Residential Wi-Fi

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 shefesh.com/conduct

Wi-Fi

WiFi is a way of transmitting information through radio waves

Any form of intercepting, spoofing, or interrupting this signal is a form of wifi hacking

WiFi security has improved over the years, but it is still vulnerable to several attacks

- Spoofing
- Cracking
- Sniffing

History of Security

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
- Retired in 2004
- Still in use in 7% of networks 💀

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
- Still by far the most commonly used

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
- Only 1.82% usage

Useful 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

WPA2

WPA2 is by far the most common (roughly 80% usage) so we will focus on that.

4 way handshake:

1. Both device and access point create a random number (ANonce and SNonce)
2. They send each other these numbers
3. They create an **Encryption Key** using these 2 numbers, and the preshared key (combination of wifi password and ESSID)
4. They send each other encrypted messages, and if they are both decryptable they know they both know the password!

- ESSID as a salt means cracking is more difficult
- Brute force is possible on WPA2, but should not be used

Cracking WPA2

- We know the ESSID, and can sniff the ANonce and SNonce (and encrypted message)
- We want to know the password

1. Sniff the required information
2. Use a dictionary (rockyou.txt) to create a list of possible PSKs and therefore encryption keys
3. Try to decrypt the encrypted message with this list, whichever one works is the password!

This is a lot of effort to do manually, but there are tools!

aircrack-ng suite

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

Using aircrack-ng

1. Set your network card to “monitor mode” (not all cards have this ability)
    a. airmon-ng check kill
    b. airmon-ng start wlan0 (or your network card name)
2. Find the BSSID of the network
    a. airodump-ng wlan0mon
    b. Cycles through channels and finds networks
3. Listen for the 2 way handshake
    a. airodump-ng -c [CHANNEL] --bssid [BSSID] -w [output file] wlan0mon
    b. Will tell you when it captures a handshake
4. Filter for EAPOL (handshake protocol) in wireshark (optional)
    a. If you don't filter and supply the .cap file directly to aircrack-ng, you will also need to supply the SSID
5. Crack the password
    a. aircrack-ng -b [BSSID] -w [WORDLIST] *.cap

Defence

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

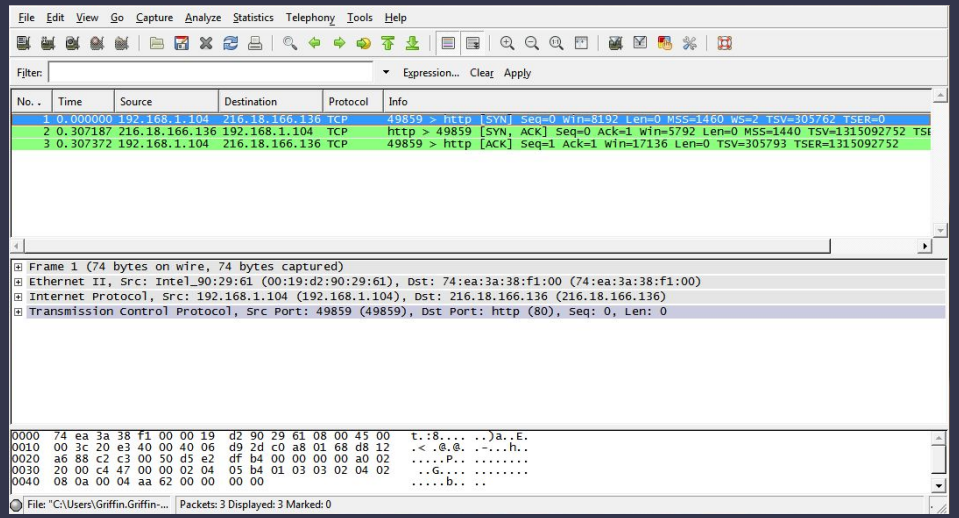
Things like this

- 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



example

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

Bounty hunting
2nd December

Deadline week
9th December

Lockpicking
16th December

Any Questions?

www.shefesh.com

Thanks for coming!