ТЕМА РАБОТЫ: «АНАЛИЗ МЕТОДОВ ПЕРЕХВАТА ПАРОЛЕЙ И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ИМ.»

Выполнил: Перминов Дмитрий Юрьевич

Группа: КС-14

ЦЕЛЬ РАБОТЫ: Проведение анализа методов перехвата паролей и противодействия им.

ЗАДАЧИ:

1. Рассмотреть методы перехвата паролей
2. Найти методы противодействия перехвата паролей
3. Провести анализ методов перехвата паролей
4. Провести анализ методов противодействий перехвата паролей

АКТУАЛЬНОСТЬ:

В настоящее время хакеры с легкостью могут перехватить ваши пароли и присвоить ваши данные. И поэтому нужно найти методы противодействия им, что бы сохранить целостность своих данных.

МЕТОДЫ ПЕРЕХВАТА ПАРОЛЕЙ

Основные методы перехвата паролей:

1. Брутфорс
2. Фишинг
3. Догадки
4. Сниффер
5. Клавиатурные шпионы

БРУТФОРС

Брутфорс(от английского bruteforce — полный перебор или метод «грубой силы») – один из популярных методов взлома паролей на серверах и в различных программах. Заключается он в том, что программа-взломщик пытается получить доступ к какой-либо программе (например, к почтовому ящику) путем перебора паролей по критериям, заданным владельцем данной программы: по словарю, по длине, по сочетаниям цифр и др.

Данный способ подбора паролей очень хорош тем, что пароль в конце концов взламывается, но это может занять весьма и весьма долгое время, зачастую даже столетия.

ФИШИНГ

Фишинг (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

ДОГАДКИ

Лучшим другом взломщиков паролей, конечно, является предсказуемость пользователей. Если действительно случайный пароль был создан с помощью программного обеспечения, предназначенного для этой задачи, то пользовательский "случайный" пароль, вряд ли будет напоминать что-то подобное.

СНИФФЕРЫ

Сниффер(нюхач, eng) - это программа, которая устанавливается под NIC (Сетевую Интерфейсную Карту), иначе называемую Ethernet карта(одна из необходимых частей аппаратных средств, для физического соединения компьютеров в локальной сети). Как известно информация по сети передается пакетами - от вашей машины к удаленной, так вот сниффер, установленный на промежуточном компьютере, через который будут проходить пакеты - способен захватывать их, пока они еще не достигли цели.

КЛАВИАТУРНЫЕ ШПИОНЫ

Клавиатурные шпионы - это программа для скрытной записи информации о нажимаемых пользователем клавишах. У термина «клавиатурный шпион» есть ряд синонимов: KeyboardLogger, KeyLogger, кейлоггер; реже встречается термины "снупер", "snoop", "snooper" (от англ. snoop - буквально "человек, вечно сующий нос в чужие дела")

Как правило, современные клавиатурные шпионы не просто записывает коды вводимых клавиш - он "привязывает" клавиатурный ввод к текущему окну и элементу ввода.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПЕРЕХВАТАМ ПАРОЛЕЙ

1. Методики поиска клавиатурных шпионов
2. Защита от фишинга
3. Многоуровневая модель обеспечения безопасности
4. Основные защитные методы

МЕТОДИКИ ПОИСКА КЛАВИАТУРНЫХ ШПИОНОВ

1. Сигнатурный поиск позволяет однозначно идентифицировать клавиатурные шпионы, при правильном выборе сигнатур вероятность ошибки практически равна нулю. Однако сигнатурный сканер сможет обнаруживать заранее известные и описанные в его базе данных объекты;
2. Эвристический поиск носит вероятностный характер. Как показала практика, этот метод наиболее эффективен для поиска клавиатурных шпионов самого распространенного типа – основанных на ловушках.
3. Мониторинг API функций, используемых клавиатурными шпионами. Данная методика основана на перехвате ряда функций, применяемых клавиатурным шпионом – в частности, функций SetWindowsHookEx, UnhookWindowsHookEx, GetAsyncKeyState, GetKeyboardState.
4. Отслеживание используемых системой драйверов, процессов и сервисов. Это универсальная методика, применимая не только против клавиатурных шпионов. В простейшем случае можно применять программы типа KasperskyInspector или Adinf, которые отслеживают появление в системе новых файлов.

ЗАЩИТА ОТ ФИШИНГА

1. С ростом количества онлайн сервисов растет и количество сетевых мошенников. Не смотря на то что сами сервисы могут быть абсолютно безопасными, нужно сохранять предельную осторожность чтобы не стать жертвой фишинговой атаки. Вот несколько рекомендаций, позволяющих избежать этого:
2. Будьте предельно внимательными когда вам приходят письма с запросом какой-либо персональной информации, либо с требованием ее обновить на сайте.
1. Если письмо не подписано цифровой сигнатурой, то нельзя быть уверенным, что оно не поддельное.
3. Мошенники часто используют специальные приемы чтобы вызвать реакцию на письмо.
4. Как правило фишинговые письма не персонализированы, т.е. не содержат вашего имени в адресе
5. Никогда не переходите по ссылкам, нажимая их прямо в письме
6. Никогда не заполняйте персональными данными HTML формы, которые расположены прямо в письме.
7. Всегда проверяйте что для передачи персональной информации используется шифрованное соединение.

МНОГОУРОВНЕВАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1. Для защиты крупных компаний и их сотрудников от мошенников, использующих техники социальной инженерии, часто применяются комплексные многоуровневые системы безопасности:
2. Данные. Деловая информация: учетные записи, почтовая корреспонденция и т. д. При анализе угроз и планировании мер по защите данных нужно определить принципы обращения с бумажными и электронными носителями данных.
3. Приложения. Программы, запускаемые пользователями. Для защиты среды необходимо учесть, как злоумышленники могут использовать в своих целях почтовые программы, службы мгновенной передачи сообщений и другие приложения
4. Компьютеры. Серверы и клиентские системы, используемые в организации. Защита пользователей от прямых атак на их компьютеры, путём определения строгих принципов, указывающих, какие программы можно использовать на корпоративных компьютерах.
5. Внутренняя сеть. В последние годы из-за роста популярности методов удаленной работы, границы внутренних сетей стали во многом условными.
6. Периметр сети. Граница между внутренними сетями компании и внешними, такими как Интернет или сети партнерских организаций.

ОСНОВНЫЕ ЗАЩИТНЫЕ МЕТОДЫ

Специалисты по социальной инженерии выделяют следующие основные защитные методы для организаций:

1. Разработка продуманной политики классификации данных, учитывающей те кажущиеся безвредными типы данных, которые могут привести к получению важной информации;
2. Обеспечение защиты информации о клиентах с помощью шифрования данных или использования управления доступом;
3. Обучение сотрудников навыкам для распознавания социального инженера, проявлениям подозрения при общении с людьми, которых они не знают лично;
4. Запрет персоналу обмен паролями либо использование общего;
5. Запрет на предоставление информация из отдела с секретами кому-либо, не знакомому лично или не подтвержденному каким-либо способом;
6. Использование особых процедур подтверждения для всех, кто запрашивает доступ к конфиденциальной информации;

ЗАКЛЮЧЕНИЕ

Цель курсовой работы выполнена. Анализ методов перехвата паролей выполнен, анализ методов противодействия перехвату проведен. Я выделил наиболее актуальные методы перехвата паролей: клавиатурные шпионы ,фишинг, брутфорс, снифферы, догадки.

Исходя из анализа методов противодействия перехвату паролей, выделяю основные требования к созданию паролей в информационных системах:.

Пароль не должен быть коротким

Пароль не должен содержать только цифры или только буквы ,

Не использоваться использовать пароль, который содержит любые данные о вас или вашей семье -всевозможные памятные даты (рождения, свадьбы и пр.), имена и фамилии родственников, номера квартир, документов или телефонов

Пароль должен быть бессмысленным

Не использовать «секретные вопросы», ответы на которые можно легко узнать или подобрать

Необходимо использовать уникальный пароль для каждого отдельного Интернет сервиса, форума, сайта.

Не хранить пароли с помощью встроенных в браузер «хранителей паролей».

Не вводить пароли в посторонних программах, на посторонних сайтах, а также не отсылайте пароли по почте

СПАСИБО ЗА ВНИМАНИЕ!