**Лекция №8: Угрозы безопасности в интернете.**

**Цель:** Ознакомить студентов с основными видами угроз безопасности в интернете, проанализировать примеры их проявления в Республике Казахстан, а также сформировать навыки распознавания, предотвращения и реагирования на киберугрозы в онлайн-среде.

**Проявления угроз безопасности в Республике Казахстан**

Помните, как быстро распространилась вредоносная *программа*-червь под названием Code *Red*? Принципом действия этого червя было заражение одного сервера и автоматическое выполнение атак на соседние сервера, с помощью чего он распространился на тысячи и тысячи операционных систем Microsoft. Code *Red* заполнял веб-сервера данными и действовал настолько успешно, что произошло *виртуальное* отключение больших сегментов сети *интернет*, так как сайты переполнились огромным количеством информации, которую они были не в состоянии обработать.

Червь Code *Red* – это лишь один из *множества* примеров, используемых для перегрузки, повреждения или хищения информации с веб-сайтов. Эти угрозы достаточно реальны, и веб-администраторы должны быть готовы к защите своего сайта от возможных атак и к предотвращению их последствий.

#### Источники

Червь Code Red стал ярким примером того, как сильно подвержен сервер различным атакам в интернете. Вы, вероятно, слышали о корпоративном шпионаже, *информационной войне*, кибертерроризме и организованной преступности в сети. Будьте уверены, в интернете существует множество настоящих "плохих парней"!

**Важно**. Угрозы существуют как внутри организации, так и вне ее. Не тратьте много сил и ресурсов на защиту от внешних угроз, не обезопасив себя от потенциальных злоумышленников внутри организации.

Согласно сведениям ФБР *администраторы безопасности* часто не замечают, что компьютерное преступление совершается сотрудниками организации. Недостаточная защита от внутренних угроз может дорого стоить. Представьте себе, что сотрудник, пусть даже случайно, получил доступ с внутреннего сайта к конфиденциальной информации о заработной плате, например, из-за неправильного указания разрешений для каталога. Нужно ли рассказывать о том, какой ущерб может нанести недовольный или нечестный сотрудник, похищающий данные? Несомненно, что угроза бизнесу и потребность в хорошей защите являются серьезной проблемой для внутренней сети.

#### Категории атак

Угрозы безопасности для веб-сайта делятся на несколько категорий атак. Атаки, влияющие на доступность и надежность сайта, называются атаками на отказ в обслуживании (Denial of Service – DoS). Атака Code Red – хороший пример атаки DoS. Другие атаки выполняют действия с содержимым и данными сайта, с их помощью злоумышленники пытаются повредить, похитить, изменить, удалить или разместить информацию на сайте. Такие атаки называются атаками на взлом или крекингом (*cracking*).

Хакерство (*hacking*) – это термин, означающий как атаки DoS, так и атаки на взлом. Для справки ниже приведены определения атак по категориям, взятые из глоссария терминов Администрации национальной безопасности (Natoinal *Security Administration*) (["Приложение А. Источники информации о безопасности"](https://www.intuit.ru/studies/courses/1002/122/lecture/24707)).

* **Denial of Service, DoS** (отказ в обслуживании) – действия, нарушающие функционирование части *автоматизированной информационной системы* в соответствии с определенной целью.
* **Hacking** (хакерство) – несанкционированное использование, попытки обмана или обхода систем безопасности компьютерной информационной системы или сети.
* **Cracking** (крекинг) – акт проникновения в компьютерную систему или сеть.

Термин "атака", как правило, используется для описания хакерских действий. В категории злоумышленных действий "DoS" и "крекинг" входят различные типы атак.

**Совет**. Некоторые работники сферы информационных технологий утверждают, что хакерство значительным образом отличается от крекинга, так как мотивы хакеров (в отличие от крэкеров) не являются вредоносными. Они считают, что хакеры помогают потенциальным жертвам обнаружить пробелы в защите, что позволяет усилить безопасность. Мы согласны с тем, что уровень обеспечения безопасности вырос, так как руководители организаций уделяют больше внимания защите своих продуктов. Мы дали лишь общее определение хакерства, которое, как нам кажется, не подлежит критике.

#### Социальные и физические атаки

Одним из наиболее эффективных методов, применяемых хакерами и крэкерами для проникновения в защищенные паролем системы, является получение конфиденциальных данных от пользователей под видом службы технической поддержки, которая просит сообщить свой пароль. *Социальный инжиниринг* (*social engineering*) – это термин, описывающий данный тип атаки, он основан на управлении личностью человека для достижения своей цели.

Некоторые атаки являются довольно незамысловатыми. Эффективной *DoS-атакой* является отсоединение источника питания системы или разрыв линий коммуникации. Такие атаки называются *физическими атаками* (physical *attack*), так как они направлены на физические компоненты информационной системы.

В некоторых атаках *физический доступ* сочетается с техническими "хитростями". Например, если злоумышленник имеет *физический доступ* к компьютеру, то он может перезагрузить его под другой операционной системой с помощью съемного диска и скопировать данные. Используя беспроводные сетевые технологии, злоумышленники "прослушивают" трафик сетей с помощью радиоприемников.

Сущность защиты от социальных и физических атак довольно проста: размещение компьютеров в безопасных местах и использование *камер видеонаблюдения*. Обучение пользователей и разработка политики безопасности позволят предотвратить социальные атаки. Об этих общих мерах безопасности мы говорить не будем. Тем не менее, проведение формальных процедур максимально снизит вероятность того, что неосторожность или безответственность станут угрозой безопасности.

#### Сетевые атаки

Угрозы и атаки в интернете являются результатами действий злоумышленников, использующих технические стратегии и махинации. Эти атаки наиболее опасны, так как их может осуществить любой пользователь в любой точке мира. Например, червь Red Code появился в Китае, похититель сотен тысяч номеров кредитных карт из CD Universe действовал в России, вирус Мелисса распространен хакером из Нью-Джерси. До сих пор неизвестно (или умалчивается), откуда была осуществлена атака на веб-сайт ЦРУ. Все эти атаки были успешными, хорошо спланированными и широко преданными огласке, они нанесли огромный вред и сильно обеспокоили общественность. Помните, что такие атаки возможны и во внутренней сети!

Сетевые атаки также попадают под категории "DoS" и "крекинг". Они используют ошибки в программном обеспечении, с их помощью блокируют доступ или незаконно проникают в систему. Другие атаки осуществляются через неправильную настройку системы или недосмотр администратора, основываются на захвате управления соединениями или процессами передачи данных. У хакеров имеется множество методов для достижения своих целей (["Удаление, повреждение и отказ в доступе к данным"](https://www.intuit.ru/studies/courses/1002/122/lecture/3519)). Постоянно появляются новые способы реализации атак, что катастрофически усложняет обеспечение безопасности компьютерных систем.

Во многих атаках используются готовые программы, имеющиеся в интернете, позволяющие упростить и автоматизировать атаку, поэтому хакерством занимаются даже малоопытные пользователи. Специалисты утверждают, что большинство хакерских действий осуществляется любителями просто из любопытства или в виде "невинного" озорства. Не исключено, что так оно и есть. Но это не имеет значения, если в результате атаки наносится серьезнейший ущерб или происходит отключение сайта, выполняющего важнейшие деловые операции. Мотивами хакеров также является желание заявить о себе, высказывание своего политического мнения, уклонение от *финансовой ответственности* и жадность. Теперь, после трагедии 11 сентября 2001 г., мы всерьез задумываемся и о проблеме терроризма.

### Задачи безопасности

В обширной, быстро меняющейся и относительно новой среде интернета невозможно обеспечить идеальную защиту. Однако можно снизить *вероятность* серьезных убытков или катастрофических последствий, приняв адекватные меры предосторожности. Если организация правильно защищена, то всегда возможно ее восстановление. Потенциальные потери сводятся к минимуму, если разработан план решения подобных проблем.

Отсюда следует, что обеспечение безопасности включает в себя три основные задачи.

* **Предотвращение** – создание защитных процедур и защищенной веб-среды, предотвращающей попытки вторжения злоумышленников и снижающей потенциальный риск или потери.
* **Обнаружение** – отслеживание действий, выполняемых в интернете, для немедленного выявления изменений в событиях, связанных с безопасностью.
* **Реагирование** – выполнение мероприятий по контролю или пресечению вредоносных действий при обнаружении атаки или вторжения.

Организации необходимо иметь также план восстановления, включающий наличие дублирующих систем и изолированных резервных копий.

### Стратегии взломщиков

Если знать методы хакеров и использование ими недостатков систем, то можно реализовать разумные решения по обеспечению безопасности. Большая часть атак направлена на слабые места оборудования, программно-аппаратных средств, операционных систем, сетевых служб и приложений. Компоненты, так или иначе связанные с интернетом, подвергаются угрозам из-за недостатков в устройствах.

В [таблице 1.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3517?page=2" \l "table.1.1) приведен краткий перечень целей хакеров и типов атак. Как видите, в каждой из категорий могут использоваться *DoS-атаки* или крекинг для доступа к сайту, нарушения его конфиденциальности, повреждения его содержимого. Этот перечень не является исчерпывающим, но дает *представление* о степени серьезности описываемых угроз.

**Совет**. Для получения подробной информации об уязвимости программного обеспечения интернета и оборудования обратитесь к книге "*Hacking* Exposed: *Network Security* *Secrets* and Solutions" S. McClure, J. Scambray, G.Kurtz, McGraw-Hill/Osborne.

|  |  |  |
| --- | --- | --- |
| Таблица 1.1. Основные цели и методы атак | | |
| **Цель** | **Тип атаки** | **Метод** |
| Основные цели и методы атак | Взлом таблиц маршрутизаторов | Сканирование файлов маршрутизатора для получения информации о сети, необходимой для реализации атак, или *изменение записей* в файлах маршрутизатора для нарушения работы сети. |
| Флудинг (перегрузка) узлов, маршрутизаторов или сетевых экранов | Перегрузка сетевых экранов или серверов для замедления их работы или полной остановки из-за обработки огромного количества информации. |
| Сниффинг (прослушивание) | Использование программного обеспечения для прослушивания сетевого интерфейса клиента, сервера или канала передачи пакетов, интересующего злоумышленника. |
| Спуфинг (подмена пользователя) | Осуществление действий под видом пользователя (как правило, используется применительно к IP-адресам). |
| Атаки на серверы | Взлом учетных записей и паролей операционной системы | Использование учетных записей, оставленных открытыми для доступа из интернета, в операционной системе веб-сервера и/или осуществление попыток угадывания пароля учетной записи для получения доступа к сетевым ресурсам узла. |
| Переполнение буфера | Возникновение переполнения системной памяти и реализация возможности хакера передать системе инструкции для запуска другой программы, позволяющей осуществить доступ в систему. |
| Расшифровка URL | Получение информации о настройках веб-сервера с помощью ошибки, генерирующей некорректный URL, для идентификации и проникновения в директории с файлами. |
| *Маскарад* | Разновидность подмены пользователя, основанная на имитации его поведения. |
| Захват | "Похищение" соединения пользователя после его легального входа в систему. |
| Атаки на содержимое и информацию | Повреждение отображаемого на веб-сайте содержимого | Получение доступа к веб-содержимому с его последующим изменением и повреждением. |
| Нарушение конфиденциальности | Получение доступа к частной или конфиденциальной информации, представляющей *государственную тайну*, коммерческие секреты или личные данные. |
| Удаление файлов | Нарушение безопасности файловой системы и удаление информации с накопителя. |
| Атаки на финансовые средства | Мошенничество | Проникновение посредством незаконной аутентификации в одной учетной записи для перемещения финансовых средств в другую учетную запись. |
| Аннулирование транзакции | Получение несанкционированного доступа к системе и удаление записи о подтверждении коммерческой транзакции. |

Сегодня *информация* о многочисленных методах атак и их целях доступна каждому. Основной трудностью, с которой сталкиваются пользователи при разработке методов защиты, является то, что в любой технологии, программном или аппаратном продукте, предназначенном для работы в сети или для поддержки веб-сайта, имеются потенциально уязвимые места.

### Взаимосвязь аспектов безопасности

Многие атаки направлены на сетевые маршрутизаторы и операционные системы, а не только на *приложение* веб-сервера. *Internet* *Information* *Server* 5 полностью интегрирован с *Windows 2000*, и если речь идет о его безопасности, подразумевается также и *безопасность* самой операционной системы *Windows 2000*. Имеют *место* атаки на сетевые устройства и на инфраструктуру сети, например, на сетевые экраны, маршрутизаторы, серверы или клиенты. *Уязвимость* этих устройств представляет собой брешь в периметровой защите, открывающей *доступ* к важной информации сайта.

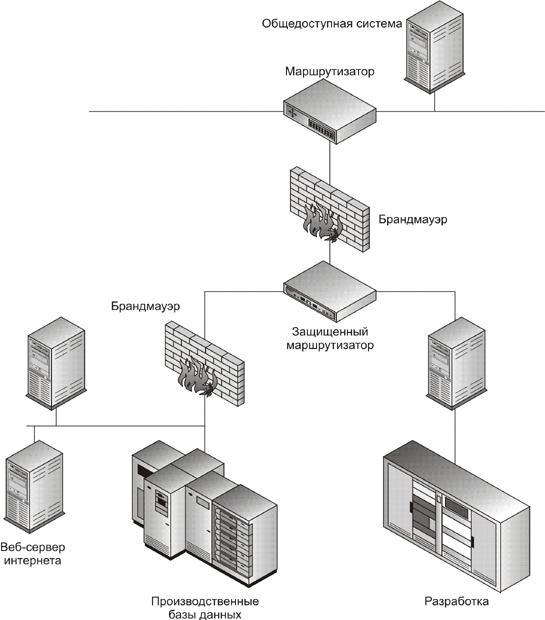
**Важно**. Мощность систем безопасности измеряется стойкостью их уязвимых мест. Веб-содержимое не является единственным ресурсом, подвергаемым риску в случае слабой системы защиты. В сети лучше всего применять различные меры и средства обеспечения безопасности. В ["Особенности процесса разработки"](https://www.intuit.ru/studies/courses/1002/122/lecture/3527)будет рассказываться об усилении безопасности сервера с помощью средств периметровой защиты.

#### Примеры уязвимых мест

Все компьютерные системы зависят друг от друга, и это обстоятельство обуславливает высокий уровень безопасности сети. Сеть становится уязвимой из-за дефекта, ошибки или недосмотра в настройках веб-сервера IIS. На [рисунке 1.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3517?page=2" \l "image.1.1) показана конфигурация сети, объясняющая некоторые сценарии развития подобных событий.

#### Открытый порт равносилен открытой двери

Сетевые экраны (firewalls) или брандмауэры защищают внутренние ресурсы, маскируя реальные IP-адреса компьютеров и блокируя попытки доступа к сети, инициированные извне, если только внешний пользователь не является законным и авторизованным сотрудником организации. Возможно нарушение безопасности веб-сервера при работе в интернете. В этом случае брандмауэр настраивается на предоставление канала для проникновения трафика только на веб-сервер. К сожалению, при слабой защите операционной системы Windows или веб-сервера открытие порта позволит опытному хакеру получить информацию о сетевых адресах, пользователях и директориях, которая позволит ему атаковать другие компьютеры сети.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/1/files/01_01.gif)

**Рис. 1.1.**Типичная конфигурация сети с веб-сайтом, имеющим базу данных

#### Проблема. Веб-приложения влияют на уровень безопасности базы данных

Еще раз обратите внимание на [рис. 1.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3517?page=2" \l "image.1.1). Веб-сайт *подключен к базе данных* организации (этот подход применяется на серьезных сайтах, что позволяет клиентам искать товары в каталогах или отправлять личные данные по запросу компании). Следовательно, веб-сайт подвергает базу данных риску, если он недостаточно защищен. Веб-сайты IIS нередко обеспечивают взаимодействие базы данных и клиента в интерактивном режиме посредством страниц Active Server Page (ASP). Эти страницы содержат программы для отображения полей поиска или форм для заполнения, которые преобразуют введенные данные в формат *структурированного языка* запросов SQL, используемого при отправке сообщений в базу данных или запросов на получение информации. Если хакер получит доступ к этой программе, он сможет создавать SQL-сообщения для просмотра или *изменения записей* в базе данных.

**Совет**. Будьте внимательны! Не оставляйте на сайте уязвимые места, через которые будут атакованы другие системы. Изучите как можно больше информации, связанной с потенциальными угрозами, для построения достойной системы защиты.

#### Политика безопасности

Помимо веб-сервера в сети присутствуют другие компьютеры, поэтому обеспечение безопасности включает в себя совместные действия всех сотрудников организации, управляющих различными системами.

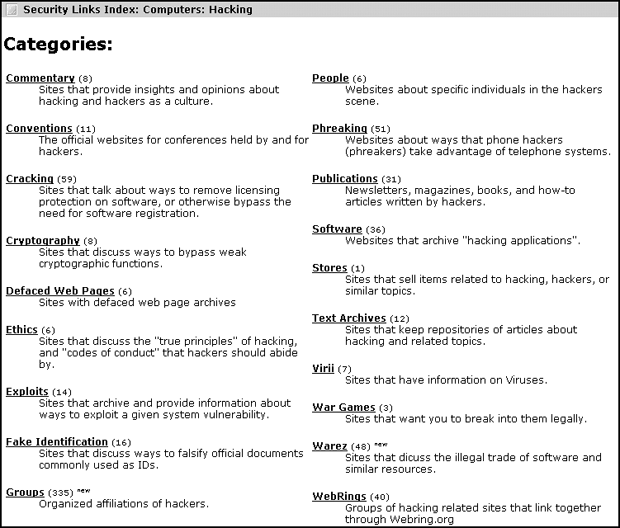
Нет никакого сомнения в том, что ни одна организация, обладающая большими информационными ресурсами, не обеспечит безопасность своей сети без применения политики безопасности, профилактических процедур и контрольных таблиц. В качестве защитника веб-безопасности вы должны обеспечить стабильность своей части этой политики, сделать ее руководством к действию для сотрудников и пользователей веб-платформы.

### Методология взлома

Первое, что необходимо знать про хакеров, – это то, что они хорошо вооружены. Многие хакеры осуществляют расширенные исследования, занимаются *самообучением*, экспериментируют с известными дефектами в популярных компьютерных программах и открывают в них новые "бреши".

Серьезные взломщики распространяют свои знания среди менее опытных хакеров, публикуя в интернете статьи, сообщения в новостях, технических форумах и конференциях, передавая информацию "из уст в уста". Большая часть информации представляет собой совершенно законные исследования, проводимые в "мирных" целях. Но разве можно быть уверенным в правильном использовании этой информации?

На [рисунке 1.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3517?page=3" \l "image.1.2) изображена страница, взятая из сайта о хакерстве Antionline.*com*, со списком доступных информационных ресурсов на тему взлома.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/1/files/01_02.gif)

**Рис. 1.2.**Страница, взятая с сайта Antionline

Находясь в обществе хакеров, взломщики имеют *доступ* к большому числу инструментов взлома и сценариев, значительно упрощающих их действия. Microsoft *IIS*, *Windows 2000* и *Windows* XP представляют собой удобные цели, поэтому многие инструменты взлома направлены именно на эти платформы. Они автоматически находят доступные компьютеры, взламывают пароли, прослушивают сетевые пакеты и используют известные уязвимые места.

#### Универсальные методы атак

Хакеры осуществляют атаки широкого диапазона действия (универсальные атаки), т.е. направленные не на конкретную организацию, а на большое число потенциальных жертв.

Вирусы и черви попадают под категорию универсальных атак. Они направлены на различные объекты и действуют случайным образом, используя для самораспространения электронную почту и нанося значительный вред. Вирусы и черви подробно описываются в ["Удаление, повреждение и отказ в доступе к данным"](https://www.intuit.ru/studies/courses/1002/122/lecture/3519).

При взломе используются универсальные подходы. В начале своих действий хакер нацеливается на большую группу объектов, после чего концентрирует усилия на объекте, имеющем уязвимые места. Разумеется, если атака выполняется из внутренней сети, выбор ее целевых объектов не будет случайным.

##### Предварительное исследование

Хакер начинает атаку с выполнения тестового опроса (ping), используя автоматизированную программу, отправляющую ping-запросы по большому числу IP-адресов для получения ответов от каких-либо узлов. При отсутствии адекватной защиты веб-сайт станет жертвой, если отправит ответ на ping-запрос. При получении ответа следующим шагом хакера будет запуск инструмента, определяющего операционную систему компьютера-респондента. После этого он узнает уязвимые места потенциальной жертвы, так как эту информацию легко найти в литературе, посвященной взлому.

##### Сканирование

После нахождения потенциальной жертвы хакер осуществляет сканирование для обнаружения на атакуемом компьютере доступных служб. С помощью инструмента, основанного на протоколах Internet Transaction Control Protocol (ITCP) и User Datagram Protocol (UDP), можно определить, выполняются ли в системе службы *Hypertext Transfer Protocol* (HTTP), Simple *Network Management* Protocol (SNMP), *Post Office Protocol* (POP) или File Transfer Protocol (FTP).

Получив информацию посредством ping-запросов и сканирования, хакер применяет целый набор инструментов, нацеленных на определенные уязвимые места, для осуществления *DoS-атаки*. Если хакер выяснил адрес и имя одного из серверов, то он попытается использовать крекинг для проникновения в систему. Например, начнет проверку учетных записей, используя автоматизированные словари паролей, чтобы угадать один из них. Он может выполнить атаку на переполнение буфера посредством отправки большого количества данных, содержащих программу типа "троянский конь", которую нужно разместить в этой информационной среде.

##### Инструменты

Методы разведки и сканирования показывают, что можно стать жертвой хакера, который затратил совсем немного времени и усилий на подготовку к атаке. Инструменты взлома выполняют за хакера всю основную работу.

**Совет**. Опытные хакеры презрительно относятся к хакерам-любителям, так как любители беспрепятственно пользуются программными продуктами, на создание которых было затрачено много усилий со стороны "продвинутых" взломщиков.

В [таблице 1.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3517?page=3" \l "table.1.2) приведен краткий перечень некоторых универсальных средств и инструментов сканирования, используемых хакерами. Косвенно они являются и средствами защиты в случае их использования для выявления слабых мест системы. Некоторые инструменты взлома основаны на платформе UNIX, что устраивает многих хакеров. В ["Жизненный цикл управления безопасностью"](https://www.intuit.ru/studies/courses/1002/122/lecture/3529)обсуждается использование средств Windows для проведения экспериментов, направленных на выявление "прорех", прежде чем их обнаружит злоумышленник.

|  |  |  |
| --- | --- | --- |
| Таблица 1.2. Универсальные инструменты хакера | | |
| **Наименование** | **Цель** | **Адрес** |
| fping (Unix) Grim's Ping (Win 2000) | Отправка одиночных ping-запросов или параллельная отправка массовых ping-запросов циклическим образом | [http://www.fping.com](http://www.fping.com/" \t "_blank) [http://www.networ-kingfiles.com//PingFinger/Grimsping.htm](http://www.networ-kingfiles.com/PingFinger/Grimsping.htm" \t "_blank) |
| Nmap | Сканирование сети для определения доступных систем и служб, используемых операционных систем | [http://insecure.org/nmap/](http://insecure.org/nmap/" \t "_blank) |
| Winscan | Сканирование портов TCP и UDP, обнаружение и отслеживание служб, работающих в системах Windows NT 4.0 и Windows 2000. | [http://www.prosolve.com/software/](http://www.prosolve.com/software/" \t "_blank) |
| LC3 (LOphtcrack) | Получение паролей из отдельных рабочих станций Windows NT и Windows 2000, сетевых серверов, главных контроллеров домена или из программы Active Directory | [http://www.@stake.com](http://www.@stake.com/" \t "_blank) |
| Nessus | Аудит сети и определение всех уязвимых мест защиты, запуск эксплоитов, отчет об успехе работы каждого эксплоита | [http://www.nessus.org](http://www.nessus.org/" \t "_blank) |
| Ethereal | Этот сниффер Ethernet прост в использовании и предназначен для интерактивного просмотра захваченных данных, вывода отчета и подробной информации о каждом пакете данных | [http://www.ethereal.com](http://www.ethereal.com/" \t "_blank) |
| *Whois* | Утилита, определяющая веб-адрес и адрес сервера хранилища учетных записей домена, в котором содержится полная контактная информация | [http://www.internic.net/whois.html](http://www.internic.net/whois.html" \t "_blank) |

#### Методы направленных атак

В отличие от универсальной атаки направленная атака (targeted *attack*) нацелена на конкретную организацию. С ее помощью хакер осуществляет ряд подготовительных действий и исследований перед нанесением основного удара. Взломщик, целью которого является ваша сеть, использует различные инструменты универсальных атак, но в этом случае атака планируется и производится в несколько этапов, с особой осторожностью, не обнаруживая разведывательных действий, направленных на сбор информации, которая поможет реализовать атаку.

##### Сбор базовых сведений

Хакеры называют процесс сбора информации о сети-жертве *сбором базовых сведений* (футпринтингом, от англ. footprinting). Этот процесс начинается с таких тривиальных вещей, как копание в мусорных корзинах, в которые выбрасываются ненужные документы, или с попыток социального инжиниринга, направленных на выяснение архитектуры сети организации. Здесь годятся любые методы, с помощью которых хакер обеспечит себе хорошую базу, от которой оттолкнется при планировании атаки. Если взломщиком является пользователь рассматриваемой сети-жертвы, то у него, возможно, уже имеется необходимая информация.

Если внешний хакер руководствуется конструктивным подходом, он систематически добывает информацию, которая поможет ему получить нужные сведения. Такой метод является асимптотическим. Взломщик использует тесты и инструменты для сбора информации и раскрывает столько неизвестных параметров (например, сетевых адресов), сколько нужно для перехода к следующему этапу атаки.

##### Составление перечня параметров

На этапе выяснения структуры сети хакер получает информацию о домене и сетевых адресах, контролируемых организацией-жертвой, выполняя запросы баз данных домена верхнего уровня Internet *Whois* или Domain Name Service (DNS). Эти структуры позволяют находить серверы сети-жертвы с помощью веб-браузеров и почтовых клиентов. Таким образом, хакер получит ссылки на любой открытый IP-адрес, используемый компанией для серверов интернета или электронной почты. С помощью бесплатных или платных программ хакер сможет выяснить адреса и диапазоны IP-адресов, доступных в организации, а также провести довольно сложные исследования по определению адресов других узлов в сети-жертве.

##### Зондирование

Имея на руках определенный набор IP-адресов, хакер проводит зондирование целевого объекта, сканируя его для получения дополнительной информации. Взломщики обычно используют инструмент для выдачи тестовых ping-запросов (чтобы выяснить, какие системы находятся в рабочем состоянии), инструмент для определения используемых операционных систем, а также средство сканирования портов для выявления служб, работающих на узле. В качестве альтернативы используется комплексное автоматизированное средство, такое как Nmap, однако взломщик, соблюдающий осторожность, предпочтет остаться незамеченным, используя более деликатный подход.

##### Эксплоиты

После успешного исследования целевых узлов хакер инициирует атаку с помощью специальной программы-эксплоита (exploit). Если целью атаки является отказ в обслуживании, то результат, скорее всего, не заставит себя долго ждать. В противном случае хакер запустит программу крекинга или переполнения буфера, которая позволит ему проникнуть в систему. Иногда хакер использует веб-сайт в качестве отправной точки для проникновения в другую систему. Интернет-атака, направленная на базу данных, является примером такой атаки.

Хорошо спланированная направленная атака более сложна, нежели среднестатистическая универсальная атака. Нередко первое проникновение хакера в систему является лишь этапом сложного плана по длительному нахождению в системе-жертве. По этой причине среди хакеров распространено размещение в системе программы типа "троянский конь" или "черный ход" для захвата данных и упрощения повторного проникновения в систему.

##### Методы скрытия

Опытные хакеры, особенно те, кто осуществляет атаки с целью финансовой выгоды, стараются скрыть свое присутствие и "замести следы". Они выполняют сканирование, ускользая от внимания сетевых администраторов и систем обнаружения вторжений (IDS). После успешного завершения нужных действий взломщики скрывают следы своего присутствия, удаляя записи в журналах и редактируя протокол аудита. Нужно ли говорить о том, насколько трудно защищаться от атак, когда вы даже не подозреваете о них?

### Перечень угроз

Можно ли уберечь себя от атаки хакера? Возможно, что нет. Если организация добилась успеха в своей сфере деятельности, и ее *корпоративная сеть* подключена к интернету, то она является "лакомым кусочком" для взломщиков. Однако можно усложнить задачу хакеров. О том, как это сделать, рассказывается далее.

Ниже приведен перечень угроз, о которых шла речь в данной лекции.

* Категории атак:
  + отказ в обслуживании;
  + хакерство (несанкционированное проникновение в систему);
  + взлом защиты (крекинг).
* Цели атак:
  + вывести из строя или проникнуть в инфраструктуру сети;
  + захватить управление серверами;
  + получить доступ к конфиденциальной информации или уничтожить содержимое;
  + похитить ресурсы или средства, отменить транзакции.
* Методология хакерства:
  + случайный поиск или разведка для определения жертв;
  + сбор базовых сведений;
  + создание перечня параметров;
  + зондирование;
  + выполнение эксплоита;
  + сокрытие действий.

Вопросов для закрепления

1. Какие существуют основные виды угроз безопасности в интернете?
2. В чем заключалась особенность распространения червя Code Red?
3. Что такое атака типа DoS и каковы ее последствия?
4. Объясните разницу между терминами **"хакерство"** и **"крекинг"**.
5. Приведите примеры социальных и физических атак.
6. Какие атаки могут быть осуществлены через внутреннюю сеть организации?
7. Почему внутренние угрозы считаются не менее опасными, чем внешние?
8. Приведите примеры проявлений интернет-угроз в Республике Казахстан.
9. Как организации в Казахстане могут повысить уровень защиты от кибератак?
10. Почему важно учитывать внутренние угрозы в казахстанских компаниях?
11. Какие меры предосторожности можно предпринять для предотвращения атак на веб-сайты?
12. Что может произойти, если веб-сервер подключен к базе данных и при этом не защищен должным образом?
13. Почему "открытый порт" называют "открытой дверью" в системе безопасности?
14. Как хакеры используют предварительное сканирование и ping-запросы для планирования атак?
15. Какие универсальные инструменты используют хакеры для атак? Назовите не менее двух.
16. Какую роль играет брандмауэр в защите сети?
17. Согласны ли вы с утверждением, что некоторые хакеры помогают улучшать системы безопасности? Почему?
18. Насколько эффективно использование политики безопасности и контрольных таблиц в организациях?
19. Как вы считаете, почему хакерские атаки стали глобальной угрозой? Приведите примеры.
20. Что важнее: предотвращение атак или быстрое реагирование на них? Обоснуйте ответ.