УДК 004 **Технические науки**

Дьяченко Никита Владимирович, *студент 2 курса по направлению «Информармационная безопансость», Донской государственный технический университет,*
Россия, г. Ростов-на-Дону
Отакулов Артур Собирович, *студент 2 курса по направлению «Информармационная безопансость», Донской государственный технический университет,*
Россия, г. Ростов-на-Дону
Акушуев Рамазан Тахирович, *студент 2 курса по направлению «Информармационная безопансость», Донской государственный технический университет,*
Россия, г. Ростов-на-Дону

ОСОБЕННОСТИ КИБЕРАТАК И ИХ СВОЙСТВА

Аннотация: В данной работе рассматриваются вопросы, касающиеся особенностей кибератак их свойства и принцип работы, а также рассматриваем защиту нападений.

Ключевые слова: информационная безопасность, кибератака, методы защиты информации.

Annotation: this paper deals with issues relating to their principles and principles of work.

Keywords: information security, cyber-attack, information protection methods.

Для защиты активов организации и ИТ-инфраструктуры необходимо иметь представление о том, как злоумышленники думают. Знание того, как проводится атака и какие инструменты используются, поможет составить план защиты. Фактически, многие организации используют те же инструменты, что и злоумышленники, чтобы помочь выявить слабые места, которые им необходимо устранить. Всегда лучше найти слабые места в вашем собственном окружении, чем атакующий, но еще более важно быстро устранить эту слабость [1].

Компьютерные преступники и кибератакеры используют ряд аппаратных и программных средств для обнаружения уязвимостей, которые можно использовать, и других средств для выполнения реальной атаки. Эти инструменты и методы могут включать следующее:

- Протокол анализаторы;
- ОС сканеры отпечатков пальцев;
- Сканеры уязвимостей;
- Использовать программное обеспечение;
- Wardialers;
- Взломщики паролей;
- Клавиатурные шпионы.

Анализаторы протокола

Анализатор протокола или анализатор пакетов (или просто анализатор) - это программа, которая позволяет компьютеру отслеживать и захватывать сетевой трафик, будь то в локальной сети или беспроводной сети. Злоумышленники могут захватывать и взламывать пароли и данные открытого текста. Анализаторы протоколов выпускаются как в версиях аппаратного обеспечения, так и в версиях программного обеспечения, или в комбинации обоих. Снифферы работают в случайном режиме, что означает, что каждый пакет данных может быть просмотрен и перехвачен. Снифферы декодируют фрейм и IP-пакет данных, что позволяет просматривать данные в открытом виде, если они не были зашифрованы.

Сканер портов — это инструмент, который используется для сканирования хостов IP на наличие открытых портов, которые были включены. Думайте о номере порта как о канале, обычно связанном со службой. Например, порт 80 предназначен для веб-трафика HTTP, порт 21 - это протокол передачи файлов (FTP), а порт 23 - это Telnet и т. д. Запрос комментариев (RFC) 1700, который теперь заменен RFC 3232, содержит список наиболее распространенных номеров портов и служб TCP / UDP. Сканеры портов используются для определения открытых портов или приложений и служб, которые включены на хост-устройстве IP. Это дает злоумышленникам ценную информацию, которая может быть использована в атаке [2].

Сканер отпечатков пальцев операционной системы (ОС) представляет собой программное обеспечение, которое позволяет злоумышленнику отправлять различные пакеты на хост-устройство IP в надежде определить операционную систему (ОС) целевого устройства по ответам. В то время как сетевые протоколы, как правило, являются стандартными, различные поставщики операционных систем могут применять их по своему усмотрению. Пакеты, отправленные со сканера отпечатков пальцев ОС, будут распознавать отличия от различных операционных систем, используемых на рабочих станциях, серверах и сетевых устройствах. Когда хост-устройство IP отвечает, сканер отпечатков пальцев ОС может угадать, какая операционная система установлена на устройстве. Когда злоумышленник узнает, какая ОС и версия установлена, у него больше шансов использовать уязвимости и эксплойты программного обеспечения. Уязвимость программного обеспечения - это ошибка или слабость в программе.

Сканер уязвимостей — это программное обеспечение, которое используется для выявления и, по возможности, проверки уязвимостей на хост-устройстве IP. Исходя из этой информации, сканер уязвимостей сравнивает известные уязвимости программного обеспечения в своей базе данных с тем, что он только что обнаружил. Сканер уязвимостей перечисляет все известные уязвимости программного обеспечения и расставляет их приоритеты как критические, основные или второстепенные [3].

Программное обеспечение для эксплойтов — это приложение, которое включает в себя известные программные уязвимости, данные и скриптовые команды, чтобы «эксплуатировать» уязвимости в компьютерной системе или хост-устройстве IP. Это программа, которая может быть использована для осуществления злонамеренных действий. Это включает в себя такие вещи, как атака типа «отказ в обслуживании», несанкционированный доступ, атака с использованием перебора паролей или переполнение буфера. Стоит помнить, что уязвимости программного обеспечения создают слабые места в системе, такие как программная ошибка, сбой или уязвимость.

Злоумышленник будет использовать эксплойт при выполнении оценки уязвимости и интрузивное тестирование на проникновение. Оценка уязвимости может выявить слабость; Тестирование на проникновение положительно подтверждает слабость, работая над тем, чтобы использовать ее. Поэтому навязчивое тестирование генерирует вредоносный сетевой трафик. Тестирование на проникновение - это то, что хакер выполняет, чтобы проникнуть в компьютерную систему или хост-устройство IP. Это может привести к получению доступа к системе, а также к данным, которые являются призом, который ищут большинство хакеров.

Злоумышленник, получив разрешение, проводит тестирование на проникновение, чтобы подтвердить, что обнаруженная уязвимость является законной, что приводит к критическому риску. Затем хакеры рекомендуют способы снижения подверженности риску как часть отчета о посмертном тестировании на проникновение.

Wardialer - это компьютерная программа, ищет компьютер на другом конце. Программа работает, автоматически набирая определенный диапазон телефонных номеров. Затем он регистрирует и вводит в базу данных те номера, которые успешно подключаются к модему. Wardialers становятся все более архаичными и реже используются из-за роста цифровой телефонии, IP-телефонии или Voice over IP (VoIP). До VoIP злоумышленники могли использовать абонентов для получения доступа к телефонным системам АТС, пытаясь

получить тональный сигнал или возможность международного набора для совершения мошеннических звонков. Кроме того, злоумышленник будет использовать Wardialer для идентификации сигналов аналогового модема и получения доступа к удаленной системе в ИТ-инфраструктуре.

Некоторые хранители могут также идентифицировать операционную систему, работающую на компьютере, и проводить автоматическое тестирование на проникновение. В таких случаях Wardialer запускает заранее определенный список общих имен пользователей и паролей в попытке получить доступ к системе.

Злоумышленник может использовать Wardialer для определения потенциальных целей. Если программа не обеспечивает автоматического тестирования на проникновение, злоумышленник может попытаться взломать модем с помощью незащищенных входов в систему или легко взломанных паролей. Администратор сетевой системы может использовать коммерческий Wardialer для идентификации неавторизованных модемов в сети предприятия. Эти неавторизованные модемы могут предоставить злоумышленникам легкий доступ к внутренней сети организации, и их необходимо контролировать или устранять.

Хотя защита от атак является довольно старым методом, он все же полезен для поиска точек доступа к компьютерам. Во многих компьютерных сетях и голосовых системах модемы подключены к телефонным линиям. Эти модемы часто подключаются либо для прямого доступа в целях поддержки, либо людьми, пытающимися обойти ограничения доступа к сети. Даже в современных подключенных к Интернету средах может быть несколько модемов, готовых ответить на другой компьютер, который звонит. Успешное подключение к компьютеру с помощью модема обеспечивает возможную точку доступа к остальной части сети организации.

Целью взлома пароля является раскрытие забытого или неизвестного пароля. Взломщик паролей - это программа, выполняющая одну из двух функций: атака с использованием перебора паролей для получения

несанкционированного доступа к системе или восстановление паролей, хранящихся в криптографическом хеше в компьютерной системе.

Криптографический хеш - это алгоритм, который преобразует большой объем данных в одно (длинное) число. После математического хэширования хэш-значение может быть использовано для проверки целостности этих данных. При попытке взлома пароля методом взлома злоумышленник пробует каждую возможную комбинацию символов, пока «взломанный» пароль не преуспеет в предоставлении доступа. Атаки по словарю - это разновидность атак методом перебора. При атаке по словарному паролю хакеры пытаются использовать более короткие и простые комбинации, включая реальные слова (отсюда и название атаки), потому что такие пароли очень распространены.

Регистратор нажатий клавиш - это тип программного обеспечения или оборудования для наблюдения, которое может записывать в файл журнала каждое нажатие клавиши, которое пользователь нажимает на клавиатуре. Регистратор нажатий клавиш может сохранять файл журнала локально для последующего извлечения или отправлять его указанному получателю. Работодатели могут использовать регистраторы нажатий клавиш, чтобы гарантировать, что сотрудники используют рабочие компьютеры только для деловых целей. Тем не менее, шпионское ПО может также включать программное обеспечение для регистрации нажатий клавиш, в надежде передать информацию, такую как пароль, неизвестной третьей стороне. В качестве аппаратного средства регистратор нажатий клавиш обычно представляет собой штекер размером с батарею, который служит соединителем между клавиатурой пользователя и компьютером.

Библиографический список:

1. Мельников, В.П. Информационная безопасность и защита информации. 3-е изд. Академия. 2008г.

2. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. 2000г.

3. Варлатая, С.К. Аппаратно-программные средства и методы защиты информации. 2007г.