Quick Write Up: Root Me

TryHackMe - Yxène

Énumération

Chercher les services/serveurs en écoute sur la machine cible

Task 2 Reconnaissance

First, let's get information about the target.

Answer the questions below

Scan the machine, how many ports are open?

Login to answer..

What version of Apache is running?

Login to answer..

What service is running on port 22?

Login to answer..

Find directories on the web server using the GoBuster tool.

Login to answer...

What is the hidden directory?

Login to answer..

Scan de ports Outil: Nmap

Scan the machine, how many ports are open?

Login to answer...

nmap -T4 10.10.3.157 # -T4: scan + rapide mais - discret

```
Nmap scan report for 10.10.3.157
Host is up (0.089s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Version des services Outil: Nmap

nmap -T4 -p22,80 -sV 10.10.3.157

What version of Apache is running?

Login to answer..

What service is running on port 22?

Login to answer...

```
Nmap scan report for 10.10.3.157 Host is up (0.088s latency).
```

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open httpApache httpd 2.4.29 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Énumération Web (port 80) Outil: dirb (ou GoBuster)

Find directories on the web server using the GoBuster tool.

Login to answer..

What is the hidden directory?

Login to answer...

dirb http://10.10.3.157 # Recherche de pages ou répertoires cachés

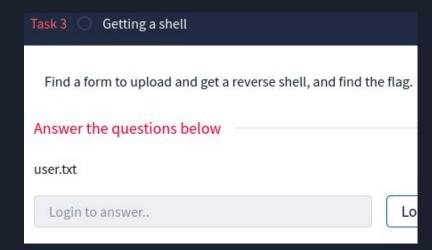
```
GENERATED WORDS: 4615

---- Scanning URL: http://10.10.3.157/ ----
==> DIRECTORY: http://10.10.3.157/css/
+ http://10.10.3.157/index.php (CODE:200|SIZE:616)
==> DIRECTORY: http://10.10.3.157/js/
==> DIRECTORY: http://10.10.3.157/panel/
+ http://10.10.3.157/server-status (CODE:403|SIZE:276)
==> DIRECTORY: http://10.10.3.157/uploads/
```

Upload Reverse shell

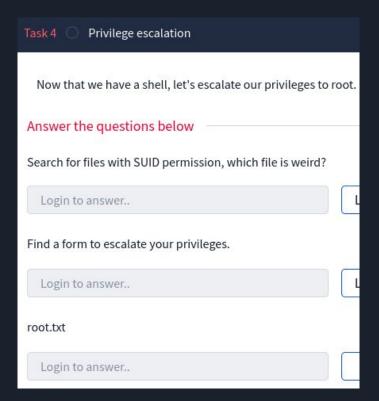
Reverse shell: Connexion initié par la machine cible vers la machine attaquante pour obtenir un terminal sur la première.

Exploiter une fonctionnalité d'upload non sécurisé du site Web pour obtenir un reverse shell.



Élévation de privilèges

On doit utiliser notre accès utilisateur (www-data) pour obtenir des droits administrateur (root) sur la machine cible.



Questions

