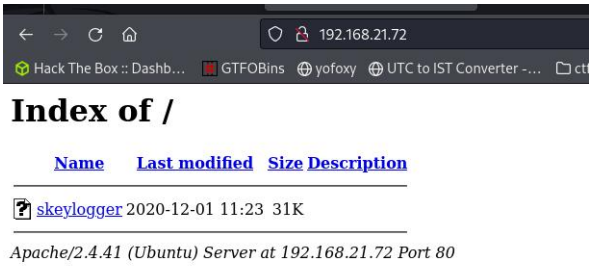
Who Wants to be the King

1.2.3 Enumeration:

```
Currently scanning: 192.168.90.0/16   |   Screen View: Unique Hosts

12 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 720

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.21.72   08:00:27:78:88:19      3     180  PCS Systemtechnik GmbH
192.168.21.167  74:4c:a1:78:d3:fb      3     180  Liteon Technology Corporation
192.168.21.179  4a:e5:44:9f:e6:e6      6     360  Unknown vendor

┌──(root㉿kali)-[/home/kali/cfss/king_of_the_kill]
└─#
```

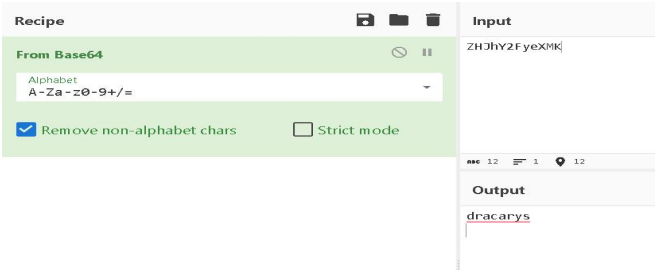
```
Nmap scan report for 192.168.21.72
Host is up (0.00047s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7f:55:2d:63:a8:86:4f:90:1f:05:3c:c9:9f:40:b3:f2 (RSA)
|   256 e9:71:11:ed:17:fa:48:06:a7:6b:5b:b6:0e:1b:11:b8 (ECDSA)
|_  256 db:74:42:c4:37:c3:ae:a0:5c:30:26:cb:1a:ef:76:52 (ED25519)
80/tcp open  http    Apache httpd 2.4.41
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 31K   2020-12-01 11:23  skeylogger
|_
MAC Address: 08:00:27:78:88:19 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 11.444 days (since Thu Sep 28 21:43:46 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.47 ms 192.168.21.72
```

- Open Ports : 80 (http) & 22 (ssh).
- A exe file " skeylogger" hosted on web.

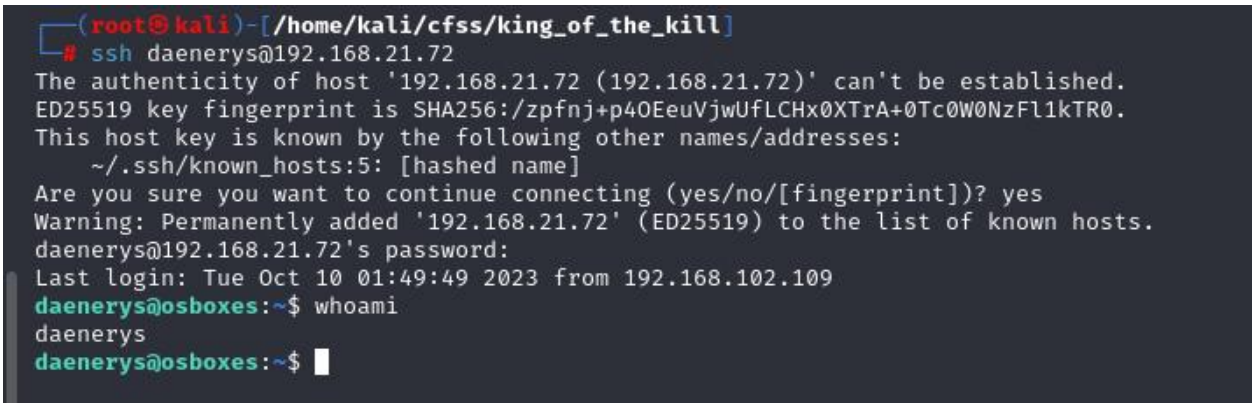


1.2.4 Initial Access:

- On executing the “skeylogger” generates a file with a base64 encoded name which gives “dracarys” (an house name in Game of Thrones series)

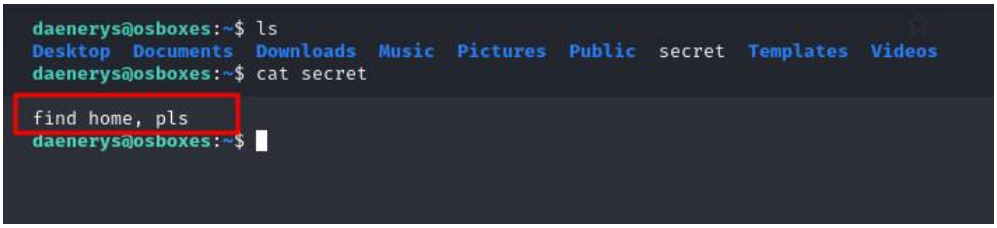


- Trying username:password as daenerys:dracarys gives a successful login to SSH.

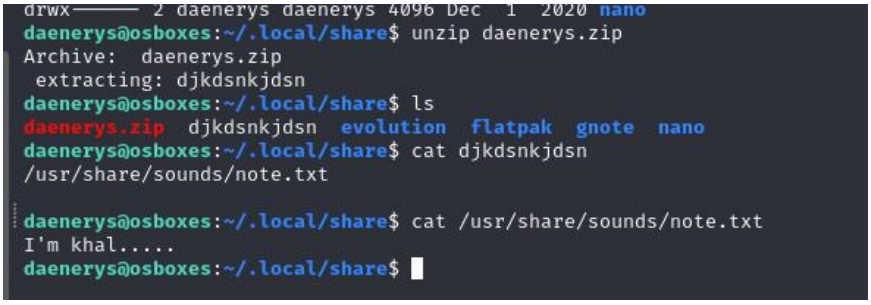


1.2.5 Privilege Escalation:

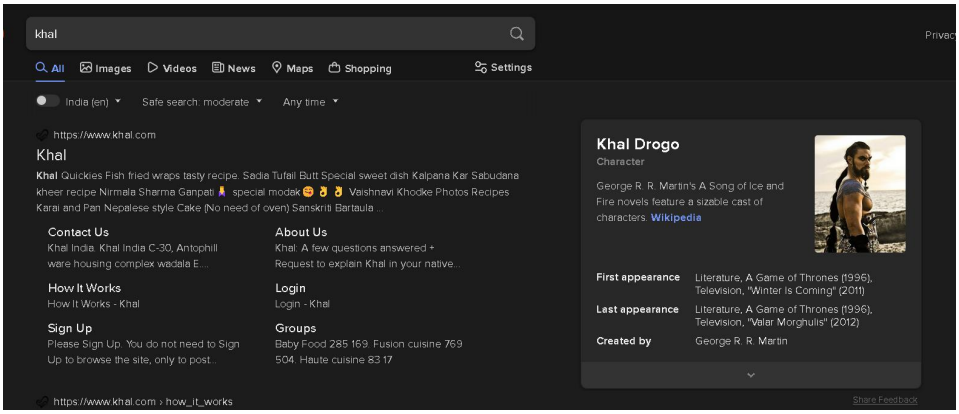
- Further enumeration provides a hint for " find home , pls"



- On listing files in " /.local/share" a file name " daenerys.zip" can be found.
- On extracting the zip file a file points to "/usr/share/sounds/note.txt" which has the text "I'm Khal…."



- By searching the given text in google, results a character name "khaldrogo". Which would be a perfect fit for remaining dots and previous hints.



- Thus using the password "khaldrogo" will gives a privileged root shell.