Лабораторная работа. Изучение сведений об атаке

1. Задачи

Изучите и проанализируйте уязвимости приложения Интернета вещей

1. Общие сведения и сценарий

Интернет вещей (IoT) состоит из цифровых соединенных между собой устройств, которые подключают к Интернету все аспекты жизни современного человека, включая наши дома, офисы, автомобили и даже наши тела. За счет ускоренной адаптации IPv6 и развертывания сетей Wi-Fi по всему миру размеры Интернета вещей возрастают по экспоненте. Отраслевые эксперты оценивают, что к 2020 году количество активных устройств IoT приблизится к 50 миллиардам. Устройства IoT особенно уязвимы для угроз безопасности, поскольку безопасность не всегда рассматривалась в архитектуре продуктов для Интернета вещей. Кроме того, устройства IoT часто продаются со старыми встроенными операционными системами и программным обеспечением, для которых не выпускаются обновления.

1. Необходимые ресурсы

* ПК или мобильное устройство с доступом к Интернету

1. Найдите информацию об уязвимостях приложений Интернета вещей

С помощью удобной вам поисковой системы найдите информацию об уязвимостях приложений Интернета вещей (IoT). В процессе поиска найдите пример уязвимости Интернета вещей для каждой из вертикалей Интернета вещей: промышленность, энергетика, здравоохранение и правительственные организации. Подготовьтесь к обсуждению вопроса о том, кто может использовать уязвимости и почему, что послужило причиной уязвимости и что можно сделать для ограничения уязвимости? Вот некоторые ресурсы, с которых предлагается начать поиск.

[Ресурсы Интернета вещей Cisco](http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html)

[Основы безопасности Интернета вещей](https://iotsecurityfoundation.org/)

[Угрозы безопасности Интернета вещей изнутри организаций](http://www.businessinsider.com/iot-cyber-security-hacking-problems-internet-of-things-2016-3)

**Примечание**. Для поиска информации о проблемах безопасности можно использовать веб-обозреватель на виртуальной машине, установленной в ходе предыдущей лабораторной работы. С помощью этой виртуальной машины можно предотвратить установку вредоносного ПО на вашем компьютере.

Из результатов своего исследования выберите одну уязвимость приложения Интернета вещей и ответьте на следующие вопросы.

* + 1. В чем состоит эта уязвимость?

Наиболее распространенная уязвимость среди IoT-устройств – слабые, стандартные или указанные в коде прошивки пароли.

* + 1. Кто может ею воспользоваться? Дайте пояснение.

Это позволяет злоумышленнику быстро подбирать пароли из общедоступных баз. Тем самым получая доступ к сети, частью которой является IoT-устройство.

* + 1. Почему возникает эта уязвимость?

Уязвимость возникает из-за халатности разработчиков или игнорирования рекомендаций по безопасности паролей со стороны пользователей.

* + 1. Что можно сделать для снижения возможности использовать эту уязвимость?

Необходимо просвещать людей в сфере информационной безопасности. Например, оповещать пользователя о том, что заданный им пароль – слабый. Вводить более глубокие проверки кода прошивок IoT-устройств.