



BLUETOOTH DISCOVERY USING KALI LINUX



By: Howard Luis

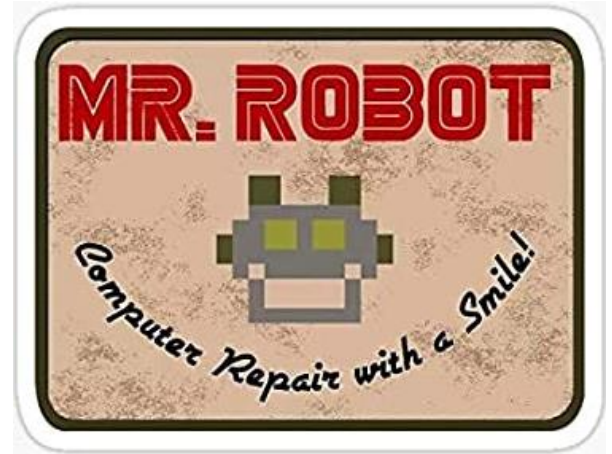
What is Bluetooth?

- Bluetooth is a short-range wireless networking protocol



Why Bluetooth discovery?

- I was inspired by an episode of “Mr. Robot”
- Bluetooth is everywhere!
- During the pentesting segment, we did not go over any bluetooth pen testing



Installing and Configuring Bluetooth Tools

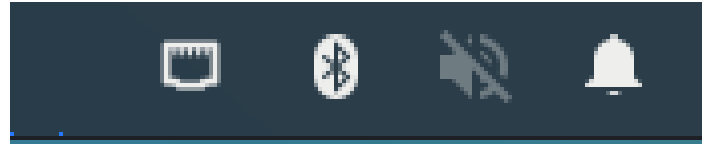
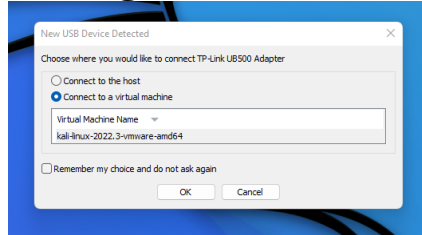
- Bluetooth comes in installed with Kali, but I read several posts that it wasn't working properly.
 - Had to install, update, upgrade the OS.

```
(kali㉿kali)-[~]  
$ sudo apt install bluetooth bluez bluez-tools rfkill  
  
(kali㉿kali)-[~]  
$ sudo apt update  
  
(kali㉿kali)-[~]  
$ sudo apt upgrade
```

```
(kali㉿kali)-[~]  
$ sudo rfkill list  
[sudo] password for kali:  
0: hci0: Bluetooth  
    Soft blocked: yes  
    Hard blocked: no  
2: hci1: Bluetooth  
    Soft blocked: yes  
    Hard blocked: no  
  
(kali㉿kali)-[~]  
$ sudo rfkill unblock bluetooth
```

Installing and Configuring Bluetooth Tools Cont...

- Since I was using a VM, I had to use a bluetooth scanner dongle I bought.



- Bluetooth service is disabled and inactive on boot.

```
(kali@kali)-[~]
└─$ sudo systemctl enable bluetooth.service --now
Synchronizing state of bluetooth.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable bluetooth

(kali@kali)-[~]
└─$ sudo systemctl restart bluetooth.service

(kali@kali)-[~]
└─$ sudo systemctl status bluetooth.service
● bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled; preset: disabled)
   Active: active (running) since Thu 2022-08-25 22:29:48 EDT; 10s ago
```

Installing and Configuring Bluetooth tools cont..

- After further research, one of the tools, sdptool (service discover protocol) was not working properly due to compatibility issues:

```
(kali㉿kali)-[~]  
$ sudo nano /etc/systemd/system/dbus-org.bluez.service
```

```
[Service]  
Type=dbus  
BusName=org.bluez  
ExecStart=/usr/libexec/bluetooth/bluetoothd --compat
```

```
(kali㉿kali)-[~]  
$ sudo systemctl daemon-reload
```

```
(kali㉿kali)-[~]  
$ sudo systemctl restart bluetooth
```

```
(kali㉿kali)-[~]  
$ sudo chmod 777 /var/run/sdp
```

Tools used for bluetooth discovery

```
(kali㉿kali)-[~]  
$ hciconfig
```


```
(kali㉿kali)-[~]  
$ bluetoothctl
```

```
(kali㉿kali)-[~]  
$ hcitool
```

```
(kali㉿kali)-[~]  
$ l2ping
```

```
(kali㉿kali)-[~]  
$ sdptool
```

```
(kali㉿kali)-[~]  
$ btscanner
```

Time	Address	Clk off	Class	Name
				
btscanner 2.0 keys: h=help, i=inquiry scan, b=brute force scan, a=abort scan, s=save summary, o=select sort, enter =select, Q=quit				

Bluetooth Discovery Demo

screenshots of results

```
(root@kali)-[/home/kali]
# sudo hcitool scan
Scanning ...
D4:17: [REDACTED]
```

```
(root@kali)-[/home/kali]
# hcitool lescan
LE Scan ...
[REDACTED]
C4:30:18:CD:BF:18 LG RN5(18)
[REDACTED]
```

```
(root@kali)-[/home/kali]
# l2ping C4:30:18:CD:BF:18
Ping: C4:30:18:CD:BF:18 from E8:48:B8:C8:20:00 (data size 44) ...
16 bytes from C4:30:18:CD:BF:18 id 0 time 19.82ms
16 bytes from C4:30:18:CD:BF:18 id 1 time 51.00ms
16 bytes from C4:30:18:CD:BF:18 id 2 time 48.33ms
```

```
(root@kali)-[/home/kali]
# sdptool browse C4:30:18:CD:BF:18
Browsing C4:30:18:CD:BF:18 ...
Service Name: Audio/Video Service
Service Provider: MCSLOGIC
Service RecHandle: 0x10000
Service Class ID List:
"Audio Sink" (0x110b)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 25
"AVDTP" (0x0019)
uint16: 0x0102
Profile Descriptor List:
"Advanced Audio" (0x110d)
Version: 0x0102
```

root@kali: /home/kali

File Actions Edit View Help

Time	Address	Clk off	Class	Device
2022/08/27 13:03:18 68:7f	[REDACTED]	0x43b8	0x0c043c	[REDACTED]

keys: h=help, i=inquiry scan, b=brute force scan, a=abort scan, s=save summary, o=select sort
, enter=select, Q=quit
starting inquiry scan
Found device 68:7f [REDACTED]

Impact of bluetooth discovery

- Finds target hosts
- This step leads to vulnerability assessment then to the known bluetooth exploitations
- Leads to attacks such as:
 - Bluesnarfing
 - Bluejacking
 - Bluetooth Impersonation Attacks (BIAS)
 - Bluebugging
 - **Blueborne attack**

Mitigation

- Turn off bluetooth function when it is not needed
 - Turn off discovery mode on bluetooth
- Don't accept any file request transfers from unknown sources
- When there are unknown pair requests, do not accept them

Research

- null-byte.wonderhowto.com
- unix.stackexchange.com
- <https://bbs.carchlinux.org>