РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ БЕСПРОВОДНЫХ ПРОКСИ-СТАНЦИЙ В КОРПОРАТИВНОЙ WLAN-СЕТИ

И.Н. Бабков, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, ib9809@mail.ru;*
Э.А. Бударин, *к.т.н., доцент, Военная академия связи им. Маршала Советского Союза С.М. Буденного, budarin_ilya@mail.ru;*
А.Ю. Кистуга, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, anton.kistruga@gmail.com;*
М.Э. Бударин, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, budarin.makar@gmail.com.*

УДК 654

Аннотация. Исследованы признаки несанкционированного доступа нелегитимного устройства к *WLAN*-сети посредством подключения к легитимному устройству, работающему в режиме точки доступа *Wi-Fi*. Предложена методика обнаружения нелегитимного устройства по данным признакам.

Ключевые слова: информационная безопасность; безопасность беспроводных сетей; признаки; методика; точки доступа; прокси-станции; беспроводные сети.

DEVELOPMENT OF WIRELESS PROXY STATION DETECTION METHODOLOGY IN THE CORPORATE WLAN NETWORK

Ivan Babkov, *Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Eduard Budarin, *Ph.D., Associate Professor, in Military Sciences, Department of Security of Special Purpose Infocommunication Systems, The S.M. Budyonny Military Academy of the Signal Corps;*
Anton Kistruga*, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Makar Budarin, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. Signs of unauthorized access of a rogue device to the *WLAN* network by connecting to a legitimate device operating as a *Wi-Fi* access point were investigated. A methodology for detecting a rogue device based on these signs has been developed.

Keywords: information security; wireless network security; signs; methodology; access points; proxy stations; wireless networks.

Введение

В современных условиях развития технологий все чаще применяются беспроводные локальные сети. С их помощью можно объединить большое количество устройств, наладить их совместную работу и быструю коммуникацию. В настоящее время практически в любой сфере деятельности встречается использование беспроводных локальных сетей, в частности, в крупных компаниях, которым необходимо организовать работу сотрудников в офисе [1]. Корпоративная *WLAN* (*Wireless Local Area Network*) может быть как замкнута на территории соответствующего помещения, так и иметь доступ к сети интернет. Основным достоинством такой беспроводной сети является мобильность всех сотрудников, так как доступ к информации у них будет из любой точки помещения, где имеется

сигнал, мощности которого достаточно для подключения к сети. Но у беспроводной сети есть существенный недостаток – слабая защищенность при недостаточной работе над администрированием. Тем не менее, все большее количество компаний внедряют в своих офисах подобный способ организации сети.

Уязвимость корпоративной *WLAN*

Беспроводные сети постоянно совершенствуются, каждый год идет работа над их улучшением, повышается функциональность и внедряются новые технологии защиты информации. Однако, даже со всеми современными методами защиты нельзя с полной уверенностью утверждать, что беспроводные локальные сети являются полностью безопасными [2]. С использованием *WLAN* в офисе организации появляется серьезная уязвимость для несанкционированного доступа в закрытую сеть, заключающаяся в подключении к легитимному устройству сотрудника, работающего в режиме точки доступа *Wi-Fi*. Для дальнейшего исследования введем термин «беспроводная прокси-станция» для подобных устройств. В статье была смоделирована и исследована данная уязвимость, проведена симуляция вышеописанной ситуации, приведены меры профилактики, а также предложен способ обнаружения присутствия в корпоративной сети нелегитимного устройства, использующего данную уязвимость [12].

Описание проблемы

Чаще всего в корпоративных беспроводных сетях используют всевозможные современные методы защиты. Однако, злоумышленники могут находить обходные пути для получения доступа [3]. Один из них заключается в особенностях работы устройств в режиме точки доступа *Wi-Fi* (*WLAN*-*WLAN* тетеринг беспроводной прокси-станции). Предположим, сотруднику компании, будучи подключенным к корпоративной *WLAN*, понадобилось параллельно включить на своем устройстве подобный режим точки доступа. Тогда стороннее устройство, которое подключается к данной *Wi-Fi* сети, получает доступ к корпоративной *WLAN*. Более того, трафик стороннего устройства будет присутствовать в сети организации с *MAC*-адресом и *IP*-адресом легитимного устройства, работающего в режиме прокси-станции, что сильно усложняет выявление подобных инцидентов [4]. Эта проблема может привести к серьезным последствиям для компании, включая утечку конфиденциальных данных и вредоносных атак на сеть. Кроме того, подключение нелегитимного устройства может снизить производительность сети и повлиять на качество работы, что в свою очередь повлечет за собой финансовые и репутационные потери, так как вызовет снижение доверия клиентов к организации.

Меры профилактики

Стоит отметить, что в первую очередь в подобных ситуациях виноват будет сотрудник, развернувший на своем устройстве ненадежную точку доступа *Wi-Fi*, тем самым сделав корпоративную сеть незащищенной [5]. В таком случае, первоначальной целью злоумышленника станет подключение к этой точке доступа.

Во избежание таких ситуаций изначально следует провести инструктаж по сетевой безопасности для всех сотрудников, имеющих доступ к сети. В инструктаж необходимо включить блоки, разъясняющие опасность создания точек доступа, памятки по созданию надежного пароля, а также советы по целесообразному использованию корпоративной сети. Большинство инцидентов, связанных с проникновением в сеть через точку доступа *Wi-Fi*, происходят по причине очень

простого, либо вовсе отсутствующего пароля на развернутой сотрудником точке доступа [9], в то время как сам сотрудник может даже не подозревать, что таким образом он подвергает опасности всю корпоративную сеть. Даже, если пароль назначен, злоумышленник может применить метод подбора пароля «грубой силой» (*Brute force*) [18].

Следующим шагом необходимо ввести новые правила пользования корпоративной сетью. Существует несколько вариантов вводимых изменений. Наиболее надежным и радикальным методом является запрет на подключение к сети с личных устройств, а на корпоративной технике – отключение функции точки доступа на программном уровне. Менее радикальный метод – разрешить подключение к сети с личных устройств, но запретить создание точек доступа внутри этой сети. Такой вариант будет менее надежным, так как у сотрудников останется возможность создавать точки доступа, а контроль выполнения правил потребует дополнительных технических решений.

Все введенные правила необходимо зафиксировать во внутренних документах компании, ввести санкции за их нарушение и потребовать сотрудников ознакомиться, а также дать соглашение и расписаться.

Выявление беспроводных прокси-станций

Несмотря на все меры профилактики инцидентов, могут происходить случаи нарушения предписаний: сотрудник создает слабозащищенную точку доступа *Wi-Fi* внутри корпоративной сети, а злоумышленник, с легкостью подобрав к ней пароль, подключается и получает доступ к сети [6].

Для таких случаев требуется разработать методику обнаружения устройств внутри сети, работающих в режиме точки доступа *Wi-Fi* и подключенных к ним нелегитимных устройств для дальнейшего предотвращения несанкционированного доступа к целевой *WLAN*. Необходимо определить признак создания мобильной точки доступа, либо подключения третьего устройства к ней, а также выявить создавшего точку доступа сотрудника. Для выполнения вышеперечисленных задач, в первую очередь, используется специализированное программное обеспечение для мониторинга сетевого трафика – *Wiresharк*. Проводится анализ сетевого трафика на предмет нестандартных запросов и ответов, анализ *IP* и *MAC* адресов, обнаружение нескольких подключений с одних и тех же адресов, сопоставление адресов с запросами [7].

Методика исследования

За основу исследования взята легенда: в офисе компании налажена *WLAN*-сеть для внутренней работы сотрудников и взаимосвязи отделов. Некоторый сотрудник, будучи подключенным к данной сети со своего устройства, параллельно включает режим точки доступа *Wi-Fi.* Третье лицо, являющееся злоумышленником, цель которого – получение доступа к закрытой корпоративной сети, подключается к точке доступа *Wi-Fi* сотрудника компании. Данная схема изображена на рис. 1.

Рисунок 1

Для симуляции атаки было использовано следующее оборудование:

- Виртуальная машина в целевой сети с установленным *Kali Linux*, используемая для перехвата и анализа трафика.
- Беспроводная сетевая карта – *Mercusys MW*300*UH*.
- *Wi-Fi* роутер – *Eltex NTU-RG*-1402*G-W* (в качестве точки доступа к корпоративной *WLAN*).
- Смартфон под управлением ОС *Android* (в качестве легитимного устройства сотрудника с развернутой точкой доступа).
- Ноутбук под управлением ОС *Windows* (в качестве нелегитимного устройства злоумышленника).

В последующих пунктах описана работа на виртуальной машине с *Kali Linux* [16]. Алгоритм анализа трафика для выявления присутствия нелегитимного устройства в сети [17]:

1. Для анализа сетей и перехвата трафика необходимо переключить беспроводную сетевую карту в режим монитора. Это делается командой «*airmon-ng start wlan*0», где *wlan*0 – имя сетевой карты (рис. 2).

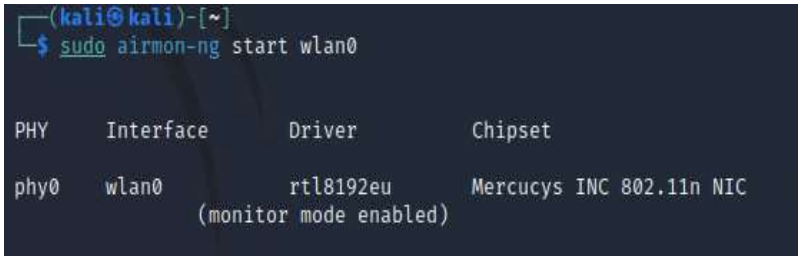

Рисунок 2

2. Для захвата пакетов беспроводных сетей в радиусе действия необходимо ввести команду «*airodump-ng wlan*0». Имя целевой сети, работающей в качестве корпоративной – «*BudWiFi*» (рис. 3).

Рисунок 3

3. Для запуска захвата трафика *Wi-Fi* сети «*BudWiFi*» необходимо ввести команду «*airodump-ng --bssid 'A*8:*F*9:4*B*:*CE*:91:19' *--essid 'BudWiFi' -c* 1 *-w /usr/BudWiFicaptures wlan*0», где:

- *A8:F9:4B:CE:91:19 – BSSID* нашей сети из таблицы выше;
- *BudWiFi – ESSID* нашей сети из таблицы выше;
- *1* – значение *CH* из таблицы выше;

- */usr/BudWiFicaptures* – каталог для сохранения (рис. 4).

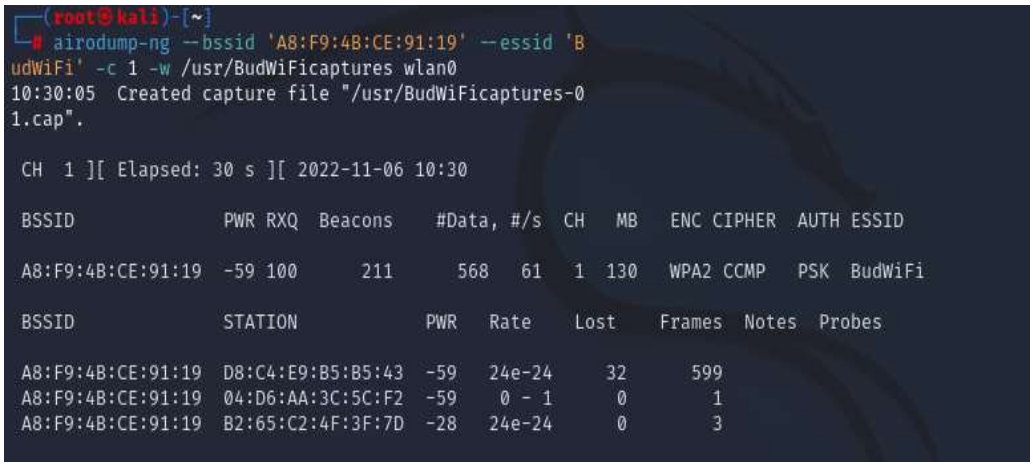

Рисунок 4

4. Необходимо ожидать некоторое время процесса захвата, в течение которого симулировать работу с устройств сотрудника и злоумышленника – обращаться к различным сетевым сервисам, открывать веб-страницы и т.п. Для того, чтобы полученный трафик было возможно расшифровать, должно произойти «рукопожатие» (*Handshake*) – подключение любого устройства к целевой *Wi-Fi* сети во время перехвата. Таким образом происходит общение клиента и роутера во время подключения, т.е., передача зашифрованного пароля во время аутентификации. В данном случае было произведено самостоятельное подключение к сети третьего устройства (рис. 5).

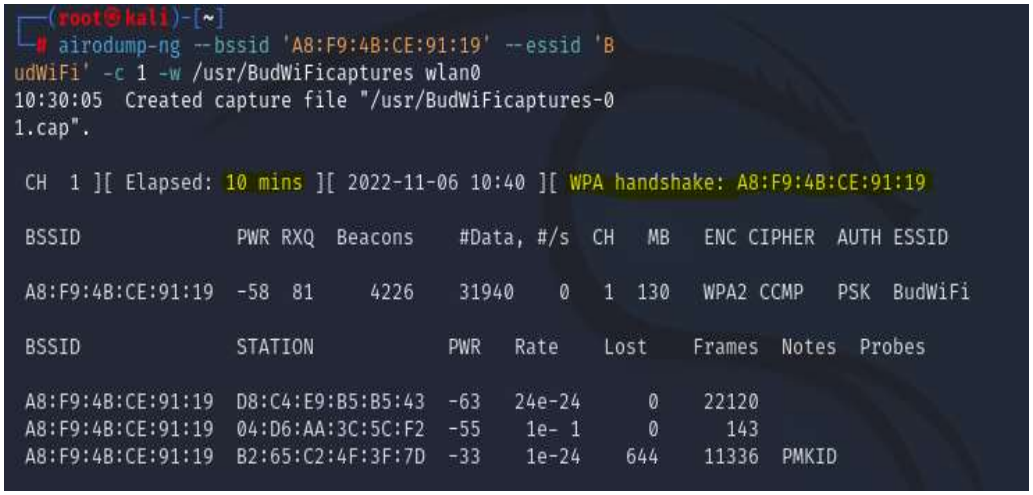

Рисунок 5

5. Для анализа полученного трафика необходимо открыть *Wireshark* и провести настройку для дешифрования: *Edit – Preferences – Protocols – IEEE* 802.11 *– Enable decryption – Edit...* (рис. 6).

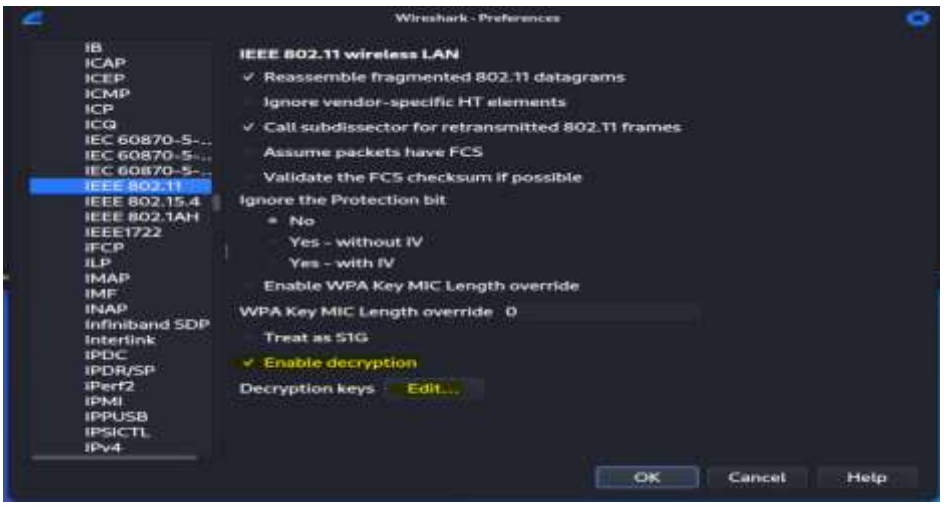

Рисунок 6

6. На данном этапе необходимо ввести пароль целевой *Wi-Fi* сети. В *Key type* нужно выбрать *wpa-pwd* для ввода пароля и имени сети в простом буквенном виде, после ввести данные в поле *Key* (рис. 7).

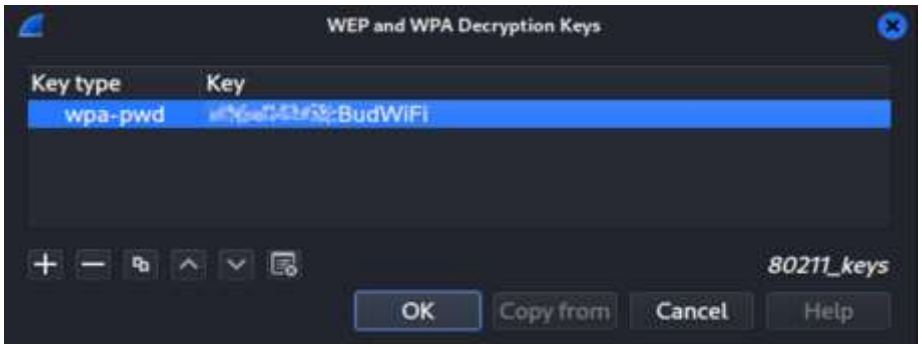

Рисунок 7

7. Далее необходимо открыть *.cap* файл, полученный с захвата трафика сети (рис. 8).

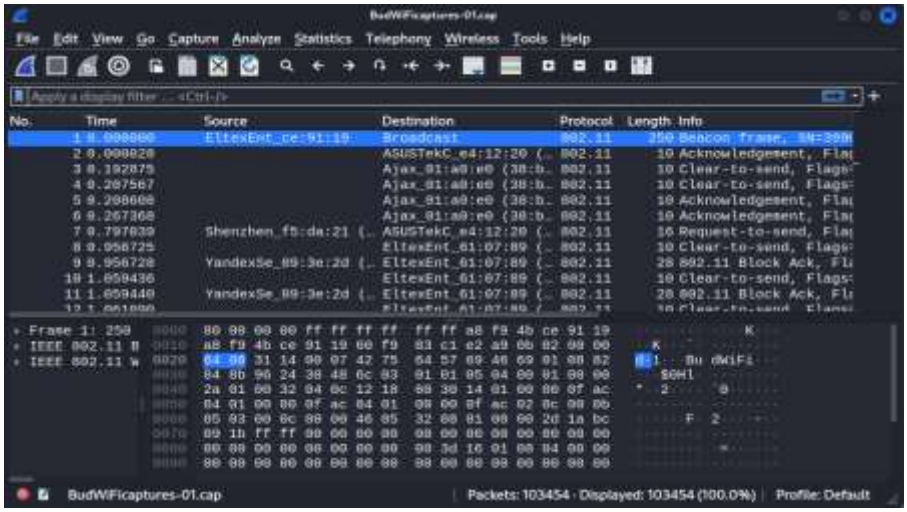

Рисунок 8

После специалистом производится анализ сетевого трафика на предмет нестандартных запросов и ответов, анализ *IP* и *MAC* адресов, обнаружение нескольких подключений с одних и тех же адресов, сопоставление адресов с запросами [19].

Признак присутствия в сети точки доступа с нелегитимным подключением

В ходе исследования был обнаружен признак, по которому можно определить, что в сети присутствует нелегитимное подключение через точку доступа, развернутую на легитимном устройстве. Данный способ уже на протяжении долгого времени используют операторы мобильной связи для предотвращения «раздачи» мобильного интернета клиентом несанкционированно подключенным устройствам [10]. Способ основан на анализе параметра пакета данных на сетевом уровне и полностью применим к исследуемой проблеме.

TTL (*Time To Live*) – это предельный период времени, за который пакет данных может существовать до своего исчезновения. На разных устройствах значения *TTL* разнятся. К примеру, на устройствах под управлением ОС *iOS* и *Android TTL* по умолчанию равен 64, на ПК и ноутбуках под ОС *Windows* – 128. Для описанного метода выявления нелегитимного подключения значение *TTL* в соответствии с типом устройства не играет большой роли [13].

При работе устройства в режиме точки доступа, всем пакетам сторонних подключенных к этой точке доступа устройств присваивается значение на единицу меньше соответствующего им *TTL*. Каждый переход через дополнительную точку доступа будет дальше уменьшать данный показатель. Если произойдет множество скачков от одного клиента к другому, значение станет равным 0 – в таком случае все данные в пакете уничтожатся. Рассмотрим ситуацию на примере исследованной схемы работы *TTL* (рис. 9).

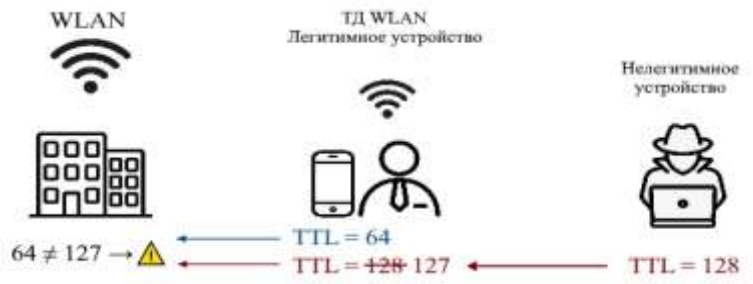

Рисунок 9

Если легитимное устройство не работает в режиме точки доступа *Wi-Fi* или работает в пассивном режиме (т.е. подключенные к нему сторонние устройства отсутствуют), то во всех заголовках соответствующих ему пакетах можно наблюдать одно и то же значение *TTL* (в данном случае – 64). Если же при анализе трафика обнаруживается несоответствие значений *TTL* в разных захваченных пакетах, и при этом *IP* и *MAC* адреса отправителей совпадают, то наверняка можно сделать вывод, что в сети присутствует нелегитимное подключение. В данном случае видно, что итоговые значения в разных пакетах – 64 и 127, соответственно, пакеты были отправлены с двух разных устройств, хотя их *IP* и *MAC* адреса совпадают [14].

После обнаружения подобного инцидента необходимо незамедлительно принять меры по его устранению. Следует зафиксировать данные отправителя и

сохранить пакеты, указывающие на инцидент, после чего немедленно прервать подключение устройства в режиме беспроводной прокси-станции к корпоративной *WLAN*-сети. По зафиксированным *IP* и *MAC* адресам можно выявить сотрудника, развернувшего точку доступа *Wi-Fi* [8].

Недостаток метода

Данный метод полностью соответствует методу обнаружения тетеринга (использования мобильного телефона в качестве точки доступа других устройств к услугам сети передачи данных оператора) операторами мобильной связи, поэтому обладает тем же недостатком, заключающемся в подмене значения *TTL* по умолчанию на нелегитимном устройстве. Рассмотрим ситуацию на примере исследованной схемы при подмене *TTL* (рис. 10).

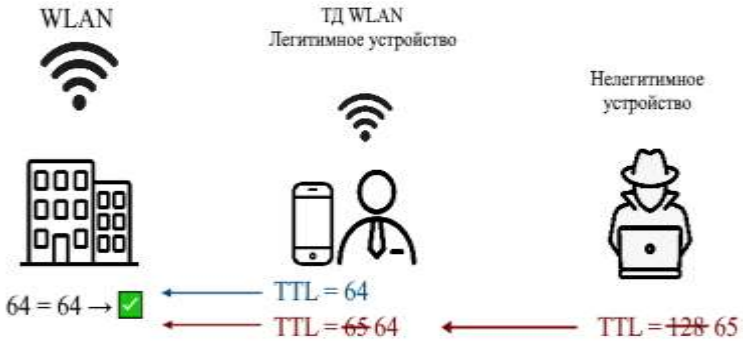

Рисунок 10

Для того, чтобы значение *TTL* соответствовало значению легитимного устройства после прохождения трафика к целевой *WLAN*, на нелегитимном устройстве устанавливается значение *TTL* устройства, работающего в режиме точки доступа с добавленной единицей. В данном случае *TTL* на легитимном устройстве равно 64, поэтому для соответствия значений на нелегитимном устройстве задается *TTL*, равный 65 по умолчанию. Таким образом, в анализируемом трафике во всех пакетах будет фигурировать одно и то же значение, соответствующее легитимному устройству, что полностью исключает обнаружение стороннего подключения к корпоративной *WLAN* данным методом [15].

Заключение

В статье рассмотрена проблема безопасности корпоративных *WLAN*, изучена уязвимость беспроводных корпоративных сетей при использовании в них беспроводных прокси-станций, приведены меры профилактики, а также предложена методика обнаружения использования данной уязвимости в сети. Методика позволяет выявить нелегитимное подключение к легитимному устройству, работающему в режиме точки доступа *Wi-Fi* и подключенному к корпоративной *WLAN*-сети, но только в случае, если на нелегитимном устройстве не проводилась подмена значения *TTL*. Для обеспечения безопасности корпоративных сетей необходимо внедрять данную методику, но также следует изучать и разрабатывать и другие способы предотвращения доступа к закрытым сетям. В будущих исследованиях планируется изучить возможность выявления подобных инцидентов и по другим признакам.

Литература

1. Ковцур М.М., Юркин Д.В., Герлинг Е.Ю., Ахрамеева К.А. Безопасность беспроводных локальных сетей – Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 1.
2. Сергеев А.Н. Основы локальных компьютерных сетей. – Лань, 2022. – С. 1-2.
3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах – М.: ДМК Пресс, 2011. – С. 2.
4. Петрова Т.В., Ковцур М.М., Карельский П.В., Поляничева А.В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. – С. 2.
5. Киструга А.Ю., Ковцур М.М., Оганесян А.Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 2.
6. Ковцур М.М., Кириллов Д.И., Михайлова А.В., Потемкин П.А. Исследование подходов анализа трафика беспроводных сетей с использованием библиотеки Pandas // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 2-3.
7. Юркин Д.Ю., Ворошнин Г.Е., Ковцур М.М., Мисливский Б.С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования Mikrotik // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. – С. 3.
8. Дрепа В.Е., Киструга А.Ю., Ковцур М.М., Кузьмина О.И., Петров В.А. Исследование метода Fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 – Заметки ученого, 2022. – С. 8.
9. Докшин А.Д., Ковцур М.М., Прудников С.В., Таргонская А.И. Исследование подходов для аутентификации пользователей беспроводной сети с применением различных LDAP решений // Наукоемкие технологии в космических исследованиях Земли, 2021. – С. 4.
10. Steffen Schulz, Hossen A. Mustafa, Wenyuan Xu, Ahmad-Reza Sadeghi, Maria Zhdanova, Vijay Varadharajan Tetherway: A Framework for Tethering Camouflage // Conference: Wireless Network Security (WiSec), 2012. – С. 7-9.
11. Kovtsur M.M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H.M.R. IPTV access methods with RADIUS-server authorization // Journal of Information Technology Management, 2022. – С. 7-9.
12. Анализ безопасности корпоративной беспроводной сети // Habr URL https://habr.com/ru/articles/427393/ (дата обращения – март 2023 г.). – С. 2-3.
13. Я всегда с собой беру… // Habr URL https://habr.com/ru/companies/ruvds/articles/598493/ (дата обращения – апрель 2023 г.). – С. 7-9.
14. Что такое TTL и как с его помощью обхитрить провайдера // IT Knowledge Base URL https://disnetern.ru/ttl/ (дата обращения – апрель 2023 г.). – С. 7-9.
15. Как изменить TTL в Windows 10 и раздать безлимитный интернет со смартфона на компьютер // Timeweb Community URL

https://timeweb.com/ru/community/articles/kak-izmenit-ttl-v-windows-10-i-razdat-bezlimitnyy-internet-so-smartfona-na-kompyuter (дата обращения – апрель 2023 г.). – С. 7-9.
16. Герлинг Е.Ю., Зебзеев Е.А., Киструга А.Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. – С. 4-7.
17. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения – Информационные технологии и телекоммуникации, 2021. – Т. 9. – С. 4-7.
18. Коцыняк М.А., Бударин Э.А., Карпов М.А., Муртазин И. Р., Иванов Д. А. Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взаимодействия открытых систем // В сборнике: Состояние и перспективы развития современной науки по направлению информационная безопасность. Анапа, 2020. – С. 4.
19. Новиков П.А., Лепешкин О.М., Шуравин А.С., Бударин Э.А. Модель сетевого мониторинга защищенности сети передачи данных // В сборнике: Неделя науки СПбПУ. Санкт-Петербург, 2020. – С. 4-7.