Bluetooth Hacking Cheat Sheet (Beginner → Advanced)

1. Basic Bluetooth Commands

Command	Description
hciconfig	Check Bluetooth interfaces
hcitool scan	Scan for discoverable Bluetooth devices
hcitool dev	List local Bluetooth devices
bluetoothctl	Bluetooth control tool

2. Useful Tools

Tool	Use Case
bluez	Official Linux Bluetooth stack
bluetoothctl	Managing Bluetooth devices
bluelog	Bluetooth device logger
spooftooph	Bluetooth spoofing tool
obexftp	File transfer over OBEX FTP

3. Common Attacks

Attack	Description
Bluesnarfing	Unauthorized access to files via OBEX
Bluejacking	Sending unsolicited messages
Bluebugging	Gain full control over device
DoS Attacks	Flood Bluetooth service to crash device

4. Pentesting Workflow

Step	Description
Discovery	Find nearby devices (hcitool, bluelog)
Fingerprinting	Get details: MAC, vendor, services
Exploitation	Use tools for attacks (spooftooph, bluesnarfer)
Post-Exploitation	Access data, escalate control

5. Tips & Notes

- Range of normal adapters is limited (~10m).
- For advanced sniffing, Ubertooth One or dedicated adapters are required.
- Use a high-gain antenna for better performance.
- Always test in controlled/legal environments.