Capturing Handshakes With Hcxdumptool

Aim

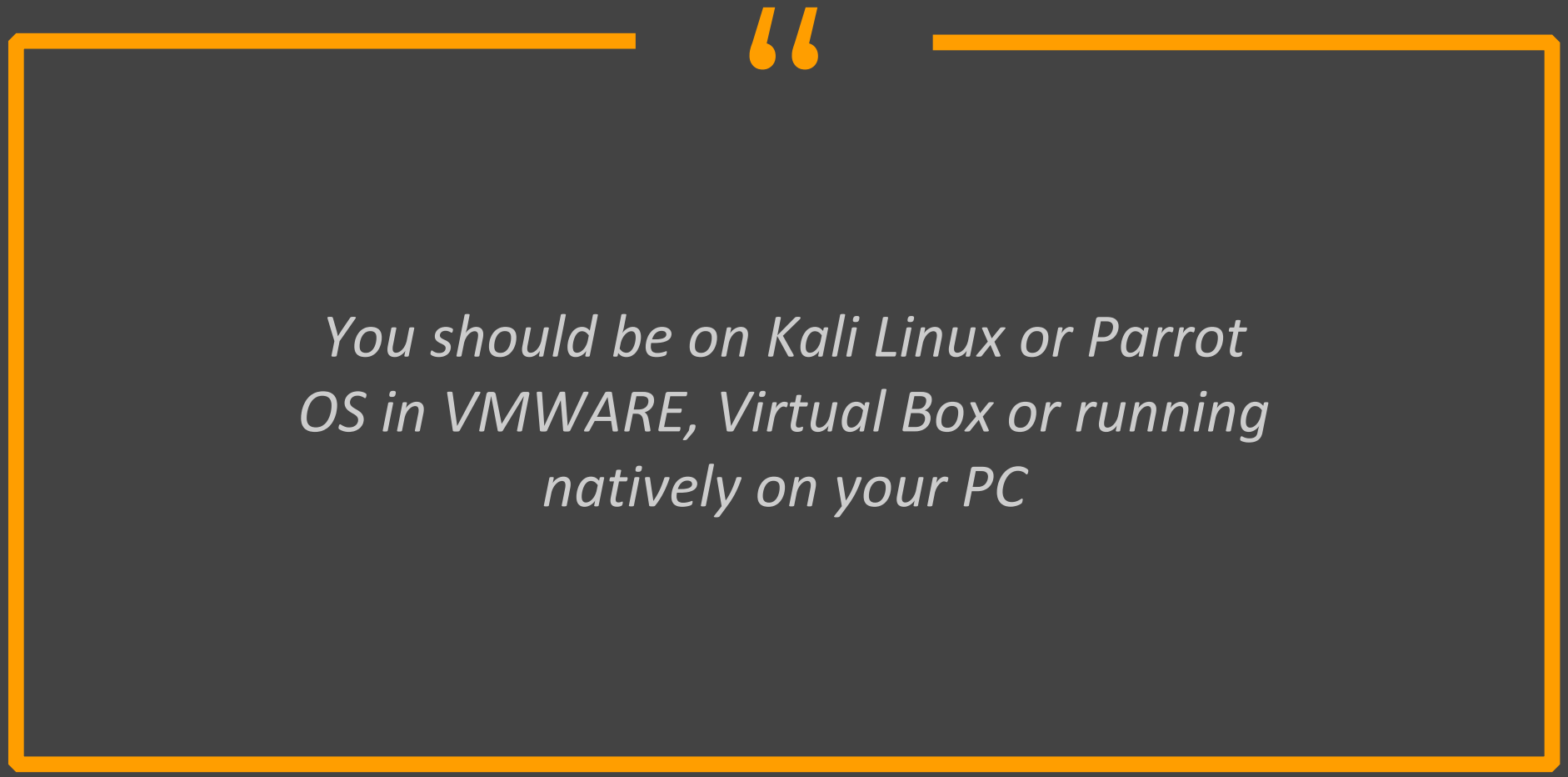
- In this Lecture we are going to see how we can capture handshake packets with Hcxdumptool

We are going to see different methods to crack this handshake with Hashcat (GPU based cracker) in the subsequent lectures

Capturing Handshakes is the first step and most important step for cracking wifi password. Hcxdumptool provides another method to capture the handshakes and is the recommended method to capture packets by Hashcat developers which is another excellent password cracking tool

Hcxdumptool is an easy and straightforward way to capture handshakes.

- ✓ You do not need to de authenticate the clients
- ✓ You can capture handshakes in bulk for all available networks which makes the whole process much simpler



Step- 1

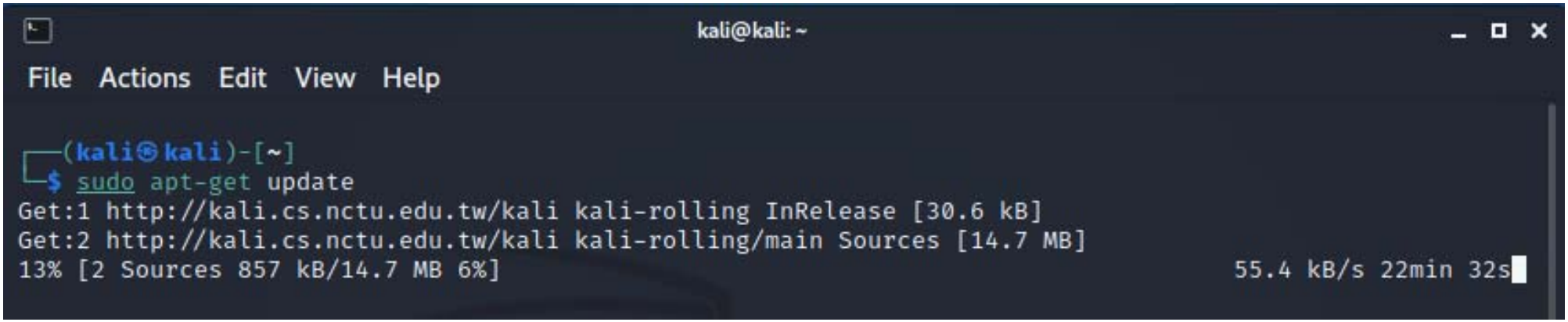
- Installing Hcxdumptool

By default, the tool does not come with Kali linux and you may need to install it

Step- 1

- Update the kali linux packages

```
>sudo apt-get update
```



Step- 1

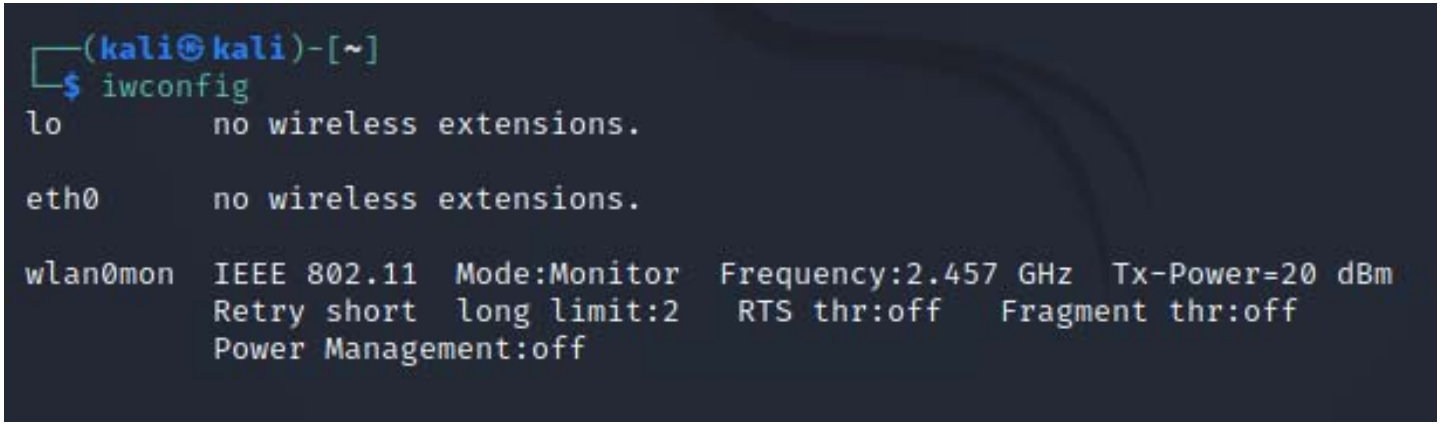
- Install the tool

```
>sudo apt-get install hcxdumptool
```

Step- 2

- Check the wifi adapters available on your machine

>iwconfig	Check the device name



Step- 2

- Stop the services that may interfare with handshake capture

```
>sudo systemctl stop NetworkManager
>sudo systemctl stop wpa_supplicant
```

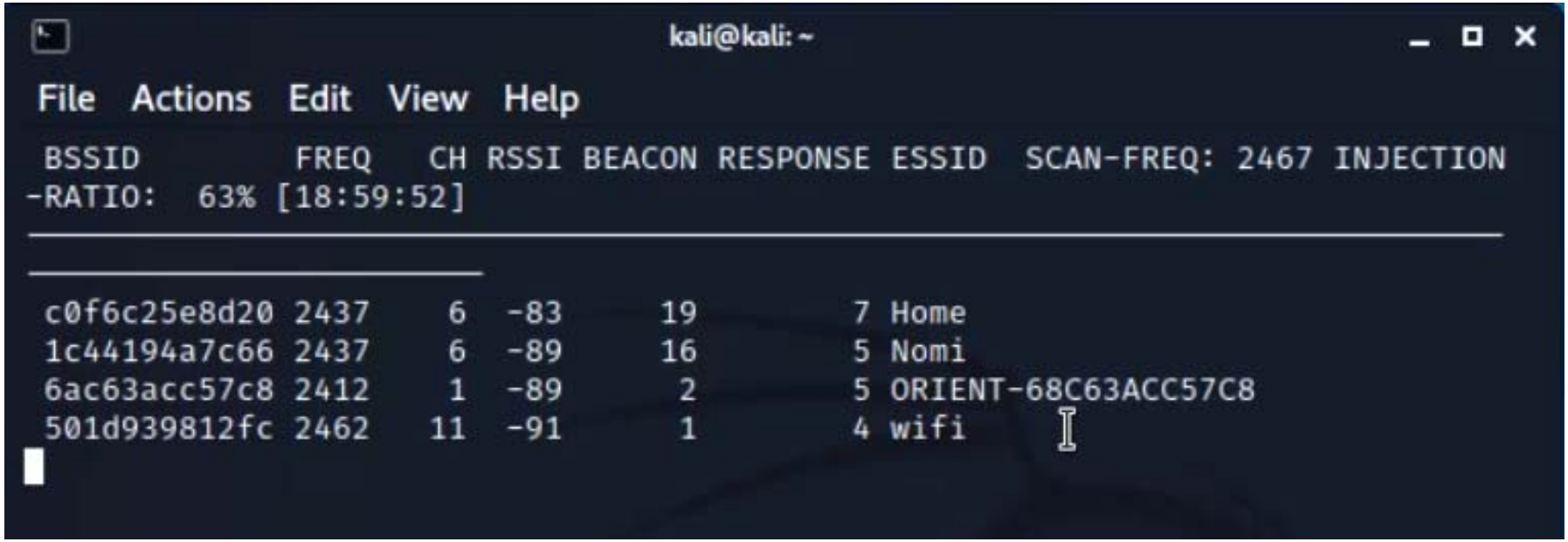
- After the handshake is captured you can restart the services with following command

```
>sudo systemctl start NetworkManager
```

Step- 3

- Scan for available networks

```
>sudo hcxdumptool -i wlan0 --do_rcascan
```



Step- 4

- Capture traffic with hcxdumptool

```
> sudo hcxdumptool -i wlan0 -o dumpfile.pcapng –active_beacon –enable_status=15
```

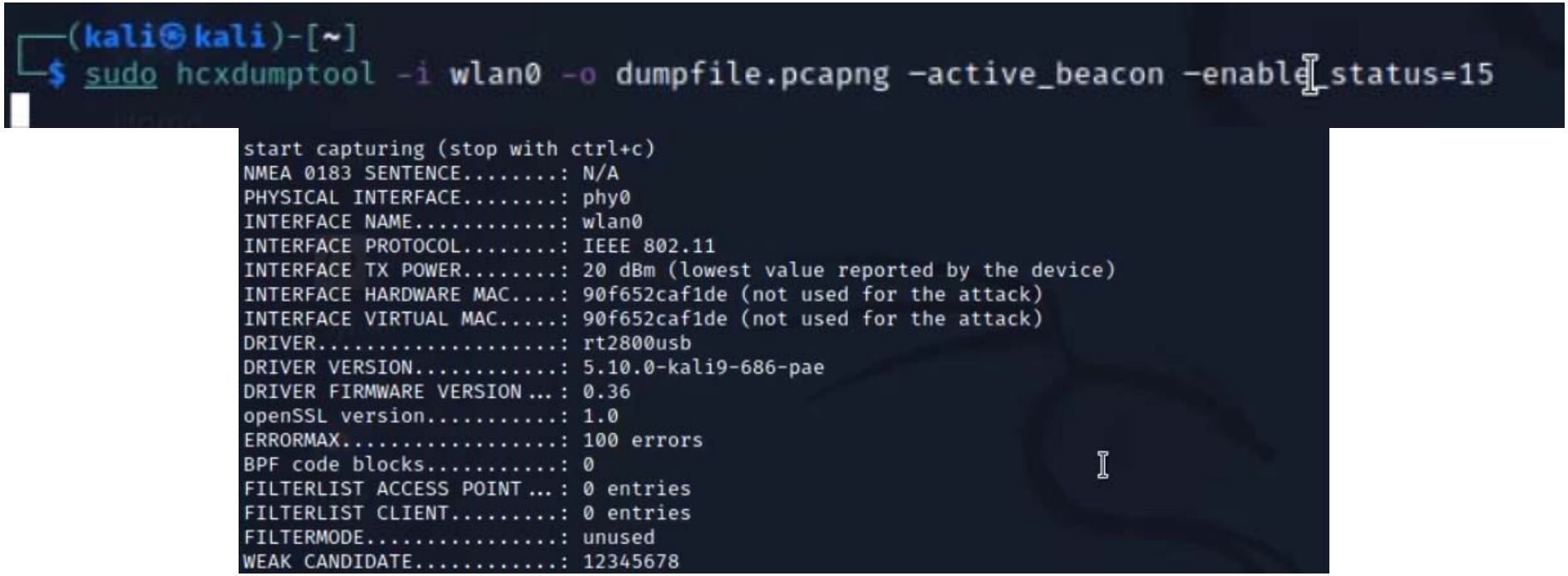
Here :

- dumpfile.pacapng is the file where handshake will be stored
- -wlan0mon is the interface name.

Step- 4

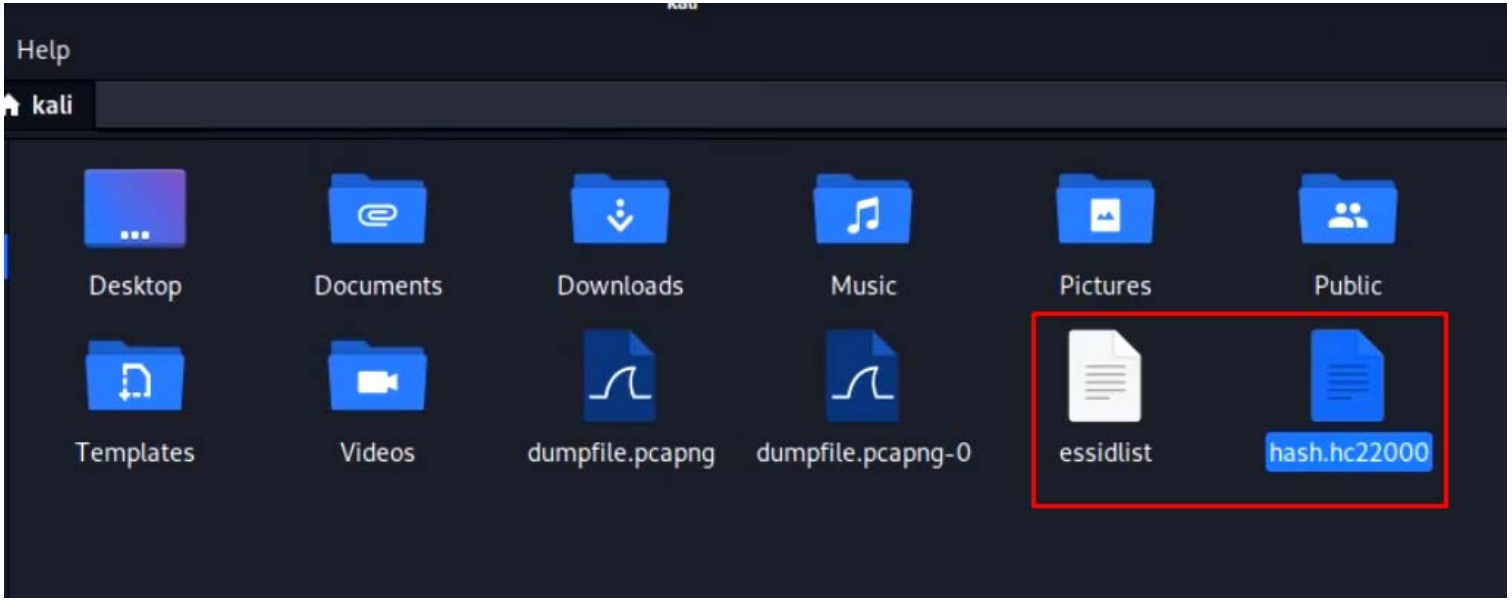
- Capture traffic with hcxdumptool

> sudo hcxdumptool -i wlan0 -o dumpfile.pcapng –active_beacon –enable_status=15



Step- 4

After a minute or two, stop the capture with Ctrl+C and you will have your captured packets file stored in your home directory



DEMO

Hcxdumptool references

- ✓ https://miloserdov.org/?p=7801
- ✓ https://github.com/ZerBea/hcxdumptool

THANKS