WiFi Reconnaissance Quick Reference

Monitor Mode Setup

Check Wireless Interfaces

```bash
iwconfig
```

Enable Monitor Mode

```bash
sudo airmon-ng check
sudo airmon-ng start [your-adapter-name]
```

Verify Monitor Mode

```bash
iwconfig
# Look for interface name change (e.g., [adapter-name]mon)
```

Basic Network Discovery

Scan All Networks

```bash
sudo airodump-ng [your-monitor-interface]
```

Scan All Frequencies (2.4GHz + 5GHz)

```bash
sudo airodump-ng --band abg [your-monitor-interface]
```

Focused Target Scanning

```bash
sudo airodump-ng -c [channel] --bssid [target-mac] \
-w capture-file [your-monitor-interface]
```

Advanced Reconnaissance

Show Acknowledgment Frames

```bash
sudo airodump-ng --showack [your-monitor-interface]
```

Monitor Probe Requests

```bash
sudo airodump-ng -M [your-monitor-interface]
```

Understanding Airodump Output

- **BSSID**: MAC address of access point
- **PWR**: Signal strength (lower = stronger)
- **ENC**: Encryption type (WPA2/WEP/OPN)
- **ESSID**: Network name
- **CH**: Channel number
- **#Data**: Packet count

Common Troubleshooting

Monitor Mode Won't Enable

```bash
sudo airmon-ng check kill
sudo airmon-ng start wlx18d6c71070ff
```

Check Adapter Support

```bash
iw list | grep -A 10 "Supported interface modes"
```

Adapter Not Recognized

```bash
lsusb
dmesg | tail -20
```

Professional Methodology

1. **Passive scanning first** - Never announce presence
2. **Document everything** - Keep detailed notes
3. **Map the landscape** - Understand all networks before targeting
4. **Identify weak points** - Look for outdated encryption
5. **Plan approach** - Use recon data for next phases

Key Security Indicators

- **OPN**: No encryption (open network)
- **WEP**: Broken encryption (easily cracked)
- **WPA**: Outdated, has vulnerabilities
- **WPA2**: Current standard (dictionary attack vulnerable)
- **WPA3**: Modern standard (strongest available)