The purpose of this work is to consider different types of attacks on web applications, options for implementing and protecting against these attacks, as well as ways to check and evaluate the security of web resources against intruders.

Ключевые слова: веб-разработка, интернет-магазин, защита данных, защита информации, хакер, взлом, тестирование, пентест, тестирование на проникновение.

Keywords: web development, online store, data protection, information security, hacker, hacking, testing, pentest, penetration testing.

В современном мире, в Интернете хранится много информации, в том числе и персональных данных. И всегда есть люди, которые хотят получить эту информацию незаконным путем. Их называют хакерами. Согласно большой политехнической энциклопедии, хакер - программист, пользователь вычислительной системы (обычно Интернета), занимающийся поиском незаконных способов получения несанкционированного доступа к защищённым данным.

Существует несколько типов атак на интернет-ресурсы: mailbombing (увеличение трафика и количества присылаемых сообщение, в результате чего происходит сбой сервиса); заражение сервера, где развернут веб-ресурс, компьютерным вирусом; переполнение буфера (программные ошибки, которые приводят либо к аварийному завершению программы, либо дают полный доступ к системе); сторонние программы – вирусы, трояны, почтовые черви, снифферы; сетевая разведка (сбор информации – сканирование портов, запрос DNS, проверка защиты компьютера и проверка системы); сниффинг пакетов (получаемые пакеты пересылаются на обработку, в результате чего можно получить не только информацию о системе, но и персональные данные - пароли, сообщения и другие файлы); IP-сниффинг (использование IP-адреса для атаки на локальную сеть); man-in-the-middle (перехват информационного канала, в результате чего появляется доступ ко всей передаваемой информации); инъекция (внедрение сторонних кусков кода в ход передачи данных, которые не мешают работе приложения, но производят необходимые действия); DoS-атака и DDoS-атака (атака, имеющая своей целью заставить сервер не отвечать на запросы) и т.д.

Согласно статистике за 2018 год, наиболее часто совершаются инъекционные атаки, а реже всего – подделка запросов со стороны сервера. Наибольшее среднее число атак в день приходятся на веб-приложения в сфере IT, а наименьшее – в сфере энергетики и промышленности.

Как показали исследования, в Интернете есть множество программ в открытом доступе для разного вида атак на веб-ресурсы. Есть ряд популярных программ для реализации DoS и DDoS атак. Наиболее популярными и известными являются приложения Kali Linux, LOIC, UDP Flooder и т.д. Также есть ряд программ, которые ориентированы не на один вид атаки, а на несколько – Metasploit (набор инструментов для создания эксплойтов), oclHashcat (приложение для взлома паролей), Social-Engineer Toolkit (программа для имитации атак в сфере социальной инженерии). Стоит отметить, что данные программы могут использоваться как в преступных целях, так и в целях тестирования собственных интернет-ресурсов.

Также есть программы, основная цель которых – выявление конкретных уязвимостей. Например, программа Acunetix WVS является сканером веб-уязвимостей, в том числе SQL-инъекций и межсайтового скриптинга (в основном используется для сайтов на платформе WordPress). Также некоторые приложения используются в сфере криминалистики, они собирают, обрабатывают и анализируют информацию о кибератаках, например Maltego, Helix3 Pro, EnCase.

Но есть типы атак, которые можно проверить и без специализированных приложений. Например, проверить, не ведется ли DoS или DDoS атака можно через командную панель Windows. Сделать это очень просто – необходимо проверить, пингуется ли сайт, то есть провести команду ping.

Для оценки защищенности веб-ресурса, как и любого другого приложения, используются различные методы анализа и тестирования. Тестирование веб-приложения сопряжено с интенсивной деятельностью в области тестирования совместимости, тестирования производительности, автоматизации тестирования с использованием широкого спектра инструментальных средств [1,79].

Один из способов тестирования веб-приложений в области безопасности – это тестирование на проникновение (penetration testing или pentest). Пентест представляет собой осуществление ряда действий, которые могут совершить злоумышленники для взлома веб-ресурса, чтобы выявить уязвимые места в системе. Фактически, проводится легальный хакерский взлом ресурса.

Тестирование на проникновение применяется для выявления уязвимостей в системе безопасности ресурса, практической их демонстрации, получения объективной оценки текущего уровня безопасности, определения рекомендаций по устранению уязвимостей.

В основном тестирование на проникновение проходит методом черного ящика. При использовании метода черного ящика у тестировщика либо нет доступа к внутренней структуре и коду приложения, либо недостаточно знаний для их понимания, либо он сознательно не обращается к ним в процессе тестирования [1,70]. Фактически, при такой методе у тестировщика есть лишь адрес веб-ресурса, который необходимо проверить.

Существуют общепризнанные стандарты и руководства по обеспечению информационной безопасности. Самые известные и распространенные из них – это OWASP (Open Web Application Security Project) Testing Guide, OWASP Top10, Web Application Security Consortium Threat (WASC) Classification, а также стандарты серии ISO 17799/27000.

Данный вид тестирования является одним из самых спорных вариантов проведения анализа продукта. Одной из проблем пентеста является сложное его презентации, как услуги по проверке безопасности. Ведь в процессе такой проверки можно получить реальный доступ к конфиденциальным данным заказчика, что не каждому придется по душе. Еще одной проблемой является тот факт, что при таком анализе учитываются только те уязвимости, которые уже известны, а в современном мире велика вероятность появления нового способа атаки на ресурсы. К тому же, для проведения тестирования на проникновение необходимо обладать достаточно большой квалификацией, а также глубоким пониманием природы уязвимостей и техники проведения атак в разных условиях. Таким образом, тестирование на проникновение нельзя автоматизировать [2,3].

Таким образом, существует множество разных видов атак на веб-ресурсы, причем с развитием технологий растет вероятность появления новых и более совершенных вариантов атак. Но вместе с тем будут появляться и новые варианты защиты от этих атак. В Интернете существует множество программ в открытом доступе, позволяющих как взломать интернет-ресурс, так и проверить возможность взлома, все зависит от цели использования приложения.

Для проверки и оценки защищенности ресурса используются разные виды тестирования, один из которых – тестирование на проникновение или пентест. Это исследование защиты ресурса путем попыток его взлома уже известными способами взлома, которые могут использовать злоумышленники. Для использования такого вида

тестирования необходимо обладать специфическими и глубокими познаниями в области кибербезопасности.

Список использованных источников

1. Куликов С. Тестирование программного обеспечения. Базовый курс. - [Текст], EPAM Systems, 2015–2017. - 296 с.
2. Пентест как предчувствие - URL: http://docplayer.ru/37718942-Pentest-kak-predchuvstvie.html (дата обращения: 29.10.2018).
3. Рязанцев В.Д. Большая политехническая энциклопедия. – [Текст], М.: Мир и образование, 2011. – 704 с.
4. Виды хакерских атак на веб-ресурсы – URL: http://www.it-click.ru/articles/web-studio/hacking-web-site.aspx.
5. Статистика атак на веб-приложения: итоги 2017 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2018/
6. 10 лучших инструментов для хакинга в 2017 году. -URL: https://proglib.io/p/best-hacking-tools/

81.93.29

АНАЛИЗ ТАКТИКО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ИЗВЕСТНЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

Автор: Евдокимова Ксения Львовна, учащаяся 5 курса Московского авиационного института (национальный исследовательский университет) «МАИ» Учебный центр «Интеграция».

Научный руководитель: к. т. н., доцент Стрельчук Сергей Григорьевич.

Аннотация.

Целью данной работы является повышение достоверности и криптографической стойкости передаваемой конфиденциальной информации путем перекодирования кодограмм с помощью криптографического сканера.

Ключевые слова: комплексная защита информации, конфиденциальная информация, криптографическая стойкость, открытые каналы связи, сканирование, криптографические символы, фантомные каналы связи, телекодовая информация, корреляционные каналы связи

Известные методы формирования низкочастотных фантомных систем передачи [1, 2] реализуются с помощью искусственных цепей (рисунок 1.1) и фильтров в виде резонансных колебательных контуров (рисунок 1.2), которые можно с успехом применять для защиты информации от ее разглашения в линиях связи.

На рисунке 1.1 изображена схема высокочастотного уплотнения двухпроводной телефонной линии связи, работающей в полудуплексном режиме, дополнительным телеграфным каналом.

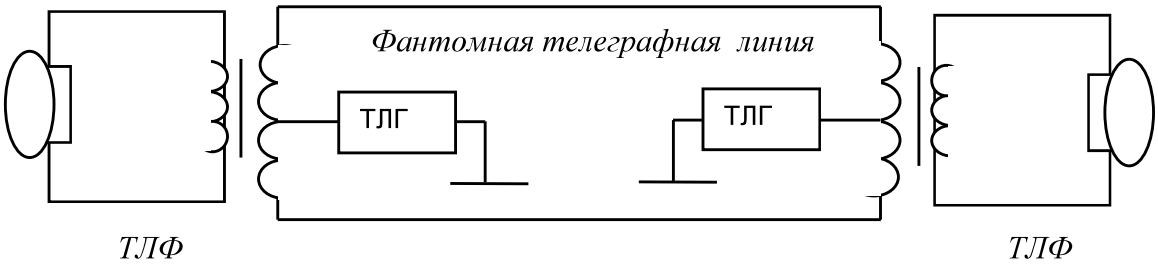

Рисунок 1.1 – Защита телекодовой информации от ее разглашения путем использования известной двухпроводной полудуплексной телефонной линий с уплотнением фантомной телеграфной цепью

Из рисунка 1.1 следует, что конфиденциальная передача телеграфной информации в двухпроводной телефонной линии связи возможна при условии, что осуществляется такое изменение такта телеграфирования, которое криптографическому аналитику не известно. Тактико-техническая характеристика, а именно: криптографическая стойкость такого известного фантомного канала связи является низкой, так как не используются кодировочные ключи.

На рисунке 1.2 представлена схема защиты телекодовой информации от разглашения при передаче ее по телефонному каналу аппаратуры высокочастотного уплотнения, из которой видно, что криптографическая защита телеграфной (телекодовой) информации в телефонной двухпроводной линии может выполняться как за счет изменения такта телеграфирования, так и путем создания неопределенности выбора полосы пропускания n – 1 частотных фильтров. Однако криптографическая стойкость является тоже невысокой, так как число n полосовых фильтров мало.

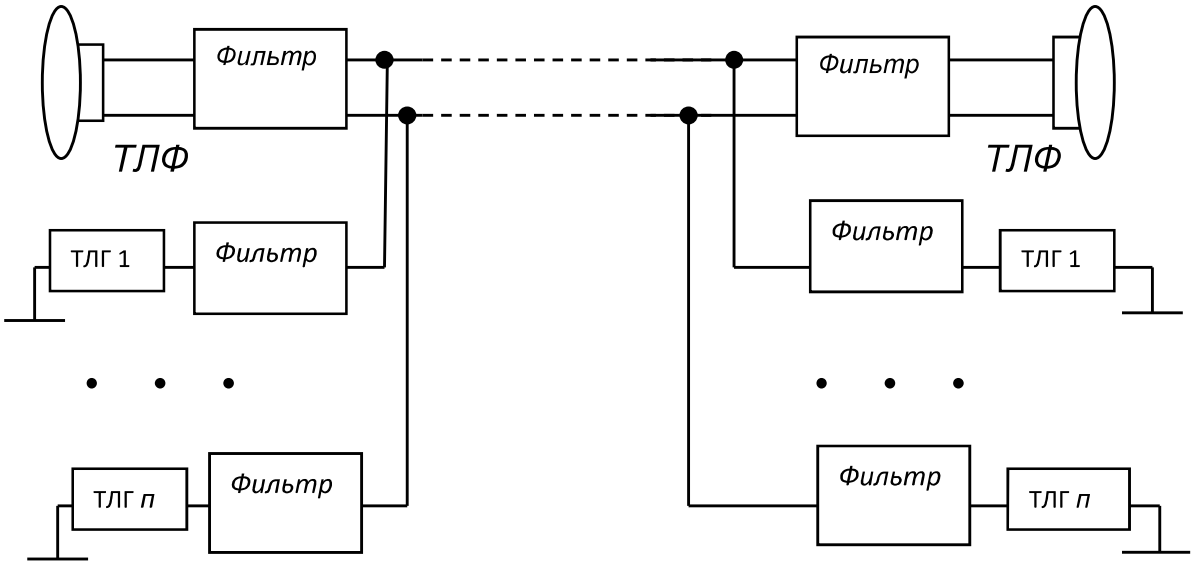

Рисунок 1.2 – Защита телекодовой информации путем использования известной схемы уплотнения двухпроводной телефонной линии n телеграфными цепями с помощью n + 1 электрических фильтров