**УДАЛЕННЫЕ АТАКИ НА ИНТРАСЕТИ**

**Удалённая сетевая атака** — информационное разрушающее воздействие на распределённую вычислительную систему (ВС), осуществляемое программно по каналам связи.

Цель предпринимаемых злоумышленниками атак на компьютеры из интрасетей, подключенных к Интернет, состоит в получении доступа к их информационным и сетевым ресурсам. Примером первого типа ресурсов бывают базы данных, файл-серверы и т.п. Ко второму типу ресурсов относятся сетевые сервисы, к примеру. Интернет. электронная почта͵ телеконференции и т.д.

Принципиальным отличием атак, осуществляемых злоумышленниками в открытых сетях, является фактор расстояния от ПК, выбранного в качестве жертвы, или "прослушиваемого" канала связи до местоположения злоумышленника. Этот фактор нашел выражение в определении подобного вида атак как "удаленных".

Под удаленной атакой принято понимать несанкционированное информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.

Dưới một cuộc tấn công từ xa, thông thường phải hiểu một tác động thông tin trái phép lên hệ thống máy tính phân tán, được thực hiện bằng phần mềm thông qua các kênh liên lạc.

Для удаленной атаки можно выделить наиболее общие схемы их осуществления. Такие удаленные атаки получили название типовых.

Đối với một cuộc tấn công từ xa, các kế hoạch phổ biến nhất để thực hiện chúng có thể được xác định. Các cuộc tấn công từ xa như vậy được gọi là các cuộc tấn công điển hình.

Тогда типовая удаленная атака - это удаленное несанкционированное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной системы. Объектом удаленных атак могут стать следующие виды сетевых устройств: оконечные устройства; каналы связи, промежуточные устройства: ретрансляторы, шлюзы, модемы и т.п. Рассмотрим классификацию удаленных атак по следующим шести основным критериям:

Sau đó, một cuộc tấn công từ xa điển hình là một tác động thông tin trái phép từ xa, được thực hiện bằng phần mềm thông qua các kênh truyền thông và là điển hình cho bất kỳ hệ thống máy tính phân tán nào. Các loại thiết bị mạng sau đây có thể trở thành đối tượng của các cuộc tấn công từ xa: thiết bị đầu cuối; kênh giao tiếp, thiết bị trung gian: bộ lặp, cổng, modem, v.v. Chúng ta hãy xem xét việc phân loại các cuộc tấn công từ xa theo sáu tiêu chí chính sau:

1. По характеру воздействия удаленные атаки делятся на пассивные и активные (примером первого типа атак является, к примеру, прослушивание каналов связи и перехват вводимой с клавиатуры информации; примером второго типа является атака "третий посередине", когда злоумышленник может к примеру, подменять данные информационного обмена между двумя пользователями и/или интрасети или между пользователем и запрашиваемым им сетевым сервисом, пересылаемые в обоих направлениях),

1. Theo bản chất của tác động, các cuộc tấn công từ xa được chia thành thụ động và chủ động (ví dụ về kiểu tấn công đầu tiên là nghe các kênh liên lạc và chặn thông tin nhập từ bàn phím; chẳng hạn, có thể thay thế thông tin trao đổi dữ liệu giữa hai người dùng và / hoặc mạng nội bộ hoặc giữa người dùng và dịch vụ mạng được yêu cầu, được gửi theo cả hai hướng),

2. По цели воздействия, ᴛ.ᴇ. исходя из нарушения трех базовых возможных свойств информации и информационных ресурсов - их конфиденциальности, целостности и доступности, плюс нарушение доступности всей системы или ее отдельных служб (пример атаки - "отказ в обслуживании");

2. Theo mục đích tác động, ᴛ.ᴇ. tiếp tục từ việc vi phạm ba thuộc tính cơ bản có thể có của thông tin và tài nguyên thông tin - tính bảo mật, tính toàn vẹn và tính khả dụng của chúng, cộng với vi phạm tính khả dụng của toàn bộ hệ thống hoặc các dịch vụ riêng lẻ của nó (ví dụ về một cuộc tấn công là "từ chối dịch vụ") ;

3. По условию начала осуществления воздействия атака должна быть безусловной (предпринимается злоумышленником в любом случае), или может активизироваться либо при посылке определенного запроса от атакуемого объекта͵ либо при наступлении ожидаемого события на атакуемом объекте;

3. Theo điều kiện bắt đầu tác động, cuộc tấn công phải được thực hiện vô điều kiện (do kẻ tấn công thực hiện trong mọi trường hợp), hoặc nó có thể được kích hoạt khi một yêu cầu nhất định được gửi từ đối tượng bị tấn công hoặc khi một sự kiện dự kiến ​​xảy ra. trên đối tượng bị tấn công;

4. По наличию обратной связи с атакуемым объектом различают атаки с обратной связью или без обратной связи (такая атака принято называть однонаправленной);

4. Theo sự hiện diện của phản hồi với đối tượng bị tấn công , các cuộc tấn công có phản hồi hoặc không có phản hồi được phân biệt (một cuộc tấn công như vậy thường được gọi là một chiều);

5. По расположению субъекта атаки относительно атакуемого объекта бывают внутрисегментными (средства взлома сети или, к примеру, прослушивания каналов связи должны располагаться в том же сегменте сети, который интересует злоумышленника) или межсегментными (в данном случае дальность расстояния от жертвы до злоумышленника не имеет значения);

5. Theo vị trí của đối tượng tấn công so với đối tượng bị tấn công, chúng nằm trong phân đoạn nội bộ (phương tiện tấn công mạng hoặc, ví dụ, nghe các kênh liên lạc phải được đặt trong cùng phân đoạn mạng mà kẻ tấn công đang quan tâm đến) hoặc đoạn giao nhau (trong trường hợp này, khoảng cách từ nạn nhân đến kẻ tấn công không quan trọng);

6. по уровню эталонной модели взаимосвязи открытых систем 0SI Международной Организации Стандартизации (ISO), на котором осуществляется воздействие. Атака может реализовываться на всех семи уровнях - физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном. Средства обеспечения безопасности интрасетей на базе такой модели регламентируются стандартом ISO7492-2. Эти же рекомендации могут применяться и для разработки, создания аналогичных механизмов в Интернет-сетях, так как группа протоколов ТСР/IР соответствует уровням 1-4 модели, а прикладной уровень в сетях соответствует верхним уровням (5-7).

6. Ở cấp độ của Tổ chức Tiêu chuẩn hóa Quốc tế (ISO), Mô hình Tham chiếu Kết nối Hệ thống Mở 0SI bị ảnh hưởng. Cuộc tấn công có thể được thực hiện ở tất cả bảy cấp độ - vật lý, kênh, mạng, truyền tải, phiên, đại diện và ứng dụng. Các công cụ bảo mật cho mạng nội bộ dựa trên mô hình này được quy định bởi tiêu chuẩn ISO7492-2. Các khuyến nghị tương tự có thể được áp dụng cho việc phát triển và tạo ra các cơ chế tương tự trong mạng Internet, vì nhóm giao thức TCP / IP tương ứng với các mức 1-4 của mô hình và mức ứng dụng trong mạng tương ứng với các mức trên (5 -7).

Среди выше перечисленных УА можно выделить пять базовых и наиболее часто предпринимаемых в настоящее время типовых удаленных атак:

Trong số các AO được liệt kê ở trên, có năm cơ bản và hiện đang được thực hiện thường xuyên nhất các cuộc tấn công từ xa điển hình:

**1. Анализ сетевого трафика**

Анализ сетевого трафика путем его перехвата (сниффинга) является внутрисегментной атакой и направлен на перехват и анализ информации, предназначенной для любого ПК, расположенного в том же сегменте сети, что и злоумышленник. Злоумышленник может захватить все проходящие через себя пакеты путем перевода своей сетевой платы в смешанный режим (promiscuous mode).

Реализация данной атаки позволяет злоумышленнику изучить логику работы сети (для получения информации, помогающей ему осуществить последующий взлом) либо перехватить конфиденциальную информацию, которой обмениваются узлы компьютерной сети. Многие протоколы (например, POP3, FTP и пр.) передают информацию об используемых паролях доступа по каналу связи в открытом виде.

1. Phân tích lưu lượng mạng

Phân tích lưu lượng mạng bằng cách đánh chặn (đánh hơi) là một cuộc tấn công nội bộ và nhằm mục đích đánh chặn và phân tích thông tin dành cho bất kỳ PC nào nằm trong cùng phân đoạn mạng với kẻ tấn công. Kẻ tấn công có thể chiếm đoạt tất cả các gói tin đi qua anh ta bằng cách đặt card mạng của anh ta ở chế độ lăng nhăng.

Việc thực hiện cuộc tấn công này cho phép kẻ tấn công nghiên cứu logic của mạng (để lấy thông tin giúp hắn thực hiện các vụ hack tiếp theo) hoặc đánh chặn thông tin bí mật được trao đổi giữa các nút của mạng máy tính. Nhiều giao thức (ví dụ, POP3, FTP, v.v.) truyền thông tin về mật khẩu truy cập đã sử dụng qua kênh giao tiếp dưới dạng văn bản rõ ràng.

**2. Подмена доверенного субъекта**

Подмена доверенного субъекта и передача сообщений по каналам связи от его имени позволяет получить злоумышленнику доступ к удаленной системе от имени этого доверенного субъекта. Подобные атаки эффективно реализуются в системах с нестойкими алгоритмами идентификации и аутентификации хостов и пользователей. Например, подобные атаки эффективны для систем, использующих аутентификацию источника по его IP адресу, для злоумышленника в этом случае нетрудно формировать пакеты с IP адресами, которым «доверяет» удаленный узел.

2. Thay thế một chủ thể đáng tin cậy

Giả mạo một chủ thể đáng tin cậy và gửi tin nhắn qua các kênh liên lạc thay mặt cho thực thể đáng tin cậy cho phép kẻ tấn công có được quyền truy cập vào hệ thống từ xa thay mặt cho thực thể đáng tin cậy này. Các cuộc tấn công như vậy được thực hiện hiệu quả trong các hệ thống có các thuật toán không ổn định để xác định và xác thực máy chủ và người dùng. Ví dụ, các cuộc tấn công như vậy có hiệu quả đối với các hệ thống sử dụng xác thực nguồn bằng địa chỉ IP của nó; trong trường hợp này, kẻ tấn công không khó để tạo các gói có địa chỉ IP mà máy chủ từ xa "tin cậy".

**3. Введение ложного объекта компьютерной сети**

Реализация данной атаки позволяет навязать ложный маршрут потока информации так, чтобы этот маршрут лежал через компьютер злоумышленника, позволяет «заманить» легального пользователя на ПК злоумышленника (например, подменив WEB-сайт) с целью получения конфиденциальной информации.

3. Giới thiệu một đối tượng mạng máy tính sai

Việc thực hiện cuộc tấn công này có thể tạo ra một lộ trình luồng thông tin sai lệch để lộ trình này nằm qua máy tính của kẻ tấn công, nó cho phép “dụ” người dùng hợp pháp đến PC của kẻ tấn công (ví dụ: bằng cách thay đổi trang WEB) theo thứ tự để có được thông tin bí mật.

**4. Отказ в обслуживании.**

Атака должна быть предпринята͵ если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов. В этом способе проникновения используется возможность фрагментирования пакетов, содержащаяся в спецификации IР. Нападающий передает чересчур много фрагментов пакетов, которые должны быть смонтированы принимающей системой. В случае если общий объём фрагментов превышает максимально допустимый размер пакета͵ то система "зависает" или даже выходит из строя.

4. Từ chối dịch vụ.

Một cuộc tấn công phải được thực hiện nếu không có phương tiện xác thực địa chỉ của người gửi và vô số yêu cầu kết nối ẩn danh có thể được gửi từ máy chủ đến máy chủ bị tấn công thay mặt cho các máy chủ khác. Phương pháp thâm nhập này tận dụng tính năng phân mảnh gói có trong đặc tả IP. Kẻ tấn công đang truyền quá nhiều đoạn gói tin để được hệ thống nhận tập hợp lại. Nếu tổng số lượng mảnh vỡ vượt quá kích thước gói tối đa cho phép, thì hệ thống sẽ "treo" hoặc thậm chí bị treo.

**5. Сканирование компьютерных сетей**

Сетевое сканирование осуществляется злоумышленником на предварительной стадии атаки. Сканирование компьютерной сети позволяет получить злоумышленнику такую информацию, необходимую для дальнейшего взлома, как типы установленных ОС, открытые порты и связанные с ними сервисы, существующие уязвимости. Сам факт сетевого сканирования лишь говорит о реализации стадии, предваряющей атаку, и является важной информацией для сетевого администратора.

5. Quét mạng máy tính

Việc quét mạng được thực hiện bởi kẻ tấn công ở giai đoạn sơ bộ của một cuộc tấn công. Việc quét mạng máy tính cho phép kẻ tấn công có được thông tin cần thiết để tấn công thêm, chẳng hạn như các loại hệ điều hành được cài đặt, các cổng mở và các dịch vụ liên quan cũng như các lỗ hổng hiện có. Thực tế quét mạng chỉ nói lên việc thực hiện giai đoạn trước cuộc tấn công và là thông tin quan trọng đối với người quản trị mạng.

**Технологии обнаружения атак**

Для защиты от анализа сетевого трафика с использованием снифферов известны следующие подходы:

• Диагностика перевода сетевой платы удаленного ПК в смешанный режим путем установки различных средств мониторинга. Данный подход к защите достаточно трудоемок и не является универсальным, поэтому используется недостаточно часто.

• Сегментация сетей - чем больше сегментов, тем меньше вероятность и последствия реализации внутрисегментной атаки.

• Шифрование сетевого трафика и использование безопасных протоколов удаленной аутентификации пользователей (S/KEY, CHAP и др.).

Для защиты от от Подмены доверенного субъекта необходимо применение стойких алгоритмов идентификации и аутентификации хостов и пользователей. Нельзя допускать в компьютерную сеть организации пакеты, посланные с внешних ПК, но имеющих внутренний сетевой адрес.

Для защиты от Введения ложного объекта компьютерной сетинеобходимо использовать более стойкие протоколы идентификации и аутентификации хостов и устройств.

Для защиты от Отказа в обслуживании (DoS) необходимо использовать стойкие протоколы аутентификации, ограничивать доступ в сеть с использованием межсетевых экранов, применять системы обнаружения вторжений, разрабатывать адекватные политики безопасности, использовать для поддержки сервисов программные продукты, в которых устранены уязвимости, позволяющие выполнить подобные атаки.

В настоящее время большую актуальность представляет защита от распределенных DoS атак (DDoS), реализуемых путем заражения («зомбирования») множества ничего не подозревающих ПК, которые в заданный момент времени начинают посылать «шторм запросов» на объект атаки.

Для защиты от сетевого сканирования необходимо применять подходы, позволяющие скрыть внутреннюю структуру сети и идентифицировать факт сканирования, например, использовать межсетевые экраны, системы обнаружения вторжений.

Таким образом, для защиты от рассмотренных выше атак используют:

• Межсетевые экраны;

• Виртуальные частные сети;

• Стойкие протоколы аутентификации;

• Системы обнаружения вторжений;

• Анализ журналов безопасности (аудита) компьютерных систем.