Titel

|  |  |  |
| --- | --- | --- |
| Version / Datum | Änderungen | Bearbeiter |
| 0.1 – 25.04.18 | Erste Version | ES |

1. Übersicht

TBD

* 1. General requirements

In this section we will describe the potential tools for the penetration testing of the bluetooth devices.

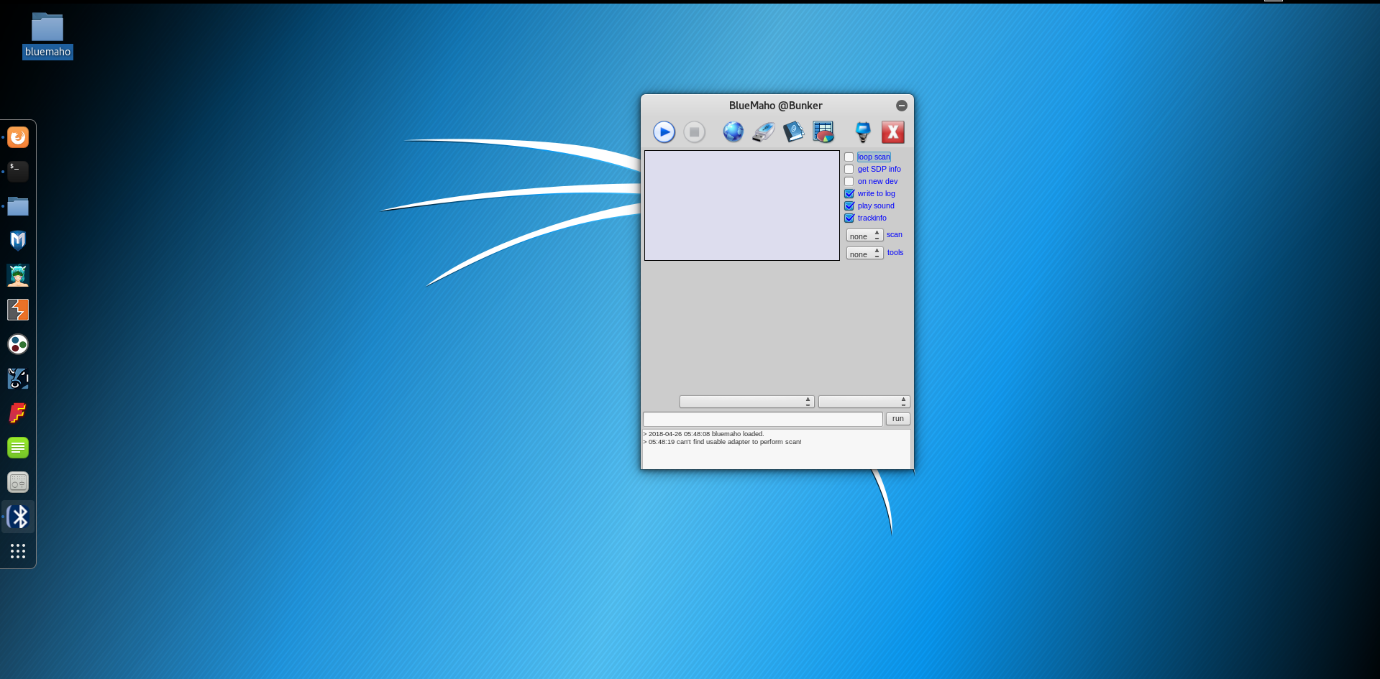
* + 1. Blue Maho Package

Blue Maho is a GUI shell interface for testing security of the bluetooth devices and it is a part of the Linux KALI. It is an open source, written in Python and it uses wxPython. It can be used to test the device for the known vulnerabilities or to find unknow vulnerabilities (it is customizable).

Main features of the Blue Maho are:

* **scan for devices**
* **fingerprint** – show advanced info, SDP records, vendor, etc.
* **track devices** – show where and how much times device was seen
* **on\_new\_device** – specifying which command should run when new device is found
* **using multiple dongles** – one for scaning (loop scan) and one for running tools or **exploits**
* **send files**
* **save results in database**
* **test remote device for known vulnerabilities**
* **test remote device for unknown vulnerabilities**

Blue Maho can be started with Linux KALI with typing „bluemaho.py“ in the Terminal. After that GUI interface will open and you can start using it.



* + 1. Bluediving

Bluediving is a Bluetooth penetration testing suite. It has been implemented in C and Perl programming language. It implements different attacks like:

* Bluebug,
* BlueSnarf,
* BlueSnarf++,
* BlueSmack

This tool has some features such as:

* RFCOMM scanner,
* L2CAP packetgenerator

There are also some tools which are implemented by the Bluediving tool:

* carwhisperer,
* redfang,
* bss

**Instalation**

* Open Terminal
* Run cpan install XML::Simple
* TBD

1. References

[1] <http://bluetooth-pentest.narod.ru/>

[2] <https://blackarch.org/bluetooth.html>

[3] <https://github.com/balle/bluediving>

[4] <https://tools.kali.org/wireless-attacks/bluemaho>