

# 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

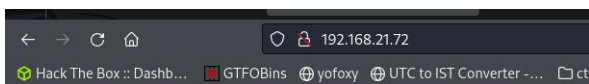
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.21.72	08:00:27:78:88:19	3	180	PCS Systemtechnik GmbH
192.168.21.167	74:4c:a1:78:d3:fb	3	180	Liteon Technology Corporation
192.168.21.179	4a:e5:44:9f:e6:e6	6	360	Unknown vendor

(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.



## Index of /

Name	Last modified	Size	Description
<a href="#">skeylogger</a>	2020-12-01 11:23	31K	

Apache/2.4.41 (Ubuntu) Server at 192.168.21.72 Port 80

```
(root@kali)-[/home/kali/cfss/king_of_the_kill]
# ls
scan  skeylogger

(root@kali)-[/home/kali/cfss/king_of_the_kill]
# file skeylogger
skeylogger: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=ba22a62cfb23e5f98841e89718b9d3f5e76bdf94, for GNU/Linux 3.2.0, with debug_info, not stripped
```

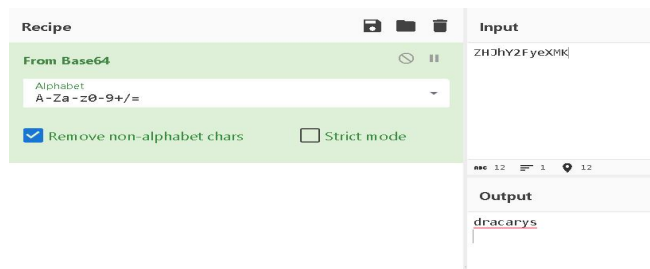
### 1.2.4 Initial Access:

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

```
(root@kali)-[/home/kali/cfss/king_of_the_kill]
# ./skeylogger

(root@kali)-[/home/kali/cfss/king_of_the_kill]
# ls
scan  skeylogger  ZHJhY2FyeXMk

(root@kali)-[/home/kali/cfss/king_of_the_kill]
# cat ZHJhY2FyeXMk
ls<Enter>cat <Right><Enter>
```



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

```
(root@kali)-[/home/kali/cfss/king_of_the_kill]
# ssh daenerys@192.168.21.72
The authenticity of host '192.168.21.72 (192.168.21.72)' can't be established.
ED25519 key fingerprint is SHA256:/zpfnpj+p40EeuVjwUfLCHx0XTrA+0Tc0W0NzF1kTR0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.21.72' (ED25519) to the list of known hosts.
daenerys@192.168.21.72's password:
Last login: Tue Oct 10 01:49:49 2023 from 192.168.102.109
daenerys@osboxes:~$ whoami
daenerys
daenerys@osboxes:~$
```

## 1.2.5 Privilege Escalation:

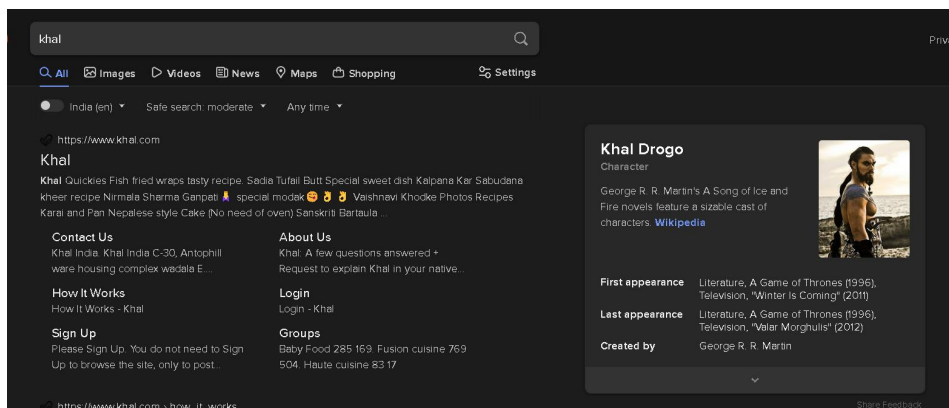
- Further enumeration provides a hint for “ find home , pls”

```
daenerys@osboxes:~$ ls
Desktop Documents Downloads Music Pictures Public secret Templates Videos
daenerys@osboxes:~$ cat secret
find home, pls
daenerys@osboxes:~$
```

- 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....”

```
drwxr-xr-x 2 daenerys daenerys 4096 Dec 1 2020 nano
daenerys@osboxes:~/.local/share$ unzip daenerys.zip
Archive: daenerys.zip
  extracting: djkdskjdsn
daenerys@osboxes:~/.local/share$ ls
daenerys.zip djkdskjdsn evolution flatpak gnote nano
daenerys@osboxes:~/.local/share$ cat djkdskjdsn
/usr/share/sounds/note.txt
daenerys@osboxes:~/.local/share$ cat /usr/share/sounds/note.txt
I'm khal.....
daenerys@osboxes:~/.local/share$
```

- 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.

```
daenerys@osboxes:~$ whoami
daenerys
daenerys@osboxes:~$ su root
Password:
root@osboxes:/home/daenerys# whoami
root
root@osboxes:/home/daenerys#
```