А.Р. КЛИНОВИЦКИЙ, А.А. ВОРОНИН

РАЗРАБОТКА И ПРАКТИЧЕСКАЯ ПОДГОТОВКА ЭКСПЕРИМЕНТАЛЬНОЙ БАЗЫ ДЛЯ ПРОВЕРКИ РАБОТЫ СИСТЕМЫ ПЕРЕХВАТА СЕТЕВОГО ТРАФИКА КОМПАНИИ И АЛГОРИТМОВ ЭВРИСТИЧЕСКОГО АНАЛИЗА ПЕРЕХВАЧЕННЫХ ДОКУМЕНТОВ

Владимирский Государственный Университет им. А.Г. и Н.Г. Столетовых

Защита информации включает в себя деятельность по предотвращению утечки защищаемой информации, а также умышленных или непреднамеренных действий, способных ее вызвать. Но зачастую для обеспечения безопасности коммерческой тайны компании требуется не только препятствовать несанкционированному перехвату важной информации, но и самостоятельно организовывать такой перехват в целях своевременного обнаружения каналов утечки, будь она вызвана вредоносным программным обеспечением, или действиями сотрудников, случайно или по злому умыслу «сливающих» информацию на сторону.

Как известно, сотрудники компании зачастую не придают значения тому, какие документы они отправляют, к примеру, на свою «домашнюю» электронную почту, расположенную на каком-нибудь бесплатном хостинге, не защищенном должным образом. И случается так, что руководство слишком поздно понимает, что часть их профессиональных секретов стала известна конкурентам, а момент уже упущен и определить, кто виноват и как именно это произошло, уже почти невозможно.

Контроль обмена информацией между вычислительной сетью компании и глобальными сетями, такими, как Интернет – это одна из основ информационной безопасности современного предприятия наряду с борьбой с НСД, внешними атаками и прочим.

Для организации системы перехвата трафика и анализа перехваченных документов, необходимо правильно установить и настроить ряд программных и аппаратных решений, а также нужным образом сконфигурировать сеть. Все эти моменты и будут описаны далее в этой статье на примере участка сети кафедры ИЗИ.

Анализ конфигурации сети и внесение необходимых изменений.

В первую очередь был проведен осмотр помещений, идентификация и перепись всех основных элементов вычислительной сети компании, их расположения, марок и конфигурации.

Был составлены следующие схемы:

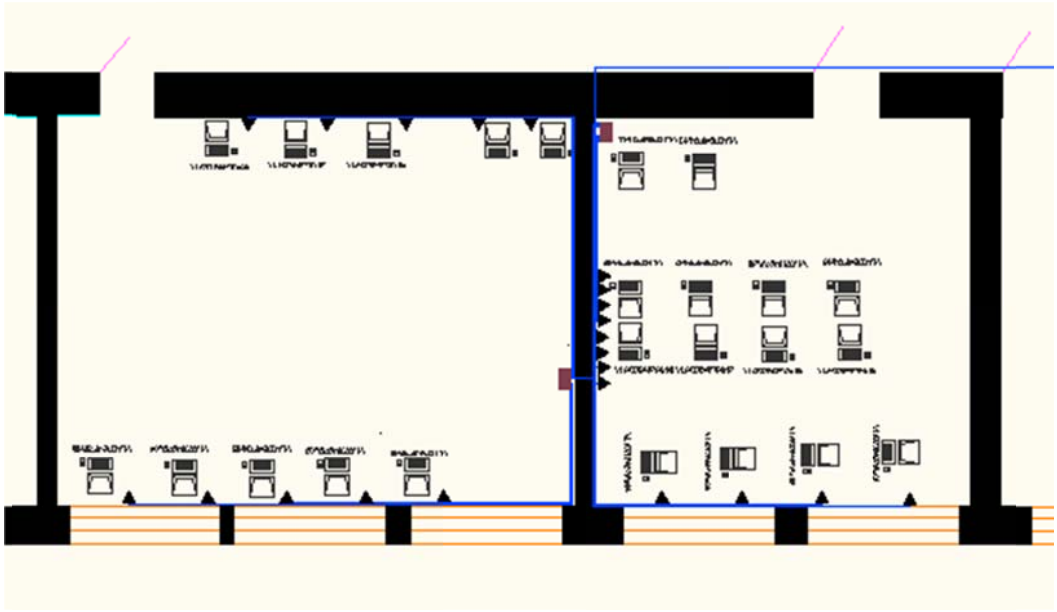

Рис.1. Схема сети лабораторий.

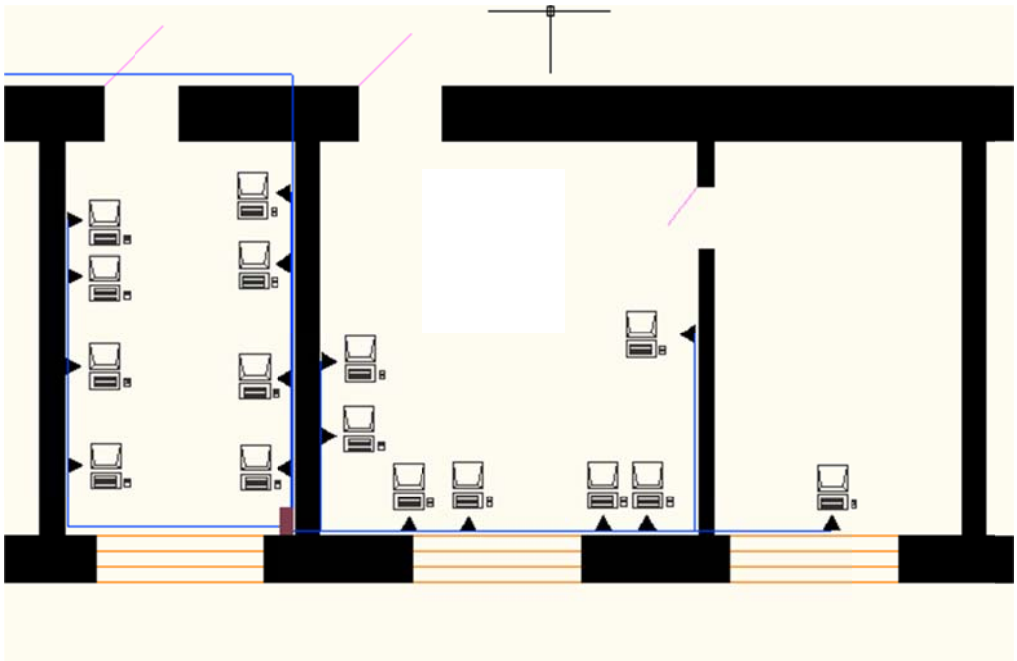

Рис. 2. Схема сети кафедры.

Как видно, выход во внешнюю сеть из обоих помещений осуществляется через коммутаторы (свитчи). Именно к коммутатору подключается сетевой кабель из внешней сети, через который и проходят все исходящие и входящие данные. Следовательно, нашей целью является организовать контроль трафика именно в этой точке.

Среди ряда возможных вариантов организации перехвата информации и «доставки» ее на ПК с соответствующим программным обеспечением, нами были рассмотрены следующие:

1) Организовать ARP-спуфинг на все компьютеры внутренней сети, которые требуется контролировать, таким образом, чтобы весь трафик сначала отсылался на нужный ПК, а затем уже по основному адресу, и также возвращался обратно.

2) Произвести перекроссировку сетевого кабеля, идущего во внешнюю сеть, через ПК с двумя сетевыми картами в режиме моста (bridge). На этом ПК установить соответствующее программное обеспечение для захвата проходящих транзитных пакетов.

3) Организовать зеркалирование трафика средствами управляемого коммутатора (подробнее об этом методе далее).

Первый способ был отброшен почти сразу, ввиду того, что подобная организация движения пакетов привела бы к очень большой нагрузке как на анализирующий ПК, так и на сеть в целом. Это вызвало бы существенные задержки в работе и ухудшение скоростных характеристик сети.

Второй способ имеет свои плюсы, как то гарантия перехвата всех пакетов, которые физически могут пройти только через анализирующий ПК, но и минусы, главный из которых, опять же, ухудшение пропускной способности канала, через который с внешней сетью связан не один десяток компьютеров, а также повышенная нагрузка на сам ПК. Хотя эти негативные воздействия и были бы на порядок ниже, чем в случае применения ARP-спуфинга.

Самым лучшим вариантом, как с точки зрения простоты и надежности, так и неизменности характеристик сети, на наш взгляд, является использование

специальных функций зеркалирования трафика, которые предоставляют подавляющее большинство современных управляемых коммутаторов.

Методика организации перехвата и анализа трафика для обоих описанных выше сетей абсолютно аналогична, поэтому дальнейшая работа проводилась на одном из двух участков сети кафедры, а именно, в лабораториях.

Нас интересовал коммутатор, к которому непосредственно подключена внешняя сеть (на схеме справа сверху). Но, как выяснилось после изучения информации о модели, этот коммутатор неуправляемый, а, следовательно, на нем нельзя организовать зеркалирование трафика.

Второй же коммутатор (на схеме снизу слева), служащий для соединения компьютеров одной из лабораторий друг с другом и с «внешним» коммутатором, марки Cisco Switch 500 Series, управляемый и обладает необходимым функционалом.

В результате, было принято решение просто поменять эти два коммутатора местами, что и было сделано.

Далее, после осуществления необходимых настроек через веб-интерфейс коммутатора и специализированную программу Cisco Network Assistant, на коммутаторе была включена функция анализатора коммутируемых портов (SPAN). Теперь коммутатор отсылал весь трафик, проходящий через порт, к которому была подключена внешняя сеть, на порт с подключенным к нему анализирующим ПК. Таким образом, основная цель - получать на нашем ПК весь трафик между внутренней и внешней сетями, - была достигнута. При этом производительность сети никаким образом нарушена не была.

Установка и настройка необходимого программного обеспечения.

Дальнейшую работу с информацией можно подразделить на два этапа: разделение информационных потоков, сборка конкретных файлов и сообщений из всей массы поступающего трафика и анализ этих файлов.

Для первого этапа было решено использовать готовое программное обеспечение, так как создание собственного не дало бы никаких существенных

плюсов, но при этом потребовало бы очень значительных временных затрат и больших сил на написание и отладку.

Было проанализировано три самых известных приложения с необходимым функционалом, это ShowMeToo, LanDetective и LanGrabber. Все эти программы имеют демо-версии, так что была возможность протестировать их самостоятельно.

Как оказалось, программа LanGrabber является надстройкой над популярными библиотеками WinPCap, использующей его возможности. В плюс программе моно отнести ее богатые настройки, позволяющие выбрать очень многие параметры вплоть до признаков определения типа файла. Но в результате тестирования она показала неудовлетворительные результаты, собирая далеко не все файлы, передававшиеся по сети. Также ее работа была слишком неустойчивой, периодически программа зависала, и ее приходилось перезапускать.

Программа ShowMeToo при более внимательном рассмотрении оказалась устаревшей предшественницей программы LanDetective, более не поддерживаемая разработчиком. Вследствие этого, от нее тоже пришлось отказаться.

Победителем вышла программа LanDetective, которая показала прекрасную стабильность в работе и высокую точность обнаружения и сбора файлов из поступающей информации. Также в плюсы ей можно отнести большое количество поддерживаемых протоколов. Программа может работать с HTTP, FTP, POP3, SMTP, Jabber, Oscar и так далее. Все перехваченные файлы LanDetective сохраняет в указанную директорию на диске, откуда их «принимает» программа-анализатор.

Реализация специализированного приложения для анализа файлов.

Для непосредственного анализа самих файлов было решено написать свое приложение, функционал которого и планируется в будущем наращивать дополнительными алгоритмами эвристического анализа.

На данный момент написанная программа обладает следующими возможностями:

- обнаружение новых перехваченных файлов в момент их появления (мониторинг ведется в реальном времени);

- анализ каждого полученного файла по всем встроенным алгоритмам на предмет соответствия определенным критериям поиска, что позволяет сделать вывод о наличии либо отсутствии искомой информации в этом файле;
- вывод результатов на экран: когда был перехвачен файл, от кого и кому он был отправлен, каков результат его проверки.

Важно отметить хорошо оптимизированный алгоритм работы программы. Отслеживание появления новых файлов осуществляется через WinAPI, не нагружая жесткий диск лишними действиями. Каждый файл обрабатывается в своем потоке, тем самым приложение способно распределять нагрузку равномерно на все вычислительные мощности компьютера и одновременно обрабатывать большое количество поступающих файлов.

На данный момент в программе поддерживается два основных алгоритма анализа информации. Это сравнение CRC полученных файлов с эталонными, что позволяет выявить передачу точных копий конкретных документов, а также контекстный поиск по содержимому. Поддерживаются форматы TXT, RTF, DOC, DOCX, PDF и другие. Контекстный поиск ведется в кодировках ANSI, OEM, Unicode BE и Unicode LE. Также нельзя не отметить поддержку регулярных выражений, что позволяет искать не только конкретные слова и словосочетания, но и совпадения по заданной маске.

В ходе проведенных испытаний вся система показала отличные результаты: высокую точность в перехвате и анализе информации, а также великолепную стабильность в работе. Для проверки пользователям компьютеров в обоих лабораториях была в определенный момент дана команда скачивать одни документы из внешней сети и закачивать другие на внешний сервер. Максимальное количество файлов, находившихся одновременно в обработке в программе, достигало 16, программа успешно справлялась с этой нагрузкой без сколько-либо заметных падений производительности. Также отдельно стоит отметить точность анализа перехваченных файлов, программа всегда точно определяла, содержат ли они искомые данные, и информировала об этом пользователя.

Таким образом, можно сказать, что методика организации контроля трафика, а также база для дальнейших испытаний разрабатываемых новых алгоритмов эвристического анализа готова. Все, что потребуется в дальнейшем, это лишь добавить новые функции в цепочку «фильтров» программы-анализатора. Помимо этого планируется ввести дополнительные варианты извещения администратора об обнаружении искомых файлов в потоке, например, отправкой почтовых или СМС-сообщений.

Сведения об авторах

Клиновицкий Артем Ростиславович
Владимирский Государственный Университет им. А.Г. и Н.Г. Столетовых
Студент
artiomvip@gmail.com

Воронин Алексей Александрович
Владимирский Государственный Университет им. А.Г. и Н.Г. Столетовых, кафедра Информатики и Защиты Информации
К.т.н., доцент кафедры Информатики и Защиты Информации
aleksey.voronin@vlsu.ru