Соловьев М.С.

МЕТОДЫ АНАЛИЗА СЕТЕВОЙ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ ПРИ ОПРЕДЕЛЕНИИ ИЗМЕНЕНИЙ СТРУКТУРЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Анализ сетевой информации, полученной на основе пассивного сбора пакетов из вычислительной сети (ВС) корпоративной информационной системы (ИС), позволяет определять несанкционированные и непреднамеренные изменения топологии и состава общего программного обеспечения ВС, не создавая при этом дополнительной нагрузки на данную корпоративную ИС.

Пассивный процесс получения копий сетевых пакетов основывается на «прослушивании» (Promiscuous mode) сетевого интерфейса. Для реализации пассивного процесса получения копий сетевых пакетов используется библиотека Pcap, содержащая файлы описания необходимых для пассивного сбора сетевых пакетов функций на языке C/C++. В процессе анализа используются следующие подходы к распознаванию типов операционных систем (ОС): распознавание по типичным сетевым приложениям и распознавание по особенностям реализации стека TCP/IP. При распознавании типа ОС по типичным сетевым приложениям могут использоваться следующие методы анализа содержимого полученных копий сетевых пакетов: метод анализа набора открытых сетевых портов и «баннерный» метод анализа. Первый основан на определении сетевых приложений, функционирующих на хосте, на основе открытых портов данного хоста и получении вывода о типе ОС по набору сетевых приложений. Второй «баннерный» метод анализа основывается на том, что многие сетевые приложения в начале сеанса диалога сообщают информацию о себе (о названии и версии приложения, о версии ОС).

При определении типа ОС по особенностям реализации стека TCP/IP могут использоваться два метода анализа: сигнатурный метод анализа и метод анализа, основанный на определении закона изменения параметра Initial Sequence Number (ISN). Сигнатура – текстовая строка, содержащая значения определенных полей TCP/IP пакета. В настоящее время существуют готовые свободно распространяемые базы сигнатур для определения типа ОС. Используя метод анализа, основанный на определении закона изменения параметра ISN, необходимо выделять пакеты, содержащие запросы на установление TCP соединения, содержащие параметр ISN. Проанализировав некоторое количество запросов установления соединения, можно определить закон изменения параметра ISN хоста и по нему установить версию ОС.

Для определения топологии ВС из каждого сетевого пакета выделяются MAC, IP адреса отправителя и значение параметра TTL. Определение топологии ВС производится с учетом того, что различные MAC адреса определяют различные узлы, находящиеся в одном сегменте ВС с машиной, на которой осуществляется сбор сетевой информации. Пакеты, в которых параметр TTL не уменьшался, позволяют установить соответствие между IP и MAC адресами узлов, находящихся в одном сегменте ВС с машиной, на которой осуществляется сбор сетевой информации.

Оставшиеся пакеты позволяют определить значения IP адресов узлов, находящихся в других сегментах ВС, и количество маршрутизаторов на

маршруте от точки сбора до этого узла. Постоянный анализ сетевой информации дает возможность контролировать состояние корпоративной ИС, отмечать изменения в ее структуре и выявлять причины этих изменений.

Работа выполнена под руководством доц. кафедры РКС Федюшина А.И.