Хакеры появились в то же самое время, что и Internet. В 1960 годах хакером назывался высококвалифицированный программист. Теперь это слово имеет несколько иное значение. Начало семидесятых и конец восьмидесятых - лучшие годы для хакеров. Тогда было больше ламмеров, операционные системы только начинали появляться, компьютеры на основе таких систем имели много ошибок и дыр. Хакеры в то время были более свободными.

Основная часть

Очевидно, что смысл сети сетей, состоит в разумности ограничения круга пользователей того или иного сервер! Если подобный сервер закупорен полностью, то и работать может с ним, лишь тот, кто его закупорил. Поэтому, любая компания, прежде чем принять решение вступлении в сообщество Internet, дает себе отчет в том, что существует возможность проникновения в свой главный сервер неких посторонних лиц. Вот эти посторонние лица и называются хакерами. Да, хакеры - это те, кто взламывают сети. Делается это разными способами. Например, через порт терминала или порт электронной почты.

Выбрав жертву, хакер, прежде всего, определяет, имеются ли на сервере плохие пароли, плохо настроенный софт или испорченная операционка. Затем выбирается метод собственной безопасности. Самый распространенный способ проникнуть в сеть так, чтобы остаться незамеченным - это взлом по цепочке:

1) Взламываем Netl.

2) Netl используем для взлома Net2.

3) Net2 свободна для доступа в Net3.

И пошло - поехало дальше

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. Очевидно, что для предотвращения возможного взлома или устранения его последствий требуется пригласить квалифицированного специалиста по информационной безопасности -

профессионального хакера.

Вандалы

Самая известная 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. Кракеров, которые даже с течением времени ни миновали эту стадию, а только все более совершенствовали свои навыки разрушения, иначе, чем социальными психопатами, не назовешь.

Шутники

Наиболее безобидная часть кракеров, 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. 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. 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, будь то кражи 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 свое 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 каждым пользователем, 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.

До сих пор мы все время рассматривали хакеров - кракеров с позиций распределенных систем, но не нужно забывать, что самая многочисленная категория кракеров занимается более обыденными вещами, а именно: снятием защиты с коммерческих версий программных продуктов, изготовлением регистрационных ключей для условно-бесплатных программ и т.п. Но в контексте этой статьи они не упоминаются. В заключение напомним, что более подробно с данным материалом вы можете ознакомиться в новой книге авторов "Атака через Internet”.

Взломав сеть, хакер заметает следы и уничтожает всю компрометирующую себя информацию. И через некоторое время сматывается. В настоящее время имеется много типов хакеров, каждый из которых весьма различен.

Хакеры

Народ, вламывающийся в систему ради забавы, не нанося ощутимого вреда компьютерам. Хакеры врываются в систему, оглядываются, и затем пробуют взломать даже более безопасную систему. Они не делают прибыль из хакинга.

Кракеры

Хакер исследует компьютерные системы на устойчивость к взломам с целью отыскивания слабых мест, программных и аппаратных ошибок, которые потом будут устранены. Его задача - информировать пользователей, системных администраторов и разработчиков о найденных уязвимостях. Он разрабатывает мероприятия, позволяющие их устранить. Его цель - совершенствование и развитие!

Кракер же организует атаку на компьютерную систему с одной целью - получения несанкционированного доступа к чужим данным.

К счастью, кракеры тоже не все поголовно уж такие закоренелые и корыстные злодеи. Среди них нередко встречаются просто люди со своеобразным чувством юмора. Пожалуй, сейчас таких даже большинство. Именно им мы обязаны появлению веселых картинок на главных страницах солидных сайтов. Или надписей по типу: "Здесь был Вася". Им же принадлежит авторство вирусов, радующих нас музыкой, переворачиванием экрана и т.д.

Гораздо больше неприятностей доставляют кракеры-вандалы. Поведение этой разновидности кракеров напоминает хулигана, гордо выводящего на свежеокрашенной стене неприличное слово. Они так самоутверждаются! Целью проникновения для них является попытка доставить максимум неприятностей жертве нападения, вплоть до разрушения системы. Чаще всего так действуют новички, впервые пробующие свои силы. Обычно они не задерживаются на этой стадии и либо, набирая опыт и мастерство, переходят в следующую категорию - кракеров-профессионалов, либо бросают это занятие.

И, наконец, самая малочисленная, но самая опасная по масштабам причиняемого ущерба категория - профессиональные кракеры. Профессионалы осуществляют взлом компьютерных систем с конкретной целью - украсть или подменить информацию. Делается это всегда с корыстной целью, нередко взломщик исполняет заказ со стороны. Так с их помощью недобросовестные бизнесмены расправляются с конкурентами. Так осуществляется промышленный и обычный шпионаж. Так организуется паника на бирже ценных бумаг. Вспомните недавний случай с ложным сообщением о ранении Барака Обамы, появившемся в результате взлома аккаунта Associated Press в твиттере! Такого рода атаки уже требуют согласованных действий группы исполнителей. И здесь уже нет никаких сомнений, профессиональные кракеры - настоящие преступники.

Фрикеры

Это человек, который проникает в телефонные сети или другие защищенные телекоммуникационные системы. Например, когда в 1970-е годы в телефонных сетях начали использовать тональный набор, телефонные фрикеры стали использовать изготовленные ими самими оборудование, чтобы подбирать сигналы для прослушивания переговоров. Несмотря на сложные барьеры безопасности, используемые сегодня большинством провайдеров, такое воровство повсеместно распространено.

Заключение.

В заключении хотелось бы подчеркнуть, что никакие аппаратные,

программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях.

В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.