УДК 004.056.5

Н. А. Суханов[1], Д. А. Фотев[1], Е. В. Рыжкова[2]*

Безопасность открытых сетей

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: nik.suhanov@internet.ru

Аннотация. В современном мире открытые сети встречаются повсеместно: на улице, в заведениях, торговых центрах и других публичных местах. Их безопасность сомнительна, поскольку в случае, если организация или человек, раздающий сеть не позаботились должным образом об ее защищенности, то под угрозу ставятся все пользователи, подсоединенные к ней. Уязвимость также может проявиться и в сайтах, которые будет посещать жертва. Например, небезопасный протокол передачи данных HTTP не шифрует данные вовсе, позволяя любому человеку, подключенному к точке доступа, считывать их. Мошенники могут очень легко это эксплуатировать с помощью инструментов, доступных всем, и заполучить доступ к данным, путем различных атак, таких как «злой близнец», Deauth и прочие.

Ключевые слова: открытые сети, wifi, перехват данных, http, wireshark, set

N. A. Syhanov [1], D. A. Fotev[1], E. V. Ryzhkova[2]*

Open Network Security

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: nik.suhanov@internet.ru

Abstract. In the modern world, open networks are ubiquitous: jutside, in establishments, shopping centers, and other public places. Their security is questionable, since if the organization or person providing the network has not properly ensured its security, then all users connected to it are at risk. Vulnerability can also be present in the websites that the victim may visit. For example, the insecure data transfer protocol HTTP does not encrypt data at all, allowing anyone connected to the access point to read it. Scammers can easily exploit this with tools available to everyone and gain access to data through various attacks, such as «evil twin», Deauth, and others.

Keywords: open network, wifi, data interception, http, Wireshark, install

Введение

В настоящее время практически все люди проводят много времени онлайн. Это связано с доступностью открытых Wi-Fi в общественных местах, таких как кафе или поезда. Люди всегда стремятся подключиться к бесплатному Wi-Fi быстрее, даже не задумываясь о безопасности этого действия. Это связано с неосведомленностью о том, как легко можно эксплуатировать открытые точки доступа, чтобы получить конфиденциальные данные или подменить данные ее пользователей.

Целью данного исследования является повышение осведомленности слушателей, с помощью демонстрации простоты реализации атак на открытые сети.

Это не только способствует повышению уровня цифровой грамотности, но и может заинтересовать людей в повышении безопасности себя и окружающих, программными, техническими или социальными средствами.

Методы и материалы

Wireshark – это популярное у специалистов программное обеспечение для анализа трафика в компьютерных сетях. Этот бесплатный инструмент позволяет изучать различные сети и протоколы, отслеживать сетевую активность в реальном времени или из файла, проводить детальную обработку и визуализацию пакетов данных. У программы есть удобный графический интерфейс, отображающий информацию на всех уровнях протокола, а также статистические и графические инструменты для анализа сетевой активности (рис. 1).

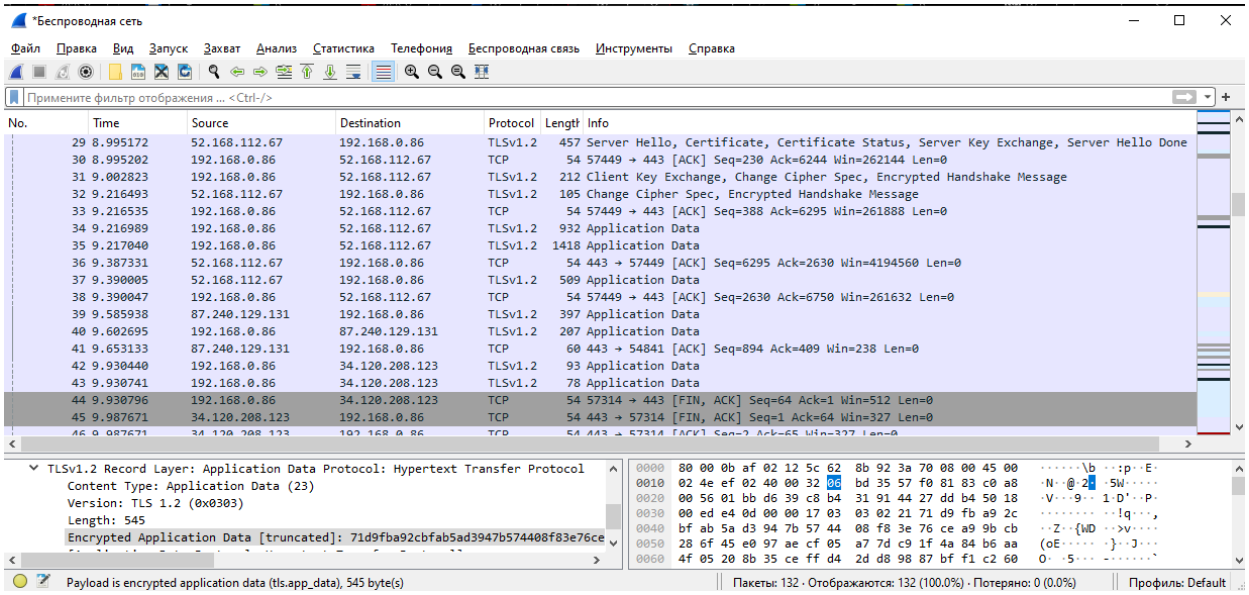

Рис. 1. Окно просмотра интернет трафика

Wireshark помогает в диагностике сети, пассивном анализе сетевой инфраструктуры и других задачах. Важно помнить, что, как и любое другое программное обеспечение для анализа сетей, Wireshark может быть использовано для злоумышленных целей, как, например, просмотр данных незащищенного трафика HTTP. [1]

PyShark – это Python библиотека, которая позволяет анализировать и фильтровать сетевой трафик. Она дает возможность пользователю создавать собственные программы под свои потребности. В отличие от WireShark, PyShark предлагает более гибкие настройки. Использование PyShark имеет смысл, поскольку позволяет создать индивидуализированную версию WireShark с нужными функциями и возможностями, вместо использования стандартного десктопного приложения (рис. 2).

```python
import pyshark

def get_http(request):
    if hasattr(request, "http"):
        if hasattr(request.http, "user_agent"):
            if request.http.request_method == "POST" and hasattr(request, "urlencoded-form"):
                form = getattr(request, "urlencoded-form")
                data = form._get_all_fields_with_alternates()
                print(f"GOT A PASSWORD PACKET. READING:\nUser: {data[2]}\nPassword: {data[5].show}")


capture = pyshark.LiveCapture(interface='Беспроводная сеть')

capture.apply_on_packets(get_http)
```

Рис. 2. Программа для перехвата пароля из HTTP трафика конкретного сайта

SET – набор инструментов для социальной инженерии и не только. Конкретно нас интересует инструмент, клонирующий сайт, раздающий его и затем перехватывающий весь трафик, который на него поступает (рис. 3).

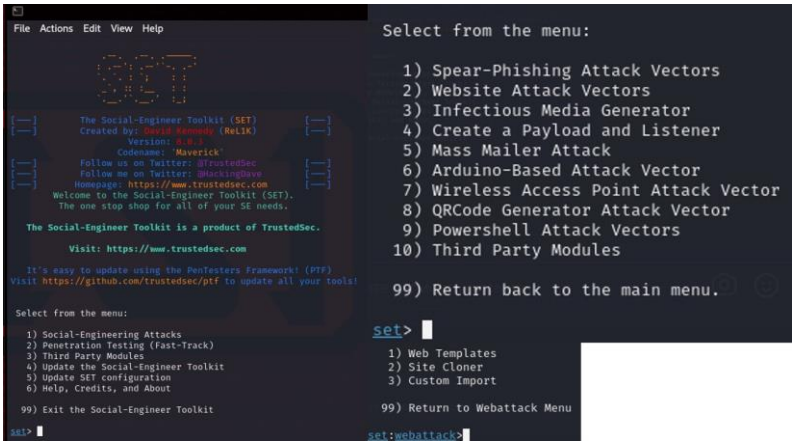

Рис. 3. Инструмент SET и выбранный инструмент для клонирования сайта

Ettercap – еще один инструмент для реализаций различных атак через открытые сети. В данном исследовании была использована функция DNS Spoofer.

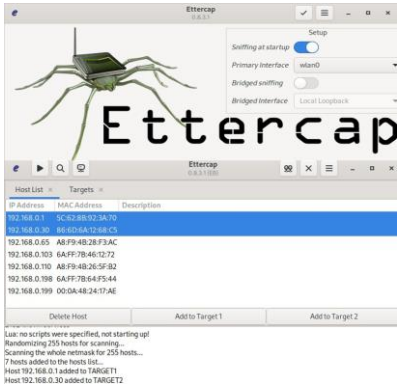

Рис. 4. Инструмент Ettercap, выбранные IP адреса для спуфинга

Результаты

В ходе работы с Wireshark, в тестовых условиях был перехвачен пароль для некоторого сайта, работающего через протокол HTTP (рис. 5).

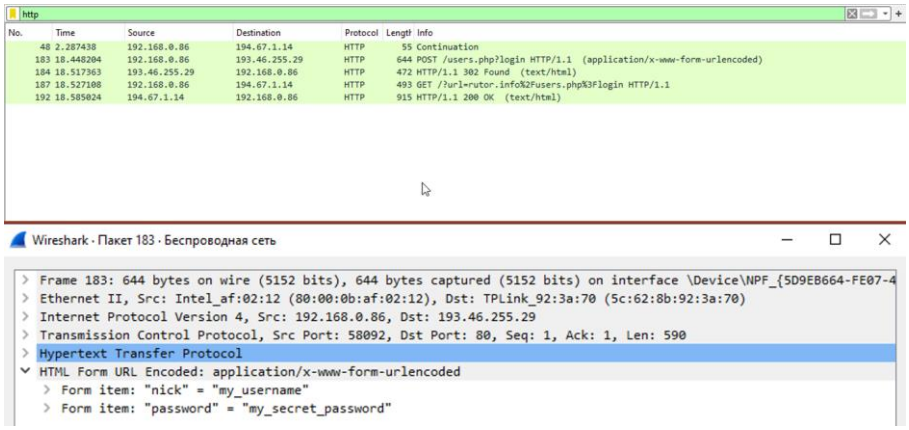

Рис. 5. Просмотр имени пользователи и пароля в HTTP пакете

После запуска программы, написанной на Python с использованием библиотеки PyShark, были введены данные на сайте использующем HTTP. Результат представлен на рисунке 6.

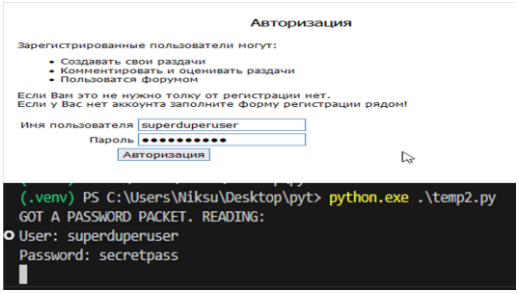

Рис. 6. Запущенная программа и перехваченные имя пользователя и пароль

Используя SET в тестовых условиях был создан клон сайта СГУГиТ и размещен в сети по IP-адресу рабочей станции. С помощью Ettercap все интернет пакеты, направленные к оригинальному сайту СГУГиТ, были перенаправлены к клону сайта после чего была осуществлена попытка авторизации и перехват данных (рис. 7).

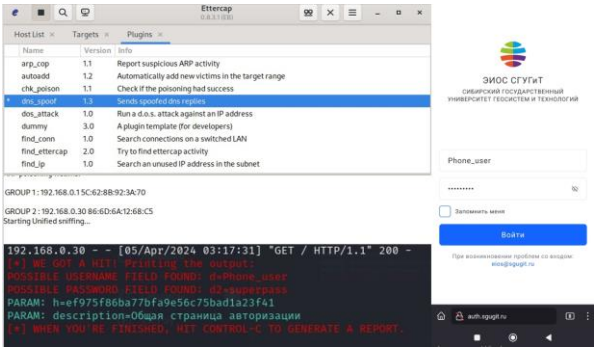

Рис. 7. Запущенная атака и перехват данных с клона сайта

Обсуждение

Все атаки были осуществлены с использованием инструментов, доступных каждому. Они находятся в открытом доступе в сети, с открытым исходным кодом. Каждый человек, у которого есть компьютер или ноутбук, способен осуществить атаки, предоставленные в данном исследовании, не имея знаний в информационной безопасности, так как инструкции или примеры использований прилагаются ко всем инструментам [2].

Заключение

С использованием всех указанных инструментов, которые можно легко получить, злоумышленник может провести атаки на открытые сети и получить доступ к конфиденциальным данным, даже без опыта в этой области, что и было продемонстрировано. Учитывая это, можно сказать, что открытые точки доступа не являются безопасными по своей сути и эта ситуация усугубляется ещё сильнее тогда, когда об их безопасности не заботятся вообще, тем самым подвергая пользователей серьёзной угрозе нарушения конфиденциальности их данных [3].

Благодарности

Авторы выражают благодарность Сибирскому государственному университету геосистем и технологий за поддержку авторов исследования академической стипендией.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика [Электронный ресурс] / М.,2014. – Режим доступа: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf. – Загл. с экрана.

2. Шайхулов Э. А., Смирнов А. П., Болдина О. Б., Азаренко Г. Ю., Благова И. Ю. Современные методы обучения информационной безопасности / Современная наука и инновации. – М.,2023.

3. Герасимов, А. С. Виды сетевых атак и методы защиты от них [Текст] / Актуальные вопросы инноваций и современные научные открытия: Сборник научных статей по материалам II Международной научно-практической конференции. – Уфа,2023.