

# Bluetooth Spoofing

Bluetooth devices are all around us. Some of them are vulnerable to open write instructions. In this pdf, you can learn, how we can see classic and BLE (Bluetooth low energy) devices and their services without even pairing.

Commands=====

hciconfig

hciconfig

hci0 up

hcidtool scan

hcidtool info (mac address of the target device)

l2ping (mac address of the target device)

sudo apt install golang git build-essential libpcap-dev libusb-1.0-0-dev libnetfilter-queue-dev

git clone <https://github.com/bettercap/bettercap>

cd bettercap

make build

make install

git clone <https://github.com/bettercap/caplets.git>

cd caplets

make install bettercap

help

help ble.recon

ble.recon on

ble.show

ble.enum (mac address of the target device)