Evil Narwhal

Spring 2018

GROUP 10: JESSE THADEN,
VIET TRAN,
WENJIE YANG,
WESLEY CHUNG

What Is Evil Twin?

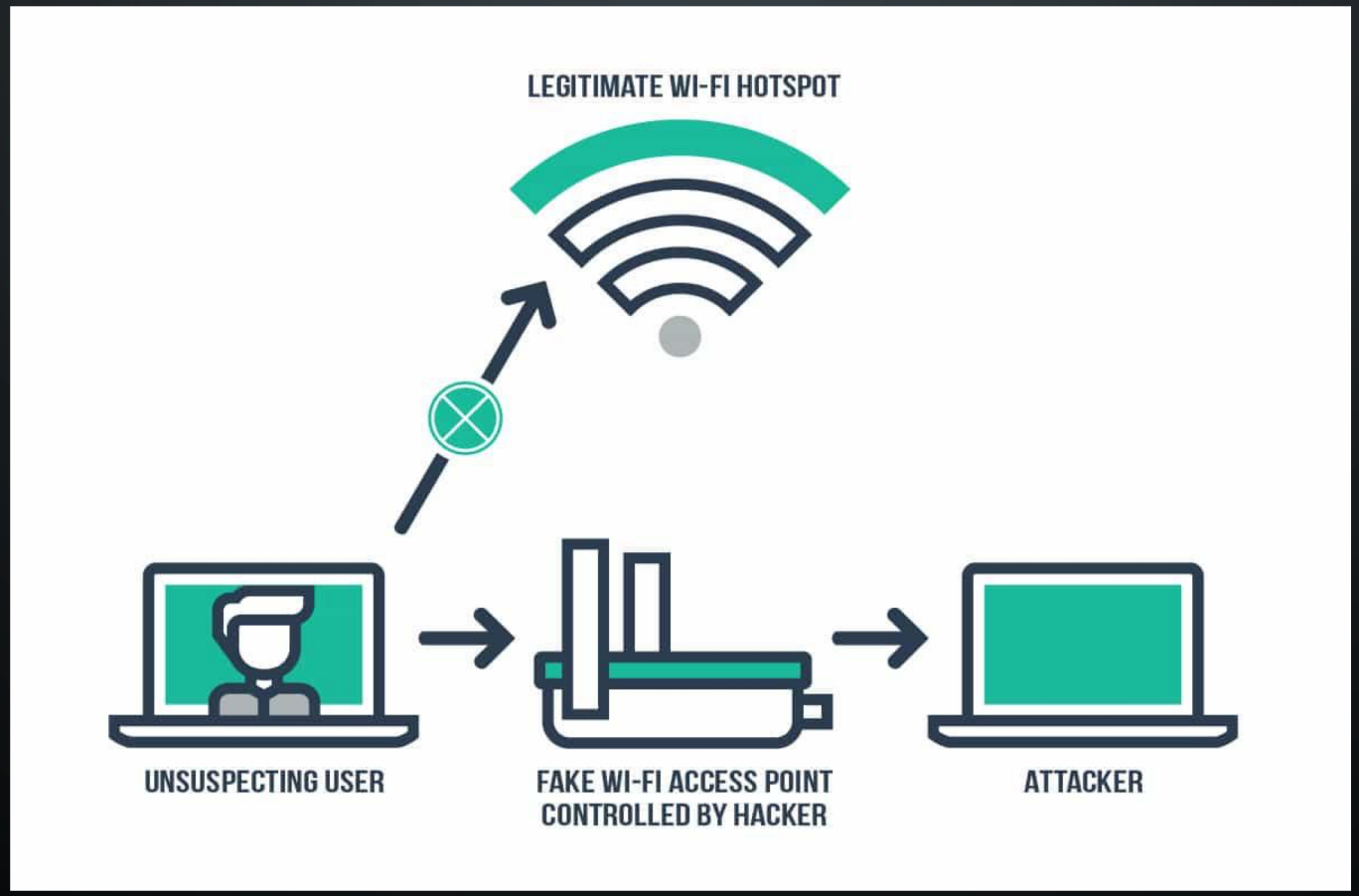
- An “evil twin” is a kind of rogue AP. It is a fraudulent Wi-Fi access point, which tries to hook clients to connect to the fake network to steal information.

MOTIVATION

-- Feel anxious to crack Wi-Fi passwords?

-- To provide an easier way to steal Wi-Fi passwords

OVERVIEW


LEGITIMATE WI-FI HOTSPOT
UNSUSPECTING USER
FAKE WI-FI ACCESS POINT
CONTROLLED BY HACKER
ATTACKER

WHAT WE USED:

Airmon-ng, Airodump-ng

- Packet capture and export of data to text files for further processing

Hostapd

- It is used to create a wireless hotspot.

Dnsmasq

- Lightweight DNS/DHCP server. It is used to resolve dns requests from/to a machine and also acts as DHCP server to allocate IP addresses to the clients.

Apache

- Runs our fake website that users get redirected to locally.

STEP 1: CHOOSE THE TARGET ACCESS POINT

- Run airmon-ng and airodump-ng to get a list of access points.
- Let the user type in the AP they want to attack

STEP 2: SET UP THE EVIL TWIN

- Set up a fake access point by creating a hostapd configuration file
- Set up DHCP server by creating a dnsmasq configuration file
- Configure iptables to reroute traffic
- Deauth user from real access point

STEP 3: CREATE FAKE WEBSITE

- Start the Apache server to run fake website
- Wait for user to type in credentials

STEP 4: USE THE STOLEN CREDENTIALS

- HTTP form will POST to php file that writes credentials to a file
- With the stolen credentials, log into actual network and scan that network

DEMO

PROBLEMS ENCOUNTERED

- Unable to make sure our fake AP is closer or stronger than the real one
- Unable to make victims automatically connect to our fake AP
- Need two wireless adapters (one for deauth, other for hostapd)

IMPROVEMENTS

- We can use some database to store credentials for future use
- We can try to redirect HTTPS traffic too
- Make it more deceiving