МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01ммзи
_____ Слепенчук Р.А.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области безопасности современных платёжных технологий
- Написание отчета по практике о проделанной работе.
- Написание тезисов по выбранной теме.
- Подготовка презентации по проведённому исследованию.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Изучить шаблон атаки на современные платежные технологии.
2. Ознакомиться с критериями и подкритериями безопасности платежных систем.
3. На основе критериях безопасности проанализировать популярные платежные системы в России.
4. На основе полученных знаний написать отчет по практике о проделанной работе.

Безопасность современных платёжных технологий

С каждым годом процент использования платежных система, для совершения торговых сделок, неумолимо растет. Помимо очевидного удобства и эффективности, платёжные технологии предоставляют большой простор действий для злоумышленника. С каждым годом технологии защиты становиться все сложнее, а злоумышленники все изощрение. Что бы обезопасить персональные данные и средства пользователей необходимо изучить действия злоумышленников при атаке и на их основе разработать критерии оценки безопасности той или иной платежной системы.

Предварительным этапом атаки на финансовую структуру являться сбор информации о цели атаки. Злоумышленники собирают сведенья которые помогут преодолеть системы защиты организации и провести подготовительную работу для дальнейших действий. Их интересуют такие сведенья как:

- Сведенья о сервисах на сетевом периметре и используемом ПО;
- Сведенья о сотрудниках (электронные адреса, телефоны, должности, ФИО и т. п.);
- Сведенья о партнёрах и конкурентов;
- Сведенья о бизнес-процессах.

Так как при активном сканирование риск быть замеченным защитами системами организации слишком велик, злоумышленники используют пассивные методы добычи информации. Так же преступник могут покупать сведенья у недобросовестных сотрудников.

После сбора информации злоумышленники производят приготовительные действия, такие как:

- Разработка или адаптация ВПО для используемых в организации версий ПО и ОС;
- Подготовка фишинговых писем;
- Организация инфраструктуры (регистрация доменов, аренда серверов, покупка эксплойтов и т. п.);
- Подготовка инфраструктуры для отмывания денег и их обналичивания;
- Тестирование инфраструктуры и ВПО.

После всестороннего изучения и подготовки происходит первоначальное проникновение. Наиболее распространенным и эффективным методом проникновения являться фишинговые письма, рассылаемые по списку электронных адресов сотрудников организаций. Часто письма направляться якобы от имени каких-либо других финансовых организаций или органов государственной власти. Вредоносное программное обеспечение обычно содержится во вложениях таких писем. Чуть реже используется вариант, когда файл предлагается загрузить с внешнего ресурса по ссылке из тела письма.

После открытия вложения или загруженного файла (чаще всего документа формата программного пакета Microsoft Office) происходят скрытая загрузка и запуск программного обеспечения, предоставляющего атакующим удаленный доступ к компьютеру. В большинстве случаев для внедрения кода использовались известные уязвимости указанного программного пакета.

Другой вариант первичного распространения вредоносного ПО — взлом сторонних компаний, которые не столь серьезно относятся к защите своих ресурсов, и заражение сайтов, часто посещаемых сотрудниками целевой организации.

После успешного проникновения злоумышленники стараться получить права администратора на компьютерах сотрудниках и серверах используя уязвимости системы. Распространение уязвимости:

- Использование устаревших версий ПО и отсутствие актуальных обновлений безопасности для ОС;
- Множественные ошибки конфигурации (в том числе избыточные привилегии пользователей и ПО, а также установку паролей локальных администраторов через групповые политики);
- Использование словарных паролей привилегированными пользователями;
- Отсутствие двухфакторной аутентификации для доступа к критически важным системам.

После получении привилегированного доступа злоумышленники получают данные всех пользователей (идентификаторы, пароли или хеш-суммы паролей). Эти данные используются для подключения к другим компьютерам в сети. Преступники исследуют компьютеры сотрудников на использование приложений с помочью которых проводиться денежные операции.

Закрепившись в системе, злоумышленники могут длительное время наблюдать и собирать информацию об внутренней инфраструктуре организации, об бизнес-процессах, изучают выбранные системы и действия сотрудников, чтобы замаскировать хищение под внутренние операции организации. Основными способами хищений являются:

- перевод средств на подставные счета через системы межбанковских платежей;
- перевод денежных средств на криптовалютные кошельки;

- управление банковскими картами и счетами;
- управление выдачей наличных средств в банкоматах.

После произведённого хищения преступники с целью затруднить расследование, полностью выводят из строя узлы сети стирая загрузочные записи и таблицы разделов жестких дисков.

Критерии безопасности платёжных систем необходимы как для компаний, которые их разрабатывают, так и для пользователей. Первые получают возможность создать гарантированно надёжную систему, а вторые – способность оценить безопасность той или иной системы. Что бы обеспечить комплексную защиту той или иной платежной системы необходимо учесть множество различных критериев, рассмотрим основные из них.

Основной критерий, без которого не обходиться ни одна электронная платежная система это – Защита аккаунта паролем. Дополнительная защита обеспечивается требованием к паролю: длина пароля, различный регистр букв, наличие спец символов и цифр. Так же не лишним будет ограничение пароля по сроку действия.

Еще одним немаловажным критерием являться – Использование безопасного соединения с вебсайтом, где рассматривается применения SSL-шифрования, наличие незащищённого контента и какой протокол транспортного уровня используется.

Так же стоит отметить группу критериев, обеспечивающих защиту с помощью дополнительных устройств и аккаунтов. В нее входит:

1. Подтверждение совершаемых операций с помощью SMS, e-mail и тд.
2. Дополнительная привязка почты/телефона к аккаунту.

3. Информирование клиента об операциях, совершаемых с электронным кошельком по SMS и e-mail.

Все критерии безопасности представлены в таблице 1 со значениями показателя безопасности для каждого из них для результирующей оценки безопасности платежной системы.

Критерии и подкритерии безопасности (их особенности)		**Значение показателя безопасности, %**
1) Первичная защита аккаунта СЭП		
1. Защита аккаунта паролем (критерий 1)		
Наличие пароля аккаунта		10
Надежность пароля	Минимальный пароль 1 символ	0
	Минимальный пароль 5-6 символов	5
	Минимальный пароль 8 символов	10
	Наличие доп. условий (спец. символы, буквы верхнего регистра, цифры)	5
Наличие строки надежности пароля		2
Ограничение срока действия пароля СЭП		3
2. Использование безопасного соединения с веб-сайтом (критерий 2)		
Безопасность SSL-соединения	Не используется SSL-шифрование	0
	Применяется SSL-шифрование, но есть незащищенный контент, представляющий серьезную опасность	3
	Применяется SSL-шифрование, но обнаружен незащищенный контент	5
	Используется SSL-шифрование (безопасное соединение)	10
Используемый протокол	С протоколом TLS 1.1	5
	С протоколом TLS 1.2	10
2) Безопасность при авторизации в СЭП		
Подтверждение входа с помощью мобильного телефона, сервиса E-num или e-mail (критерий 3)	Мобильный телефон	5
	Сервис E-num	5
	E-mail	5
3) Авторизация с помощью технических настроек		
1. Возможность ограничения доступа по IP-адресу (критерий 4)		5
2. Выдача персонального цифрового сертификата для доступа в СЭП (критерий 5)		5
4) Подтверждение операций с кошельком дополнительным паролем		
Подтверждение операций (критерий 6)	С помощью SMS присылаемое на моб. телефон или e-mail	5
	С помощью сервисов E-num, Google Authenticator или другими подобными системами	5
	С помощью дополнительного платежного пароля	5
5) Дополнительные способы и методы, обеспечивающие безопасность денежных средств		
Возможность привязки почты/телефона к СЭП дополнительно (критерий 7)		3
1. Возможность выпуска или приобретения виртуальной карты с коротким сроком действия и лимитом средств (критерий 8)		3
2. Наличие идентификации с подтверждением документами пользователя (критерий 9)		3
3. Использование секретных вопросов или секретного слова (критерий 10)		3
4. Ограничение сессии – автоматический выход из системы по истечении времени неактивности пользователя (критерий 11)		3
6) Информационные способы обеспечения безопасности		
1. Информирование пользователя по SMS или e-mail об операциях, проводимых с электронным кошельком (критерий 12)		3
2. Наличие журнала посещений пользователем СЭП (критерий 13)		3
3. Наличие инструкций и рекомендаций по безопасности для пользователей СЭП (критерий 14)		3
4. Наличие службы поддержки (критерий 15)	По телефону	3
	Через форму обратной связи или e-mail	2

Таб. 1

Защищённость системы электронных платежей зависти от количества набранных процентов из 100. Оценка A(отлично) – от 90% и выше, B(хорошо – от 80% до 89%, C(удовлетворительно) – от 70% до 79%, F(неудовлетворительно) – менее 70%.

Для исследования были взяты 12 самых популярных на территории России систем электронных платежей, так как из-за большого числа пользователей атаки злоумышленников более вероятны. Исследования проводились по критериям из таблицы 1.

Исследование показало, что лишь две системы электронных платежей – WebMoney и OKPAY – имеют оценку «хорошо» (B). Всего три системы – VISA QIWI-кошелек, PayPal и RBK Money получили оценку «удовлетворительно» (C). Все остальные платежные системы получили оценку неудовлетворительно.

Для проведения электронных платежей можно рекомендовать использовать системы, получившие оценку «удовлетворительно» и выше, но при условии, что пользователь будет следовать инструкциям и рекомендациям, незамедлительно реагировать на подозрительные действия со своим электронным кошельком и сообщать об этом в службу поддержки.

Результаты исследование всех систем электронных платежей представлены в таблицы 2.

№	СЭП	Критерий															
		Защита аккаунта СЭП паролем		Безопасность при авторизации в СЭП	Авторизация с помощью технических настроек		Подтверждение операций с кошельком доп. паролем	Дополнительные способы и методы						Информационные способы обеспечения безопасности			Оценка, сумма показателей
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	VISA QIWI-кошелек	27	20	0	0	0	5	3	3	3	0	3	3	0	3	6	C – 76 %
2	Яндекс. Деньги	18	15	0	0	0	5	3	0	3	3	0	3	3	3	6	F – 62 %
3	WebMoney	15	20	0	5	5	5	3	3	3	3	3	3	3	3	6	B – 80 %
4	PayPal	25	20	0	0	0	5	3	0	3	3	3	3	0	3	6	C – 74 %
5	RBK Money	18	20	0	5	0	5	3	0	3	3	3	3	0	3	6	C – 72 %
6	Rapida online	10	20	0	0	0	5	3	3	3	0	3	3	0	0	6	F – 56 %
7	Элекснет	10	8	0	0	0	5	3	0	3	3	3	3	0	0	6	F – 44 %
8	Wallet One	15	20	0	0	0	5	3	0	3	0	3	3	3	0	6	F – 61 %
9	Comepay-кошелек	20	15	0	0	0	5	0	0	3	0	3	3	0	0	6	F – 55 %
10	Payeer-кошелек	20	15	5	0	0	5	3	0	3	3	3	3	3	0	6	F – 69 %
11	OKPAY	25	20	5	5	0	0	3	0	3	3	3	3	3	3	6	B – 82 %
12	MoneyMail	10	15	0	0	0	5	3	0	3	0	0	3	3	0	6	F – 48 %

Таб 2.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики ознакомился с используемыми в наше время платёжными системами, их критериями и шаблонами атак на данные системы, а также с изучил какие системы, используемые в России, являются наиболее защищёнными безопасные.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. Т.А. Маркина. В.А. Хрупов. «ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ»
2. [Электронный ресурс] - http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf
3. [Электронный ресурс] - http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf
4. [Электронный ресурс] – https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/