Using `airodump-ng` with Fixed Channels

🔍 Objective

Learn how to use `airodump-ng` to monitor a specific Wi-Fi channel and capture wireless traffic, while addressing the common "fixed channel: -1" error.

📌 Prerequisites

- **Operating System**: Kali Linux or any Linux distribution with Aircrack-ng suite installed.
- **Wireless Adapter**: Compatible with monitor mode and packet injection (e.g., Atheros, Realtek chipsets).
- **Tools**: Aircrack-ng suite (`airmon-ng`, `airodump-ng`, etc.).

🛠️ Setting Up Monitor Mode on a Specific Channel

1. **Identify Wireless Interface**:
   Open a terminal and list your network interfaces:

   ```
   iwconfig
   ```

   Look for interfaces like `wlan0`, `wlan1`, etc.

2. **Stop Network Manager** (if running):

   ```
   sudo systemctl stop NetworkManager
   ```

   This prevents the Network Manager from interfering with your wireless interface.

3. **Enable Monitor Mode on Specific Channel**:

   ```
   sudo ip link set wlan0 down
   sudo iw dev wlan0 set type monitor
   sudo iw dev wlan0 set channel 6
   sudo ip link set wlan0 up
   ```

   Replace `wlan0` with your interface name and `6` with your desired channel.

4. **Verify Monitor Mode**:

   ```
   iw dev wlan0 info
   ```

Ensure the interface is in monitor mode and on the correct channel.

🛑 Troubleshooting "Fixed Channel: -1" Error

If you encounter the "fixed channel: -1" error, it may be due to driver or kernel issues. Here are some solutions:

1. Use `--ignore-negative-one` Flag:

```
sudo airodump-ng --ignore-negative-one mon0
```

This flag tells `airodump-ng` to ignore the channel mismatch error.

2. Reinstall Aircrack-ng Suite:

```
sudo apt-get install --reinstall aircrack-ng
```

This ensures you have the latest version of the tools.

3. Patch Kernel or Drivers:

If using Atheros or Realtek chipsets, consider updating or patching your kernel or drivers. For instance, the `compat-wireless` package may help resolve driver-related issues.

4. Use Alternative Tools:

If issues persist, consider using alternative tools like `airodump-ng-ng` or `kismet` for wireless monitoring.

📶 Capturing Wireless Traffic on a Specific Channel

1. **Start `airodump-ng`**:

   ```
   sudo airodump-ng --channel 6 --write capturefile mon0
   ```

   This command captures traffic on channel 6 and saves it to `capturefile`.

2. **Monitor Output**:
   Observe the terminal for information about nearby access points and associated clients.

⚠️ Important Notes

- **Channel Hopping**: `airodump-ng` does not hop channels when a fixed channel is specified. Use `airodump-ng` without the `--channel` flag to scan all channels.
- **Legal Considerations**: Always ensure you have explicit permission to perform penetration testing on any network. Unauthorized access is illegal and unethical.