Enter Wonderland and capture the flags.

Wonderland

WRITE-UP by Frozenk

date : 2024-04-12

Table des matières

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up "Frozenk" a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

1.1

Nmap :

```
[Apr 11, 2024 - 16:57:40 (CEST)] exegol-thm /workspace # sudo nmap -sT -sV -Pn
-p- 10.10.75.218 -sV -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-11 16:58 CEST
Nmap scan report for 10.10.75.218
Host is up (0.057s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 8eeefb96cead70dd05a93b0db071b863 (RSA)
|   256 7a927944164f204350a9a847e2c2be84 (ECDSA)
|_  256 000b8044e63d4b6947922c55147e2ac9 (ED25519)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Follow the white rabbit.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.56 seconds
```

FeroxBuster :

```
http://10.10.75.218/poem
```

Alice doit etre le Username,la page Poem contient surement le Password Visiblement non, Je telecharge l'image et essaye Steghide :

```
[Apr 11, 2024 - 17:11:20 (CEST)] exegol-thm /workspace # steghide extract -sf
white_rabbit_1.jpg
Enter passphrase:
wrote extracted data to "hint.txt".
[Apr 11, 2024 - 17:11:33 (CEST)] exegol-thm /workspace # cat hint.txt
follow the r a b b i t#
```

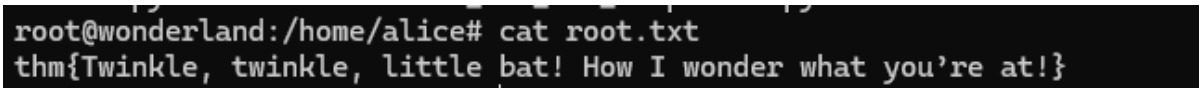
SSH surement Alice:follow the r a b b i t Non

solution ici : `view-source:http://10.10.75.218/r/a/b/b/i/t/`

```
style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail
```

1.2

PRIVSC : **Utilisation de PwnKit pour ROOT**



Frozenk

Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**