Explore

CTF	HackTheBox
Category	Writeup
Created	@July 7, 2021 9:36 PM
Date	
Description	
Fields	Pentest
Level	Easy
Tags	Android

I don't know why all the info of the ports from `nmap` are mess up...

Info

Credential

User	Password	Service	Note
kristi	Kr1sT!5h@Rp3xPl0r3!		

Path

Android machine !?

1. I haven't exploit any Android system yet, so I totally don't know what to expect. Though, I google and from this article, I know that I should somehow connect via `adb` to gain root of the machine.

User

1. From the HTB page, we know it is an Android machine.
2. From `nmap`, it is running an Banana Studio SSH Server, which is an application to host a SSH on the android, and the port 5555 is open, which is usually an Android Debug port.
3. By trying, I found that we can use `adb` to connect to the machine through port `2222`, but it is offline immediately. (Turns out, this just the SSH server opening, so it responses the connect.)

```
$ adb connect $ip:2222 && adb devices
connected to 10.10.10.247:2222
List of devices attached
10.10.10.247:2222       offline
```

4. There seems nothing we can do, so do an all-ports scan, and found some open ports running HTTP.
5. Google 'ES File Explorer Name Response' and found CVE-2019-6447. Although the `nmap` shows 'ES File Explorer Name Response' is running on port 42135, since it don't work and the script suggest it should run on port 59777, we run it against port 59777 and get good luck.

```
$ curl -X POST $ip:59777 -H 'Content-Type: application/json' --data '{command: "getDe
viceInfo"}'
{"name":"VMware Virtual Platform", "ftpRoot":"/sdcard", "ftpPort":"3721"}
```

6. By looking around the files use own written script `CVE-2019-6447.py`, I found `user.txt` in `/sdcard/`.
7. By command `listPics`, it shows there is a `creds.jpg` at `/storage/emulated/0/DCIM/`, so download it and get the credential in the image. Use the credential to login SSH and gain user.

Root

1. Since `adb` server scans odd number ports from 5555 to 5585 for the running devices to connect, we can use SSH to do port forwarding from our `localhost:5555` to the `localhost:5555` of the machine to let us use `adb` against the machine.

```
$ ssh -L 5555:localhost:5555 kristi@$ip -p 2222 -N
$ adb devices
List of devices attached
localhost:5555  device
emulator-5554   device
```

2. Connect to the machine using `adb`, and we gain root.

```
$ adb -s emulator-5554 shell
x86_64:/ # whoami
root
x86_64:/ # find / -name root.txt 2>/dev/null
/data/root.txt
```

Reference

How to start exploit an Android machine

- https://www.hacknos.com/investigator-vulnhub-walkthrough/

CVE-2019-6447 (ES File Explorer)

ES File Explorer

- https://www.exploit-db.com/exploits/50070
- https://github.com/fs0c131y/ESFileExplorerOpenPortVuln

ADB

- https://developer.android.com/studio/command-line/adb