[info]

**Introduction**

La machine distante est un linux dont l’adresse IP est 10.10.10.68.

Compétences mises en œuvre :

* Enumération des ports et services.
* Identifier un objet connecté.
* Chercher les identifiants par défaut.
* Retrouver le contenu d’un fichier effacé.

**Enumération**

On commence avec une énumération de ports et services avec nmap :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.68 |

[nmap]

Le port 80 est ouvert, il contient juste une page d’accueil, nous allons faire une énumération de dossiers et de fichiers dessus avec dirsearch :

|  |
| --- |
| $ dirsearch -w wordlist -f -e ".php,.txt" -u http://10.10.10.68/ |

[dirsearch]

Le contenu nous fait penser à PI-Hole, qui est un DNS pour éviter les publicités, ce qui coïncide avec le port 53 d’ouvert. Vu que le service ssh tourne, il se peut que le couple identifiant/mot de passe soit celui par défaut, une recherche sur le site : indique que par défaut les credentials sont : pi:raspberry.

**Exploitation**

L’accès en ssh est possible avec l’identifiant et le mot de passe par défaut :

|  |
| --- |
| $ ssh [pi@10.10.10.68](mailto:pi@10.10.10.68) |

[ssh]

Et nous pouvons aller chercher le premier flag :

|  |
| --- |
| $ ls /home/  $ cat /home/pi/Desktop/user.txt |

[usertxt]

**Elévation de privilège**