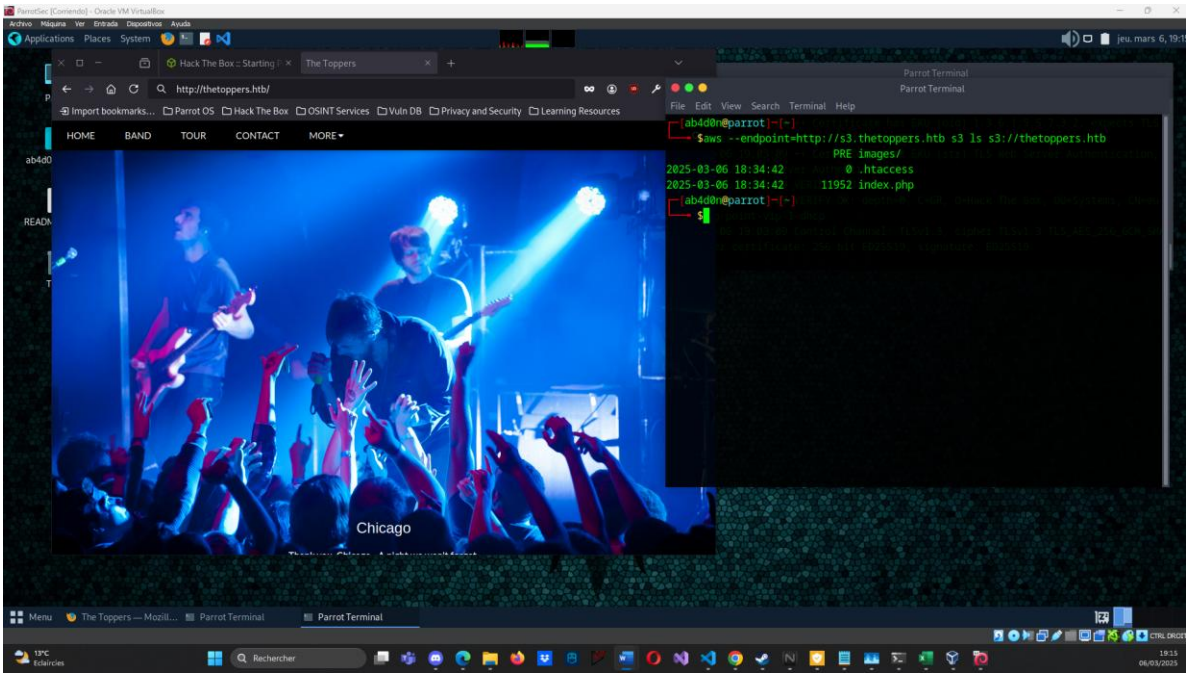
```
aws configure
```

Ensuite on ajoute ce sous-domaine à notre liste de hosts :

```
echo "10.129.22.182 s3.thetoppers.htb" | sudo tee -a /etc/hosts
```

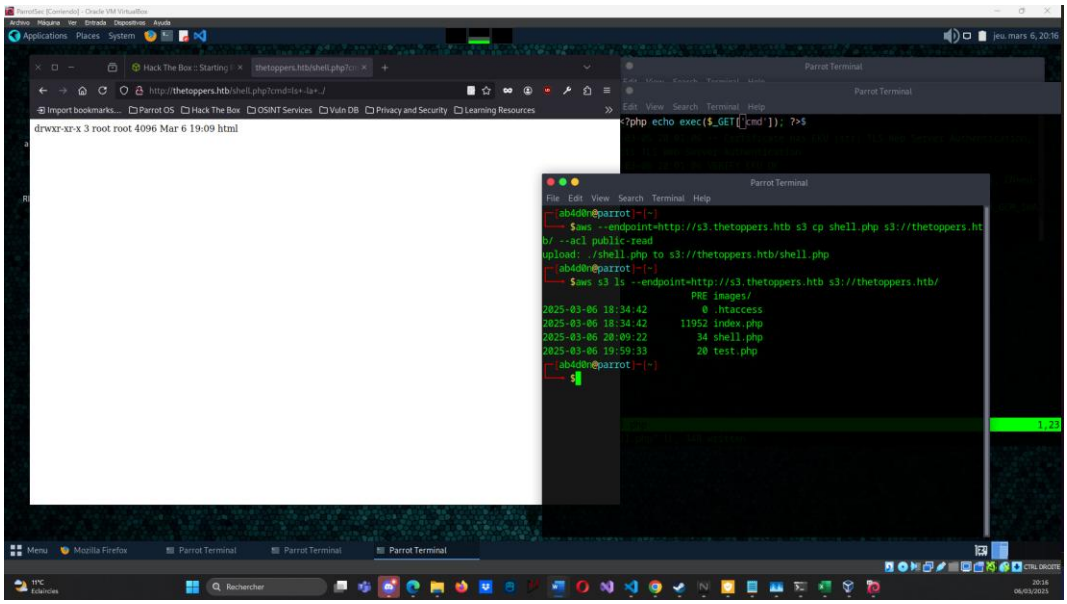
Pour continuer on va sur le site https://aws.amazon.com/cli/ pour chercher les différentes commandes qui peuvent nous être utiles, et ensuite on continue par lister le contenu du bucket accessible :

```
aws --endpoint=http://s3.thetoppers.htb s3 ls s3://thetoppers.htb
```



Exploitation détaillée

On observe que le serveur est configuré pour exécuter des fichiers en php (scrypting language). On procède donc par créer un webshell en PHP, et ensuite on l'envoie sur le bucket.



Une foi le shell ce trouve bien dedans on change la commande sur le browser directement pour chercher où se trouve le flag et on l'affiche avec cat.

http://thetoppers.htb/shell.php?cmd=cat +../flag.txt

Leçons apprises

Cette machine illustre plusieurs erreurs de configuration qui peuvent compromettre un système hébergé sur le cloud :

1. **Mauvaise configuration du stockage AWS S3**
    - Un bucket S3 accessible publiquement, servant de webroot, permet à un attaquant d'uploader des fichiers malveillants.
2. **Manque de restrictions sur l'upload**

- L’absence de filtres sur les types de fichiers téléversés permet l’exécution de code arbitraire.

3. **Absence d’authentification stricte**
    - Certains services AWS S3 n’exigent pas de credentials, facilitant l’accès non autorisé.

Mesures correctives :

- Restreindre l’accès public aux buckets S3.
- Mettre en place une validation stricte des fichiers uploadés (extensions, type MIME).
- Appliquer le principe du moindre privilège aux services AWS.