Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.382.7+004.056

Мандрик
Валерия Юрьевна

Защита персонального компьютера пользователя от атак подмены информации

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Борботько Т.В.
д.т.н., профессор

Минск 2019

ВВЕДЕНИЕ

Пользователи персональных компьютеров часто эксплуатируют сервисы, обеспечивающие их упрощенную аутентификацию при доступе к ящикам электронной почты и другим аккаунтам. Такая тенденция усложняет проблему информационной безопасности. Ее решение лежит в плоскости разработки организационно-технических мероприятий, направленных на противодействие атакам подмены и снижению риска утечки персональных данных. В соответствие с тем, тема работы является актуальной.

На данный момент киберпреступность распространена в различных формах, но одной из самых опасных является атака типа «Человек по середине». Данная атака представляет собой механизм, когда преступник выступает в роли посредника при передаче информации. Этот вид атаки является распространенным и разрушительным. Атаки «Человек по середине» являются тактическим средством для достижения цели, которая может заключаться в шпионаже за отдельными лицами или группами для перенаправления усилий, средств, ресурсов или внимания. И пусть от данной атаки можно защититься с помощью шифрования, трафик может перенаправляться на фишинговые сайты либо передавать его к месту назначения или регистрации, что делает обнаружение подобных атак невероятно сложным.

Цель магистерской диссертации заключалась в разработке и организационно-технических мероприятиях, обеспечивающих противодействие атакам подмены информации на персональном компьютере пользователя.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке организационно-технических мероприятий, обеспечивающих противодействие атакам подмены информации на персональном компьютере пользователя. Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 Изучить особенности записи, хранения и использования кэш компьютера.

2 Изучить особенности реализации атак подмены информации.

3 Выполнить исследования эффективности существующих средств защиты и разработать рекомендации по их использованию.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XVII Белорусско-российской научно-технической конференции (Минск, 2019).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 тезис доклада в сборнике материалов конференции.

Личный вклад соискателя

Все основные результаты, выводы получены соискателем самостоятельно. Все опытные данные получены во время непосредственной работы соискателя.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 53 страницы, 20 наименований в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится общее описание методов и средств кэширования информации. Рассматриваются основные сервисы, используемые при доступе к веб-ресурсам.

Вторая глава посвящена анализу атак подмены информации. Подробно рассматриваются методы получения информации при атаках. Так же приведено описан выбор метода защиты персонального компьютера в случае ARP-spoofing атаки.

В третьей главе описывается метод эмулирования ARP-spoofing атаки.

Для реализации данной атаки была использована программная среда Intercepter-NG. Она является универсальной улитой для имитации атаки «Человек посередине». Основными функциям Intercepter-NG являются:

– перехват переписки сервисов мгновенного обмена сообщениями, включая ICQ, IRC и прочие;

– «извлечение» паролей служб электронной почты, работающих по протоколам IMAP, POP3 и SMTP;

– доступ к авторизационным сведениям вебформ (HTTP);

– возможность совершения MITM-атак, понижая уровень безопасности взаимодействия по протоколу;

– подмена скачиваемых файлов, что позволяет вместо инсталляционного архива передать модификацию, содержащую зловредный программный продукт: вирус, кеулоггер или троян.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Условием существования и ведения успешной экономической деятельности для любой организации является обеспечение безопасности и непрерывности бизнеса, что невозможно без поддержания постоянной безопасности информации, с которой оперирует данная организация, ее партнеры и клиенты. Безопасность информации подразумевает обеспечение её доступности, целостности и конфиденциальности. Атаки Man in the middle (Человек посередине) нарушают все эти три условия, поэтому при поддержании безопасности информации, необходимо обеспечить защиту от данного вида атак. На данный момент самыми популярными атаками Man in the middle являются:

1 Создание двойника выходной точки.

2 ARP-spoofing.

3 Подмена DHCP-сервера.

В результате исследования была проведена эмуляция атаки ARP-spoofing, где опытным путем было продемонстрировано, насколько легко можно получить данные о логинах и паролях с любого компьютера через кэшируемую в браузере информацию. В случае данной атаки компьютер начинает считать шлюзом не роутер, а компьютер атакующего. Атакующий получает запросы от «жертвы» и передаёт их в пункт назначения (например, запрашивает содержимое веб-сайта в Интернете), получив ответ от пункта назначения, он направляет его «жертве».

Атака ARP-spoofing используется в локальной сети, построенной на коммутаторах. С ее помощью можно перенаправить поток ethernet-фреймов на другие порты, в соответствии с MAC-адресом. После чего злоумышленник может перехватывать все пакеты на своем порту. Таким образом, атака ARP-spoofing позволяет перехватывать трафик машин, расположенных на разных портах коммутатора.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Мандрик, В.Ю. Защита персонального компьютера пользователя от атак подмены информации / В.Ю. Мандрик, Т.В. Борботько// Технические средства защиты информации : тезисы докладов XVII Белорусско-российской науч.-техн. конф./ Минск: БГУИР, 2019. С. 49. (Минск, 11 июня 2019 г.).