Защита от сетевых атак.

Выполнил: Садирдинов Закиржан П4-Э

- Сетевая атака — это намеренное (возможно, с преступным умыслом) вторжение в операционную систему удаленных или локальных вычислительных сетей. За атаку может быть ответственна как группа злоумышленников, так и отдельное лицо. При помощи специальных инструментов хакер присваивает себе административные права, тем самым получая контроль над системой.Главные цели киберпреступников — дестабилизация работы сайтов и серверов либо их полный вывод из строя, добыча скрытой информации (конфиденциальные данные пользователей, тексты документов).

- Защита КС включает следующие структурные элементы:
- - описание способов профилактики и устранения последствий атак на корпоративную сеть;
- - применяемые базовые принципы защиты информации;
- - методы моделирования угроз;
- - описание ответных действий при атаке;
- - описание процедуры аварийного восстановления;
- - описание сетевых сегментов.

- В этой связи под базовыми принципами защиты информации необходимо понимать следующее:
- **- принцип открытости системы** (использование общепринятых стандартизированных алгоритмов зачастую гораздо лучше и эффективнее, чем использование малоизвестных или самостоятельно разработанных защитных алгоритмов);
- **- принцип простоты** (при взаимодействии с конечным пользователем система защиты должна быть простой, чтобы не создать путаницу; сложные механизмы должны быть отделены от пользователя);
- **- принцип минимальной уязвимости** (в случае если нужно защитить информацию от копирования, нужно просто снять с системных блоков пишущие устройства, а не применять сложных прав доступа к ним);
- **- принцип наименьших привилегий** (по умолчанию все порты и доступ к файлам для пользователей закрыты, сами пользователи разделены на группы и получают минимальных набор прав, необходимый для выполнения их производственных функций);
- -принцип **контроля** (всегда необходимо контролировать состояние системы, поддерживая ее техническое состояние на актуальном уровне, при этом также необходимо контролировать поведение администратора системы с помощью аудита, не забывая, что человек является слабым звеном в системе).

- **Разновидности сетевых атак и методики защиты от них**

- На сегодняшний день известны следующие виды сетевых атак:
- mailbombing;
- применение специализированных приложений;
- переполнение буфера;
- сетевая разведка (сбор сведений при помощи приложений, находящихся в свободном доступе);
- IP-спуфинг (хакер выдает себя за законного пользователя);
- DDOS-атака (путем перегрузки обслуживание обычных пользователей делается невозможным);
- Man-in-the-Middle (внедрение с целью получения пакетов, передаваемых внутри системы);
- XSS-атака (ПК клиента подвергаются атаке через уязвимости на сервере);
- фишинг (обман жертвы путем отправки сообщений с якобы знакомого адреса).
- О первых трех вариантах стоит рассказать отдельно, так как они самые сложные и самые распространенные.

- **Mailbombing**
- Суть действия в том, что e-mail пользователя буквально заваливается письмами. Для этого используется массовая рассылка. Цель — отказ работы почтового ящика или всего почтового сервера.
- Для проведения этой атаки не нужны особые навыки. Достаточно знать электронный адрес потенциальной жертвы и адрес сервера, с которого можно отправлять сообщения анонимно.
- Первое правило защиты, к которому может прибегнуть каждый, — не давать адрес своего почтового адреса сомнительным источникам. Специалисты задают определенные настройки на web-сайте провайдера. Лимит количества писем, поступающих с определенного IP, ограничен. Когда приложение «видит», что число сообщений перевалило предел нормы, письма «на автомате» отправляются в корзину. Но ничто не мешает преступнику проводить рассылку с разных адресов.

- **Специальные программы**
- Использование особых приложений — самый распространенный способ вывода серверов из строя. В ход идут вирусы, трояны, руткиты, снифферы.
- Вирус — вредоносный софт, заточенный на выполнение определенной функции. Внедряется в другие программы (легальные в том числе) на ПК жертвы. После встраивания приступает к осуществлению прописанной «миссии». Например, проводит шифровку файлов, блокирует загрузку компьютерной платформы, прописав себя в BIOS, и т.д.
- «Троянский конь» — это уже не программная вставка, а полноценное вредоносное приложение, которое маскируется под безобидное. Троян может выглядеть, к примеру, как игра. Если пользователь ее запустит, начнется распространение файла. Программа рассылает свои копии по всем электронным адресам, которые есть на ПК жертвы. Чаще всего «троянский конь» похищает данные банковских карт, электронных кошельков — словом, стремится получить доступ к финансовым ресурсам.
- Сниффер ворует пакеты данных, переправляемых ПК на разные сайты. Для этого используется сетевая плата, функционирующая в режиме promiscuous mode. В таком режиме все пакеты, переправленные через карту, отправляются на обработку приложению. Таким образом, может быть открыт доступ к конфиденциальным сведениям — например, списку паролей и логинов от банковских счетов.
- Руткит скрывает следы преступлений злоумышленников, маскирует вредоносную деятельность, из-за чего администратор не замечает происходящего.

- **Переполнение буфера**
- Злоумышленник занят поиском программных или системных уязвимостей. При обнаружении таковых провоцируется нарушение границ оперативной памяти, работа приложения завершается в аварийном режиме, выполняется любой двоичный код.
- Защита состоит в том, чтобы обнаружить и устранить уязвимости. Также используются неисполнимые буфера, но этот метод способен предотвратить только те атаки, в которых применяется код.

Способы защиты от сетевых атак:

1. Двухфакторная аутентификация (2FA):
   Пользователь должен предоставить два различных элемента для подтверждения своей личности, например, пароль и одноразовый код, полученный через SMS, приложение аутентификации или аппаратный токен.
2. Ограничение доступа по IP:
   Разрешение доступа только с определенных, доверенных IP-адресов.
   Логирование и мониторинг попыток доступа.
3. VPN (Виртуальная частная сеть):
   Использование VPN для обеспечения безопасного и шифрованного соединения между удаленными местами и центральной сетью.
4. Обнаружение вторжений (IDS) и Системы предотвращения вторжений (IPS):
   IDS служит для обнаружения аномалий и потенциальных атак.
   IPS предотвращает или ограничивает атаки, обнаруженные IDS.
5. Брандмауэры:
   Конфигурация брандмауэров для фильтрации трафика, разрешая доступ только к необходимым службам и портам.
   Регулярное обновление правил брандмауэра.
6. Регулярные обновления и патчи:
   Установка операционных систем, приложений и аппаратного обеспечения на обновленных версиях.
   Внимательное отслеживание и устранение уязвимостей с использованием последних патчей.
7. Защита от отказа в обслуживании (DDoS):
   Использование технологий DDoS-защиты для обнаружения и отражения атак.
   Распределение нагрузки и использование Content Delivery Network (CDN).
8. Шифрование трафика:
   Использование SSL/TLS для шифрования данных между клиентами и серверами.
   Шифрование хранимых данных.
9. Системы мониторинга и реагирования на инциденты:
   Реализация систем мониторинга, которые непрерывно анализируют трафик и системные журналы на наличие подозрительной активности.
   Разработка плана реагирования на инциденты.
10. Обучение пользователей:
    Обучение сотрудников и пользователей базовым принципам безопасности, таким как управление паролями, осведомленность о фишинге и т.д.

Каждый из этих методов может представлять собой важное звено в общей стратегии кибербезопасности, и их эффективность может быть усилена при их комбинировании.