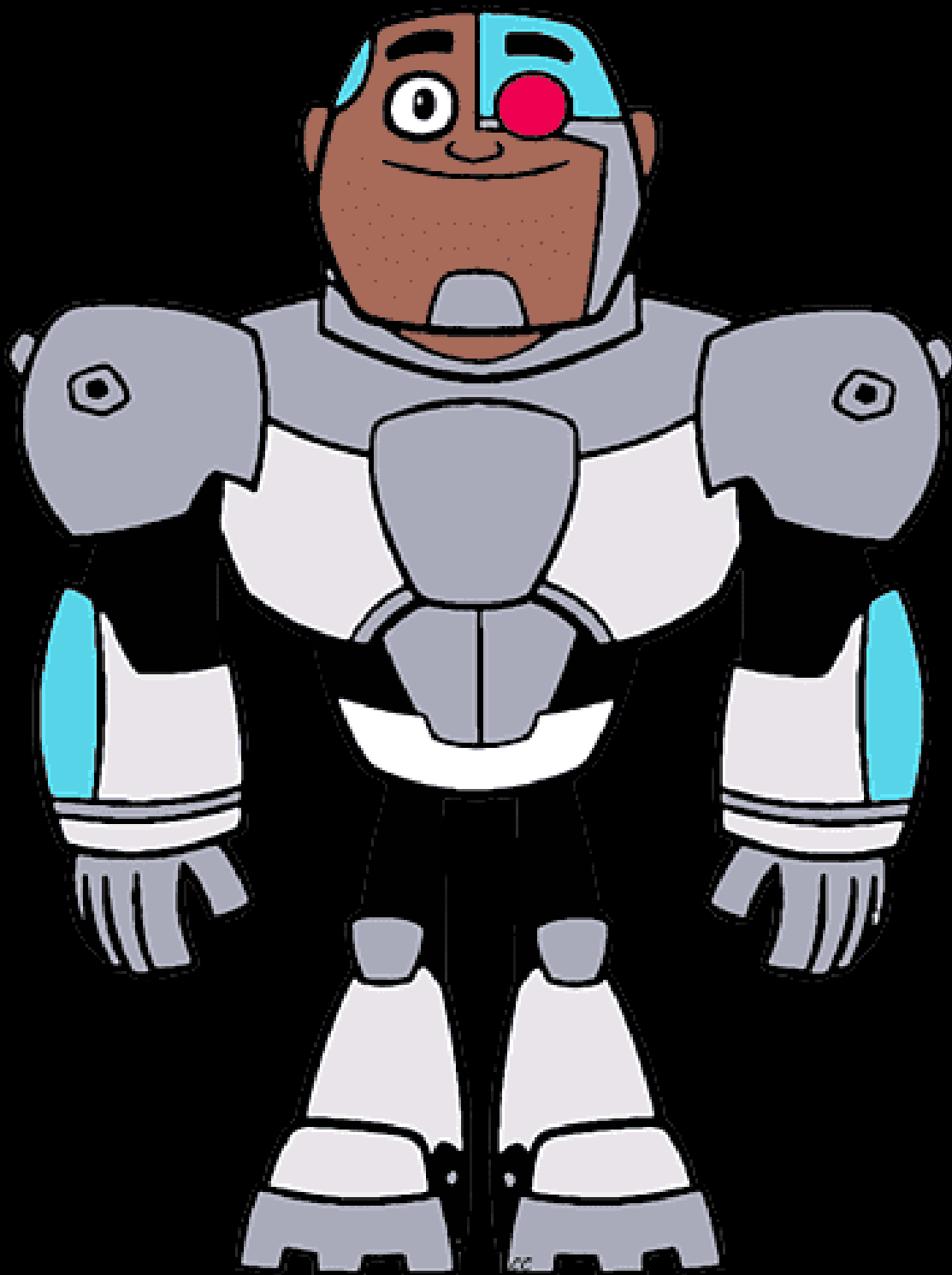


PROJET

CTF

DÉFI CYBORG

contexte scolaire



Source :



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
```

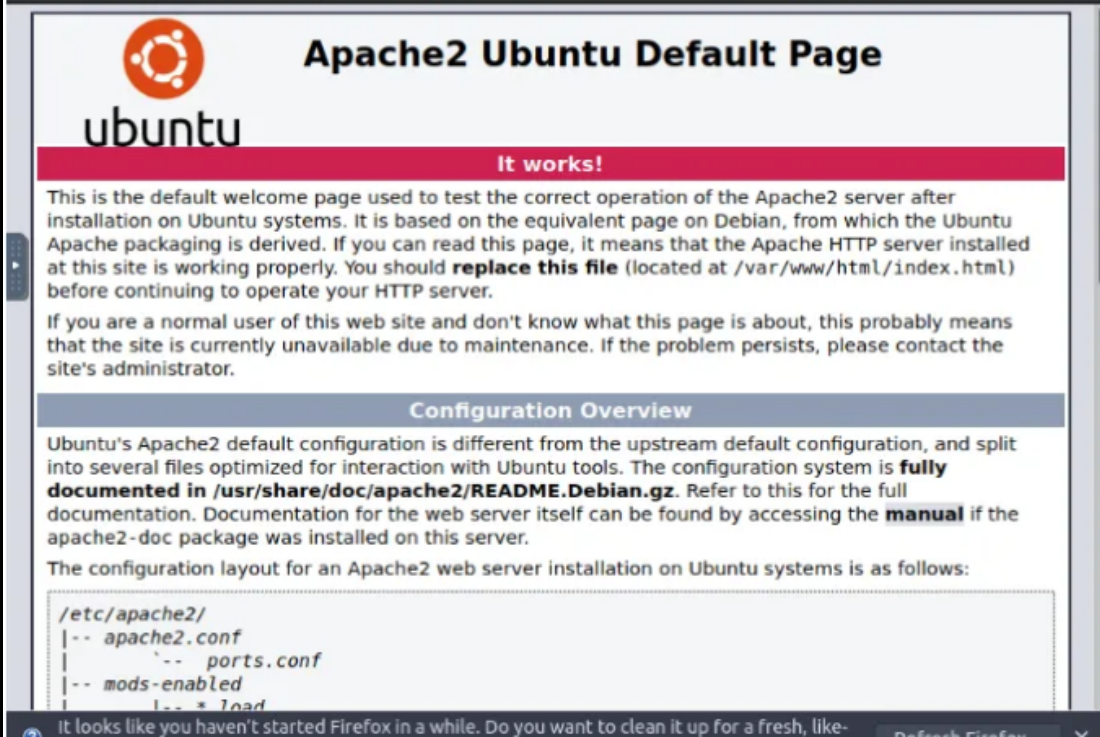
Nous pouvons voir que les ports SSH et HTTP sont ouverts :

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://www.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;

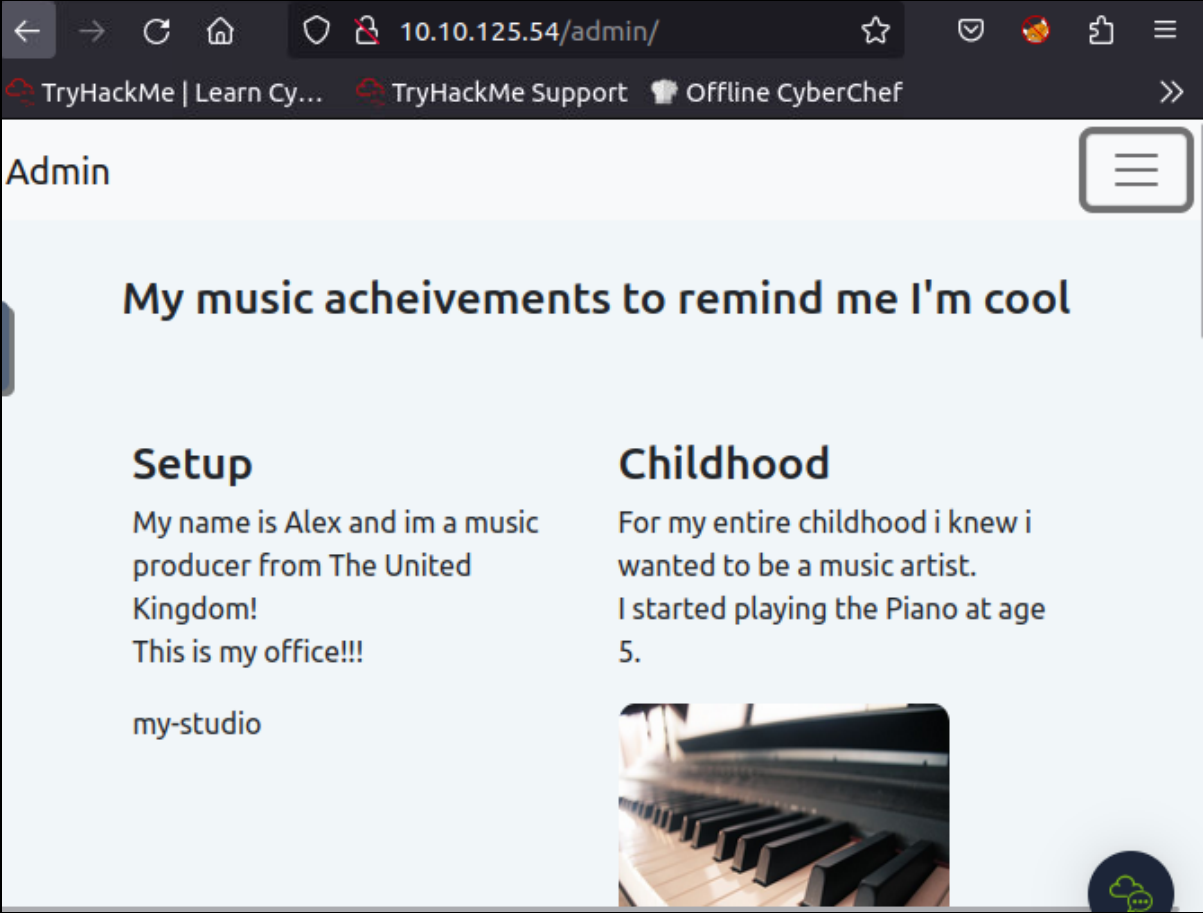
        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }
    </style>
  </head>
  <body>
    <div>
      <div>
        <img alt="Ubuntu logo" data-bbox="78 758 115 782"/>
        <h1>Apache2 Ubuntu Default Page</h1>
      </div>
      <div>
        <h2>It works!</h2>
        <p>This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
        <p>If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
      </div>
    </div>
    <div>
      <h3>Configuration Overview</h3>
      <p>Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
      <p>The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
      <pre>/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- mods-available
|   |-- *.load
|   |-- *.conf
|-- localizations
|-- *.load
|-- *.conf
-->
    </div>
  </body>
</html>
```

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

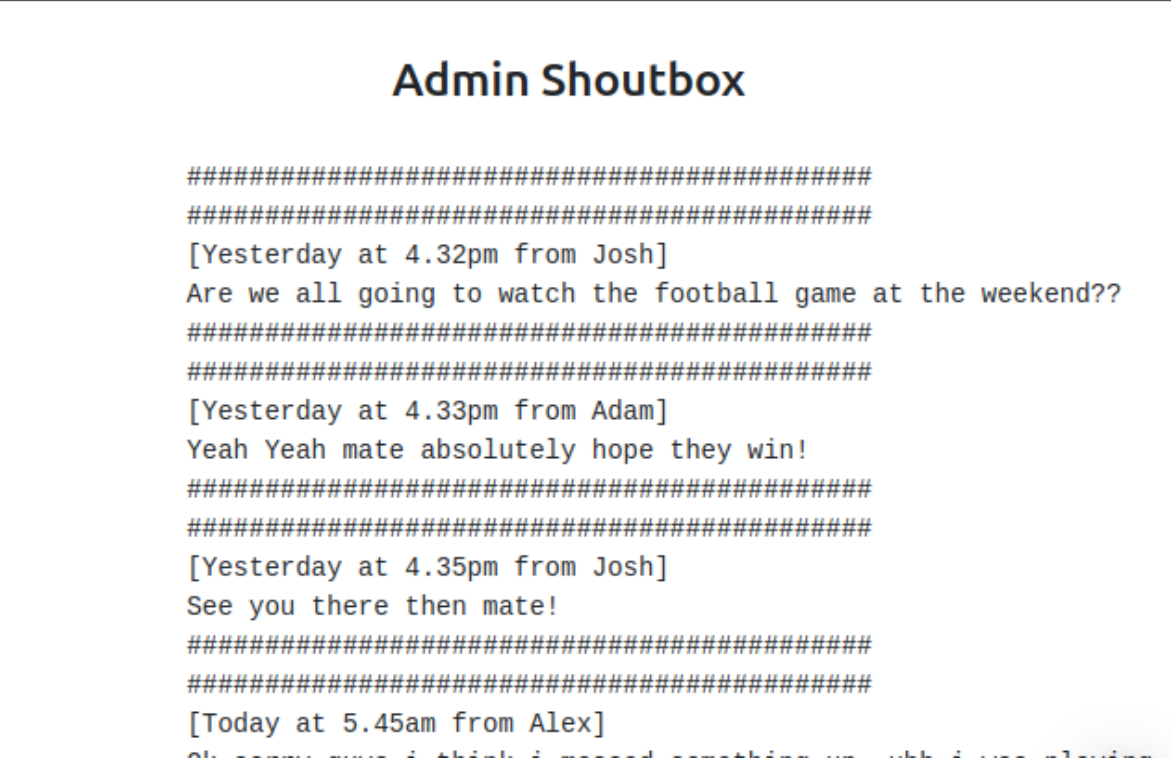
Pour ce faire ,nous avons eu 2 strategies :

- 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

Scan the machine, how many ports are open?	<input type="text" value="2"/>	Correct Answer	Hint
What service is running on port 22?	<input type="text" value="ssh"/>	Correct Answer	
What service is running on port 80?	<input type="text" value="http"/>	Correct Answer	
What is the user.txt flag?	<input type="text" value="flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}"/>	Correct Answer	Hint
What is the root.txt flag?	<input type="text" value="flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}"/>	Correct Answer	Hint