Мы можем порекомендовать за концептуальную основу взять выделенную нами последовательность этапов преобразования учебной задачи в задачу реальную:

1) выполнение учебной задачи по определенному алгоритму;

2) поиск новых, выходящих за пределы конкретного алгоритма, способов решения задачи;

3) критическая оценка найденных способов, завершающаяся выбором оптимального.

При таком способе рассмотрения, учебная задача по информатике, описанная алгоритмом, может быть использована только на первом этапе обучения. Обучающийся должен быть всемерно мотивирован не к сухому выполнению действий инструкции, а к попыткам искать аналоги своих действий. Переход между первым и вторым этапом может быть организован через постепенное нарастание самостоятельности в этом поиске, сочетающееся с постоянной мотивацией со стороны преподавателя.

Между вторым и третьим этапом лежит изучение способов оценки эффективности найденных на втором этапе решений. Задачи по информатике могут быть оценены как с точки зрения параметров качества компьютерной программы (так как всякий результат, который выдает компьютер есть продукт действия компьютерной программы), так и с точки зрения той предметной области, которая определена содержанием самой задачи.

В.А. Клеменьтев, РГППУ
студент группы КТ-504
Руководитель: ст. преп. кафедры СИС
С.В. Ченушкина

СНИФЕРЫ: МЕТОДЫ ОБНАРУЖЕНИЯ

Анализатор трафика, или сниффер (от англ. to sniff – нюхать) – сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Во время работы сниффера сетевой интерфейс переключается в т. н. «режим прослушивания» (Promiscuous mode), что и позволяет ему получать пакеты, адресованные другим интерфейсам в сети.

Перехват трафика может осуществляться:

1) обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);

2) подключением сниффера в разрыв канала;

3) ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;

4) через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

5) через атаку на канальном (2) (MAC-spoofing) или сетевом (3) уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х широко применялся хакерами для захвата пользовательских логинов и паролей, которые в ряде сетевых протоколов передаются в незашифрованном или слабозашифрованном виде. Широкое распространение хабов позволяло захватывать трафик без больших усилий в больших сегментах сети практически без риска быть обнаруженным.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через сниффер трафика позволяет:

Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ).

Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов – мониторов сетевой активности).

Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации.

Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами)

Поскольку в «классическом» снифферe анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов.

Наибольшую опасность снифферы представляли в те времена, когда информация передавалась по сети в открытом виде (без шифрования), а локальные сети строились на основе концентраторов (хабов). Однако эти времена безвозвратно ушли, и в настоящее время использование снифферов для получения доступа к конфиденциальной информации – задача отнюдь не из простых.

Дело в том, что при построении локальных сетей на основе концентраторов существует некая общая среда передачи данных (сетевой кабель) и все узлы сети обмениваются пакетами, конкурируя за доступ к этой среде, причем пакет, посылаемый одним узлом сети, передается на все порты концентратора и этот пакет прослушивают все остальные узлы сети, но принимает его только тот узел, которому он адресован.

Снизить угрозу сниффинга пакетов можно с помощью таких средств как: аутентификация, криптография, антиснифферы, коммутируемая инфраструктура.

Рассмотрим основные методы.

*Метод простого ping-а***.** Большинство пакетных снифферов работают на обычных компьютерах с обычным стеком TCP/IP. Это значит, что если ты отправишь запрос на эти компьютеры, они ответят. Суть в том, чтобы отправить запрос к IP адресу компьютера, а не на его Ethernet адаптер.

Метод усложненного ping-а. Метод пинга может быть улучшен несколькими способами:

Любой протокол, который генерирует ответ, может быть использован, будь то запрос на установление соединения TCP или протокол UDP, такой как порт 7 (echo).

Любой протокол, который может генерировать ошибку на целевую машину может быть использован. Например, неправильные значения в заголовке IP могут быть использованы для генерации ошибки ICMP.

Иногда адрес broadcast (будь то "местный broadcast" вроде 255.255.255.255 или же "направленный broadcast" вроде 10.0.0.255) требуется для использования для того чтобы миновать программную фильтрацию IP адресов. Это в свою очередь создает другую проблему в том, что многие машины не отвечают на broadcast запросы (такие ответы создают сетевые проблемы, такие как 'smurf').

Метод ARP. Метод ARP похож на метод ping, только ARP пакеты используются вместо ping. Объяснение (по-испански) дается по адресу: http://www.apostols.org/projectz/neped/ на котором также есть программа, названная neped для детектирования этим методом.

Вариация этой техники использует факт, что машины кэшируют ARP таблицы. Каждый ARP содержит полную информацию об отправителе и получателе, а так же информацию о цели.

Другими словами, когда мы отправляем простой ARP на broadcast адрес, мы включаем в него свою собственную информацию о принадлежности IP Ethernet. Все остальные, находящиеся на линии, запоминают эту информацию на следуюшие несколько минут.

Таким образом мы можем сделать что-то вроде отправки не-broadcast ARP, затем broarcast ping. Любой, кто отвечает на ваш ping, без отправки вам ARP, мог получить ваш MAC адрес только из прослушанного ARP фрейма. (Чтобы еще раз убедиться в этом, используйте другой MAC адрес в ping'e)

Метод DNS. Многие прослушивающие программы автоматически делают запросы обратного DNS IP адресов, которые они видят. Таким образом прослушивающий режим может быть обнаружен при помощи просмотра DNS траффика, который он создает.

Этот способ может обнаружить машины с двойным подключением и может работать удаленно. Тебе нужно просматривать входящие запросы к DNS серверу твоей организации. Просто сделай ping всех машин в компании в отношении машин, о которых известно, что они не существуют. Любой, кто делает запросы обратного DNS тех адресов, пытаются найти адрес IP, увиденный в ARP пакетах, что делают только программы прослушивания.

Та же самая техника работает местно. Сконфигурируйте детектор в прослушивающем режиме, потом отправьте датаграммы IP на плохие адреса и следи за запросами DNS.

Одна интересная проблема с этой техникой заключается в том, что хакерские программы прослушивания имеют тенденцию резолвить IP адреса как только они появляются, в то время как коммерческие программы откладывают поиски в DNS на время просмотра пользователем раскодирования протокола.

Метод исходящего маршрута. Другая техника включает в себя конфигурацию информации о маршруте источника внутри заголовка IP. Это может быть использовано для детектирования снифферов в соседних сегментах.

Создайте пакет ping, но включите отдельный маршрут в него, чтобы он был отправлен через другую машину в том-же сегменте. У этой машины должна быть отключена маршрутизация, таким образом что она фактически на будет передавать пакет на целевой компьютер.

Если вы получаете ответ, то скорее всего что целевой компьютер прослушал пакет из линии. В ответ, проверь поле TTL для того чтобы определить причину, по которой пакет вернулся. (был ли он прослушан, или же просто был промаршрутизирован)

Детальное пояснение. При использовании отдельного маршрута источника, добавляется опция к IP заголовку. Маршрутизаторы проигнорируют IP адрес назначения и вместо этого направят пакет на следующий IP адрес, указанный в опции маршрута источника.

Метод ловушки. В то время как ping или ARP методы работаю только во внутренней сети, метод ловушки работает везде.

Так как так много протоколов разрешают пароли "открытым текстом", и хакеры используют фильтры для поиска этих паролей, метод ловушки удовлетворяет эту необходимость. Он просто состоит из настройки клиента и сервера на любой части сети, которая используется клиентом для выполнения скрипта подключения используя telnet, pop, imap, или любой другой незашифрованный протокол. Сервер настроен с аккаунтами, которые не имеют реальных привилегий, или же сервер полностью виртуальный (в этом случае аккаунты просто не существуют).

Как только хакер отфильтрует имена пользователей/пароли из линии, он или она попытается подключиться, используя эту информацию. Обычные системы обнаружения вторжений или отслеживания аудитом могут быть настроены на то чтобы записывать в лог такие явления и давать сигнал о том, что прослушивающий хакер нашел траффик и попытался использовать эту информацию.

Метод хоста. Определение сниффера на локальном компьютере. Когда хакеры взламывают вашу систему, они часто оставляют программы жучки, выполняемые на заднем плане для того чтобы прослушивать пароли и аккаунты пользователей из линии.

Также можно воспользоваться *программными* средствами для определения наличия снифферов: программа AntiSniff, CPM - проверка ружима прослушивания на машине ЮНИКС, Neped – программа для определения пакетных снифферов запущенных на локальном сегменте.

А.В. Козлова, РГППУ
асп. кафедры ИТ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО ФОРМИРОВАНИЯ ПОЗНАВАТЕЛЬНОЙ САМОСТОЯТЕЛЬНОСТИ СТУДЕНТОВ

Способность самостоятельно, быстро и правильно ориентироваться в постоянно меняющихся условиях профессиональной деятельности на сегодняшний день является одним из самых востребованных качеств будущих специалистов.