Ethical Student Hackers

WiFi Hacking

SHEFFIELD Ethical Student Hackers

Breaking into security.

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Introduction

In simple terms, WiFi is a radio signal travelling from a device to another.

Intercepting or manipulating this signal forms the basis of WiFi hacking.

WiFi security has improved over the years, but there are still various types of attacks that hackers can perform on unsuspecting people:

- Sniffing: on-air spying on packets
- Spoofing: making a malicious ‘clone’ of a router
- Cracking: brute force attack on keys

History & Useful Terms

WEP—Wired Equivalent Privacy

- Required a 10-digit or 26-digit hexadecimal preshared key (PSK)
- Weak encryption
- Easy to spy on other people on the same network
- Not secure overall, quickly cracked

WPA—Wi-Fi Protected Access

- introduced TKIP, the Temporal Key Integration Protocol, and a Message Authentication Code
- could connect to a WiFi network without automatically exposing your traffic to everyone else in the network

WPA2

- TKIP replaced with AES-CCMP, a more secure encryption method
- not vulnerable to the same attacks as TKIP

History & Useful Terms

WPA3

- announced in January 2018, after WPA2 ‘KRACK’ attacks were made public
- for security reasons, PSK got replaced by SAE (Simultaneous Authentication of Equals), which identifies peer devices among each other
- makes cryptographic attacks more difficult

Useful Terms

- SSID: the visible name of the network
- ESSID: SSID which could apply to multiple access points
- BSSID: access point MAC address
- WPA2-PSK: WiFi networks that have the same password for everyone who wants to connect to them
- WPA2-EAP: WiFi networks that demand a username and a password, which are sent to a RADIUS server
- RADIUS: a server for client authentication

More on WPA2

- authentication is done through the 4-way handshake between the client and the access point
- both need to know the key, which is derived from the ESSID and the password
- the ESSID being used as a salt means that performing dictionary attacks is more difficult, since the key is different for different access points
- Brute force is still possible on WPA2 (personal), but it should not be used on WPA2-EAP

Aircrack-ng

Aircrack-ng is a useful collection of tools used for measuring the security of a WiFi network by means of monitoring, attacking, testing or cracking.

The relevant tools used for attacking WPA networks are:

- aircrack-ng, for cracking
- airodump-ng, for creating captures
- airmon-ng, for monitoring

WiFi Sniffing

In order to capture the 4-way handshake, you need a Network Interface Card (NIC) with monitor mode.

To activate monitor mode on an interface (e.g., wlan0), you use the command:

- airmon-ng start wlan0 (this will add “mon” to its name)

If there are other processes using the network adapter, this command can be helpful:

- airmon-ng check kill

Useful flags

- --bssid sets the BSSID to monitor
- --channel sets the channel
- -w to capture packets to a file

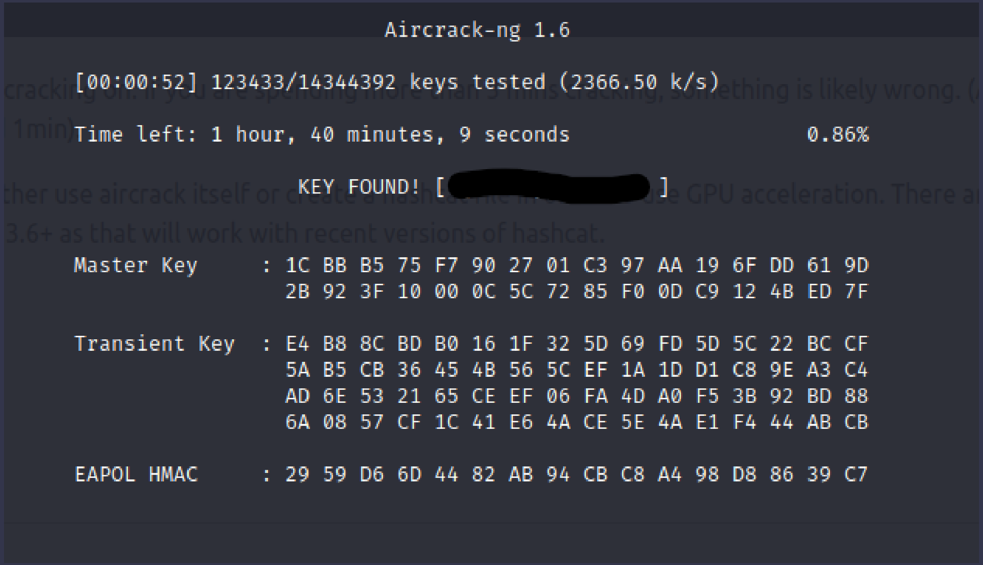
WiFi Cracking

Aircrack-ng will be used to crack the key of a WiFi network by making use of data from a packet capture (.cap) file.

The relevant flags that will help us do that are:

- -b for specifying a BSSID
- -w for specifying a wordlist

rockyou.txt is located in /usr/share/wordlists on Kali Linux



```
                              Aircrack-ng 1.6

      [00:00:52] 123433/14344392 keys tested (2366.50 k/s)

      Time left: 1 hour, 40 minutes, 9 seconds                   0.86%

                         KEY FOUND! [ [redacted] ]


      Master Key     : 1C BB B5 75 F7 90 27 01 C3 97 AA 19 6F DD 61 9D
                       2B 92 3F 10 00 0C 5C 72 85 F0 0D C9 12 4B ED 7F

      Transient Key  : E4 B8 8C BD B0 16 1F 32 5D 69 FD 5D 5C 22 BC CF
                       5A B5 CB 36 45 4B 56 5C EF 1A 1D D1 C8 9E A3 C4
                       AD 6E 53 21 65 CE EF 06 FA 4D A0 F5 3B 92 BD 88
                       6A 08 57 CF 1C 41 E6 4A CE 5E 4A E1 F4 44 AB CB

      EAPOL HMAC     : 29 59 D6 6D 44 82 AB 94 CB C8 A4 98 D8 86 39 C7
```

Example command:

aircrack-ng -b insert_bssid_here –w insert_wordlist_ here insert_file_location_here

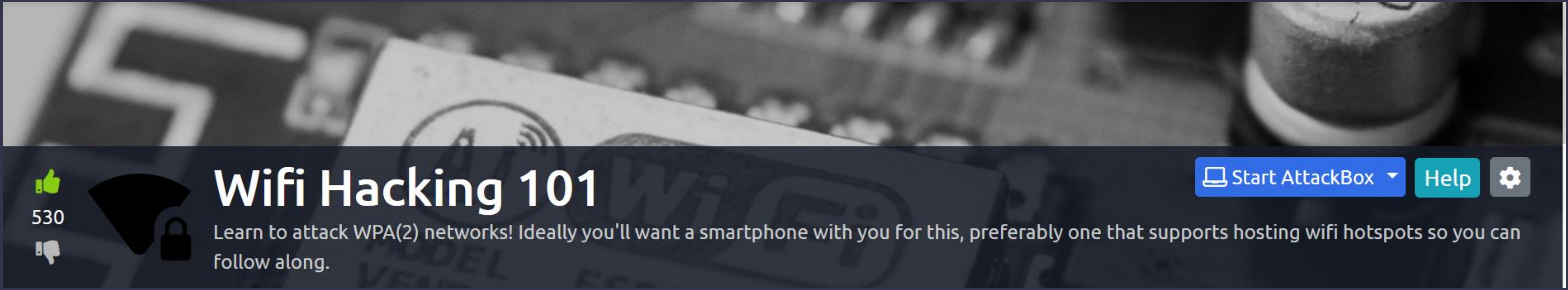
SHEFFIELD Ethical Student Hackers

Breaking into security.

Practical Exercises

The practical part of this session consists of completing a tryhackme room called “Wifi Hacking 101”.

The link for this room is: https://tryhackme.com/room/wifihacking101



Wifi Hacking 101

Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.

Upcoming Sessions

What's up next?
www.shefesh.com/sessions

14th March - Cryptography

21st March – Advanced Web Hacking

28th March – CTF/Session?

4th April – HTB Sesssion

Any Questions?

SHEFFIELD ETHICAL STUDENT HACKERS

www.shefesh.com

Thanks for coming!

SHEFFIELD Ethical Student Hackers

Breaking into security.