Ethical Student Hackers

WiFi

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.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

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

Cont.

WPA2

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

WPA 3

- 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

Glossary of Acronyms

- 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.

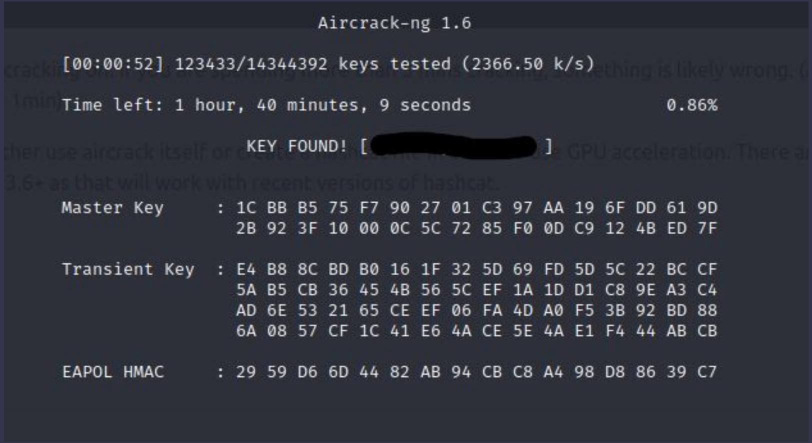
The relevant flags that will help us do that are:

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

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

Example command:

- aircrack-ng -b insert_bssid_here –w insert_wordlist_ here insert_file_location_here



```
                               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
```

Defense

Any thoughts on how we can defend against WiFi password cracking?

The Basics

Change the default SSID and password!!

- It may seem obvious but many businesses and homes fail to do this basic and obvious task
- The password can be made far more challenging to crack than many default network passwords

In business, invest in an IDS or a larger security package

- This takes the onus and responsibility of your shoulders
- There are many affordable home solutions as well although most home networks will come with some sort of protection and intrusion protection

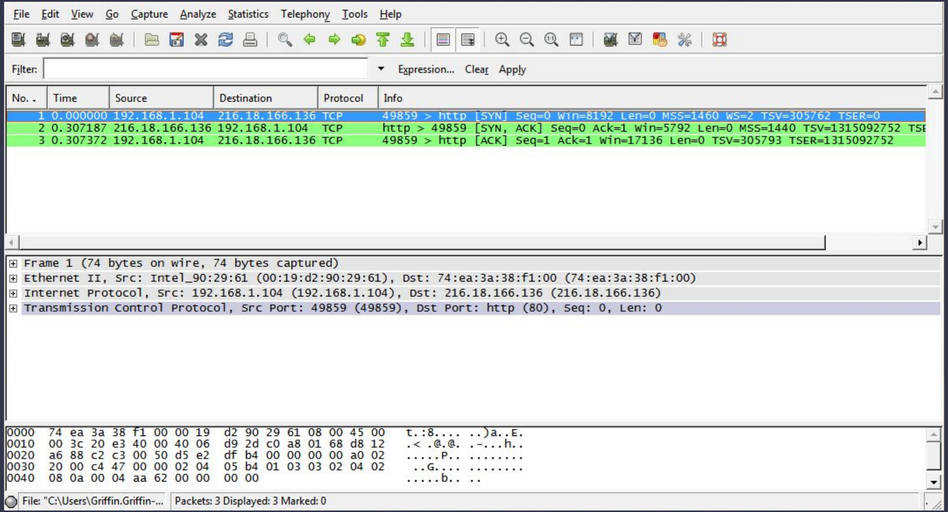
Things like this

- In many cases, the first step to good security is education
- Just by being here and learning about WiFi attacks, you know what to look out for and what to avoid in your professional and personal life

Getting Technical

Wireshark

- Wireshark monitors network traffic and exports it into .pcap files which can be useful for post-attack forensics
- Has the potential for live monitoring if a developer can find distinctions between normal and malicious traffic



```
No. .  Time      Source          Destination     Protocol  Info
     1 0.000000  192.168.1.104   216.18.166.136  TCP       49859 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 TSV=305762 TSER=0
     2 0.307187  216.18.166.136  192.168.1.104   TCP       http > 49859 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1440 TSV=1315092752 TSE
     3 0.307372  192.168.1.104   216.18.166.136  TCP       49859 > http [ACK] Seq=1 Ack=1 Win=17136 Len=0 TSV=305793 TSER=1315092752
```

```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Intel_90:29:61 (00:19:d2:90:29:61), Dst: 74:ea:3a:38:f1:00 (74:ea:3a:38:f1:00)
⊞ Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 216.18.166.136 (216.18.166.136)
⊞ Transmission Control Protocol, Src Port: 49859 (49859), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  74 ea 3a 38 f1 00 00 19  d2 90 29 61 08 00 45 00   t.:8.... ..)a..E.
0010  00 3c 20 e3 40 00 40 06  d9 2d c0 a8 01 68 d8 12   .< .@.@. .-...h..
0020  a6 88 c2 c3 00 50 d5 e2  df b4 00 00 00 00 a0 02   .....P.. ........
0030  20 00 c4 47 00 00 02 04  05 b4 01 03 03 02 04 02    ..G.... ........
0040  08 0a 00 04 aa 62 00 00  00 00                     .....b.. ..
```

File: "C:\Users\Griffin.Griffin-... Packets: 3 Displayed: 3 Marked: 0

Practical

- Try to crack the WiFi access point we have set up
  - One WPA2 wifi access point
  - One laptop connected to the wireless network (you can look at the screen)
- SSID: ShefESH_DO_NOT_CONNECT
- 5c:b1:3e:40:bf:52, 5c:b1:3e:40:bf:53
- Walkthrough of cracking WPA2: https://shefesh.com/assets/wiki/wifi_hacking.pdf

- Backup tryhackme: https://tryhackme.com/room/wifihacking101

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

20th November - Workroom 2 - Bounty Hunting

27th November - Workroom 2 - ???

4th December - Hicks LT10 - CTF

Any Questions?

www.shefesh.com

Thanks for coming!