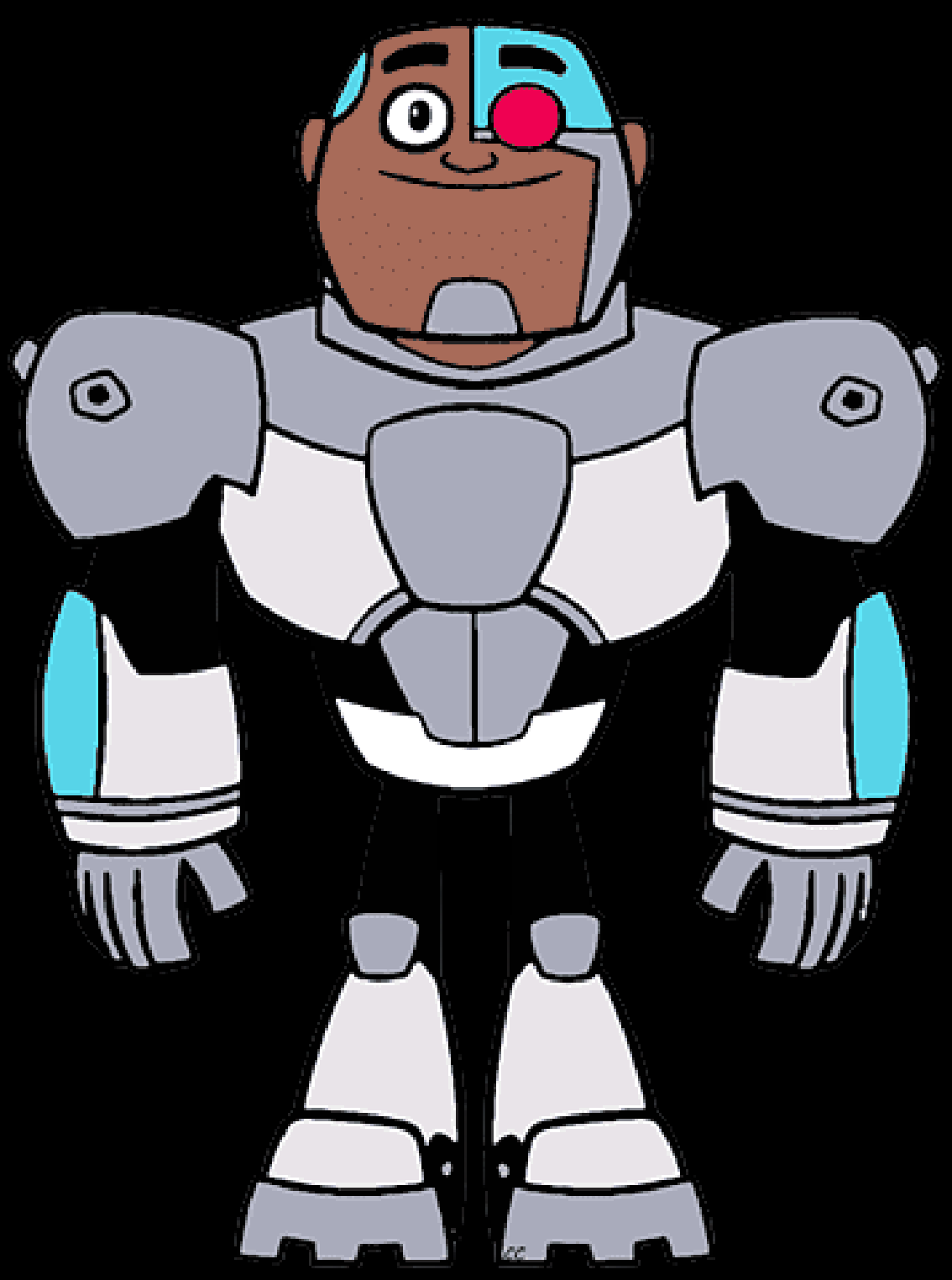
PROJET

CTF

DÉFI CYBORG

contexte scolaire



Source :

Try Hack Me

AKAZAF ABDELLAH

Objectif

Trouver une vulnérabilité du système en se servant des outils adaptés

- J’ai commencé par lancer une machine virtuelle pour cet exercice. j’ai utilisé l’attack box proposé par Tryhackme.

- L’AttackBox de TryHackMe est une machine virtuelle Ubuntu hébergée dans le cloud.

- J’ai tenté de compromettre la machine et lire les fichiers user.txt et root.txt.

STRATÉGIE ?

1. SCANNING

- Nous allons scanner le systeme cible pour identifier les services et les ports ouverts

2. ÉNUMÉRATION

- Nous allons collecter des informations (les services et les utilisateurs) afin de découvrir des vulnérabilités

3. EXPLOITATION

- Nous allons utiliser les failles et les vulnérabilités pour accéder à des informations sensibles.

SCANNING "nmap"

Voici la commande pour scanner le système :

```
root@ip-10-10-120-11:~# nmap -vv 10.10.120.11
```

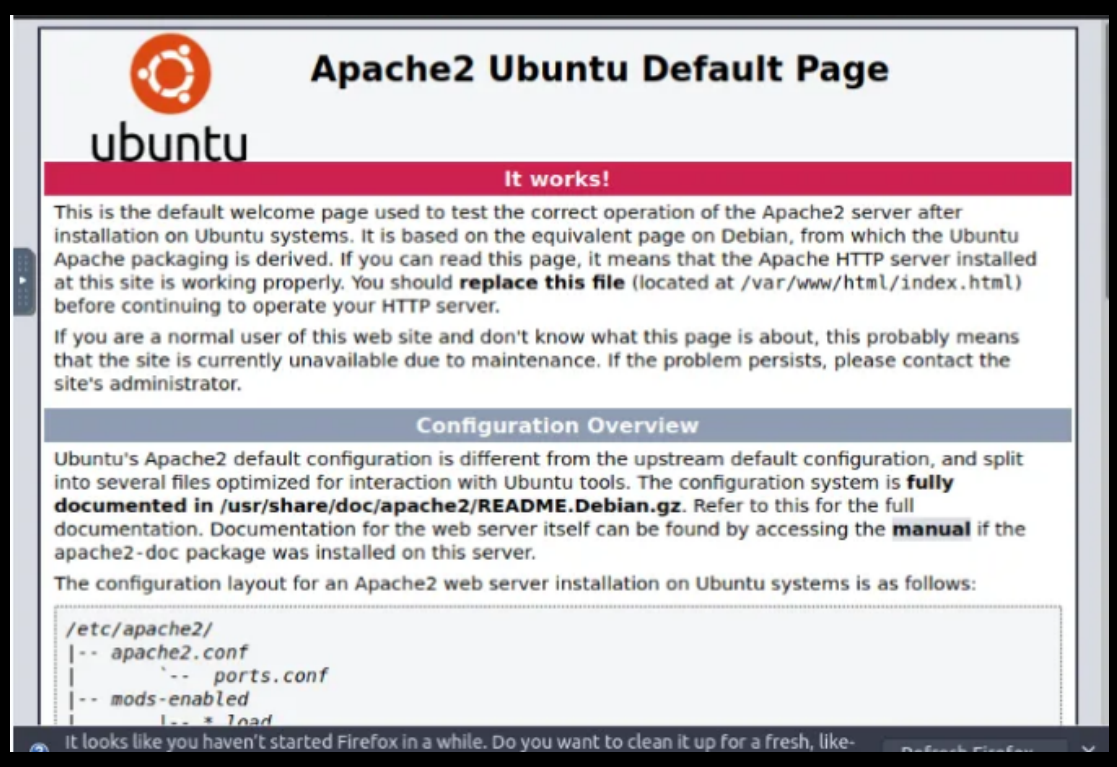
Nous pouvons voir que les ports SSH et HTTP sont ouverts :

```
PORT     STATE    SERVICE       REASON
22/tcp   open     ssh           syn-ack ttl 64
80/tcp   open     http          syn-ack ttl 64
111/tcp  open     rpcbind       syn-ack ttl 64
389/tcp  open     ldap          syn-ack ttl 64
3389/tcp open     ms-wbt-server syn-ack ttl 64
5901/tcp open     vnc-1         syn-ack ttl 64
6001/tcp open     X11:1         syn-ack ttl 64
7777/tcp filtered cbt           no-response
7778/tcp filtered interwise     no-response
```

Le port 80 associé au protocole HTTP, représente une cible potentielle pour notre attaque.

ENUMÉRATION

Ensuite, le port 80 est ouvert, vérifions à quoi ressemble Le site Web. Puisque c'est un "http", il peut contenir des vulnérabilités.
"curl http://10.10.125.54 " affichera le contenu du site web.



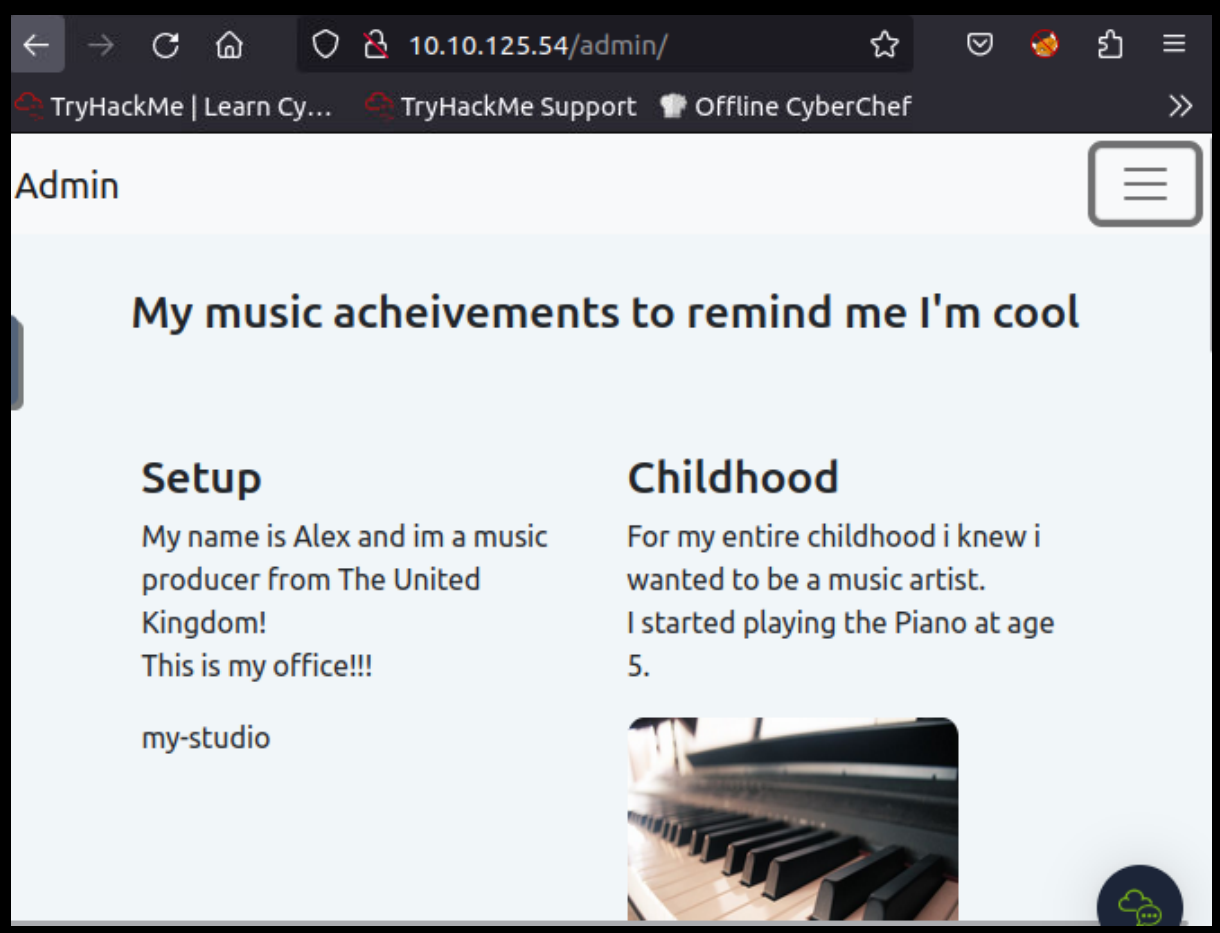

```
root@ip-10-10-27-77:~# curl http://10.10.125.54

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http:
.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }
```

J’ai decidé de rechercher des répertoires cachés de ce site web qui pourraient éventuellement contenir des mots de passe.

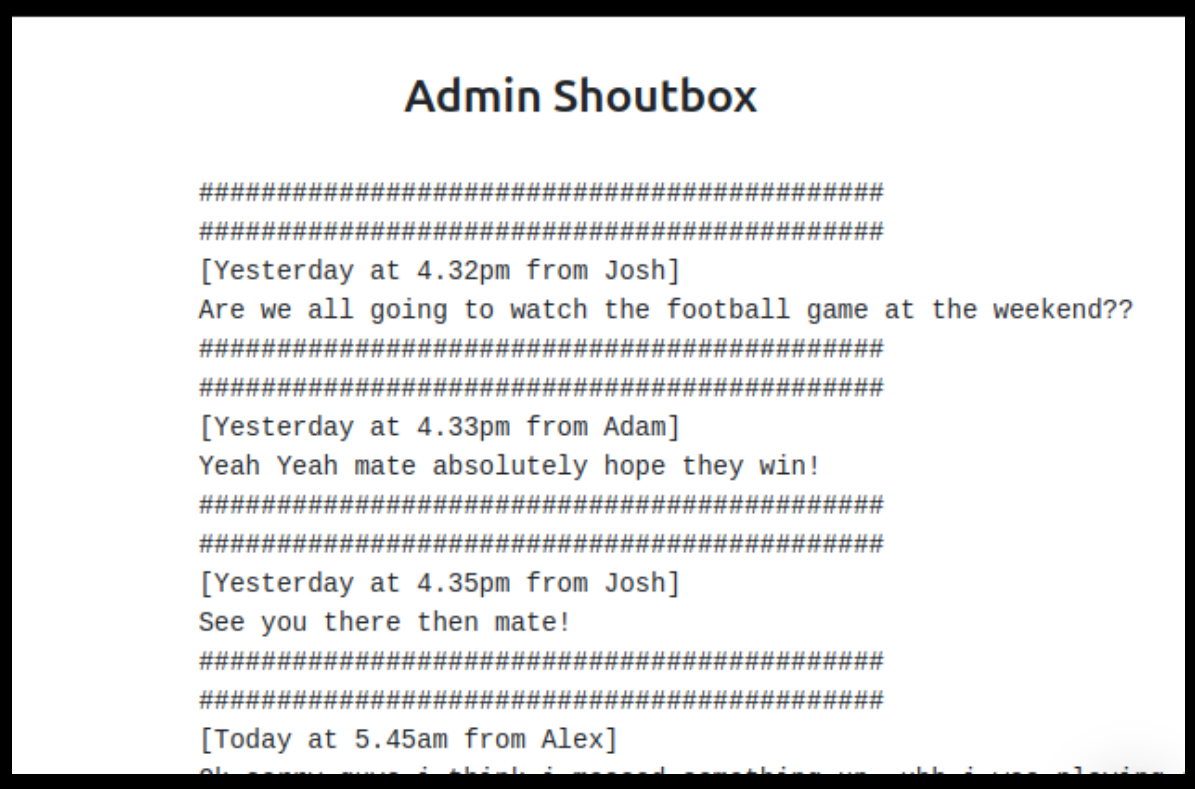
Pour ce faire ,nous avons eu 2 strategies :

- Je pouvais utiliser la commande "**gobuster"**
- Je pouvais tester l’URL suivante : **"http://10.10.125.54/admin"** pour potentiellement accéder à la section du site réservée à l'administration, pouvant contenir des outils de gestion, des formulaires de connexion et d'autres fonctionnalités destinées aux administrateurs du site.

J’ai testé l’url **"http://10.10.125.54/admin"** et j’ai eu accées a cette page :



En navigant sur cette page web ,j’ai pu trouver les utilsateurs : **"Josh ,Adam et Alex”**



POINT BLOQUANT :

jE n’ai pas pu terminer le défi en raison des éléments suivants :

CONNEXION INTERNET :

- Nous avons rencontré un problème de connexion à Internet, et donc l'AttackBox n'était pas opérationnelle.

DURÉE DE TÂCHE :

- Nous avons rencontré un problème de connexion à Internet, et donc l'AttackBox n'était pas opérationnelle.

DISPONIBILITÉ DE L’OUTIL :

- l'AttackBox de TryHackMe n'était disponible que pendant une heure.

Malgré ces obstacles, nous avons pu avancer quand même en mettant en place différentes alternatives : **création de plusieurs comptes AttackBox, répartition des tâches pour faire face aux contraintes de temps, et utilisation d'un point d'accès Wi-Fi mobile**

Grace aux recherches sur Internet, j’ai pu compléter les questions de l’exercice.Mon but, sera de refaire l’exercice