**🛰️ Kismet Challenge Lab – Wireless Hacking 101**

**🧠 What is Kismet?**

Kismet is a **wireless network detector**, sniffer, and intrusion detection tool.

* It captures **Wi-Fi traffic** passively (without connecting)
* It can detect **hidden networks**
* Great for **reconnaissance** in wireless hacking

📌 Kismet works with most Wi-Fi cards in **monitor mode** on **Linux systems**.

**🛠️ Why Learn Kismet?**

| **Reason** | **Why it Matters** |
| --- | --- |
| 🎯 Wireless Recon | See all networks and devices nearby (even hidden ones) |
| 🕵️ Passive Monitoring | Capture traffic without sending packets (stealth mode) |
| 🛡️ WIDS Function | Detect rogue access points, spoofing, and attacks |
| 📊 Data for Mapping | Useful for creating a Wi-Fi heatmap or coverage report |

**🔧 Basic Setup**

1. **Install Kismet** (on Kali Linux or Ubuntu):
2. sudo apt update
3. sudo apt install kismet
4. **Enable Monitor Mode on Wi-Fi**:
5. sudo ifconfig wlan0 down
6. sudo iwconfig wlan0 mode monitor
7. sudo ifconfig wlan0 up
8. **Run Kismet**:
9. sudo kismet

Open in browser: http://localhost:2501

**👨‍🔬 Kismet Challenge Task Ideas**

| **Task** | **What You Learn** |
| --- | --- |
| 📡 Scan Your Area | List all Wi-Fi networks (SSID, signal, encryption, channel) |
| 🔒 Find Hidden SSIDs | Detect networks even if SSID is not broadcast |
| 📱 Track Devices | See MAC addresses of phones, laptops connected to Wi-Fi |
| 🧠 Analyze Traffic | Observe beacon frames, probe requests (device fingerprints) |
| 🔐 Check Encryption | See which networks use WPA2, WEP, or are Open |

**📁 What to Report in Your Lab Notes**

* Total number of networks discovered
* Encryption methods used (WEP, WPA, WPA2, open)
* Any hidden SSIDs detected
* MAC addresses of devices
* Channels most used (for detecting channel hopping or jamming attacks)

**⚠️ Legal Warning**

✅ Only run Kismet on **your own network** or in a **legal lab environment**.  
Unauthorized sniffing of other people's Wi-Fi is **illegal** in most countries.