XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.142-143, 2005.

УДК 50.41.00, 50.37.23

А.А.Леонтьев (5 курс, каф. ИБКС), В.В.Платонов, к.т.н., проф.

ОБНАРУЖЕНИЕ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ В ПРОТОКОЛАХ СТЕКА TCP/IP

В работе ставятся задачи анализа протоколов на возможность встраивания не служебных данных, получения методов обнаружения скрытых каналов (СК), разработки и реализации системы обнаружения СК в протоколах IP, TCP и HTTP.

С древних времен существовало два способа защиты информации от несанкционированного доступа: криптография и стеганография. Но в отличие от криптографии стеганография скрывает сам факт существования сообщения. Скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимания объект (контейнер), который затем пересылается адресату по незащищенным каналам связи. Стеганография может использоваться в различных целях. Законные цели включают водяные знаки на изображениях в целях защиты прав собственности. Незаконными являются передача секретной информации, скрытое общение террористов и др. Чтобы обезопасить систему от несанкционированной передачи информации, нужно контролировать все потоки информации. При этом нужно иметь в виду, что, потенциально, скрытая информация может быть передана в любом сообщении.

В большинстве современных систем взаимодействие происходит на базе сетей TCP/IP. Ввиду их большого распространения наибольшую опасность представляют каналы передачи скрытой информации, реализованные при помощи механизмов именно этих протоколов. Поэтому работа посвящена способам обнаружения скрытых каналов в протоколах стека TCP/IP.

СК, как и любая атака, использует некоторые уязвимости системы. В нашем случае – это избыточность заголовков протоколов стека TCP/IP и отбрасывание неправильно сформированных пакетов только после анализа и разбора, когда пакет уже перехвачен.

Вообще говоря, существует 3 метода обнаружения атак: анализ поведения пользователя, анализ протокола и анализ сигнатур. В работе показано, что анализ протоколов и анализ поведения пользователя могут быть с успехом применены для поиска СК. Анализ сигнатур неприменим для обнаружения СК, потому что СК в основном определяется передаваемым содержимым, которое каждый раз разное. Если же сигнатура все-таки есть, то она очень мала, всего лишь несколько байт, что явно недостаточно.

Для протоколов TCP и IP СК разделены на 2 вида, соответствующие видам уязвимостей стека протоколов, которые они используют: СК, инкапсулирующие данные в неиспользуемые поля или поля, значения которых случайны и СК, вставляющие информацию вместо заголовка протокола.

Анализ протоколов позволяет обнаружить оба вида СК. Для того чтобы использовать анализ протоколов для заголовков IP и TCP были проанализированы все поля и выявлены значения, допустимые для этих полей. Некоторые из этих значений никогда не могут встретиться, другие не могут появиться только из-за того, что соответствующим образом настроена политика безопасности системы, либо изменены значения по умолчанию на хосте-отправителе. Если при анализе полей заголовка обнаружены неожиданные аномальные значения, объявляется тревога.

С протоколом HTTP все обстоит намного сложнее. Поскольку он не имеет жесткой структуры и точно определенных значений для каждого из полей заголовка, то к нему не применим метод анализа протокола, однако можно использовать анализ поведения

пользователя. Для этого выявлены виды информации, которые нужно контролировать. По полученным данным составляется профиль работы пользователя. В случае отклонения от профиля, объявляется тревога.

Результатом работы стала система обнаружения СК в заголовках протоколов TCP и IP методом анализа протокола. Эта система запускается на целевом хосте и контролирует входящий и выходящий трафик на канальном уровне, захватывая все пакеты, что позволяет ей получить всю необходимую информацию о трафике. Значения полей заголовков, определенные политикой безопасности и настройками системы, содержатся в файле конфигурации, из которого они считываются в начале работы системы и затем используются в качестве дополнительной информации. На всем протяжении работы системы, информация о возможных аномалиях и предупреждения о возможном использовании СК, выводятся на экран либо в файл.

Итак, в работе проведен анализ возможностей встраивания скрытых сообщений в сетевой пакет, выявлены способы обнаружения и предотвращения использования скрытых каналов, использующих сетевые пакеты протоколов TCP, IP и HTTP в качестве контейнеров. Для обнаружения СК в протоколах TCP, IP и других протоколах, имеющих жесткую структуру эффективнее использовать анализ протоколов. Для HTTP лучше использовать анализ поведения пользователя.

Исследование показало, что для СК может использоваться практически любой сетевой протокол любого уровня модели TCP/IP. Система обнаружения СК, обеспечивающая прекращение и предотвращение утечки конфиденциальной информации, должна являться неотъемлемой частью полноценной системы защиты от сетевых атак. Также, для более эффективного и быстрого анализа она должна являться частью системы обнаружения вторжений или системы предотвращения вторжений.

Перспективой дальнейшего развития работы должен стать анализ других протоколов сетевого, транспортного и прикладного уровней модели TCP/IP (включая те, которые можно использовать для организации СК с использованием времени), использующихся в локальных и глобальных сетях, и реализация результатов этого анализа.