[info]

**Introduction**

Sunday est une machine Solaris dont l’adresse IP est 10.10.10.76. L’accès utilisateur peut prendre un certain temps, mais une fois sur le bon port, c’est rapide. L’élévation de privilège n’est pas compliquée, il suffit de jouer avec la commande wget.

Compétences mises en œuvre :

* Enumération des ports et services.
* Enumération des identifiants d’un service ssh.
* Cracking de mot de passe (/etc/shadow).
* Enumération et abus des droits de l’utilisateur.

**Enumération initiale**

On commence avec une énumération des ports et services avec **nmap** :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.76 |

[nmap]

Il y a beaucoup de ports ouverts, nous pouvons refaire un scan pour voir si d’autre ports non communs sont utilisés :

|  |
| --- |
| $ nmap -T4 -p1-65535 10.10.10.76 |

[nmap2]

Deux ports apparaissent : le port **22022** fait tourner un service **SunSSH**, et l’autre port semble bloqué.

**Obtenir un accès utilisateur**

Nous allons tenter une énumération d’utilisateur sur le port 22022 avec un programme perl :

**Obtenir un accès Administrateur**

Bla