Однако существует ряд проектов по унификации описания и сбору унифицированных данных атак, например, Common Weakness Enumeration. Развитие таких проектов, видимо, позволит получить необходимую информацию о проведении атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Schneier B.* Attack Trees [Электронный ресурс] /Brus Schneier // Dr. Dobb's Journal, 1999. Режим доступа: http://www.schneier.com/paper-attacktrees-ddj-ft.html.

2. *Camtepe, S.A.* A Formal Method for Attack Modeling and Detection [Электронный ресурс] /Seyit Ahmet Camtepe, Bulent Yener // TR-06-01, Rensselaer Polytechnic Institute, Computer Science Department. 2006. Режим доступа: http://citeseer.ist.psu.edu/751069.html.

3. *Sheyner, O.* Automated Generation and Analysis of Attack Graphs /Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, Jeannette M. Wing // Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2002. P. 273 – 284.

4. *Jha, S.* Two Formal Analyses of Attack Graphs /S. Jha , O. Sheyner, J. Wing// Proceedings of the 15th IEEE Computer Security Foundations Workshop. Nova Scotia, Canada, June 2002. P. 49–63.

5. *Sheyner,O.* AttackGraph Tool 0.5 [Электронный ресурс]. Режим доступа: http://www.cs.cmu.edu/~odobzins/scenariograph/as_files/AttackGraph-0.5.tar.gz

6. *Von Ohiemb, D.* Formal security analysis with Interacting state machines /David Von Ohiemb, Volkmar Lotz, Dieter Gollmann, Karjoth Günter, Michael Waidner// Lectute Neotes in Computer Science, 2002, № 2502. P. 212–228.

Д.В. Мордвин, Е.С. Абрамов
Россия, г. Таганрог, Технологический институт ЮФУ

РАЗРАБОТКА ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ МОДЕЛИРОВАНИЯ ЛВС

На данный момент в свободном распространении не существует программ моделирования сетей TCP/IP для целей ознакомления и обучения студентов принципам работы сети, стека протоколов TCP/IP, сетевых служб, сетевых атак. Существуют программы для рисования структуры сети и моделирования сети с целью ее оптимизации, но этого не достаточно.

На данный момент изучение логики работы сети, сетевых протоколов, сетевых атак происходит в теории и при помощи так называемых логов от работы специальных утилит, например tcpdump.

В связи с этим встала задача разработать программу, которая бы позволяла не только моделировать ЛВС, но и моделировать пакеты, сетевой трафик, работу протоколов, служб, сетевые атаки.

Моделирование сетевых устройств

В программе доступно пять типов устройств: компьютеры с сетевой картой, серверные станции, концентраторы, коммутаторы, маршрутизаторы.

Каждое из этих устройств представляет собой отдельный объект, который можно помещать на форму для создания сети, перемещать по форме, соединять с другими устройствами. С каждым из устройств связаны его параметры, которые можно задавать после помещения объекта на форму.

Для каждого устройства смоделированы основные логические свойства, которые имеют реальные устройства такого типа.

Программа не моделирует реальные физические свойства устройств, такие как скорость передачи пакетов, потери пакетов. Моделируются только те свойства, которые помогут глубже понять логику работы сети.

Компьютер (host). Для компьютеров смоделированы такие параметры, как IP-адрес, маска подсети, адрес основного шлюза, адрес DNS сервера. Хранит информацию о том, с какими устройствами в сети связан напрямую.

Также возможно задать фильтрацию пакетов по IP-адресам, портам, типу протокола это означает, что на устройстве установлен программный фаервол.

Серверные станции. Наследуют свойства обычных рабочих станций, но так – же имеют возможность задать типы сервисов, которые будут выполнять данные серверы (например DNS, Kerberos и т.д.).

Концентратор (hub). Устройство хранит информацию о том, с какими устройсвами в сети связано напрямую. Моделируется обычное поведение концентратора – при приеме пакета на один из портов, пакет копируется на все остальные подключенные порты устройства, то есть отсылает пакет всем остальным связанным с ним устройствам.

Коммутатор (switch). Наследует все свойства концентратора и при включении в сеть ведет себя так же, как концентратор. Помимо этого, для каждого коммутатора смоделировано самообучение, создана таблица связи его портов с устройсвами в сети. Когда на какой-либо из его портов приходит пакет с какого-либо сетевого устройства, эта информация заносится в таблицу. Эта таблица в дальнейшем используется для направления пакетов на соответствующие устройства. Таблицу можно конфигурировать и вручную.

Маршрутизатор (router). Для устройства задается количество портов, каждому порту присваевается IP-адрес. Устройство хранит информацию о том, с какими устройсвами в сети связано напрямую. На устройстве смоделирован протокол маршрутизации RIP.

Все устройства соединяются кабелем, который обозначает лишь логическое соединение и не имеет никаких физичесикх характеристик.

Моделирование пакетов

Программа позволяет самостоятельно моделировать TCP, UDP и ICMP пакеты. Для этого на доступ открыты почти все поля заголовков IP, TCP, UDP и ICMP.

Моделирование трафика

Программа позволяет самостоятельно моделировать трафик. Разрешается смоделировать трафик передачи данных по протоколам TCP или UDP, трафик ICMP, либо генерировать трафик из самостоятельно смоделированных пакетах.

В программе можно задавать скорость симуляции, останавливать симуляцию в любой момент, менять свойства устройств, просматривать свойства пакетов.

Использование программы

С помощью данной программы студенты смогут визуально ознакомиться с логикой работы протоколов, сетевых устройств, смоделировать сетевые атаки. Наиболее легко будет в такой программе смоделировать атаки отказа в обслуживании и распределенного отказа в обслуживании. Такая программа позволит сделать обучение наглядным и легким.

Для данной программы планируется смоделировать и реализовать логику работы реальных сетевых служб, таких как Kerberos, X509 и т.д., что позволит изучать не только протоколы работы сети, но и протоколы идентификации и другие.

Обманные системы

Обманные системы (deception system, honeypot) позволяют перейти от глухой обороны к активным действиям, взять инициативу на себя.

Для проведения таких активных действий надо, с одной стороны, привлечь противника какой-нибудь целью, чтобы он потратил время на проникновение, а с другой – эта цель не должна быть реальной, чтобы свести к нулю риск проникновения. Смысл приманки один – завлечь противника, чтобы он стал тратить свое

время и ресурсы на получение доступа к несуществующим или не имеющим реальной ценности ресурсам, тем самым можно выиграть время на отслеживание нарушителя, а при необходимости и на сбор следов его противоправной деятельности.

Honeypot, по существу, это система, специально построенная для того, чтобы быть атакованной, обычно в качестве ложной цели или оповещения о хакерской активности. Вообще говоря, термином "honeypot" принято называть системы, моделирующие известные уязвимости, эмулирующие другие системы или рабочие системы, модифицированные таким образом, чтобы на них создалась замкнутая среда.

Система типа "honeypot" предназначена для установки на один компьютер, перенаправления в нее всего трафика, либо только аномального, и обработки его внутри программы подобно тому, как оно было бы реально обработано соответствующими программами.

Существуют также системы типа "honeynet". Это системы представляют собой распределенные по сети системы honeypot.

Это не единичная система, а сеть, состоящая из многих компьютеров. Эта сеть располагается за межсетевым экраном (firewall), на котором все входящие и исходящие данные фиксируются и контролируются.

Полученная информация впоследствии анализируется с целью изучения средств, тактики и мотивов злоумышленников. Honeynet может использовать множество систем одновременно: Solaris, Linux, Windows NT, маршрутизатор Cisco, коммутатор Alteon и т.д.

Программа, которая рассматривается в этой статье, может быть модифицирована для использования в обманной системе.

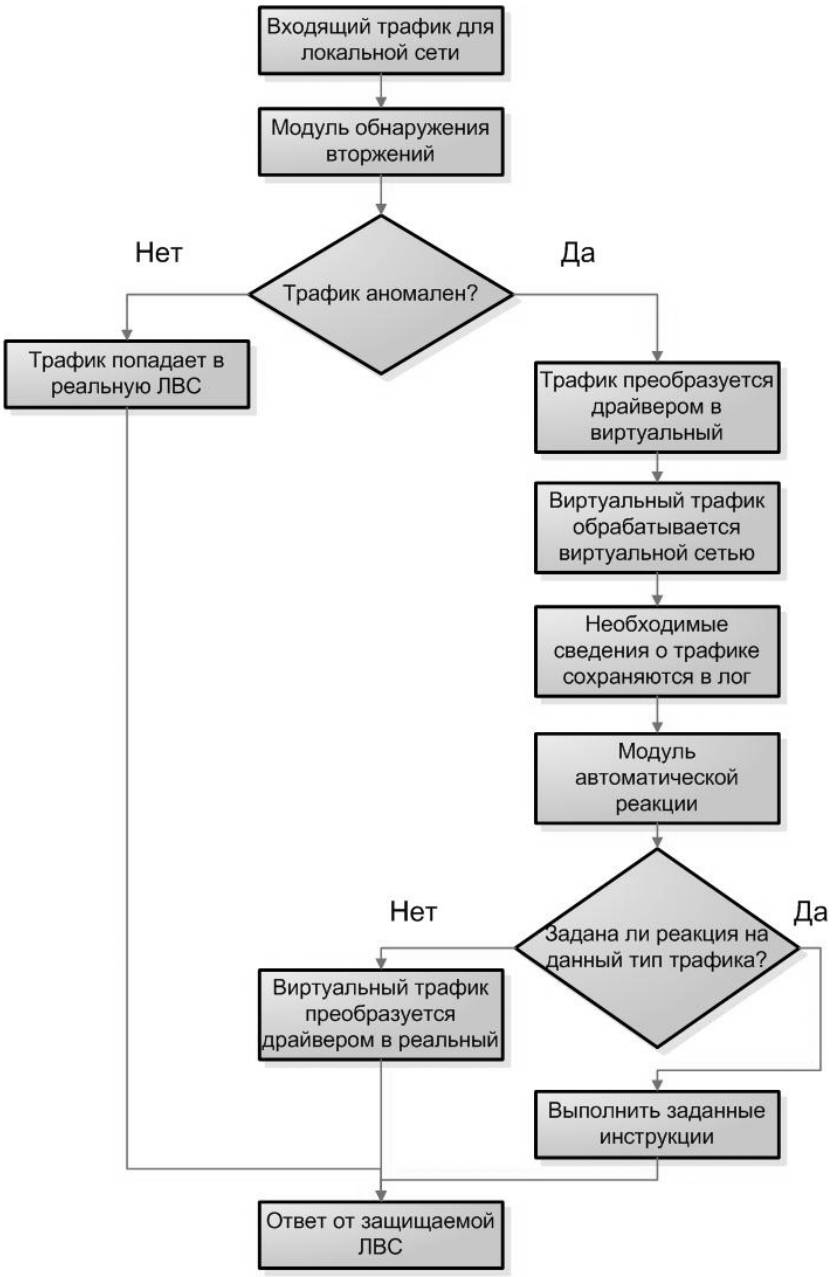
Для этого необходимо смоделировать временные параметры работы сети, такие как время передачи отдельных пакетов и время их обработки близко к реальным значениям. Визуализация передаваемых пакетов в программе должна быть отключена. В программе создается виртуальная локальная сеть. Система обнаружения атак, обрабатывающая весь входной трафик для реальной локальной сети, в случае обнаружения аномального трафика принимает решение о его перенаправлении в виртуальную сеть.

В этом случае специальный драйвер преобразует реальные пакеты, приходящие на сетевую карту компьютера в пакеты для данной программы, направляет их в смоделированную сеть, которая их корректно обрабатывает. Ответ от сети преобразуется драйвером в реальный пакет и отправляется обратно отправителю. Во время обработки аномального трафика в виртуальной сети ведется лог, который поможет позже подробно разобрать произошедшую ситуацию.

Необходимым моментом такой системы будет модуль автоматической реакции при обработке аномального трафика в виртуальной сети. Такой модуль, например может сразу определить источник аномального трафика и принять в его направлении заданные меры.

Поясним сказанное на схеме.

Если драйвер будет перенаправлять пакеты в виртуальную сеть только по решению системы обнаружения вторжений, а в остальных случаях не препятствовать нормальной работе реальной сети, это станет полноценным способом защиты реальной сети. Использование обманной сети позволит выиграть время, собрать доказательную базу вторжения, провести попытку идентификации злоумышленника, провести ответную атаку, защитить свою реальную сеть от новых типов атак.



Система будет представлять собой систему типа "honeynet", но собранную на одном компьютере, что позволит значительным образов сократить количество ресурсов (рабочих станций, сетевых устройств), используемых для защиты реальных вычислительных систем. Обманная система будет представлять собой один компьютер с установленными на нем тремя программами. Вместо того, чтобы создавать реальную обманную сеть, можно создать виртуальную. Обманная система может стать настоящим “атакующим оружием” администраторов безопасности сетей.