12.11.2023

Курс:

Практическая работа к уроку № Lesson_7

--
Безопасность Bluetooth

Задание_1:

Изучить утилиты для работы с bluetooth. Отчет — скриншоты с результатами исследований.

Атаки на Bluetooth и защита от них:

- BlueSnarf
  Защититься можно, установив авторизацию для OPP и не принимая неизвестных подключений.
- BlueBug
  Чтобы защититься, надо установить свежую прошивку модуля Bluetooth на телефоне и отклонять неизвестные подключения.
- BlueDump
  На данный момент защиты не существует. Но не зная адрес доверенного устройства, злоумышленник не сможет атаковать: перебрать все возможные адреса за короткое время невозможно.

Утилиты для работы с Bluetooth:

- Hcitool
- Bluelog
- Blueranger
- Bluesnaffer
- Btscanner
- Redfang
- Spooftooph

1. hcitool

```
systemctl enable bluetooth.service
systemctl start bluetooth.service
hciconfig hci0 start

hcitool dev
hcitool scan
hcitool inq
hcitool name 00.xx.xx.xx
```

Задание_2:

Отключить режим обнаружения на смартфоне, попытаться найти его с помощью Redfang. Отчет — скриншоты с результатами исследований.

Redfang позволяет найти скрытое Bluetooth-устройство.

```
fang -h
fang -r 00803789EE76-00803789EEff -s
```

Задание_3:

(*) Разобрать дамп hci-соединения. Указать, к какому устройству осуществлялся доступ, увенчался ли он успехом, назвать имя устройства, класс и смещение времени. Отчет должен содержать информацию об адресе, имени, смещении во времени и наличии доступа за время дампа.
https://drive.google.com/open?id=1_XjbChRUdY06R6ZNXmNUpvJmi9UGUa5q — ссылка на файл дампа.

Выводы:

Ссылки / дополнительные материалы

1. 1. Стандарт Bluetooth.
2. Стандарт протокола LMP.
3. Описание уязвимостей.
4. Построение связей в MPLS — для продвинутых.

Используемая литература
Для подготовки данного методического пособия были использованы следующие ресурсы:

1. Man-page Bluelog.
2. Man-page Spooftooph.
3. Стандарт протокола LMP.
4. Стандарт Bluetooth

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.
> - https://gb.ru

Выполнил: AndreiM