Основные понятия компьютерной безопасности 2

Хакеры и кракеры, или "Что такое хорошо и что такое плохо?" 2

Новые законы УК РФ, связанные с "преступлениями в сфере компьютерной информации" 4

Нарушения безопасности сети 5

Классификация удаленных атак на распределенные вычислительные системы 8

1. По характеру воздействия 8

2. По цели воздействия 9

3. По условию начала осуществления воздействия 9

4. По наличию обратной связи с атакуемым объектом 10

5. По расположению субъекта атаки относительно атакуемого объекта 10

6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие 11

Методы защиты от атак из сети 11

Как защититься от ложного ARP-сервера? 11

Как защититься от ложного DNS-сервера? 11

Как администратору сети защититься от ложного DNS-сервера? 11

Как администратору DNS-сервера защититься от ложного DNS-сервера? 12

Как защититься от навязывания ложного маршрута при использовании протокола ICMP? 12

Как защититься от отказа в обслуживании? 13

Как защититься от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP 13

Список используемой литературы: 15

# Основные понятия компьютерной безопасности

Для того чтобы рассматривать в дальнейшем вопросы безопасности в Internet, необходимо напомнить основные понятия, которыми оперирует теория компьютерной безопасности. Вообще говоря, их всего три: это угрозы, уязвимости и атаки. Хотя искушенному читателю смысл их и так достаточно хорошо ясен, постараемся неформально пояснить его.

Итак, *угроза* безопасности компьютерной системы - это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Иначе говоря, угроза - это нечто плохое, что когда-нибудь может произойти. Уязвимость компьютерной системы - это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нежелательные события. Наконец, *атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака - это реализация угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система защиты должна адекватно реагировать на любое из них.

Далее, исследователи обычно выделяют три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании. Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова "раскрытие" используются термины "кража" или "утечка". Угроза *целостности* включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие. Угроза *отказа в обслуживании* возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

# Хакеры и кракеры, или "Что такое хорошо и что такое плохо?"

Просматривая большое количество статей (главным образом, в электронных журналах) о проблемах компьютерного взлома, нельзя не обратить внимание на тот факт, что ни в одной статье не проводится та грань, которая, по нашему мнению, четко разделяет всех, так или иначе связанных с компьютерной безопасностью. В основном, мнение компьютерного мира по этому поводу либо сугубо негативное (хакеры - это преступники), либо - скромно-позитивное (хакеры - "санитары леса"). На самом деле у этой проблемы существует по меньшей мере две стороны: положительная и отрицательная - и между ними проходит четкая граница. Эта граница разделяет всех профессионалов, связанных с информационной безопасностью, на *хакеров (hackers)* и *кракеров (crackers)*. И те, и другие во многом занимаются решением одних и тех же задач - поиском уязвимостей в вычислительных системах и осуществлением атак на данные системы ("взломом").

Самое главное и принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная задача хакера в том, чтобы, исследуя вычислительную систему, обнаружить слабые места (уязвимости) в ее системе безопасности и *информировать* пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей. Другая задача хакера - проанализировав существующую безопасность вычислительной системы, сформулировать необходимые требования и условия повышения уровня ее защищенности.

С другой стороны, основная задача кракера состоит в непосредственном осуществлении взлома системы *с целью получения несанкционированного доступа к чужой информации* - иначе говоря, для ее кражи, подмены или для объявления факта взлома. Кракер, по своей сути, ничем не отличается от обычного вора, взламывающего чужие квартиры и крадущего чужие вещи. Он взламывает чужие вычислительные системы и крадет чужую информацию. Вот в чем состоит кардинальное различие между теми, кого можно назвать хакерами и кракерами: первые - исследователи компьютерной безопасности, вторые - просто взломщики, воры или вандалы. Хакер в данной терминологии - это специалист. В качестве доказательства приведем определение из словаря Guy L. Steele:

**HACKER** сущ. 1. Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум. 2. Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

Данная трактовка понятия "хакер" отличается от принятой в средствах массовой информации, которые, собственно, и привели к подмене понятий. В последнее время многие специалисты по компьютерной безопасности начали аккуратнее относиться к этим терминам.

Низменность мотивов кракеров приводит к тому, что 90% из них являются "чайниками", которые взламывают плохо администрируемые системы, в основном благодаря использованию чужих программ (обычно эти программы называются *exploit*). (Причем это мнение тех самых 10% профессиональных кракеров.) Такие профессионалы - бывшие хакеры, ставшие на путь нарушения закона. Их, в отличие от кракеров-"чайников", остановить действительно очень сложно, но, как показывает практика, отнюдь не невозможно (см. противоборство Митника и Шимомуры в п. 4.5.2). Очевидно, что для предотвращения возможного взлома или устранения его последствий требуется пригласить квалифицированного специалиста по информационной безопасности - профессионального хакера. Однако, было бы несправедливо смешать в одну кучу всех кракеров, однозначно назвав их ворами и вандалами. По нашему мнению, кракеров можно разделить на три следующих класса в зависимости от цели, с которой осуществляется взлом: вандалы, "шутники" и профессионалы.

*Вандалы* - самая известная (во многом благодаря повседневности вирусов, а также творениям некоторых журналистов) и, надо сказать, самая малочисленная часть кракеров. Их основная цель - взломать систему для ее разрушения. К ним можно отнести, во-первых, любителей команд типа: rm -f -d \*, del \*.\*, format c:/U и т.д., и, во-вторых, специалистов в написании вирусов или "троянских коней". Совершенно естественно, что весь компьютерный мир ненавидит кракеров-вандалов лютой ненавистью. Эта стадия кракерства обычно характерна для новичков и быстро проходит, если кракеру удается совершенствоваться (ведь довольно скучно осознавать свое превосходство над беззащитными пользователями). Кракеров, которые даже с течением времени не миновали эту стадию, а только все более совершенствовали свои навыки разрушения, иначе, чем социальными психопатами, не назовешь.

*"Шутники"* - наиболее безобидная часть кракеров (конечно, в зависимости от того, насколько злые они предпочитают шутки), основная цель которых - известность, достигаемая путем взлома компьютерных систем и внесением туда различных эффектов, выражающих их неудовлетворенное чувство юмора. "Шутники" обычно не наносят существенный ущерб (разве что моральный). На сегодняшний день в Internet это наиболее распространенный класс кракеров, обычно осуществляющих взлом Web-серверов, оставляя там упоминание о себе. К "шутникам" также можно отнести создателей вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т.п.). Все это, в принципе, либо невинные шалости начинающих, либо - рекламные акции профессионалов.

*Взломщики* - профессиональные кракеры, пользующиеся наибольшим почетом и уважением в кракерской среде, основная задача которых - взлом компьютерной системы с серьезными целями, как то кража или подмена хранящейся там информации. В общем случае, для того, чтобы осуществить взлом системы, необходимо пройти три основные стадии: исследование вычислительной системы с выявлением изъянов в ней, разработка программной реализации атаки и непосредственное ее осуществление. Естественно, настоящим профессионалом можно считать того кракера, который для достижения своей цели проходит все три стадии. С некоторой натяжкой также можно считать профессионалом того кракера, который, используя добытую третьим лицом информацию об уязвимости в системе, пишет программную реализацию данной уязвимости. Осуществить третью стадию, очевидно, может в принципе каждый, используя чужие разработки. Но то, чем занимаются взломщики - это обычное воровство, если абстрагироваться от предмета кражи. К сожалению, у нас, в России, все не так просто. В стране, где большая часть программного обеспечения, используемого пользователями, является пиратским, то есть украденным не без помощи тех же взломщиков, почти никто не имеет морального права "бросить в них камень". Конечно, взлом компьютерных систем с целью кражи ни в коем случае нельзя назвать достойным делом, но и упрекать кракеров-взломщиков могут только те, кто легально приобрел все используемое программное обеспечение.

# Новые законы УК РФ, связанные с "преступлениями в сфере компьютерной информации"

Для тех, кто хочет посмотреть на проблему безопасности с другой стороны, со стороны кракера, хочется напомнить, что с 1997 года начали действовать новые статьи УК РФ, где, к сожалению, довольно расплывчато и нечетко описывается та возможная уголовная ответственность, которую могут нести граждане РФ за "преступления в сфере компьютерной информации" (Глава 28 УК РФ):

***Статья 272.*** *Неправомерный доступ к компьютерной информации.*

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.  
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

***Статья 273.****Создание, использование и распространение вредоносных программ для ЭВМ.*

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.  
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

***Статья 274.*** *Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.*

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.  
2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

По своей сути данный закон должен быть направлен именно на кракеров. Однако, первое, что бросается в глаза, это то, что не предусмотрено такое правонарушение, как взлом программного обеспечения. Это позволило известному Санкт-Петербургскому кракеру открыто показаться на 5 канале телевидения и вдоволь посмеяться над принятым законом. С другой стороны, расплывчатость формулировок статей закона, в случае их формальной трактовки, позволяет привлечь к уголовной ответственности практически любого программиста или системного администратора (например, допустившего ошибку, которая повлекла за собой причинение определенного законом ущерба). Так что программы теперь лучше вообще не писать.

Если же серьезно, то применение на практике данного закона чрезвычайно затруднено. Это связано, во-первых, со сложной доказуемостью подобных дел (судя по зарубежному опыту) и, во-вторых, с естественным отсутствием высокой квалификации в данной области у следователей. Поэтому, видимо, пройдет еще не один год, пока мы дождемся громкого успешного уголовного процесса по "преступлению в сфере компьютерной информации".

# Нарушения безопасности сети

Начиная с 1987 года пользователи персональных компьютеров сталкиваются с различными компьютерными вирусами. Однако казалось, что миру сетей, большая часть из которых базировалась на ОС UNIX, ничто не угрожает. Поэтому события ноября 1988 года всколыхнули не только тех, кто имел дело с компьютерами и сетями, но и широкую общественность. 2 ноября 1988 года выпускник Корнельского университета Роберт Таппан Моррис запустил свою программу, которая вышла из-под контроля автора и начала быстро перемещаться по сети. В короткий срок вирус-червь заполнил многие узлы Internet, загружая операционные системы своими копиями, вызывая отказы в обслуживании и т.п. Анализ данной атаки будет проведен в главе 8, сейчас же отметим несколько интересных моментов.

В сетевом компьютерном мире имя Роберта Морриса было известным. Еще в 1985 году в AT&T Bell Labs им был опубликован технический отчет, посвященный слабостям реализации TCP/IP в версии 4.2 BSD UNIX [7]. Но этот отчет написан... Робертом Моррисом-старшим - отцом автора червя. Моррис-старший в это время занимал должность научного руководителя Национального Центра Компьютерной Безопасности (NCSC - National Computer Security Center) - эксперта по компьютерной безопасности. Моррис старший много лет проработал в лаборатории AT&T Bell, где в 60-х годах принимал участие в разработке программ Core Wars. К этому необходимо добавить, что лето 1988 года Моррис-младший провел в этой же лаборатории, где был занят переписыванием программ системы безопасности для компьютеров, работающих под управлением ОС UNIX. Кстати, инцидент с программой-червем практически никак не сказался на карьере Морриса-старшего. В начале 1989 года он был избран в специальный консультативный совет при Национальном институте стандартов и министерстве торговли. В задачу этого совета входит выработка заключений и рекомендаций по вопросам безопасности вычислительных систем правительственных органов США, а также решение вопросов, возникающих при разработке и внедрении стандартов защиты информации.

Червь Морриса инфицировал 6200 компьютеров. Подсчитанные потери, хотя формально червь не наносил какого-либо ущерба данным в инфицированных хостах, были разделены на прямые и косвенные. К прямым потерям были отнесены:

1. остановка, тестирование и перезагрузка 42700 машин;
2. идентификация червя, удаление, чистка памяти и восстановление работоспособности 6200 машин;
3. анализ кода червя, дизассемблирование и документирование;
4. исправление UNIX систем и тестирование.

Прямые потери были оценены более чем в 32 000 000 долларов. К косвенным потерям были отнесены:

1. потери машинного времени в результате отсутствия доступа к сети;
2. потери доступа пользователей к сети.

Косвенные потери были оценены более чем в 66 000 000 долларов. Общие затраты были оценены на сумму в 98 253 260 долларов.

В результате этого инцидента мир получил представление о компьютерной опасности, а Internet - постоянную головную боль. После анализа результатов атаки была образована CERT (Computer Emergency Response Team), которая стала отслеживать случаи атак и вырабатывать рекомендации по защите компьютеров и сетей.

В качестве примеров приведем относительно последние случаи успешных атак на серверы Internet:

1. В августе 1996 года атакован сервер департамента юстиции США. В течение нескольких часов страницы сервера были заполнены фашистской атрибутикой и содержали пародию на Билль о телекоммуникациях.
2. 6 сентября 1996 года атаке подвергся сервер компании PANIX, являющейся одним из крупнейших провайдеров Internet. В результате атаки компания несколько дней не могла предоставлять услуги своим абонентам.
3. В октябре 1996 года на сервере ЦРУ вместо "Welcome to the Central Intelligent Agency" появился заголовок "Welcome to the Central Stupidity Agency" и непристойные тексты.
4. 5 ноября 1996 года был атакован WWW-сервер газеты Нью-Йорк Таймс, в результате чего было практически невозможно следить за ходом президентских выборов.
5. В ноябре 1996 года румынские кракеры заменили на WWW-сервере правительства портрет президента Илиеску на портрет его соперника Константинеску.
6. 5 марта 1997 года взломан сервер NASA в Центре управления космическими полетами Годдарда. Кракеры разместили на страницах сервера свое обращение, в котором осуждалась коммерциализация Internet и выражался протест против судебного преследования знаменитых взломщиков Кевина Митника и Эда Каммингса. В обращении содержалась угроза атаки на "корпоративную Америку" .
7. 20 марта был вскрыт сервер Сэнфорда Уоллейса - президента рекламной фирмы Cyber Promotions. Кракеры поместили в UseNet копию похищенного файла паролей, содержащего зашифрованные пароли, имена и телефоны клиентов фирмы.

Хотя по численности пользователей Internet наша страна сильно уступает США, но число нарушений безопасности также увеличиваются. Вот несколько последних случаев.

1. 27 октября 1996 года российскими кракерами был взломан сервер компании РОСНЕТ, среди клиентов которой Центральный банк РФ, Сбербанк России, Торгово-Промышленная Палата, Государственный Таможенный Комитет РФ и многие другие (п. 4.3.3).
2. 22 ноября 1996 года в Белоруссии на Web-узле оппозиции, представлявшего независимые новости из различных стран и регионов, была стерта вся информация.
3. Многочисленные попытки осуществить мошеннические операции с кредитными карточками заставили компанию America OnLine 14 декабря 1996 года закрыть пользователям из России доступ к своим службам.

Этот список может быть продолжен. Практически каждый день приносит все новые известия о нарушениях безопасности в различных районах мира. Но печальный опыт жертв кракеров, к сожалению, не учит других. В подтверждение этого сошлемся на исследование независимого консультанта по безопасности Дэна Фармера [8], проведенное в ноябре-декабре 1996 года. Для исследования Фармер выбрал две группы Web-серверов: основную и контрольную. В основную группу, связанную с деятельностью пользователей, исследователь включил 50 правительственных хостов, 660 банковских хостов, 274 хоста кредитных союзов, 312 хостов газет и 451 хост секс-клубов. В контрольную группу были включены выбранные случайным образом 469 хостов. Каждый из выбранных хостов оценивался на безопасность с помощью свободно распространяемого средства анализа SATAN (главу 8), одним из авторов которого является сам Фармер. Результаты исследования говорят сами за себя. По оценке Фармера более 60% хостов основной группы могут быть разрушены путем вторжения извне, дополнительно от 9 до 24% могут быть взломаны при помощи известных, но не устраненных в данных хостах, ошибок в используемых ими программах wu-ftp и sendmail. Автор считает, что еще 10-20% хостов могло быть поражено при помощи новых атак, происшедших в последнее время. Приблизительность оценок исследования вызвана тем, что автор, естественно, не пытался проникнуть в исследуемые хосты. При сравнении с контрольной группой оказалось, что уязвимость хостов основной группы вдвое выше, чем контрольной. Хотя автор не скрывал своего имени и намерений, только три администратора исследуемых хостов (два из основной группы и один из контрольной) обнаружили факт проведения исследования их хостов на безопасность.

В чем же причина того, что нарушители проникают в чужие машины? Попытаемся кратко перечислить основные причины уязвимости хостов сети:

1. открытость системы, свободный доступ к информации по организации сетевого взаимодействия, протоколам и механизмам защиты;
2. наличие ошибок в программном обеспечении, операционных системах и утилитах, которые открыто публикуются в сети;
3. разнородность используемых версий программного обеспечения и операционных систем;
4. сложность организации защиты межсетевого взаимодействия;
5. ошибки конфигурирования систем и средств защиты;
6. неправильное или ошибочное администрирование систем;
7. несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации лазеек и ошибок в программном обеспечении;
8. "экономия" на средствах и системах обеспечения безопасности или игнорирование их;
9. умолчание о случаях нарушения безопасности своего хоста или сети.

# Классификация удаленных атак на распределенные вычислительные системы

Основная цель любой классификации состоит в том, чтобы предложить такие классификационные признаки, используя которые можно наиболее точно описать классифицируемые явления или объекты. В связи с тем, что ни в одном из известных авторам научном исследовании не проводилось различия между локальными и удаленными информационными воздействиями на ВС, то применение уже известных обобщенных классификаций для описания удаленных воздействий не позволяет наиболее точно раскрыть их сущность и описать механизмы и условия их осуществления. Это связано с тем, что данный класс воздействий характеризуется сугубо специфичными признаками для распределенных вычислительных систем. Поэтому для более точного описания удаленных атак и предлагается следующая классификация.

Итак, удаленные атаки можно классифицировать по следующим признакам:

## 1. По характеру воздействия

1. пассивное (класс 1.1)
2. активное (класс 1.2)

Пассивным воздействием на распределенную вычислительную систему назовем воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу распределенной ВС приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в РВС служит прослушивание канала связи в сети.

Под активным воздействием на распределенную ВС будем понимать воздействие, оказывающее непосредственное влияние на работу системы (изменение конфигурации РВС, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных атак являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения (естественно, с большей или меньшей степенью сложности), так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (от того, что атакующий просмотрит чужое сообщение в системе, в тот же момент ничего не изменится).

## 2. По цели воздействия

1. нарушение конфиденциальности информации либо ресурсов системы (класс 2.1)
2. нарушение целостности информации (класс 2.2)
3. нарушение работоспособности (доступности) системы (класс 2.3)

Этот классификационный признак является прямой проекцией трех основных типов угроз - раскрытия, целостности и отказа в обслуживании.

Основная цель практически любой атаки - получить несанкционированный доступ к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием. Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия.

Принципиально другой целью атаки является нарушение работоспособности системы. В этом случае не предполагается получение атакующим несанкционированного доступа к информации. Его основная цель - добиться, чтобы операционная система на атакуемом объекте вышла из строя и для всех остальных объектов системы доступ к ресурсам атакованного объекта был бы невозможен.

## 3. По условию начала осуществления воздействия

Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В распределенных ВС существуют три вида условий начала осуществления удаленной атаки:

1. Атака по запросу от атакуемого объекта (класс 3.1)

В этом случае атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных ВС.

1. Атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2)

В этом случае атакующий осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект. Примером такого события может быть прерывание сеанса работы пользователя с сервером в ОС Novell NetWare без выдачи команды LOGOUT [9].

1. Безусловная атака (класс 3.3)

В этом случае начало осуществления атаки безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки. Пример атаки данного вида см. в пункте 4.4.

## 4. По наличию обратной связи с атакуемым объектом

1. с обратной связью (класс 4.1)
2. без обратной связи (однонаправленная атака) (класс 4.2)

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а, следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных ВС. В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную УА можно называть однонаправленной удаленной атакой.

## 5. По расположению субъекта атаки относительно атакуемого объекта

1. внутрисегментное (класс 5.1)
2. межсегментное (класс 5.2)

Рассмотрим ряд определений:

**Субъект атаки (или источник атаки)** - это атакующая программа или оператор, непосредственно осуществляющие воздействие.

**Хост (host)** - сетевой компьютер.

**Маршрутизатор (router)** - устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

**Подсеть (subnetwork) (в терминологии Internet)** - совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Подсеть - логическое объединение хостов маршрутизатором. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

**Сегмент сети** - физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме "общая шина". При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах. Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

В дальнейшем будет показано, что на практике межсегментную атаку осуществить значительно труднее, чем внутрисегментную. Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

## 6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

1. физический (класс 6.1)
2. канальный (класс 6.2)
3. сетевой (класс 6.3)
4. транспортный (класс 6.4)
5. сеансовый (класс 6.5)
6. представительный (класс 6.6)
7. прикладной (класс 6.7)

Международная Организация по Стандартизации (ISO) приняла стандарт ISO 7498, описывающий взаимодействие открытых систем (OSI). Распределенные ВС также являются открытыми системами. Любой сетевой протокол обмена, как и любую сетевую программу, можно с той или иной степенью точности спроецировать на эталонную семиуровневую модель OSI. Такая многоуровневая проекция позволит описать в терминах модели OSI функции, заложенные в сетевой протокол или программу. Удаленная атака также является сетевой программой. В связи с этим представляется логичным рассматривать удаленные атаки на распределенные ВС, проецируя их на эталонную модель ISO/OSI.

# Методы защиты от атак из сети

## Как защититься от ложного ARP-сервера?

В том случае, если у сетевой ОС отсутствует информация о соответствии IP- и Ethernet-адресов хостов внутри одного сегмента IP-сети, данный протокол позволяет посылать широковещательный ARP-запрос на поиск необходимого Ethernet-адреса, на который атакующий может прислать ложный ответ, и, в дальнейшем, весь трафик на канальном уровне окажется перехваченным атакующим и пройдет через ложный ARP-сервер. Очевидно, что для ликвидации данной атаки необходимо устранить причину, по которой возможно ее осуществление. Основная причина успеха данной удаленной атаки - отсутствие необходимой информации у ОС каждого хоста о соответствующих IP- и Ethernet-адресах всех остальных хостов внутри данного сегмента сети. Таким образом, самым простым решением будет создание сетевым администратором статической ARP-таблицы в виде файла (в ОС UNIX обычно /etc/ethers), куда необходимо внести соответствующую информацию об адресах. Данный файл устанавливается на каждый хост внутри сегмента, и, следовательно, у сетевой ОС отпадает необходимость в использовании удаленного ARP-поиска. Правда, отметим, что ОС Windows '95 это не помогает.

## Как защититься от ложного DNS-сервера?

Осуществление удаленной атаки, основанной на потенциальных уязвимостях службы DNS, может привести к катастрофическим последствиям для огромного числа пользователей Internet и стать причиной массового нарушения информационной безопасности данной глобальной сети. В следующих двух пунктах предлагаются возможные административные методы по предотвращению или затруднению данной удаленной атаки для администраторов и пользователей сети и для администраторов DNS-серверов.

## Как администратору сети защититься от ложного DNS-сервера?

Если отвечать на этот вопрос коротко, то никак. Ни административно, ни программно нельзя защититься от атаки на существующую версию службы DNS. Оптимальным с точки зрения безопасности решением будет вообще отказаться от использования службы DNS в вашем защищенном сегменте! Конечно, совсем отказаться от использования имен при обращении к хостам для пользователей будет очень не удобно. Поэтому можно предложить следующее компромиссное решение: использовать имена, но отказаться от механизма удаленного DNS-поиска. Вы правильно догадались, что это возвращение к схеме, использовавшейся до появления службы DNS с выделенными DNS-серверами. Тогда на каждой машине в сети существовал hosts файл, в котором находилась информация о соответствующих именах и IP-адресах всех хостов в сети. Очевидно, что на сегодняшний день администратору можно внести в подобный файл информацию о лишь наиболее часто посещаемых пользователями данного сегмента серверах сети. Поэтому использование на практике данного решения чрезвычайно затруднено и, видимо, нереально (что, например, делать с броузерами, которые используют URL с именами?). Для затруднения осуществления данной удаленной атаки можно предложить администраторам использовать для службы DNS вместо протокола UDP, который устанавливается по умолчанию, протокол TCP (хотя из документации далеко не очевидно, как его сменить). Это существенно затруднит для атакующего передачу на хост ложного DNS-ответа без приема DNS-запроса.

Общий неутешительный вывод таков: в сети Internet при использовании *существующей* версии службы DNS *не существует* приемлемого решения для защиты от ложного DNS-сервера (и не откажешься, как в случае с ARP, и использовать опасно)!

## Как администратору DNS-сервера защититься от ложного DNS-сервера?

Если отвечать на этот вопрос коротко, то, опять же, никак. Единственным способом затруднить осуществление данной удаленной атаки, это использовать для общения с хостами и с другими DNS-серверами только протокол TCP, а не UDP. Тем не менее, это только затруднит выполнение атаки - не забывайте как про возможный перехват DNS-запроса, так и про возможность математического предсказания начального значения TCP-идентификатора ISN.

В заключение можно порекомендовать для всей сети Internet поскорее перейти либо к новой более защищенной версии службы DNS, либо принять единый стандарт на защищенный протокол. Сделать этот переход, несмотря на все колоссальные расходы, просто необходимо, иначе сеть Internet может быть просто поставлена на колени перед всевозрастающими успешными попытками нарушения ее безопасности при помощи данной службы!

## Как защититься от навязывания ложного маршрута при использовании протокола ICMP?

Ранее рассматривалась удаленная атака, которая заключалась в передаче на хост ложного ICMP Redirect сообщения о смене исходного маршрута. Эта атака приводила как к перехвату атакующим информации, так и к нарушению работоспособности атакуемого хоста. Для того чтобы защититься от данной удаленной атаки, необходимо либо фильтровать данное сообщение (используя Firewall или фильтрующий маршрутизатор), не допуская его попадания на конечную систему, либо соответствующим образом выбирать сетевую ОС, которая будет игнорировать это сообщение. Однако обычно не существует административных способов повлиять на сетевую ОС так, чтобы запретить ей изменять маршрут и реагировать на данное сообщение. Единственный способ, например, в случае ОС Linux или FreeBSD заключается в том, чтобы изменить исходные тексты и перекомпилировать ядро ОС. Очевидно, что такой экзотический для многих способ возможен только для свободно распространяемых вместе с исходными текстами операционных систем. Обычно на практике не существует иного способа узнать реакцию используемой у вас ОС на ICMP Redirect сообщение, как послать данное сообщение и посмотреть, каков будет результат. Эксперименты показали, что данное сообщение позволяет изменить маршрутизацию на ОС Linux 1.2.8, Windows '95 и Windows NT 4.0. Следует отметить, что (как это видно из 4 главы) продукты компании Microsoft не отличаются особой защищенностью от возможных удаленных атак, присущих IP-сетям. Следовательно, использовать данные ОС в защищенном сегменте IP-сети представляется нежелательным. Это и будет тем самым административным решением по защите сегмента сети от данной удаленной атаки.

## Как защититься от отказа в обслуживании?

Как не раз уже отмечалось, нет и не может быть приемлемых способов защиты от отказа в обслуживании в существующем стандарте IPv4 сети Internet. Это связано с тем, что в данном стандарте невозможен контроль за маршрутом сообщений. Поэтому невозможно обеспечить надежный контроль за сетевыми соединениями, так как у одного субъекта сетевого взаимодействия существует возможность занять неограниченное число каналов связи с удаленным объектом и при этом остаться анонимным. Из-за этого любой сервер в сети Internet может быть полностью парализован при помощи удаленной атаки. Единственное, что можно предложить для повышения надежности работы системы, подвергаемой данной атаке, - это использовать как можно более мощные компьютеры. Чем больше число и частота работы процессоров, чем больше объем оперативной памяти, тем более надежной будет работа сетевой ОС, когда на нее обрушится направленный "шторм" ложных запросов на создание соединения. Кроме того, необходимо использование соответствующих вашим вычислительным мощностям операционных систем с внутренней очередью, способной вместить большое число запросов на подключение. Ведь от того, что вы, например, поставите на суперЭВМ операционную систему Linux или Windows NT, у которых длина очереди для одновременно обрабатываемых запросов около 10, а тайм-аут очистки очереди несколько минут, то, несмотря на все вычислительные мощности компьютера, ОС будет полностью парализована атакующим.

Общий вывод по противодействию данной атаки в существующем стандарте IPv4 следующий: просто расслабьтесь и надейтесь на то, что вы ни для кого не представляете интереса, или покупайте суперЭВМ с соответствующей ей сетевой ОС.

## Как защититься от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP

Как отмечалось ранее, единственным базовым протоколом семейства TCP/IP, в котором изначально предусмотрена функция обеспечения безопасности соединения и его абонентов, является протокол транспортного уровня - протокол TCP. Что касается базовых протоколов прикладного уровня: FTP, TELNET, r-служба, NFS, HTTP, DNS, SMTP, то ни один из них не предусматривает дополнительную защиту соединения на своем уровне и оставляет решение всех проблем по обеспечению безопасности соединения протоколу более низкого транспортного уровня - TCP. Однако, вспомнив о возможных атаках на TCP-соединение, что при нахождении атакующего в одном сегменте с целью атаки защититься от подмены одного из абонентов TCP-соединения в принципе невозможно, а в случае нахождения в разных сегментах из-за возможности математического предсказания идентификатора TCP-соединения ISN также реальна подмена одного из абонентов, несложно сделать вывод, что при использовании базовых протоколов семейства TCP/IP обеспечить безопасность соединения практически невозможно! Это происходит из-за того, что, к сожалению, все базовые протоколы сети Internet с точки зрения обеспечения информационной безопасности невероятно устарели.

Единственно, что можно порекомендовать сетевым администраторам для защиты только от межсегментных атак на соединения - в качестве базового "защищенного" протокола использовать протокол TCP и сетевые ОС, в которых начальное значение идентификатора TCP-соединения действительно генерируется случайным образом (неплохой псевдослучайный алгоритм генерации используется в последних версиях ОС FreeBSD).

# Список используемой литературы:

1. Теория и практика обеспечения информационной безопасности, под редакцией Зегжды П.Д., Изд. "Яхтсмен", 1996. Гайкович В., Першин А..
2. Безопасность электронных банковских систем., Изд. "Единая Европа", 1994.
3. Ростовцев А. Г. Элементы Криптологии, Изд. СПбГТУ
4. Клименко С., Уразметов В., Internet. Среда обитания информационного общества, Российский Центр Физико-Технической Информатики, 1995.