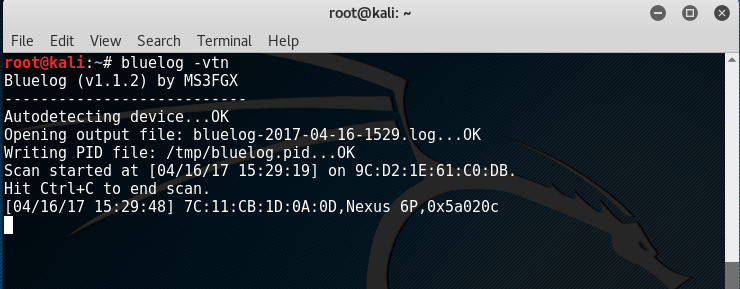
Wireless Attacks: Bluetooth Tools

Bhavneet Soni

**Wireless Attacks: Bluetooth Tools**

1. Bluelog

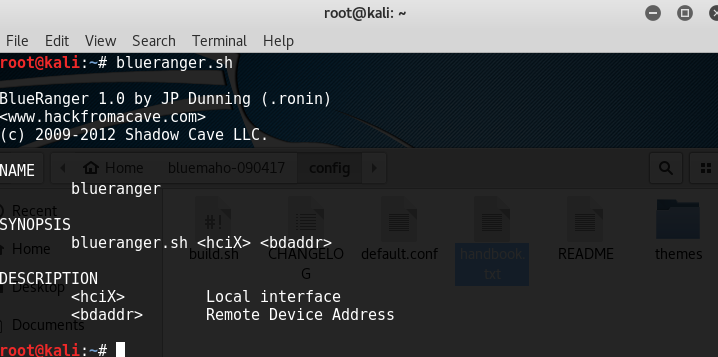
Bluelog is a Bluetooth scanner designed to tell you how many discoverable devices there are in an area as quickly as possible. It is intended to be used as a site survey tool, identifying the number of possible Bluetooth targets there are in the surrounding environment.



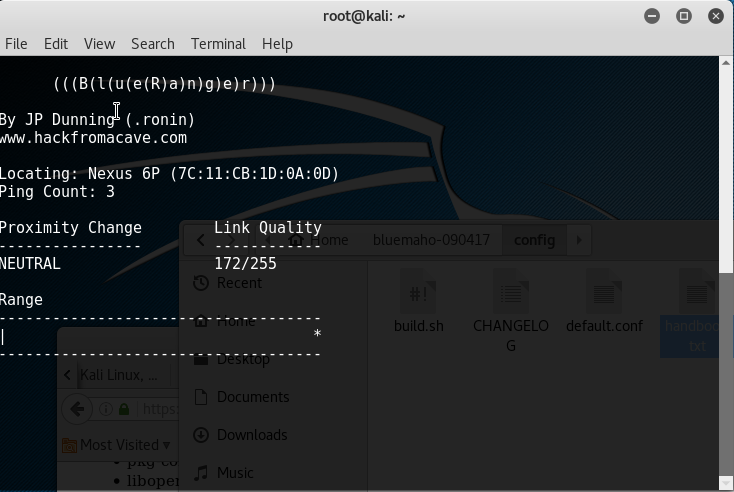
this tool finds out all the open Bluetooth items in the vicinity, we run using bluelog, -vtn option gives a verbose response showing time stamp, device name etc.

1. blueranger

BlueRanger is a simple Bash script which uses Link Quality to locate Bluetooth device radios. It sends l2cap (Bluetooth) pings to create a connection between Bluetooth interfaces, since most devices allow pings without any authentication or authorization. The higher the link quality, the closer the device (in theory).



It take two arguments, interface and device address



1. btscanner

btscanner is a tool designed specifically to extract as much information as possible from a Bluetooth device without the requirement to pair. A detailed information screen extracts HCI and SDP information, and maintains an open connection to monitor the RSSI and link quality. btscanner is based on the BlueZ Bluetooth stack, which is included with recent Linux kernels, and the BlueZ toolset. btscanner also contains a complete listing of the IEEE OUI numbers and class lookup tables. Using the information gathered from these sources it is possible to make educated guesses as to the host device type.

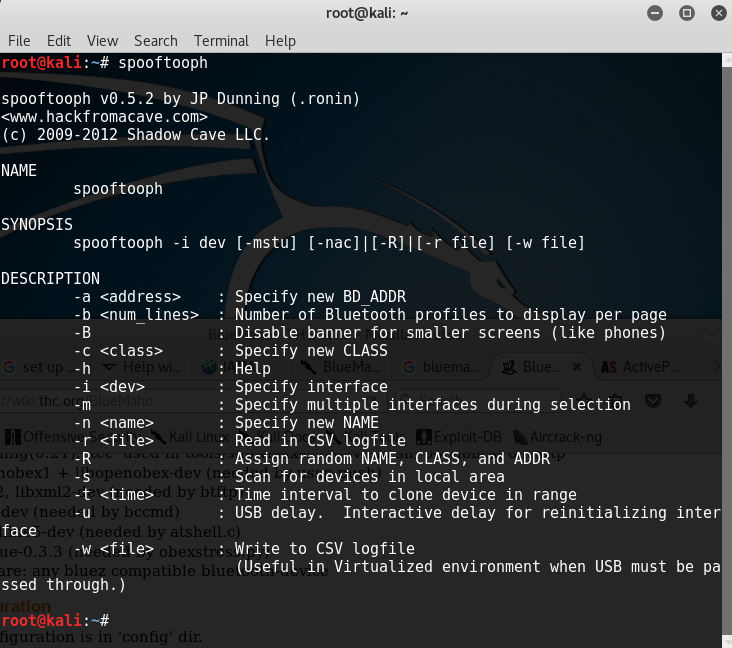
running the tool by typing the following

btscanner <device address>

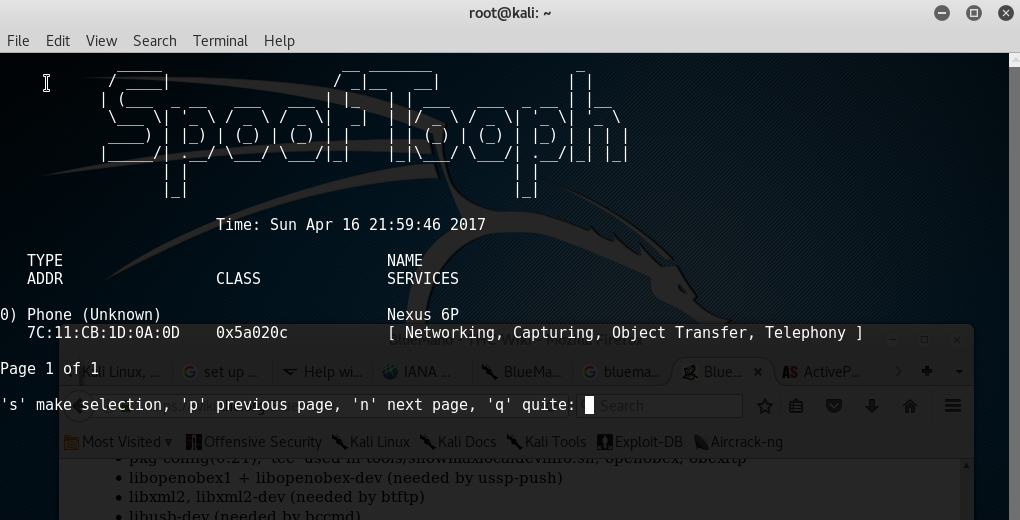


1. spooftooph

Spooftooph is designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain site. Bluetooth scanning software will only list one of the devices if more than one device in range shares the same device information when the devices are in Discoverable Mode (specifically the same Address).



we typed the command – spooftooph –i -hci0 -s -w test.csv (that save the finding sin the test csv.)



Unfortunately, the manufacturer of my phone was not supported o could not clone the information.