НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Репова Аннагозел
Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Йомудова Джахан
Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Гылычдурдыева Чынар
Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Байрамов Байгелди
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Стандарты безопасности информации. Основы стандартов безопасности были заложены изданными в 1983 г. «Критериями оценки надежных компьютерных систем». Этот документ издан в США национальным центром компьютерной безопасности (NCSC — National Computer Security Center), его часто называют Оранжевой Книгой, утверждена в 1985 г. в качестве правительственного стандарта, Оранжевая Книга определяет основные требования и специфицирует классы для оценки уровня безопасности готовых и коммерчески поддерживаемых компьютерных систем.

В соответствии с требованиями Оранжевой Книги безопасной считается такая система, которая «посредством специальных механизмов защиты контролирует доступ к информации таким образом, что только имеющие соответствующие полномочия лица или процессы, выполняющиеся от их имени, могут получить доступ на чтение, запись, создание или удаление информации».

Иерархия надежных систем, приведенная в Оранжевой Книге, помечает низший уровень безопасности как C, высший как A, промежуточный как B. В класс D попадают системы, оценка которых выявила их несоответствие требованиям всех других классов.

Основные свойствами, характерными для C-систем, являются: наличие подсистемы учета событий, связанных с безопасностью, избирательный контроль доступа. Избирательный контроль заключается в том, что каждый пользователь в отдельности наделяется или лишается привилегий доступа к ресурсам. Уровень C делится на 2 подуровня: C1 и C2. Уровень C2 предусматривает более строгую защиту, чем C1. В соответствии с этим уровнем требуется отслеживание событий, связанных с нарушениями защиты, детальное определение прав и видов доступа к данным, предотвращение случайной доступности данных (очистка освобожденной памяти). На уровне C2 должны присутствовать средства секретного входа, которые позволяют пользователям идентифицировать себя путем ввода уникального идентификатора (ID) входа и пароля перед тем, как им будет разрешен доступ к системе.

Требования уровней B и A гораздо строже и редко предъявляются к массово используемым продуктам.

Различные коммерческие структуры (например, банки) особо выделяют необходимость аудита, службы, соответствующей рекомендации C2. Любая деятельность, связанная с безопасностью, может быть отслежена и тем самым учтена. Это как раз то, что требует C2, и то, что обычно нужно банкам. Однако коммерческие пользователи, как правило, не хотят расплачиваться производительностью за повышенный уровень безопасности.

Уровень безопасности A занимает своими управляющими механизмами до 90 % времени компьютера. Более безопасные системы не только снижают эффективность, но и существенно ограничивают число доступных прикладных пакетов, которые соответствующим образом могут выполняться в подобной системе.

Приемы нарушения безопасности компьютерной сети делятся на так называемые конструктивные и деструктивные.

При конструктивном воздействии основной целью несанкционированного доступа является получение копии конфиденциальной информации, т.е. можно говорить о разведывательном характере воздействия. При деструктивном воздействии конечной целью является разрушение информационного ресурса.

Методы несанкционированного доступа к ресурсам WWW ориентированы в основном на нештатное использование программ-браузеров HTML — страниц, а так же на применение программ, расширяющих функциональные возможности браузеров для решения несвойственных им задач.

Одним из наиболее эффективных и простейших путей снижения эффективности работы сети является увеличение бесполезного или даже вредного с точки зрения решаемых задач сетевого трафика. Этот метод основан на особенности психологии людей безоговорочно доверять информации, полученной из сети. Эту особенность можно использовать для дезинформации за счет ее размещения на тех серверах, ссылки на которые являются для клиента подтверждением достоверности информации. Иногда создаются бесконечные циклы для автоматической загрузки других HTML-файлов. Несложная комбинация указателей в двух или более файлах позволяет создать замкнутый круг, когда браузер будет постоянно загружать файлы, не отображая при этом никакой полезной информации.

Большие возможности для несанкционированного доступа к Web-страницам предоставляет язык создания Web-приложений Java. Средства поддержки приложений, написанных на Java, называются апплетами (applets). Поскольку в Web-документе никак не сообщается, что за той или иной кнопкой скрывается Java-апплет, то пользователь заранее не может определить, что произойдет дальше при выборе необходимого документа или операции.

Существуют также методы несанкционированного доступа на WWW-серверы. Среди них можно отметить такие, как переполнение буфера входных/выходных данных сервера, что приводит к повреждению данных или фрагментов кода, полное выведение Web-сервера из строя путем помещения в оперативную память сервера недопустимых команд, считывание файла паролей сервера, уничтожение журнала регистрации работы пользователей в сети и т.д.

Наиболее часто встречающиеся на практике нарушения безопасности.

Использование протокола TCP/ IP. В протоколе TCP/ IP используется принцип ожидания получения квитанции о правильности получения сегмента информации. В случае неполучения подтверждения сервер удаленного доступа фиксирует незавершенное соединение. Программное обеспечение современных серверов может обрабатывать ограниченное количество незавершенных соединений, что приводит к фактическому блокированию доступа к серверным ресурсам при большом количестве незавершенных соединений.

Кроме этого, большинство реализаций протокола TCP/ IP имеют ограничение на количество соединений, которые могут быть установлены в единицу времени. Все соединения, превышающие это количество, не будут временно обрабатываться и ждать своей очереди. Если посылать, например, сорок запросов на соединение в одну минуту, то сервер будет блокировать любой доступ приблизительно на десять минут. Периодическое повторение этой операции может привести к полному отключению сервера от сети.

Подмена URL-адресов для перенаправления запросов. Такая подмена становится возможной за счет перехвата и анализа «на лету» пакетов. В общем случае меняется заголовок IP-пакета, и пакет перенаправляется на специальный сервер. Вся информация, проходящая через маршрутизатор, перенаправляется на этот сервер.

Электронная почта в основном взламывается путем внесения искажений в конфигурационные файлы SMTP- и POP-серверы или взломом паролей доступа.

Ресурсы рассылки новостей USENET можно изменять путем несанкционированного получения привилегированного доступа к потоку новостей. В случае взлома сервера один из пользователей получает возможность отправки запросов класса slave (ведомый сервер) и тем самым заблокировать доступ пользователей системы к каналу распространения новостей, а также создать для себя лично эффективный канал снятия новостей.

Угрозы компьютерным сетям. Основным из принципов построения и функционирования глобальной сети Интернет является принцип ее доступности и открытости. Это обусловливает, с одной стороны, быстрые темпы развития сети, а с другой стороны, весьма значительно обостряет процессы обеспечения безопасности. По оценкам крупнейших международных экспертов, потери компаний и банков от несанкционированного доступа в компьютерные сети ежегодно составляют сотни миллионов долларов. Поэтому вопрос обеспечения безопасности компьютерных сетей является крайне актуальной задачей.

Рассмотрим основные виды возможного нарушения безопасности компьютерной сети и пути противодействия этому.

Физический несанкционированный доступ. Подключение дополнительного компьютерного терминала к каналам связи путем использования шнура в момент кратковременного выхода из помещения пользователя.

Правила противодействия для этого случая состоят в следующем:

- покидая рабочее место не оставлять персональный компьютер в активном режиме или надежно закрывать помещение;

- компьютерный абордаж (взлом системы);

- подбор пароля к системе вручную или с использование специальной программы;

- ограничение количества попыток неправильного ввода пароля с последующей блокировкой компьютера.

Маскарад (Мистификация). Проникновение в сеть, выдавая себя за законного пользователя, с применением его паролей и других идентифицирующих шифров. Создание условий, когда законный пользователь осуществляет связь с нелегальным пользователем, будучи абсолютно уверенным, что он работает с необходимым ему абонентом.

Правила противодействия состоят в следующем:

- необходимо использовать надежные средства идентификации и аутентификации, блокирование попыток взлома системы, контроль входа в нее;

- необходимо фиксировать все события в системном журнале для последующего анализа.