УДК 004

Токарчук Н. А., Середкина Е. Д., Зюляркина Н. Д.

ИССЛЕДОВАНИЕ ПРОТОКОЛА TCP ДЛЯ ПЕРЕДАЧИ СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ.

В данной статье рассмотрено создание модулей Netfilter ядра linux для скрытой передачи сообщений через сеть интернет на основе использования протокола TCP. Так же в рамках работы решаются такие задачи, как контроль потоков сообщений к различным адресатам и взаимодействие между пользователем и модулями.

Ключевые слова: *стеганография, netfilter, tcp, linux*

Tokarczuk N. A., Seredkina E. D., Zyulyarkina N. D.

STUDY OF TCP FOR TRANSMISSION STEGANOGRAPHIC MESSAGES

This article discusses the creation of Netfilter kernel modules linux flush message transmission via the Internet through the use of protocol TCP. Also in the framework of the solved tasks such as flow control messages to various destinations, and the interaction between the user and modules.

Keywords: *steganography, netfilter, tcp, linux.*

В статье «Протокол TCP как стеганографический контейнер» [1] мы рассматривали способ изменения исходного кода ядра Linux для передачи стеганографических сообщений с помощью протокола TCP. В данной работе мы предлагаем вместо изменения исходного кода ядра Linux использовать динамически подключаемые модули Netfilter. Использование модулей Netfilter позволяет перехватывать любые пакеты при отправке и приеме, а также изменять их любым способом.

В рамках данной работы было создано два модуля Netfilter: модуль отправки и модуль приема сообщений. Данные модули могут подключаться через стандартный механизм регистрации модулей на любом компьютере с системой Linux (kernel 3.x и выше).

Отправка сообщений

Модуль отправки сообщений перехватывает созданные локальным компьютером TCP сегменты в точке перехвата NF_INET_LOCAL_OUT. Перехваченный сегмент TCP с некоторым шансом заменяется на сообщение, которое требует скрытой передачи. В результате замены данных в сегменте контрольная сумма становится неверной. Если длина поля данных сегмента меньше, чем сообщение, которое нужно передать, то это сообщение обрезается до нужной длинны, а оставшаяся часть отправляется при следующей скрытой передаче.

Принимающая сторона из-за не прошедшей проверку контрольной суммы не присылает подтверждение ACK для данного сегмента.

Согласно механизму RTO, отправитель должен переслать сообщение, на которое он не получил ACK подтверждение. В момент повторной отправки сегмента адресату, сообщение изменяется на исходное, и ему восстанавливается контрольная сумма. Данный механизм позволяет паразитировать на любом трафике, идущем от отправителя к получателю.

Прием сообщений

Модуль приема сообщения ловит сегменты в точке перехвата NF_INET_LOCAL_IN. По умолчанию считается, что все сегменты с некорректной контрольной суммой – это стеганографические сообщения. Каждый такой сегмент далее проходит проверку. Стеганографическое сообщение содержит в себе внутреннюю контрольную сумму, через соответствие которой и можно судить, настоящее ли это стеганографическое сообщение.

Контроль потоков

В нашей работе мы используем перехват сегментов на сетевом уровне, поэтому мы должны сами контролировать кому отправлять сообщения. Для отправки сообщений нескольким адресатам был организован контроль потоков сообщений. При отправке сегмента проверяется, есть ли для адреса назначения буфер со стеганографическими сообщениями, и замена данных в сегменте происходит только из нужного буфера. Если же буфер отсутствует, то сегменты всегда остаются неизменными.

Взаимодействие модулей с пользователем

Чтобы добавить сообщение в буфер необходимо передать модулю сообщение и IP-адрес назначения.

Для того, чтобы модуль мог преобразовать переданные ему данные, создана вспомогательная утилита StegFormat, которая преобразует строку вида «<сообщение> <ip-адрес>» в строку, которую может распознать модуль. IP-адрес преобразуется функцией inet_addr, содержащейся в заголовочном файле arpa/inet.h.

Преобразованная строка передается модулю с помощью виртуальной файловой системы /proc. Данная файловая система располагается в памяти и позволяет взаимодействовать с процессами ядра Linux. Самый простой пример, чтобы передать информацию достаточно выполнить команду «echo «сообщение» > /proc/<название модуля>».

При выполнении данной команды модуль регистрирует запись в него и вызывает функцию write_new_message(), которая добавляет новое сообщение в необходимый поток на основе IP-адреса.

Описанный метод передачи не является абсолютно надежным для передачи сообщений, так как если направленно просматривать трафик жертвы, то программы анализа трафика (например, Wireshark) отображают данные сообщения в открытом виде. Однако, если трафика от отправителя к получателю много, а процент скрытых сообщений достаточно мал, отследить такое сообщение при незнании способа скрытой передачи может быть достаточно сложной задачей. Для того, чтобы повысить надежность данного метода можно использовать принудительное шифрование данных.

Примечания

1. Токарчук, Н.А. Протокол TCP как стеганографический контейнер [текст]/ Н.А. Токарчук, Е.Д. Середкина, Н.Д. Зюляркина //Вестник УрФО Безопасность в информационной сфере / Издательский центр ЮУрГУ - Челябинск, 2014 – Вып. 4(14) – С.36-39

Информация об авторах отсутствует на обоих языках