Для реализации такого приложения использовалась библиотека Redux, которая также является шаблоном управления состоянием. Reduxслужит централизованным хранилищем данных для всех компонентов приложения с правилами, гарантирующими, что состояние может быть изменено только надлежащим образом.

Фактически, Reduxне накладывает каких-либо существенных ограничений на используемую структуру кода. Однако, это требует соблюдения нескольких принципов высокого уровня. Во-первых, глобальное состояние приложения должно храниться в глобальном репозитории. Во-вторых, единственным механизмом изменения этого состояния являются мутации, которые представляют собой синхронные транзакции. Асинхронные операции инкапсулируются в действия или их комбинации.

Проект реализован с соблюдением всех требований и всех перечисленных принципов.

Данный проект был протестирован с использованием готовой среды Jest, поскольку интерфейс командной строки React предоставляет параметры для приложений модульного тестирования. В процессе тестирования были выявлены недостатки в работе приложения, которые сразу же были устранены.

Детально был протестирован интерфейс приложения, в результате которого были обнаружены некоторые недостатки, которые необходимо было исправить. В результате проведенного тестирования, данное функциональное приложение превосходит своих конкурентов по большому количеству параметров.

А. В. Киселёв
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. А. Гольдаде**, д-р техн. наук, профессор

АТАКИ НА СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ

Для беспрерывной деятельности любого предприятие повсеместно используются информационные технологии. Их неотъемлемой частью является глобальная сеть Интернет. Однако вместе с широкими возможностями сеть Интернет приносит так же множество угроз для информационной безопасности. Реализация таких угроз может привести к существенным материальным затратам и репутационному ущербу. Следовательно, одной из главных задач является обеспечение

безопасности обращения информации внутри сети, выявление и предотвращение сетевых атак.

Сетевая атака – это действие, целью которого является захват контроля (повышение прав) над удалённой или локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, пользующихся этой вычислительной системой. Исследования показывают, что большинство атак происходят в рамках сетевого взаимодействия на слабозащищенные беспроводные сети IEEE 802.11 (WiFi) по принципу Deauth Attack или DoS.

Protocol	GHz
802.11	2.4
802.11a	5
802.11b	2.4
802.11g	2.4
802.11n	2.4/5

Рисунок 1 – IEEE 802.11 – стандарт сетевых протоколов для беспроводного взаимодействия

Deauth Attack или деаутентификация клиентов беспроводной сети – это отправка специального сообщения, которое сообщает точке доступа, что нужно снова пройти процесс аутентификации. Рассоединение клиентов может быть выполнено по ряду причин: восстановление скрытого ESSID (крытый ESSID не присутствует в радиовещании), захват рукопожатий WPA/WPA2 путём принуждения клиентов к разъединению, генерация ARP запросов (клиенты Windows иногда стирают их ARP кэш во время дисконекта), атака отказ в обслуживании (DoS) – бесконечная отправка пакетов деаутентификации приводит к отказу в обслуживании, содействие атаке «злой двойник» – отправка пакетов деаутентификации подавляет истинную точку доступа, при этом свои «услуги» начинает предлагать фальшивая точка доступа.

Исследование WiFi-сетей стандартными методами и инструментами, например «airport», позволяет найти и проанализировать возможные уязвимости в сети. Для анализа доступных беспроводных сетей и сбора данных типа SSID/BSID используется стандартные запросы типа <airport scan>.

Рисунок 2 – Атака на сетевое взаимодействие Deauth Attack
или деаутентификация клиентов беспроводной сети

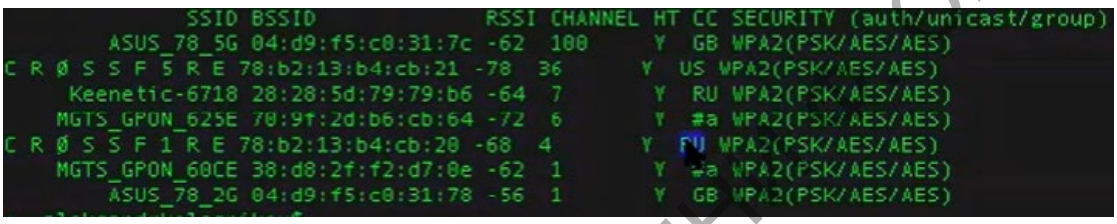

Рисунок 3 – Исследование SSID/BSID WiFi-сети

При нахождении уязвимости и доступа к открытой информации о SSID точки доступа, появляется техническая возможность провести сетевую атаку Deauth Attack для деаутентификация клиентов беспроводной сети. Как правило, атака осуществляется по SSID точки доступа с помощью модуля сетевой атаки и запроса <wifi.deauth.SSID_точки_доступа>. Такие атаки позволяют собирать информацию о пользователях, которые будут заново проходить аутентификацию, перехватывать пакеты и узнавать пароль от WiFi-сети, тем самым получать несанкционированный доступ к сети предприятия.

Отказ в обслуживании или DoS- и DDoS- атаки, так же являются наиболее известной формой атак. Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. Когда атака этого типа проводится одновременно через множество устройств – это называется распределенной атакой DoS (DDoS - distributed DoS).

Для снижения угроз атак типа DoS используют минимум три способа: функции анти-спуфинга (поможет снизить риск DoS-атак), функции анти-Dos (сможет ограничить эффективность атак, так как эти

функции часто ограничивают число полуоткрытых каналов в любой момент времени), ограничение объема трафика (traffic rate limiting).

Проанализировав самые распространенные вида атаки, можно сделать следующие выводы: не стоит использовать уязвимые протоколы, для защиты корпоративных сетей следует использовать технологии корпоративного класса, MFP, необходимо контролировать радиосреду на предмет наличия DoS атак , необходима правильная настройка оборудования и клиентских ПК, автоматизированные средства распространения обновления для ПО и антивирусов, принудительное использование VPN при работе вне корпоративной беспроводной сети.

Литература

1. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / Современные тенденции технических наук: материалы I Международной научной конференции. – 2011. – С. 8–13.

2. Парасрам Шива, Хериянто Теди, Замм Алекс и др. Kali Linux. Тестирование на проникновение и безопасность. / Kali Linux, 2020.

3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. / Питер, 2016. 5-е изд.

К. В. Кислова
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Грищенко**, ст. преподаватель

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ СБОРКИ, ТЕСТИРОВАНИЯ И РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ НА ОСНОВЕ СОВРЕМЕННЫХ ОБЛАЧНЫХ РЕШЕНИЙ

В последние несколько десятилетий стремительно возросла роль компьютерных наук и технологий. С развитием данной отрасли каждое предприятие старается не отставать от современных решений и внедрять их в свои продукты и разработки. Такой темп развития в бизнесе задает высокую конкуренцию на рынке, что заставляет компании предпринимать действия для улучшения качества и скорости реализации их программного обеспечения потребителям.

Решением данных проблем являются технологии автоматизации и облачные решения.