Антон Белый

***1) Как работает вирус троян (каким образом он получает информацию о введённых ключах авторизации)?***

Троянская программа — вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Существуют Password Trojans. Эти трояны находят на вашем компьютере пароли и отправляют их хозяину. Нет разницы, какой пароль, будь то интернет пароль, пароль от почтового ящика, этот троян найдет все эти пароли. Keyloggers трояны очень просты в использовании. Они записывают все, что было набрано на клавиатуре (включая пароли) в файл и впоследствии отправляют это все по электронной почте хозяину. Keylogger-ы обычно занимают мало места, и могут маскироваться под другие полезные программы, из-за чего их бывает трудно обнаружить. Некоторые трояны этого типа могут выделять и расшифровывать пароли, найденные в специальных полях для ввода паролей. Обычно информация с паролями отсылается хозяину трояна по электронной почте.

***2) Назовите самое примитивное устройство, с которого можно взломать компьютерную сеть.***

Компьютер. Сначала проводится предварительным сбор всей информации о заинтересовавшей цели: определение доменных имен, адресов сетей и отдельных компьютеров.

Для поиска информации о своей будущей жертве киберпреступник использует открытые источники в Internet:

· адреса и места расположения офисов на Web-узлах;

· информацию о деловых партнерах;

· номера телефонов;

· контактную информацию и номера электронной почты.

Получить такую открытую информацию можно, воспользовавшись поисковыми системами Internet. Защититься от получения киберпреступниками данного вида информации невозможно так, как она является общедоступной, необходимой для функционирования той или иной организации. Однако, следует как можно меньше предоставлять личной и контактной информации в Internet. Установив адреса или доменные имена компьютеров организации-жертвы, киберпреступник переходит к зондированию компьютерной сети, т. е. определению компьютеров, подключенных в данный момент к Internet. Эти операции киберпреступник может производить с использованием программ traseroute, Visual Route, Neo Trace. Если при зондировании киберпреступник установит, что на пути к сети установлен аппаратный брандмауэр или маршрутизатор (отдельное сетевое устройство или компьютер-шлюз), или программный файерволл, то он постарается найти в них уязвимость с использованием такой многофункциональной утилиты как Nmap (Network Mapper). После предварительного сбора информации киберпреступник переходит к сканированию сети, т. е. определению ее топологии с использованием таких утилит как ping, icmpenum и др. Далее идет процесс определения открытых портов в системе. ля этих целей злоумышленник использует вышеназванную утилиту Nmap, утилиты Super Scan, Ip Eye. Он может также воспользоваться и так называемым «швейцарским армейским ножом» - утилитой Net Cat (имя файла которой nc.exe?!!!). Защититься от сканирования сети можно, применив системы выявления вторжений, жестко установив списки доступа на брандмауэрах. Собрав досье на сеть, киберпреступник переходит к инвентаризации пользовательских ресурсов и учетных записей. Подобные операции можно совершить, воспользовавшись Win2K Resource Kit, а также встроенными командами системы, такими как net view, nbtstat и др. Для выполнения вышеуказанных действий могут использоваться утилиты epdump, enum, SMBGrind, L0phtCrack (LC4),Grinder, Legion и NAT, написанные хакерами группы Rhino9. Если все прошло удачно, т. е. киберпреступник нашел уязвимости в компьютерах сети и воспользовался ими, он получил доступ в сеть. Но теперь ему необходимо закрепиться в сети, расширить свои привилегии, чтобы использовать ресурсы сети не один раз. Для этого киберпреступник использует такие утилиты как регистраторы нажатий клавиш – Invisible Key Logger Stealth (IKS), анализаторы сетевых пакетов – снифферы – BUTTSniffer, NetXRay, утилиты перенаправления портов – fpipe. После того, как киберпреступник стал «главным» в компьютерной сети, он попытается скрыть факт своего присутствия и оставить потайной ход. Для этого он может воспользоваться как встроенными командами операционных систем – attrib +h, так и утилитами Win2K Resource Kit, может использовать наборы «отмычек» - rootkit, и программу eLiTeWrаp, позволяющая объединять несколько программ для асинхронного и незаметного выполнения. Также может использовать программы удаленного администрирования – так называемые «троянские кони» - Net Bus, Sub Seven, Back Orifice, может воспользоваться методами туннелирования (DNS, HTTP,SNMP), а также утилитами из пакета Win2K Resource Kit, и программу eLiTeWrAp, позволяющую объединять несколько программ для асинхронного и незаметного выполнения. Защитой от сокрытия следов киберпреступником может служить использование программ, подсчитывающих контрольные суммы файлов, ведение журналов регистрации событий, применение обновлений системы и антивирусных баз. И в завершение своего преступного деяния киберпреступник должен убедиться, что проделанная им работа не пропадет, а для этого ему в большинстве случаев, необходимо перегрузить операционную систему компьютера-жертвы. Для этой цели киберпреступник приводит систему в состояние DoS ( Denied of Service) путем «бомбардирования» компьютера пакетами ICMP (Smarf-атака) или UDP (Fraggle- атака) с использованием усиливающей сети. Это лишь приблизительный сценарий взлома компьютерной сети, хотя в реальной жизни он вполне возможен и осуществим.

***3) Какое самое масштабное преступление, связанное с хакерством?***

Самый известный и, несомненно, самый одарённый хакер в истории - Кевин Митник. В 1983 году Митник добился своего первого большого успеха - получил незаконный доступ к компьютеру Пентагона, за что и был впервые арестован. Неоднократно совершённые преступления вынудили ФБР начать на него "охоту". В 90-е гг. Кевин Митник был приговорён к пяти годам тюремного заключения, а ныне является консультантом по компьютерной безопасности. Самый большой успех пришёл к Кевину Митнику в 1983 году, когда он совершил поистине впечатляющее деяние. В то время он был студентом южнокалифорнийского университета. Используя один из университетских компьютеров, возможно, TRS-80 с 1,77-МГц процессором Zilog, Митник проник в глобальную сеть ARPANet, являющуюся предшественницей Internet, которая в то время была предназначена для военных целей и объединяла крупные корпорации и университеты. Проникнув в эту сеть, Митник добрался до самых защищённых компьютеров того времени, до компьютеров Пентагона. Он получил доступ ко всем файлам Министерства обороны США. В то время не было никаких следов кражи информации или порчи: Митник действовал просто из любопытства и проверял свои способности.

Но один из системных администраторов обнаружил акт вторжения и поднял тревогу. Расследование выявило автора атаки, и Кевина Митника арестовали прямо на территории университета. Он был осуждён и отбыл своё первое настоящее наказание за незаконное вторжение в компьютерную систему, проведя полгода в исправительном центре для молодёжи.

Компьютерная система Пентагона была взломана российскими хакерами, получившими доступ к личной переписке сотрудников ведомства. Эксперты напоминают, что США не в первый раз обвиняет Россию в организации кибератак на свои госструктуры и полагают, что содержание переписки может представлять ценность для разведывательных ведомств. Неизвестные российские хакеры совершили «сложно организованную кибератаку» на компьютерную систему Пентагона, сообщает телеканал NBC News со ссылкой на американских чиновников.

Сама атака была совершена еще 25 июля. Злоумышленники взломали незасекреченную систему обмена электронной почтой и получили доступ к данным около 4 тыс. военных и гражданских сотрудников Объединенного комитета начальников штабов (ОКНШ) — аналога российского Генштаба. В результате в руках киберпреступников оказалась рабочая переписка по электронной почте, которая в Пентагоне не считается секретной. Кроме того, хакеры наверняка просмотрели и личные данные ряда сотрудников.

Сразу после того, как факт взлома был установлен, Пентагон отключил часть системы внутренней почты. В то же время американские чиновники подчеркнули, что хакерская атака никак не затронула секретную информацию. При этом у правительства США пока нет оснований утверждать, что нападение было санкционировано российскими властями, и дальнейшее расследование должно выявить, была ли атака проведена независимыми хакерами. Ведущий вирусный аналитик ESET Russia Артем Баранов полагает, что любая система может иметь уязвимости, которые в свою очередь могли использоваться злоумышленниками для проникновения. В то же время эксперт отметил, что секретная информация хранится в зашифрованном виде, так что хакеры вряд ли получили доступ к особо ценным материалам.

Свят Щавровский

***4) Популярно ли хакерство сейчас?***

***5) Как вы относитесь к хакерам?***

Прямого не имею.

Положительно (мнение), если это не касается использования навыков в преступлениях.

***6) Что такое DDoS-атака?***

***24) Что такое DDoS-атаки? (Гетьман)***

***18) Какие существуют способы защиты от DDoS аттак? (Трубач)***

DoS (от англ. Denial of Service — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик. Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищённой крупной компании или правительственной организации. Особенностью данного вида компьютерного преступления является то, что злоумышленники не ставят своей целью незаконное проникновение в защищенную компьютерную систему с целью кражи или уничтожения информации. Цель данной атаки - парализовать работу атакуемого веб-узла.

Схематически DDoS-атака выглядит примерно так: на выбранный в качестве жертвы сервер обрушивается огромное количество ложных запросов со множества компьютеров с разных концов света. В результате сервер тратит все свои ресурсы на обслуживание этих запросов и становится практически недоступным для обычных пользователей. Циничность ситуации заключается в том, что пользователи компьютеров, с которых направляются ложные запросы, могут даже не подозревать о том, что их машина используется хакерами. Программы, установленные злоумышленниками на этих компьютерах, принято называть "зомби". Известно множество путей "зомбирования" компьютеров - от проникновения в незащищенные сети, до использования программ-троянцев. Пожалуй, этот подготовительный этап является для злоумышленника наиболее трудоемким. Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую архитектуру, которую называют "кластер DDoS". Такая иерархическая структура содержит:

* управляющую консоль (их может быть несколько), т.е. именно тот компьютер, с которого злоумышленник подает сигнал о начале атаки;
* главные компьютеры. Это те машины, которые получают сигнал об атаке с управляющей консоли и передают его агентам-"зомби". На одну управляющую консоль в зависимости от масштабности атаки может приходиться до нескольких сотен главных компьютеров;
* агенты - непосредственно сами "зомбированные" компьютеры, своими запросами атакующие узел-мишень.

Другая опасность DDoS заключается в том, что злоумышленникам не нужно обладать какими-то специальными знаниями и ресурсами. Программы для проведения атак свободно распространяются в Сети. Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределённых бот-сетей.

В основном защита от DoS-атак строится на правильной настройке компьютера. Следующие меры защиты способны защитить лишь от слабых DoS-атак, либо они будут использоваться в качестве снижения её эффективности.

Защита от основных видов DoS-атак

Универсальные советы

* Также есть несколько универсальных советов, которые помогут подготовить систему к DoS-атаке.
* Все серверы, которые имеют доступ во внешнюю сеть, должны быть подготовлены к удаленной аварийной перезагрузке. Также желательно наличие второго сетевого интерфейса, через который по ssh-соединению можно быстро получить доступ к серверу.
* Программное обеспечение, которое установлено на сервере, должно быть в актуальном состоянии, а именно: должно быть установлено последнее ПО, касающееся обеспечения безопасности системы.
* Все сетевые сервисы должны быть защищены брандмауэром.

Полностью защититься от DDoS-атак на сегодняшний день невозможно, так как совершенно надёжных систем не существует. Здесь также большую роль играет человеческий фактор, потому что любая ошибка системного администратора, неправильно настроившего маршрутизатор, может привести к весьма плачевным последствиям. Однако, несмотря на всё это, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния.

Лёша Ипатов

***7) Как правильно удалять аккаунты, какую-либо информацию?***

***8) Брандмауэр. Расскажи подробнее.***

Межсетево́й экра́н, сетево́й экра́н, файрво́л или брандма́уэр — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита сети или отдельных её узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Проблемы, не решаемые файрволом

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

не защищает узлы сети от проникновения через «люки» (англ. back doors) или уязвимости ПО;

не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;

не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы.

***9) Как используется цифровая подпись?***

Целью применения систем цифровой подписи является аутентификация информации - защита участников информационного обмена от навязывания ложной информации, установление факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений. Система цифровой подписи предполагает, что каждый пользователь сети имеет свой секретный ключ, который используется для формирования подписи, а также соответствующий этому секретному ключу открытый ключ, известный некоторому кругу пользователей сети и предназначенный для проверки подписи. Цифровая подпись вычисляется на основе секретного ключа отправителя информации и собственно информационных бит документа (файла). Один из пользователей может быть избран в качестве "нотариуса" и заверять с помощью своего секретного ключа любые документы. Остальные пользователи могут провести верификацию его подписи, то есть убедиться в подлинности полученного документа. Способ вычисления цифровой подписи таков, что знание открытого ключа не может привести к подделке подписи. Проверить подпись может любой пользователь, имеющий открытый ключ, в том числе независимый арбитр, который уполномочен решать возможные споры об авторстве сообщения (документа).

***10) По каким критериям выделяют те или иные типы вирусов?***

Существует несколько классификаций компьютерных вирусов:

1. По среде обитания различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.

2. По способу заражения выделяют резидентные и нерезидентные вирусы.

3. По степени воздействия вирусы бывают неопасные, опасные и очень опасные.

4. По особенностям алгоритмов вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

Загрузочные вирусы заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.

Резидентные вирусы загружается в память компьютера и постоянно там находится до выключения компьютера.

Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

Стелс-вирусы (невидимки) перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

Троянские вирусы маскируют свои действия под видом выполнения обычных приложений.

***11) Топ 10 хакеров и их атак.***

***10) Какие были самые известные истории, связанные с хакерством? (Ярошевич)***

1) Кевин Митник

Как и его предшественники, Кевин Митник начал заниматься хакерством, вторгаясь в телефонные линии. В 1981 году семнадцатилетний Кевин со своим другом взломал телефонную станцию Computer System for Mainframe Operations (COSMOS), принадлежащую компании Pacific Bell в Лос-Анджелесе. Вторгшись в систему, он переключал телефонные линии и перехватывал все звонки, идущие через эту станцию. Абоненты вскоре начали жаловаться, списывая это на ошибки и розыгрыши операторов. Кевин Митник, разумеется, отвечал на звонки сам, иногда при этом отмачивая бестактные шутки.

Но Митник на этом не остановился: он продолжал влезать в систему компании Pacific Bell и её COSMOS. Хакер сумел войти в базу данных компании и украсть информацию о нескольких абонентах. Он с лёгкостью получил доступ к телефонным счетам, паролям, комбинациям шлюзов и даже к системному руководству. Митник даже использовал переключение телефонных линий для своих личных нужд. В конце концов, один из сотрудников Pacific Bell обнаружил нарушения в системе COSMOS. Было начато расследование, которое быстро привело к телефонной будке, используемой Кевином Митником для звонков и доступа к сети; оставалось только дождаться, когда появится преступник и поймать его с поличным. Приговор суда был мягким: Митника обвинили в порче данных и краже и приговорили к трём месяцам отбывания наказания в исправительном учреждении и дали один год испытательного срока. Далее Пентагон. В 1987 году Митник оставил свою незаконную деятельность. Кевин находился на испытательном сроке, в соответствии с последним приговором суда, поэтому он не мог позволить себе никаких правонарушений. Однако вскоре Митник снова был замешан в тёмных делах.

Однажды вечером вместе со своим другом Ленни ДиСикко (Lenny DiCicco) Митник вторгся во внутреннюю сеть исследовательской лаборатории американской компьютерной компании Digital Equipment Corporation (DEC). Для Митника сделать это было несложно, так как ДиСикко являлся сотрудником данной лаборатории и одновременно был соучастником взлома. EasyNet - внутренняя сеть DEC - не выдержала хакерской атаки, и вскоре сообщники получили доступ ко всей системе.

Как и в случае с предыдущими атаками, вторжение в лабораторию было быстро обнаружено, но на этот раз Митник это предвидел и подготовился. Он зашифровал источник вызовов, сделав бесполезными все попытки выследить его. И на этот раз Митник взломал систему не из простого любопытства или для проверки своих способностей: у него было другая цель. Хакер хотел завладеть исходным кодом операционной системы VMS, разработанной компанией DEC для компьютеров VAX.

Митник предпринял все меры предосторожности, но не учёл одного - своего собственного друга. Кевин любил игры и розыгрыши, поэтому как-то раз он позвонил работодателю своего друга Ленни ДиСикко, притворившись представителем государственной власти. Он сказал, будто у одного из его служащих (ДиСикко) проблемы с налогами. ДиСикко не оценил такую шутку и решил отомстить по-своему.

ДиСикко предал Митника, сообщив своему работодателю о вторжении Митника в сеть компании. Затем он связался с ФБР и сказал, что может сдать хакера, который регулярно проникал в сеть лаборатории. Во время встречи Митника с ДиСикко хакер попал в ловушку, расставленную его собственным другом, который пришёл в сопровождении двух агентов ФБР. Митник был арестован.

Судебное дело длилось недолго: компания DEC обвинила хакера в краже информации и запросила за нанесённый ущерб более $200 000. Митника приговорили к одному году тюремного заключения, кроме того, он должен был посещать шестимесячные курсы для излечения от компьютерной зависимости.

В 1994 году Кевин Митник вернулся к своей незаконной деятельности, его разыскивало ФБР. За свои "подвиги" Митник уже прославился на весь мир. Федералы разослали повсюду его фотографии, чтобы узнавшие его люди могли позвонить властям. В течение этого и следующего года на Кевина Митника была объявлена облава, самая впечатляющая за всю историю поимки хакеров.

Митник решил атаковать другого хакера и эксперта по компьютерной безопасности - Тсутому Шимомуру (Tsutomu Shimomura). Он хорошо подготовил свою атаку и, чтобы убедиться, что никто ему не помешает, запустил её в Рождество, 25 декабря 1994 года. Митник взломал личный компьютер Шимомуры, используя неизвестную в то время методику - подмену IP-адреса, то есть разновидность вторжения, при котором взломщик пытается замаскироваться под другую систему, используя её IP-адрес.

Однако Митника подвёл брандмауэр Шимомуры, который записывал все действия, происходящие на целевой машине. На следующий же день, 26 декабря, Шимомуре позвонил один из его коллег и сообщил, что его компьютер стал жертвой вторжения. Шимомура быстро вычислил Митника и решил помочь ФБР в поимке хакера, используя свои же хакерские умения.

Для поимки Митника ФБР предоставило Шимомуре полную свободу действий, в том числе разрешило использовать хакерство. Облава превратилась в виртуальную охоту. Однажды Шимомура сообщил, например, что он застал Митника врасплох 17 января 1995 года, когда тот влез в сеть, принадлежащую Motorola, чтобы украсть секретное программное обеспечение компании.

Преследование усиливалось, и спецслужбы начали приближаться к киберпреступнику, отступающему в г. Роли, штат Северная Каролина. Чтобы засечь сотовый телефон, с которого Митник совершал свои атаки, Шимомура в течение двух дней бродил по улицам Роли с детектором связи. 15 февраля 1995 года в 2 часа ночи агенты ФБР вместе с Шимомурой ворвались в квартиру Митника. Когда знаменитый хакер увидел своего соперника, он воскликнул: "Hi, Тсутому! Мои поздравления!". После почти двухлетнего преследования Митника приговорили к пяти годам тюремного заключения. На то время это было самое суровое наказание для хакера.

2) Роберт Таппан Моррис (Robert Tappan Morris), который сейчас является штатным профессором в Массачусетском технологическом институте (МТИ) в лаборатории компьютерных наук и искусственного интеллекта, создал первого "интернет-червя".

И опять же, к созданию "червя" Морриса побудило любопытство. По его словам, основной целью его программы было оценить истинные размеры сети Интернет, т.е. определить количество подключённых к ней компьютеров. В то время к Интернету было подключено не так много машин, но вопреки расчётам Морриса, его "червь" причинил гораздо больше вреда, чем ожидалось.

"Червь" Морриса, отправленный с компьютеров МТИ, был запрограммирован на то, чтобы проверить компьютер и скопировать себя в систему, если машина ещё не была инфицирована. Проблемы начались, когда Моррису пришла в голову мысль, что некоторые системные администраторы могут придумать уловку с поддельными копиями, чтобы обмануть "червя" и заставить его думать, что компьютер уже заражён. Тогда он модифицировал код программы, чтобы "червь" оставлял свои копии каждый раз, независимо от того, инфицирован компьютер или нет.

"Червь" Морриса распространился, как пожар, заразив несколько тысяч компьютеров всего за несколько часов. Приблизительно подсчитали, что восстановление каждой инфицированной системы будет стоить от $200 до $53 000, в зависимости от компьютера. Чтобы остановить "червя", были мобилизованы различные команды программистов, для нейтрализации атаки понадобилось несколько дней.

Роберт Таппан Моррис был признан виновным в компьютерном мошенничестве и был приговорён к трём годам условно, 400 часам общественных работ и $10 050 штрафа.

3) Кевин Поулсен - это ещё одно имя, которое вошло в анналы ФБР в 80-е гг. Впервые его арестовали в 1989 году, когда ему было 24 года. Тогда его обвинили в нескольких взломах телефонных сетей и компьютерных серверов, против него были собраны разные уличающие доказательства. Но когда пришло время предстать перед судом, Поулсен решил скрыться, агенты ФБР 17 месяцев выслеживали его. Именно в это время он совершил своё самое знаменитое хакерВ прямом эфире на лос-анджелесской радиостанции KIIS-FM проходила викторина-розыгрыш. Слушателям предлагалось позвонить на радиостанцию и попытаться выиграть автомобиль Porsche 944 S2. Приз должен был достаться 102-му дозвонившемуся радиослушателю. Кевин Поулсен начал действовать: он так заблокировал телефонную сеть, что на радио никто не мог дозвониться, кроме него самого. Следовательно, Кевин стал 102-м дозвонившимся и выиграл приз. Поулсен "утёр нос" ФБР, заставив власти вновь приступить к его поиску, потому что после этого он исчез.

В апреле 1991 года ФБР, наконец, удалось арестовать Поулсена. Поимке поспособствовал анонимный донос: кто-то сообщил властям, что Поулсен делает покупки в супермаркете на окраине Лос-Анджелеса. В 1994 году ему предъявили обвинение и в результате приговорили к четырём годам тюремного заключения. В то время это был самый суровый приговор, назначенный судом за хакерство.ское деяние.

4) Люди занимаются хакерством не только из любопытства и азарта, иногда в дело замешаны деньги. Самый яркий пример - ограбление банка с целью получения денег, иногда удавалось украсть миллионы. Так, Владимир Левин (Vladimir Levin) завоевал дурную славу тем, что украл несколВ 1994 году Левин проник во внутреннюю сеть американского банка Citibank, взломав аналоговое модемное подключение банка и получив доступ к нескольким счетам. Он сумел перевести 10,7 миллиона долларов на счета в США, Финляндию, Германию, Израиль и Нидерланды. Левину помогали трое сообщников, которые должны были вернуть украденные деньги.

Однако его сообщников арестовали, когда они пытались стащить украденные деньги. Их допрос вывел на след Левина, который работал программистом в Санкт-Петербурге. Российского хакера арестовали в марте 1995 года в лондонском аэропорту Хитроу. Судебное разбирательство против него началось только в сентябре 1997 года и закончились в феврале следующего года. Левина приговорили к трём годам лишения свободы.ько миллионов долларов при странных обстоятельствах.

5) 12 февраля 2004 года был самый обычный день, но в компании Microsoft было объявлено чрезвычайное положение. Кто-то украл исходный код операционной системы Windows 2000, которой до сих пор пользуется большое количество пользователей. И что ещё хуже, неизвестный хакер выложил этот код в Wild. Кража была масштабна: 600 миллионов байт данных, 30 195 файлов и 13,5 миллиона строк кода. Утечка информации коснулась операционной системы Windows 2000 и её "старшей сестры" Windows NT4. Все сотрудники "софтового" гиганта пытались выяснить, что произошло, но никто не мог дать ответ. Данные были украдены прямо из сети Microsoft. Неизвестный хакер вошёл во внутреннюю сеть компании, взломав пароль одного из компьютеров. Исходный код быстро распространился по Интернету, особенно по P2P-сетям. К счастью, несмотря на то, что все опасались худшего, последствия этой грандиозной кражи оказались довольно мягкими.

6) Адриан Ламо (Adrian Lamo)

Адриан Ламо, безусловно, свёл с ума самое большое количество сетевых администраторов. От его деятельности пострадали такие крупные корпорации, как Microsoft, New York Times, AOL, Sun Microsystems, Yahoo!, MacDonald's и Cingular. Ему приписывают все виды атак и нарушений защиты корпоративных систем безопасности. Ламо обходил защитные системы с обескураживающей простотой. Так, во время эфира ночных новостей телекомпании NBC журналист предложил Адриану доказать свой талант прямо перед объективом камеры, и тогда хакер менее чем за пять минут проник во внутреннюю сеть самой телекомпании. В настоящее время Ламо является специалистом по безопасности и наслаждается полной свободой передвижения после того, как многие годы был под наблюдением властей США.

Хакерство возникло в 70-е гг. прошлого века, но некоторые из многочисленных группировок, сформировавшихся вокруг этого движения, существуют и по сей день.

Всё больше и больше людей получают возможность пользоваться Интернетом, а хакеров и так называемых "script kiddies" (компьютерных хулиганов-подростков) сейчас больше, чем когда-либо. Однако мы не наблюдаем бурного роста крупномасштабных атак против компьютерных систем, который был бы соразмерен увеличению числа хакеров. Движение пошло немного по другому направлению, по сравнению с периодом расцвета хакерства.

Некоторые атаки по-прежнему производят фурор, и системным администраторам приходится за это расплачиваться. Кевины Митники и Джоны Дрейперы, которые вошли в историю, уже успокоились и остепенились, а нынешние специалисты по безопасности компьютерных систем сталкиваются с менее опасной, но гораздо более массовой угрозой.

***12) Как хоть как-нибудь защитить себя от тех или иных атак (хотя бы несколько способов)?***

Яна Ярошевич

***8) Какие самые необычные компьютерные вирусы имели место? (Топ 5). В чем заключалась уловка, как впоследствии происходило заражение?***

***29) Какой вирус, на твой взгляд, самый забавный? (Ровдо)***

Открывает список червь P2PShared.U. Этот вредоносный код распространялся с помощью почтовых сообщений с темой: "McDonalds желает Вам счастливого Рождества!". В сообщении речь шла о купоне, дающем право на бесплатный обед в McDonald’s. Но именно купон и являлся носителем вредоносного кода.

BatGen.D, испанский шеф-повар. Этот вредоносный код – специалист в области приготовления вредоносных закусок на любой вкус. Он попадает на компьютеры в виде файла под названием “personalcake.bat”. На деле он представляет собой инструмент для создания вредоносного ПО, который затем спрашивает у пользователя, каким именем он бы хотел назвать творение.

На седьмом месте расположился вредоносный код Aidreden.A. После заражения компьютера на экран выводится сообщение: "Вы умрете в следующем месяце".Таким образом Aidreden.A пытается убедить пользователя в том, что его ПК якобы заражен вирусами, после чего предлагает загрузить фальшивый антивирус. Представляет собой обыкновенное окошко с кнопкой ОК. Потом открывает страницу (Microsoft Security Center) и предлагает скачать антивирус.

***9) Какой уровень наказания хакеров в нашей республике? А в какой стране самое жестокое наказание для хакеров?***

***15) Какие наказания грозят за хакерскую деятельность? (Григорьев)***

Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, - наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в крупном размере, - наказываются лишением свободы на срок от трех до десяти лет с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, - наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

98-99 год Китай, два брата, смертная казнь за взлом компьютерной системы государственного банка с целью кражи денег. Один из братьев получил отсрочку исполнения приговора за согласие дать свидетельские показания.

Паша Борисевич

***11) Как злоумышленник может получить исходный код мобильного приложения?***

Программа show java. APK (англ. Android Package) — формат архивных исполняемых файлов-приложений для Android. Декомпиля́тор — это программа, транслирующая исполняемый модуль (полученный на выходе компилятора) в относительно эквивалентный исходный код на языке программирования высокого уровня.

***12) На что в первую очередь следует обратить внимание разработчику, чтобы защитить своё приложение?***

***13) Почему операционные системы, основанные на ядре Linux, считают наиболее защищёнными от вирусов?***

***30) А есть ли на Linux антивирусы? (Ровдо)***

А зачем Linux антивирус нужен вообще, ведь Linux практически не подвержен вирусным атакам? А ответ очень прост: многие линуксоиды пользуются не только Linux, но ставят, или оставляют на компьютере, второй системой - Windows. А ответ прост: чтобы сканировать раздел Windows, когда она не работает, на возможность заражения. Многие вирусы могут легко прятаться от антивируса, но их намного легче обнаружить именно тогда, когда Windows спит. Именно так поступаю некоторые антивирусы в Windows: они перезагружают Windows и начинают её сканировать перед загрузкой. Но даже если у вас не стоит второй системой Windows, вам может потребоваться Linux антивирус, чтобы не стать разносчиком вирусов. Простая ситуация: вы взяли у друга флешку, скопировали нужные вам файлы, а в них вирус. Вам хоть бы что, и это здорово. Но вы передаёте эти файлы третьему человеку, у которого Windows, и заражаете его этими вирусами. Ну и третий вариант - это сервер, на котором стоит Linux. Но вот в офисе все работают на Windows, и вам просто необходимо мониторить интернет трафик на наличие вирусов. И в этом случае Linux антивирус хорошее решение, так как он может прекрасно работать в режиме командной строки.

Считается, что Unix-системы намного лучше защищены от компьютерных вирусов, в сравнении с операционными системами Windows. В принципе, до сих пор нет ни одного широко распространенного вируса для Linux, в то время как в среде Windows просто кишит всякой заразой. в Linux очень быстро исправляют уязвимости.

Существует мнение, что вирусов на Linux мало потому, что его доля на рынке операционных систем крайне мала, поэтому и создают вирусы для Windows, из-за его большой популярности и распространенности. Будь Linux популярнее, и для него так же написали бы кучу вирусов. Но это не так. Если взять самое популярное ПО для web-серверов, то это будет Apache. По состоянию на 2013 год доля Apache на web-серверах составляет почти 45%, а доля IIS от Microsoft — 23.10% рынка. Из этого следует, что атаки хакеров должны быть активнее к большему числу интернет-ресурсов на Apache, и должно наблюдаться больше червей, вирусов и других вредоносных программ, которые будут нацелены на Apache и те операционные системы, под управлением которых он работает, чем на Windows и IIS. Но в жизни дела обстоят иначе. Уже много времени целью для сетевых червей и всевозможных атак есть IIS от Microsoft.

Основные достоинства Linux, в плане безопасности:

* для \*nix-платформ создано крайне мало вирусов;
* существует большое количество разных Linux-дистрибутивов. Одни работают с .deb пакетами, другие с .RPM пакетами. Создание вируса, который будет одинаково хорошо работать во всех из них очень затруднительно;
* в разных дистрибутивах по-умолчанию инсталлированы разные наборы, по-разному скомпилированного программного обеспечения, что также уменьшает вероятность массового заражения вирусом;
* программы, которые скачаны из интернета, в Linux по-умолчанию не являются исполняемыми. Сперва их нужно сделать таковыми;
* главным источником ПО в Linux являются проверенные(официальные) репозитории. Это дает право утверждать, что вероятность попадания вирусов в эти источники крайне мала.

Антон Григорьев

***14) На любом ли языке можно написать вирус? Почему?***

Все современные вирусы не пишутся на абум, нужно написать такой, который хорошо прячется, модифицируется, еще лучше если дальше распространяется и умеет выполнять какую-то работу, а не просто спалить видеокарту.

Правильный ответ - на том, котором знают. Что есть вирус? это программа, которая работает с определенными тонкостями системы. На каком языке можно сделать программу - теоретически на любом. Есть тонкости, что-то на одном проще, что-то на другом, вот и вся разница. Не рекомендуется писать на Ассемблере, так как тяжело получить доступ к каким-либо API.

***16) Можно ли законно зарабатывать, будучи хакером?***

Некоторые из них помогают защитить наши компьютеры и гаджеты от кражи информации и взломов. В этом году особо отличился хакер Джун Хун Ли из Южной Кореи. Учавствовал в конкурсе, выявлял одну уязвимость за другой. Сначала он сломал браузер Chrome. Затем продемонстрировал, как с помощью этого же браузера можно организовать широкомасштабную атаку на операционную систему. Потом взломал браузер Apple. Заработав в общей сложности 225 000 долларов за два дня конкурса, Джун Хун Ли наконец расслабился и перевёл дыхание.

Гена Трубач

***17) Какими способами можно положить сайт?***

DDoS-атаки. Через инструменты разработчика.

***19) Как защищаются операции с денежными средствами?***

***20) Как можно получить доступ к удаленному компьютеру?***

это когда человек просто садится, берёт пива, пиццу и начинает работать. Начинает искать уязвимые места в системы и после их обнаружения пишет под них Exploit-ы и прочие деструктивные программы. Что нужно? Не чего сложного, просто скачать нужные программы и научится ими пользоваться и ВСЕ!!! А учится ими пользоваться проще простого!

В интернете даже видеокурс есть «Этичный хакинг и тестирование на проникновение» совершенно в свободном доступе.

Скачал сканер портов. Разыскал списки диапазонов IP адресов города и тп. В них просканировать на наличие свободных портов. Полученные адреса отправить программе «Lamescan». Ну а роль этой проги заключалось в банальном подборе пароля и логина, которые можно было выдумать самому или взять в интернете самые часто используемые пользователями.

И если она находила совпадения, а находила она их вообще всегда, то получался такой список, включающий номер IP, порта, указание логина, пароля и статус подобран ли пароль или вовсе без пароля.

***21) Как хакеры подбирают пароли от различных аккаунтов?***

Фишинг — это популярный способ получения информации от беспечных пользователей. Хакеры присылают письма, которые по внешнему виду очень похожи на настоящие ресурсы и просят пользователя якобы заново ввести логин и пароль к своей учетной записи. Еще один пример фишинговых писем — это маскировка «зловредов» под отправленные документы. Правда никаких документов на самом деле в письме нет, а вместо документов в письмо вложена GIF-картинка со ссылкой на сайт для выманивания паролей.

Свят Гетьман

***22) Что можно рассказать о безопасности и анонимности систем луковичных серверов? (Tor, к примеру)***

Tor (сокр. от англ. The Onion Router) — свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации[36]. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Написана преимущественно на языках программирования C, C++ и Python.

С помощью Tor пользователи могут сохранять анонимность в интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов — узлов.

***23) Какие существуют стандарты шифрования?***

Сегодня самым известным и простым алгоритмом, который используется в системах защиты информации организаций и предприятий, является DES (Data Encryption Standart). Он необходим для защиты от незаконного доступа к важной информации в организациях. Особенности алгоритма DES — используется ключ длиной 56 бит; зашифровать можно сообщение с помощью одной программы, а расшифровать — используя любую другую программу, соответствующую DES; высокая скорость обработки достигается за счёт несложного алгоритма и высокой стойкости. Data Encryption Standart подходит для шифрования и аутентификации данных.

***25) Какие есть различия между безопасностью персонального компьютера и безопасностью сервера / mainframe машины?***

***26) Как аппаратно обеспечивается экран?***

На сайте перечислены различные устройства, системы, платформы.

***27) Если о шифре / безопасности системы знают уже двое, то её можно взломать. Как системами безопасности обходится такой барьер?***

Даша Ровдо

***28) А почему бы не ввести на всех сайтах виртуальную клавиатуру? И тогда кейлоггер не страшен.***

Одним из самых эффективных методов защиты от кейлоггеров является использование виртуальной клавиатуры. Не стоит спешить прибегать к помощи виртуальной клавиатуры, встроенной в Windows. Эта программа не предназначена для защиты от кейлоггеров. Подобного рода виртуальные клавиатуры не защищены от считывания информации, набираемой на них. В данном случае нужна специально разработанная виртуальная клавиатура, наподобие той, что входит в состав продуктов Лаборатории Касперского. Наличие виртуальной клавиатуры в программах данной лаборатории подтверждает факт сложности обнаружения кейлоггеров. В настоящее время в большинстве серьезных банков используются виртуальные клавиатуры для защиты своих клиентов от кражи вводимой информации при доступе к интернет-банкинг системам. Новое бесплатное приложение Oxynger KeySheild позволяет защитить данные от передачи хакерам без ведома пользователя. Оно реализовано в форме виртуальной клавиатуры, помогающей безопасно вводить критически важную информацию и таким образом избегать необходимости использовать аппаратную клавиатуру, за которой, возможно, следят кейлоггеры.

Современные кейлоггеры умеют соотносить клавиатурный ввод с текущим окном и элементом ввода. Многие из них умеют отслеживать список работающих приложений, делают “фото” экрана по заданному расписанию или событию, шпионят за содержимым буфера обмена, скрытно следить за пользователем. Вся собранная информация сохраняется на диске, а затем записывается в Log-файл – что-то вроде журнала регистрации, данные могут быть переданы по электронной почте или http/ftp-протоколу. Как заявляет разработчик виртуальной клавиатуры Oxynger KeySheild, программа обезопасит пользователя от шпионского ПО и троянов за счет запрета регистрации, входа в личный кабинет и тому подобного ввода критически важных данных при помощи клавиатуры, мыши, буфера обмена и экранных действий. Специальная функция блокирования скриншотов дает возможность отменять экранные снимки на таких уязвимых для информации этапах. Еще один интересный факт об Oxynger KeySheild – возможность полностью осуществлять ввод данных без помощи мыши. Для каждой инсталляции своего экземпляра программа использует различные раскладки клавиатуры. Поскольку стандартная раскладка QWERTY давно уже не является серьезным барьером для киберпреступников, Oxynger предоставляет уникальную организацию клавиш для каждой отдельной копии ПО, что в итоге оборачивается большой головной болью для хакеров.

Разумеется, приложение Oxynger KeySheild не предназначено для ежедневного использования в рамках работы с большими объемами данных на клавиатуре. Программа нацелена на ситуации, когда пользователю требуется ввести какую-либо конфиденциальную информацию: номер карты или счета, к примеру.