How to Bluetooth Discovery using Kali Linux tools

Goal: Discover bluetooth devices using Kali Linux
Demonstration: Demonstrate different ways to gather bluetooth information using different bluetooth discovery tools available on Kali Linux.

Part 1 - Research

First, I researched what tools are available to perform recon on devices using bluetooth.

Through research, I discovered Kali Linux comes with tools for bluetooth discovery.

I watched multiple videos on how to use the following tools through the terminal on Kali:
hciconfig, hcitool, sdptool, l2ping, bluetooth and btscanner

I researched using manpages and other resources on how to use the tools properly today.

While I was trying to use the tools on the schools cyberlab kali, I noticed bluetooth scanners were not working. I needed to buy a bluetooth scanner dongle, and I also downloaded Kali linux onto oracle box vm.

I was having issues using the dongle with oracle box vm, so I installed free version of vmware, and installed Kali Linux on there. After installation and plugging in the dongle, the vm was able to connect to my USB and use the bluetooth scanner on there.

While using the tools, some of the tools were not functioning properly. I researched online for any troubleshooting, and found out there was some configuration I needed to adjust in order for some of the tools.

Part 2: Installation configuration

I learned that I had to use a separate bt scanner dongle in order to use the bluetooth tools on a vmware. I also installed vmware (Free version) and installed a vm of Kali Linux.

I configured the vm to accept the USB device and enable bluetooth.

I had to install and make sure bluetooth tools were up to date on Kali VM. The bluetooth device manager and applications were not working properly.

Used the following commands to install:

sudo apt install bluetooth bluez bluez-tools rfkill
sudo apt update

sudo apt upgrade

Then ran the following commands:
sudo rfkill list
sudo rfkill unblock bluetooth
I also to enable the bluetooth service. On boot, bluetooth is set to disabled and not running.

sudo systemctl enable bluetooth.service --now
sudo systemctl start bluetooth.service
sudo systemctl restart bluetooth.service

Bluetooth was working properly on my VM after that

The following tools were not functioning correctly:
sdptool

Researched that there was compatibility issues with that tool. I had to do the following to adjust the configuration:

sudo nano /etc/systemd/system/dbus-org.bluez.service

On the line that contains:

ExecStart=/usr/lib/bluetooth/bluetoothd
I added --compat to the end of it.

Ran:
sudo systemctl daemon-reload
sudo systemctl restart bluetooth

/var/run/sdp exists now

changed permissions on it

sudo chmod 777 /var/run/sdp

finally make sdptool work.

***Will have to rerun this configuration again if *bluez* is updated.

Part 3 - Testing the Tools

I turned on my wireless speaker to be the device that would be discovered.

Ran *hciconfig* to display if my bluetooth scanner was running.

hci1 was my bluetooth scanner.

Ran hcitool scan (scans classic bluetooth) and hcitool lescan (le = low energy, scans BLE devices)

Ran bluetoothctl
scan on

Ran sdptool browse [speaker mac address] to browse available services on the device specified. (SDP = service discover protocol)

Ran l2ping [speaker mac address] to verify if host is up

Ran btscanner to open the interface of btscanner.
Ran i for inquiry scan.
Appears to only scan for classic bluetooth.

Step 4:: Project preparation:

I decided to use my speaker as the target to use for sdptool and l2ping.
I will provide a screen shot of btscanner results as it will scan my iphone, and reveals its bluetooth address. I will blue out the results but show what happens after inquiry will run.

Ran the procedure multiple times as well as before class to ensure it runs smoothly as well as troubleshoot any issues.

Slide deck will include the following:

- the project topic, why I chose it, end goal
- research into the tools used
- devices I had to use
- screen shots of tools being used
- configuration installation
- demonstration of how to use the tools