CRACKING PASSWORDS

CASE STUDY: WIFI HACKING

WIFI SECURITY

- Wi-Fi is radio;
  - This means anyone (within range) can read what you send/receive
  - So how to keep things private and secure?

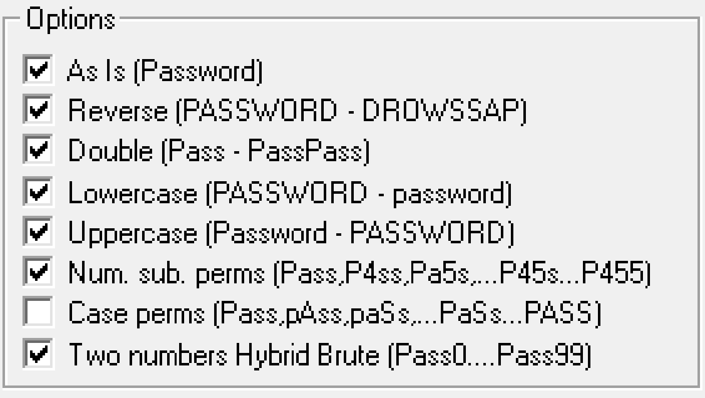
- Answer:
  - Authentication & encryption
    - Many options available: WEP, WPA, WPA2, etc.
    - With various configuration options: EAS, PSK, etc.
    - Most of them can be easily hacked if not configured properly!

STATISTICAL ATTACKS ON WIFI

- Only works on older WEP security
- Method:
  1. Capture lots of traffic (a few minutes-hours)
  2. Use some smart maths to extract password from captured traffic

DICTIONARY/BRUTE-FORCE ATTACKS ON WIFI

- Works on modern WPA/WPA-PSK
- Method:
  1. Capture authentication traffic (one user connecting to the network)
  2. Create or download a list of possible passwords
  3. Try every password in the list (a few minute to a few days depending on list size)
  4. Possibly try combinations, permutations, etc.



Options

☑ As Is (Password)
☑ Reverse (PASSWORD - DROWSSAP)
☑ Double (Pass - PassPass)
☑ Lowercase (PASSWORD - password)
☑ Uppercase (Password - PASSWORD)
☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
□ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

WIFI HACKING WORKSHOP

- We will use a custom version of Linux: Kali Linux
  - It comes with a variety of hacking tool installed
  - Using these tools against real networks or servers is illegal!

DO NOT START ANY PROGRAMS UNLESS INSTRUCTED

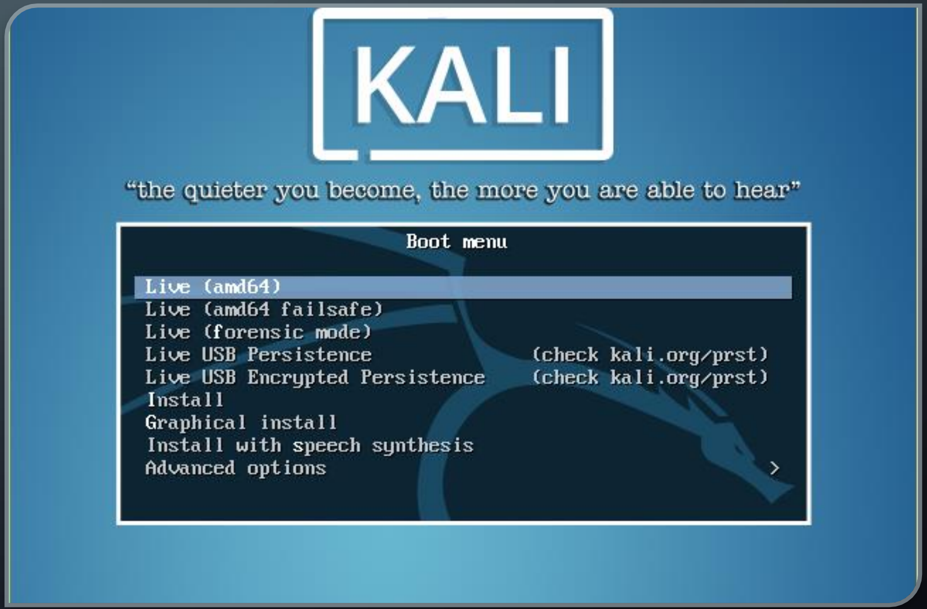
DO NOT CLICK ANY BUTTONS UNLESS INSTRUCTED

STEP 0: SETUP

1. Make sure your PC is **shut down**
2. Plug the **USB WiFi Dongle** in your PC
3. Plug in the **USB Flash Drive** in your PC
4. Turn on your PC.

You should now see this screen:

- If you don't, raise your hand.
- If you do, tap Enter to enter Live mode



```
                         Boot menu

 Live (amd64)
 Live (amd64 failsafe)
 Live (forensic mode)
 Live USB Persistence               (check kali.org/prst)
 Live USB Encrypted Persistence     (check kali.org/prst)
 Install
 Graphical install
 Install with speech synthesis
 Advanced options                                          >
```

BOOT MENU KEY PER MANUFACTURER

- **ASUS:** F2
- **Acer:** F2 or DEL
- **Dell:** F12 or F2
- **HP:** F10
- **Lenovo (Consumer Laptops):** F2 or Fn + F2
- **Lenovo (ThinkPads):** Enter then F12
- **Samsung:** F2
- **Toshiba:** F2

STEP 1: SCAN FOR NETWORKS

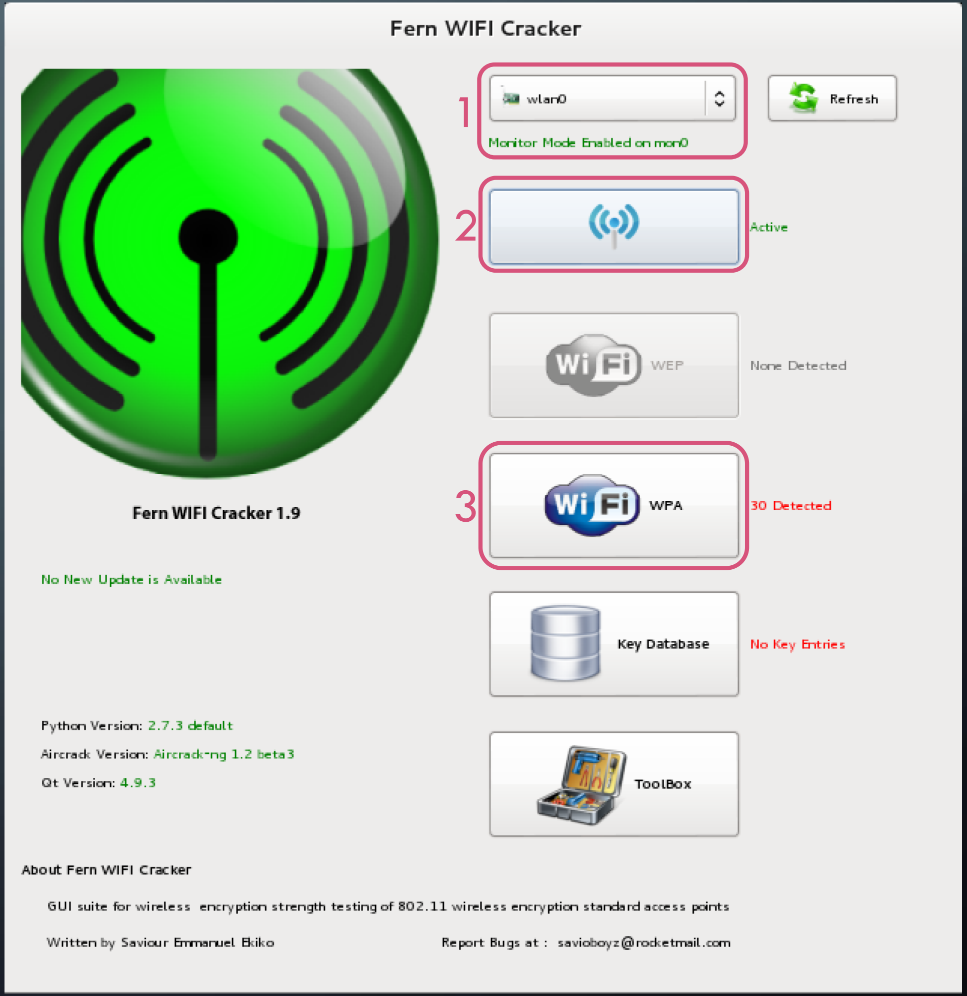
Start **Fern WIFI Cracker**

1. Select interface **wlan1**

   You should see **Monitor Mode Enabled on wlan1** in green below

2. Click **Scan for access points**

3. Click WiFi WPA



Monitor Mode Enabled on mon0

Active

None Detected

30 Detected

No Key Entries

No New Update is Available

Python Version: 2.7.3 default

Aircrack Version: Aircrack-ng 1.2 beta3

Qt Version: 4.9.3

About Fern WIFI Cracker

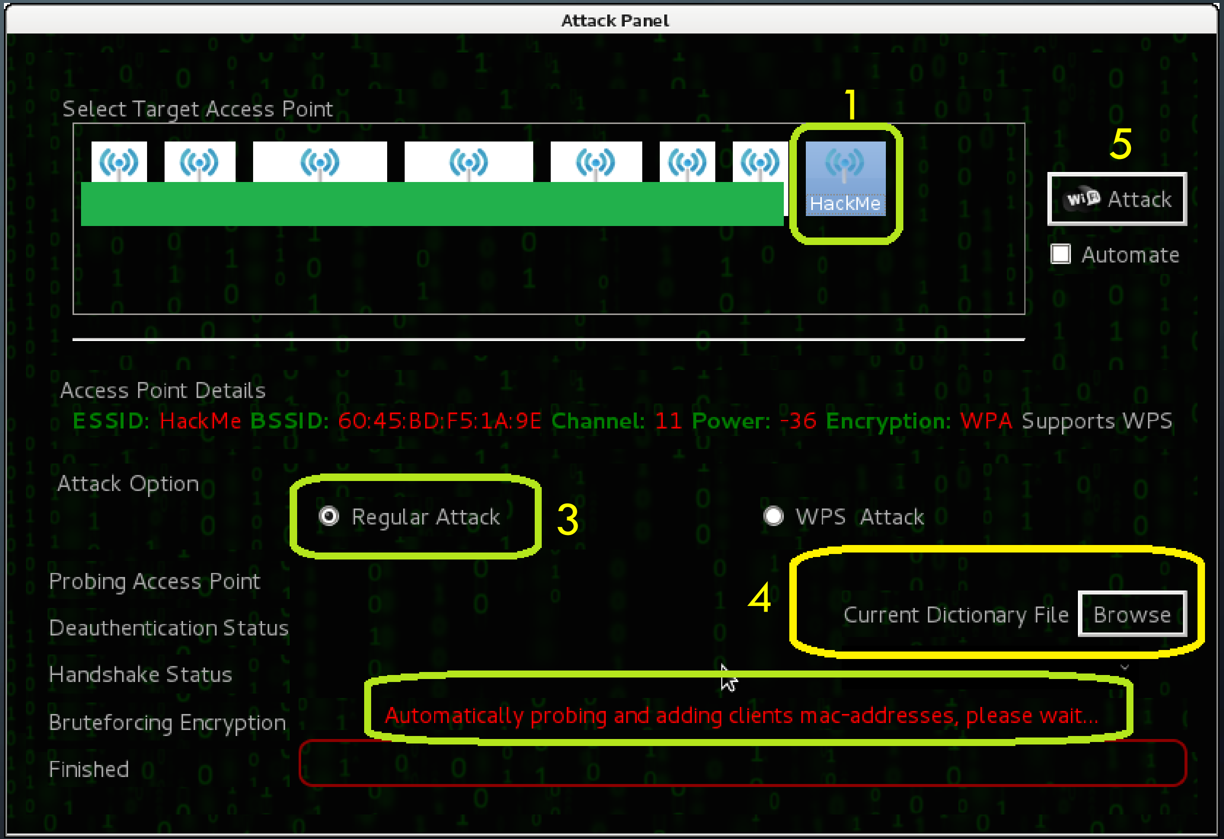
GUI suite for wireless encryption strength testing of 802.11 wireless encryption standard access points

Written by Saviour Emmanuel Ekiko   Report Bugs at : savioboyz@rocketmail.com

STEP 2: ATTACK NETWORK

1. Select the **HackMe** network
2. Make sure you have selected the **HackMe** network!
3. Select **Regular Attack**
4. Select **dictionary file**

   extras > common.txt
5. Click **Attack**



Attack Panel

Select Target Access Point

Access Point Details

ESSID: HackMe BSSID: 60:45:BD:F5:1A:9E Channel: 11 Power: -36 Encryption: WPA Supports WPS

Attack Option ● Regular Attack ○ WPS Attack

Probing Access Point

Deauthentication Status

Handshake Status

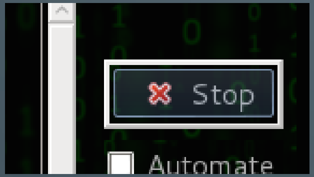
Bruteforcing Encryption

Finished

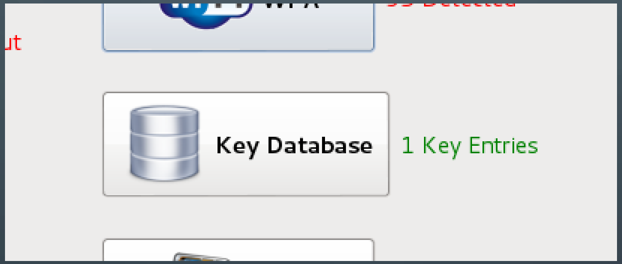
Automatically probing and adding clients mac-addresses, please wait...

STEP 3: USE PASSWORD TO CONNECT TO NETWORK

1. Stop the attack
2. Close the Attack Panel



3. Open the Key Database



4. Connect to the HackMe network using the password you just retrieved using the **USB Wi-Fi** interface

STEP4: SNIFF TRAFFIC

1. **Restart** your PC and **boot into Kali** again.
2. Connect to the network using the **USB WiFi Adapter**
3. Start **Ettercap**
4. Click **Sniff > Unified sniffing**
5. Select **wlan1**
6. Click **Scan hosts**

STEP 5: INTERCEPT TRAFFIC VIA A MAN-IN-THE-MIDDLE ATTACK

The victim:

1. Start **Terminal**
2. Type **ifconfig** and read out the **IP address of wlan1**

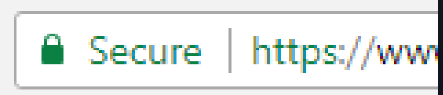
7. Open **Firefox** and navigate to **arguesecure.ewi.utwente.nl**
8. Log in with username **z.tan@utwente.nl** and password **54682**

The attacker:

3. Select IP address of the victim and **Add to Target 1**
4. Click **Mitm >ARP poisoning**
5. Tick **Sniff remote connections**
6. Click View > Connections (and enable resolve IP addresses)

RECOMMENDATIONS

- Always use the latest and most secure option available (e.g. WPA2).
- Even when using strong security, never use passwords containing words, names or dates.
  - They are vulnerable to brute force attacks
- Make sure you only enter data in websites secured with HTTPS



  - Especially on public WiFi

PASSWORD CRACKING

- Brute force attacks and dictionary attacks are possible on any passwords;
  - E.g. online accounts, phone lock screens;
  - Many leaks contain encrypted passwords - these can be cracked in the same way.

- Mitigations:
  1. Lock-out after X failed attempts;
  2. Two-factor authentication;
  3. **Unique, long, hard to guess passwords.**

WHAT DOES ALL THIS MEAN FOR RISK MANAGEMENT?

Several factors make cyber-risks much harder to manage:

- Availability of hacking tools and tutorials
- Computation power of modern computers
- Anonymity provided by the Internet

CYBER-RISK MANAGEMENT

- Is as much about the technology as it is about the human using it
  - Social engineering is used in over 2/3 of all attacks by hackers, hacktivists and nation states.*

- Is as much about prevention as it is about detection:
  - A new zero-day vulnerability was discovered every week in 2015**

* social-engineer.org

** 2016 Symantec Internet Security Threat Report