HACKING BLUETOOTH DEVICES

OBJECTIVE

The objective of this report is to showcase the method of hacking of Bluetooth devices using command-line tool in kali Linux operating system.

Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances and building personal area networks.

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.

TOOLS

The tools used are:

- **hciconfig**
- **Bettercap**

hciconfig is used to configure Bluetooth devices. hciX is the name of a Bluetooth device installed in the system.

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.

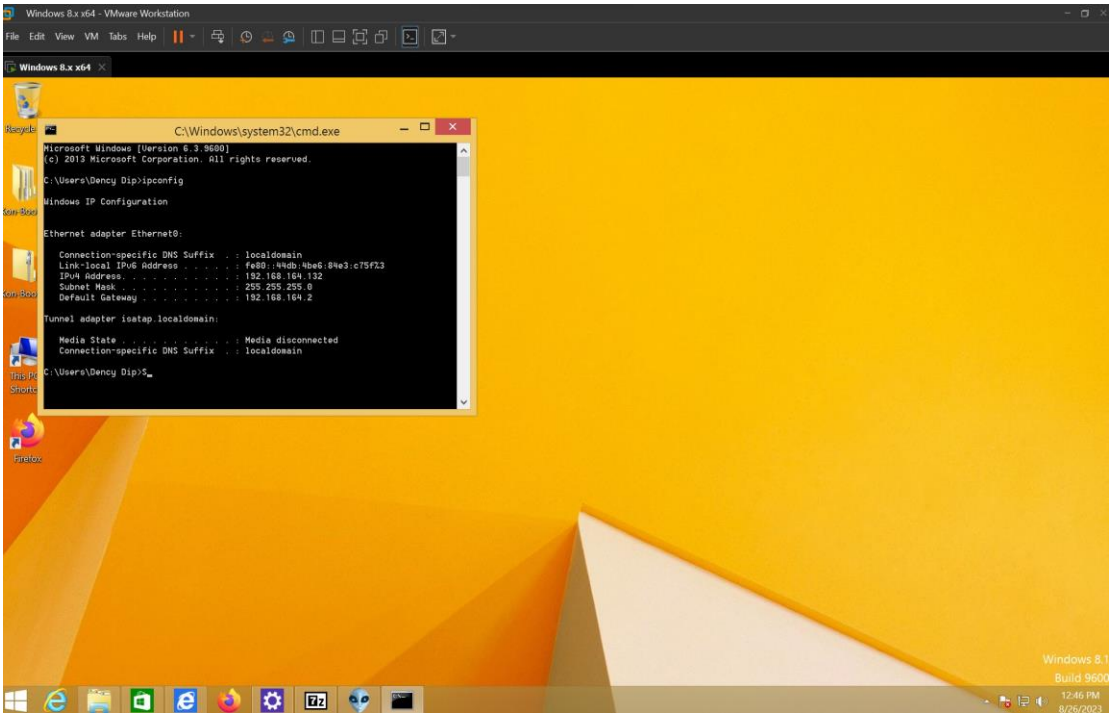
METHODOLOGY

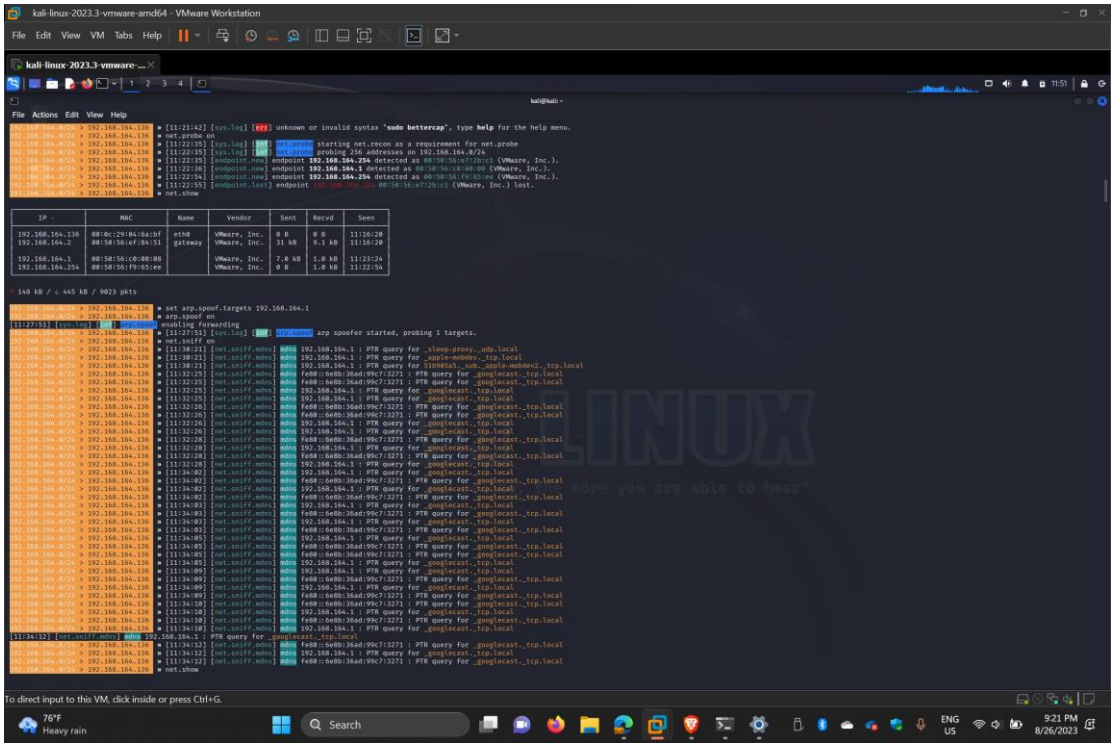
The steps involved are:

1. Configure bluetooth using **hciconfig**
2. Run the **bettercap** command
3. Then type the following command **ble.recon on**
4. Then type **net.probe on**
5. Then run **net.show** for showing the devices details
6. Run the following command **set arp.spoof.targets** followed by the target's bluetooth device IP address
7. Finally, run the command **net.sniff on** to monitor the target's activity using the bluetooth device.

8. After all the processes are over and we are done with monitoring target's activities, we need to type in the following commands one by one.
9. **net.sniff off**, **net.probe off**, **ble.recon off** and now we can exit the **bettercap**.

PROOF OF CONCEPT





CONCLUSION

In conclusion, we can say that we can hack Bluetooth devices using simple tools in the Linux operating system. So, it is required that we do not connect our Bluetooth device to any unknow system and be protected of any attacks.