Wireless Attack Demo

BY DEAN BOWEN
CYBER SECURITY ANALYST

About

- This is a demonstration of a wireless attack.
- This demonstration shows why it is important to have good password policies in place, as weak passwords can be cracked within a matter of seconds. The type of encryption being used is also important.
- Once on the network, hackers can see network shared folders, perform lateral movement (pivoting), start scanning internal infrastructure, sniffing, and other attacks.

PACKET CAPTURE

Managed mode only collects packets that are meant for that device. Monitor mode will allow the network adapter to grab any packets that are trying to reach access points.

```
kali)-[/home/kali]
nfig
  no wireless extensions.

  IEEE 802.11  ESSID:off/any
  Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
  Retry short limit:7   RTS thr:off   Fragment thr:off
  Encryption key:off
  Power Management:on

kali)-[/home/kali]
```

MONITOR MODE

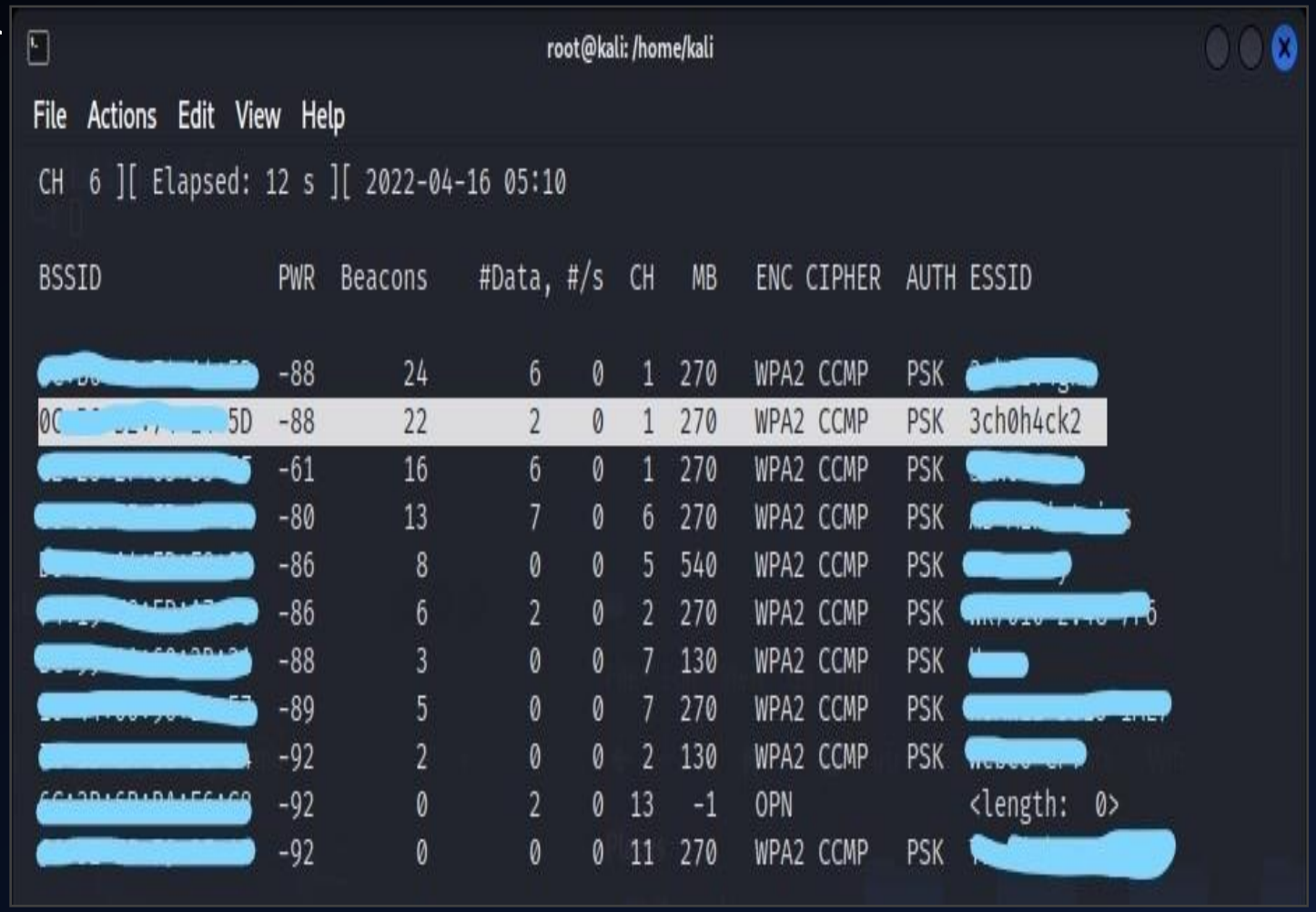
Now that we are in monitor mode we can grab some packets. The idea is to be able to capture a handshake between the client and the access point.

```
root@kali: /home/kali
ons  Edit  View  Help

kali)-[/home/kali]
on-ng start wlan0

processes that could cause trouble.
m using 'airmon-ng check kill' before putting
in monitor mode, they will interfere by changing channels
times putting the interface back in managed mode

Name
NetworkManager
wpa_supplicant

Interface       Driver          Chipset

wlan0           rtw_8821ce      Realtek Semiconductor Co., Ltd. RTL8821CE 802.11ac PC
twork Adapter
        (monitor mode enabled)

kali)-[/home/kali]
```

WIRELESS TOOLS

We can use wireless tools to monitor for clients that are connected (or trying to connect) to the specific access point that we want to attack.

NOTE: This network is using WPA2 encryption. It is best practice to use the highest encryption possible (WPA3 > WPA2 > WPA).

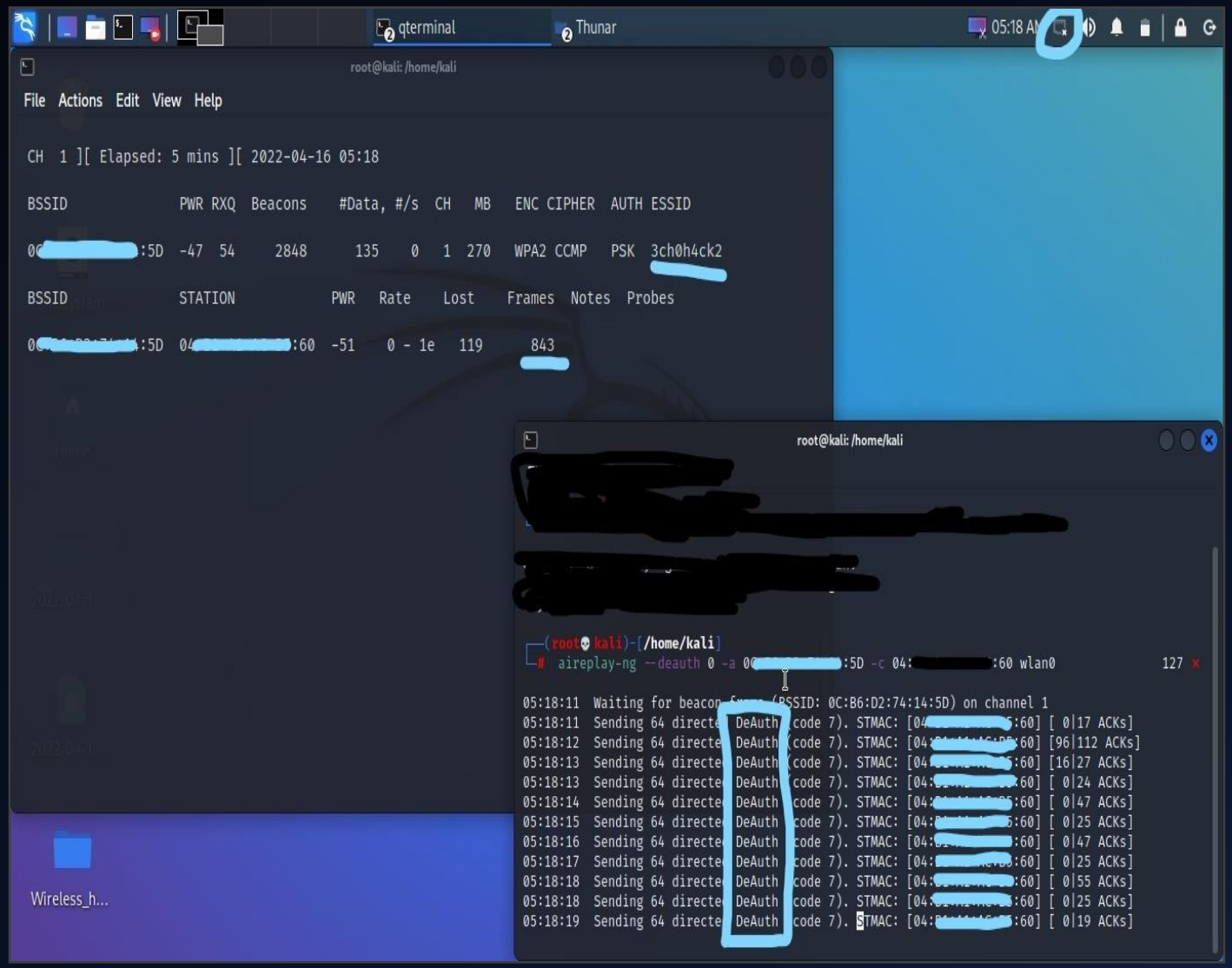


DEAUTH ATTACK

To speed things up, we can use a DeAuth attack on the clients, so that they are forced to re-connect to the access point, thereby having to resend their TCP handshake.

We can then grab that handshake, and with enough frames, we may be able to crack the password offline.

NOTE: We do not need to connect to any network to perform this.

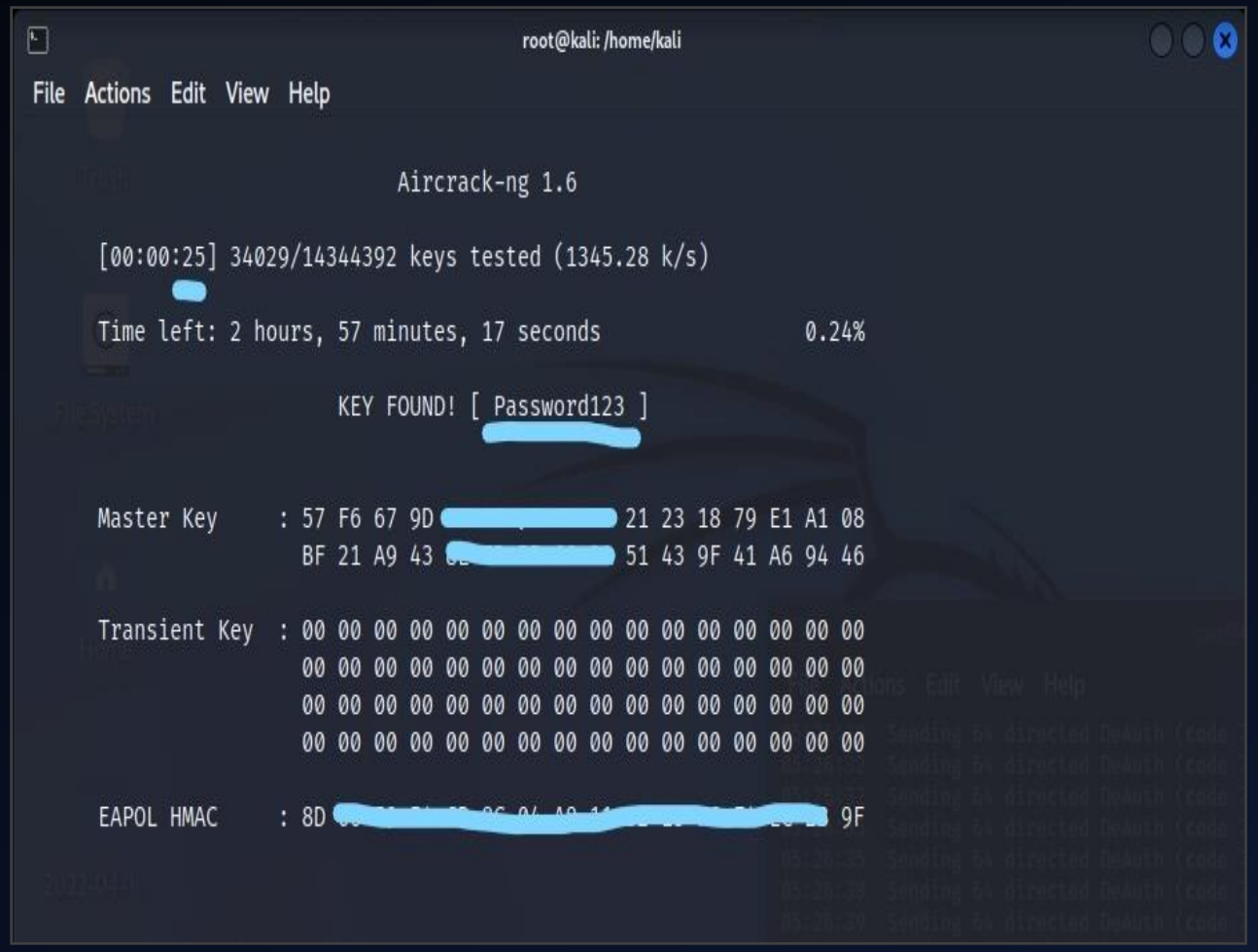


PASSWORD CRACKED

After collecting enough frames, we can start cracking the handshake. After 25 seconds we have cracked the password.

This is an extremely weak password, but passwords like this are very common, and sometimes there is no password at all (open, guest, public WiFi).

A strong password can take several years to crack (uncrackable), however, there are ways to increase the cracking speed using aggregated GPU's on powerful dedicated machines.



CONNECTING TO INTERNAL NETWORK

Once we have the cracked the password, we simply connect to the network as an authenticated device.

From there we can start exploring and probing the network for more attack vectors.

NETWORK MAPPING

Once on the internal network we can start probing devices on this network for open ports and services to exploit (see my network-based attack demo for an illustration of this).

This scan shows us three devices connected to the same access point. With the kali machine being the attacker machine.

From there more specific scans can be done to isolate the target systems, but this scan is all we need to discover machines connected to this access point.

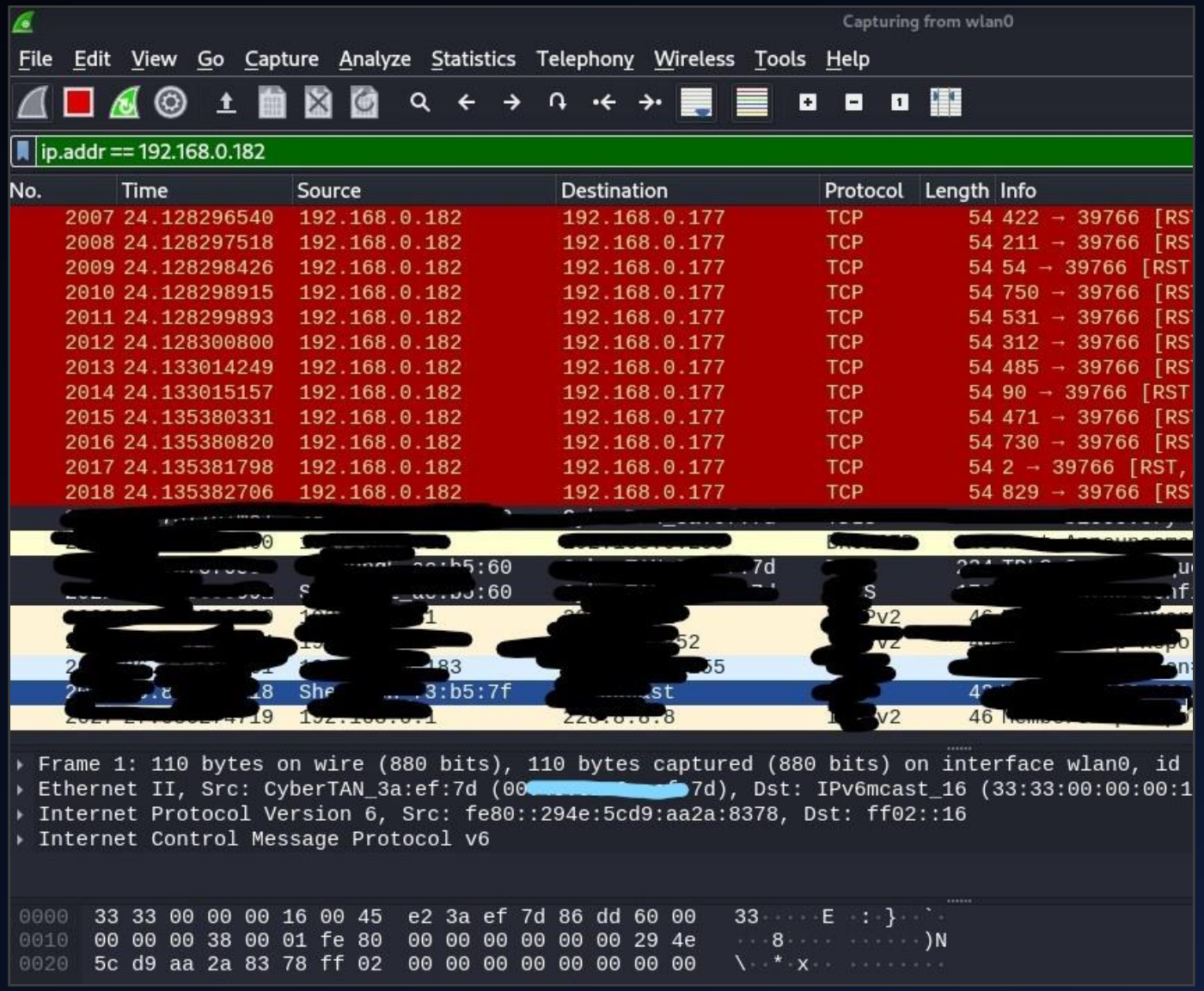
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -T5 -sn 192.168.0.*
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-16 05:58
 EDT
Nmap scan report for [redacted] (192.168.0.1)
Host is up (0.0098s latency).
MAC Address: [redacted] ([redacted])
Nmap scan report for [redacted] (192.168.0.182)
Host is up (0.096s latency).
MAC Address: [redacted] ([redacted])
Nmap scan report for kali (192.168.0.177)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.75 se
conds
```

NETWORK SNIFFING

From this point we can intercept traffic between network devices. We can also turn any machine we are able to exploit into a sniffer.

We can see our scan from the previous slide showing the source and destination of the packets on the network in real-time.

If these machines were using Telnet for example, we would be able to eavesdrop on the packets, and see unencrypted usernames and passwords (in clear text).



THANK YOU