Литература

1. Cisco официальный сайт [Электронный ресурс]. – 2015. – Режим доступа: http://www.cisco.com/ – Дата доступа: 02.02.2015

2. Гуру [Электронный ресурс]. – 2015. – Режим доступа: http://www.xgu.ru/ – Дата доступа: 02.02.2015.

3. Свободная энциклопедия Википидия [Электронный ресурс]. – 2015. – Режим доступа: http://ru.wikipedia.org/ – Дата доступа: 03.02.2015.

В.Р. Власенко (УО «ГГУ им. Ф. Скорины», Гомель)
Науч. рук. **А.В. Воруев**, канд. техн. наук, доцент

АУТЕНТИФИКАЦИЯ НА ВТОРОМ УРОВНЕ МОДЕЛИ OSI

Безопасность канального уровня можно считать синонимом безопасности локальной сети. Как правило, атаки на канальном уровне предполагают, что атакующий находится в локальной сети, либо есть некий посредник, который умышленно или неумышленно помогает выполнению атак.

Задача атакующего получить доступ к определенным ресурсам, информации или, как минимум, нарушить нормальную работу сети.Взломав сеть на канальном уровне, атакующий может перешагнуть через средства защиты на более высоких уровнях. Например, использовав подмену IP-адресса, можно обойти настроенные ACL списки или Firewall для разграничения доступа пользователей к ресурсам в сети.

Как правило, атаки выполняются в комплексе, а не по одной.

Распространенные атаки канального уровня:

Например, ARP-spoofing позволяет атакующему перехватывать весь трафик между интересующим ресурсом и каким-то пользователем. Однако, выполнить эту атаку можно только в пределах широковещательного сегмента сети. Если в сети присутствует коммутатор Cisco с настройками по умолчанию, то можно поднять тегированный канал между компьютером атакующего и коммутатором и получить таким образом доступ к другим широковещательным сегментам сети. В таком случае выполнить ARP-spoofing можно в каждом из доступных сегментов.

MAC-spoofing – атака канального уровня, заключающаяся в том, что на сетевой карте изменяется MAC-адрес, что заставляет коммутатор отправлять на порт, к которому подключен злоумышленник, пакеты, которые до этого он видеть не мог;

Переполнение таблицы коммутации – атака основана на том, что таблица коммутации в коммутаторах имеет ограниченный размер. После заполнения таблицы, коммутатор не может более выучивать новые MAC-адреса и начинает работать как хаб, отправляя трафик на все порты;

Атаки на DHCP – это может быть подмена DHCP-сервера в сети (тогда атакующий может назначать дополнительные параметры DHCP, такие как шлюз по умолчанию) или атака DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику;

Port security – функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный. Кроме того, можно указывать не конкретные MAC-адреса, разрешенные на порту коммутатора, а ограничить количество MAC-адресов, которым разрешено передавать трафик через порт.

Функции коммутаторов для обеспечения безопасности работы сети на канальном уровне:

DHCP snooping – функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику. DHCP snooping регулирует только сообщения DHCP и не может повлиять напрямую на трафик пользователей или другие протоколы. Некоторые функции коммутаторов, не имеющие непосредственного отношения к DHCP, могут выполнять проверки на основании таблицы привязок DHCP snooping (DHCP snooping binding database). В их числе:

Dynamic ARP Inspection (Protection) - функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена. Функция регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы.

IP Source Guard (Dynamic IP Lockdown) – функция коммутатора, которая ограничивает IP-трафик на интерфейсах 2го уровня, фильтруя трафик на основании таблицы привязок DHCP snooping и статических соответствий. Функция используется для борьбы с IP-spoofingом.

Литература

1. Cisco официальный сайт [Электронный ресурс]. – 2015. – Режим доступа: http://www.cisco.com/ – Дата доступа: 02.02.2015

2. Гуру [Электронный ресурс]. – 2015. – Режим доступа: http://www.xgu.ru/ – Дата доступа: 02.02.2015.

3. Свободная энциклопедия Википидия [Электронный ресурс]. – 2015. – Режим доступа: http://ru.wikipedia.org/ – Дата доступа: 03.02.2015.

А.С. Воробьева (УО «ГГУ им. Ф.Скорины», Гомель)
Науч. рук. **А.В. Воруев**, канд. техн. наук, доцент

СОЗДАНИЕ ПЛАНА ДЛЯ ВИРТУАЛЬНОГО ТУРА ПО ЗИМНЕМУ САДУ Г. ГОМЕЛЯ

Зимний сад – памятник архитектуры XIX века, входит в состав Гомельского дворцово-паркового ансамбля. Создан из оранжереи в 1877 году по указанию князя Ф.И. Паскевича в здании одного из цехов сахарного завода. Зимой оранжерея князей Паскевичей обогревалась двумя русскими печами, находившимися в подвале. Изнутри стены Зимнего сада выложены природными минералами, что позволяет лазающим растениям создавать живой зелёный ковёр. В настоящее время коллекция сада насчитывает 18 видов субтропических растений.

По заказу администрации Гомельского дворцово-паркового ансамбля был выполнен виртуальный тур по Зимнему саду. При помощи этого тура можно «пройтись» по саду, полюбоваться красотой экзотических растений, животных и рыб. Зачем это нужно? Во-первых, на Зимний сад смогут посмотреть люди, которые живут далеко за пределами Гомеля и не имеют возможности приехать. Во-вторых, это рекламные цели, ведь нет ничего интереснее, чем взглянуть на такую красоту вживую, а виртуальный тур позволит «подогреть» этот интерес. В-третьих, виртуальный тур может выполнить и образовательную функцию, ведь каждый активный элемент имеет свое описание.

Основное помещение имеет 3 точки обзора. Из каждой открывается свой вид. Также имеется 2 точки для обозрения здания Зимнего сада. Итого получается 5 точек. Пользователю достаточно сложно с первого раза сориентироваться, в какой части музея он находится. Для этого и создается план (миникарта).

Виртуальный тур создавался средствами программы Kolor Panotour Pro. План создается при помощи инструмента Floor Plan (рисунок 1).