МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

УНИВЕРСИТЕТ САТПАЕВ

Институт Информационная безопасность

Кафедра Кибербезопасность обработка и хранение данных

СРС №11

Задание: Подберите текст по специальности (скриншот ОДНОГО ЦЕЛОГО параграфа из учебника по специальности, МОЖНО ВЗЯТЬ ТЕКСТ СРС 10) и составьте аннотацию, оформите ее как слайды.

Преподаватель Нургуль Шингисовна Танкиева

Студент Абдуллин Данияр Санжарулы

Специальность Информационная безопасность

Группа ПРЯ-19

Алматы 2021 г

Бирюков А. А.

Информационная безопасность: защита и нападение

ДМК ПРЕСС ИЗДАТЕЛЬСТВО

УДК 004.065
ББК 32.973.26-018.2
Б59

Бирюков А. А.
Б59 Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.: ил.

ISBN 978-5-94074-647-8

В литературе по информационной безопасности (ИБ) в настоящее время не наблюдается недостатка. Однако в большинстве книг на эту тему приводится лишь малая часть тех сведений, которые необходимы для комплексного обеспечения информационной безопасности на предприятии. Например, в некоторых учебниках по ИБ основное внимание уделяется нормативным актам из области ИБ, но при этом крайне мало говорится о технической реализации угроз и защите от них.

С другой стороны, существует много книг, посвященных только техническим аспектам (так называемый взгляд «глазами хакера»). В этих книгах подробно описывается реализация конкретных защит, но не всегда понятно, в каких практических ситуациях она может пригодиться.

Данная книга представляет собой попытку преодолеть односторонний подход к теме ИБ. Книга предназначена для системных администраторов и пользователей малых и средних сетей, осуществляющих защиту корпоративных ресурсов. Здесь приводятся как техническая информация, описывающая атаки и защиту от них, так и рекомендации по обеспечению информационной безопасности с соответствующими примерами.

УДК 004.065
ББК 32.973.26-018.2

ISBN 978-5-94074-647-8

ГЛАВА 1

Теоретические основы

В любой организации, независимо от ее размеров, всегда есть корпоративная сеть. Даже если у вас маленькая контора, в которой всего два или три компьютера, они все равно должны быть объединены в сеть и иметь доступ в Интернет. Таковы реалии современного бизнеса, всем нужен доступ к электронной почте, всем нужен доступ к информации во Всемирной информационной паутине. Однако локальные сети бывают не только в организациях. Зачастую во многих квартирах имеется по нескольку компьютеров, и каждому из них тоже необходим доступ к ресурсам Интернета. Например, у многих пользователей дома есть основной компьютер, ноутбук, карманный компьютер или коммуникатор. Всем этим устройствам в той или иной степени нужно обмениваться файлами между собой, иметь доступ в Интернет. Для организации такого доступа используют активное сетевое оборудование: маршрутизаторы, межсетевые экраны, коммутаторы, беспроводные точки доступа и концентраторы. Хотя последние встречаются все реже. Вообще, сейчас, как правило, для доступа домашних пользователей в Интернет используют устройства, сделанные по принципу «все в одном». То есть одно устройство объединяет в себе функции межсетевого экрана, простейшего маршрутизатора, коммутатора и точки беспроводного доступа. Для домашних пользователей подобное устройство является наилучшим решением, так как одна «коробка» занимает меньше места, к ней нужно вести меньше проводов, кроме того, ее легче настраивать. В корпоративных сетях, где присутствуют более 20 рабочих станций, такие решения стараются не использовать, так как при одновременном подключении большого количества рабочих станций у многофункциональных

сетевых устройств резко снижается производительность. Кроме того, в случае выхода из строя такого устройства вы лишитесь как доступа в Интернет, так и доступа во внутреннюю локальную сеть. Так что, господа системные администраторы, если ваш дешевый Dlink прекрасно работает в домашней сети, то не торопитесь советовать руководству покупать такой же дешевый Dlink для корпоративной сети. Решать проблемы, которые потом возникнут, придется прежде всего вам.

Но вернемся к вопросам сетевой безопасности. Любая локальная сеть немыслима без сетевого оборудования. А против сетевых устройств существует масса различных атак, направленных на перехват информации, проходящей по сети, захват управления устройством или временный вывод его из строя.

У читателя может возникнуть вопрос: почему, говоря о сети, я говорю только о сетевом оборудовании, ведь в сети также работает множество приложений, например серверы баз данных или электронная почта? Отвечу так: несомненно, в сети работает множество различных приложений, но в рамках обсуждения сетевой безопасности мы обсудим работу именно сетевого оборудования, так как работу приложений мы будем рассматривать в главе «Атаки на уровне приложений».

Однако, прежде чем начать обсуждение способов осуществления этих атак и средств защиты, необходимо вспомнить (я надеюсь) основы сетевых технологий, иначе материал последующих разделов может превратиться для читателя в набор непонятных терминов. Конечно, если вы можете с лету вспомнить модель OSI, знаете, что такое Spanning Tree Protocol или PVLAN, то можете смело переходить к чтению следующих разделов.

1.1. Модель OSI

При осуществлении передачи данных от компьютера к компьютеру в сети производится множество операций. При этом пользователя совершенно не интересует, как именно это происходит, – ему необходим доступ к приложению или компьютерному ресурсу, расположенному в другом компьютере сети. На самом деле вся передаваемая информация проходит много этапов обработки. Прежде всего она разбивается на блоки, каждый из которых снабжается управляющей информацией. Получившиеся в результате блоки оформляются в виде сетевых пакетов, затем эти пакеты кодируются, передаются с помощью электрических или световых сигналов по сети в соответствии с выбранным методом доступа, далее из принятых пакетов

вновь восстанавливаются заключенные в них блоки данных, блоки соединяются в данные, которые и становятся доступны другому приложению. Приведенное здесь описание является упрощенным пояснением происходящих процессов. Часть из указанных процедур реализуется только программно, другая часть – аппаратно, а какие-то операции могут выполняться как программами, так и аппаратурой. Упорядочить все выполняемые процедуры, разделить их на уровни и подуровни, взаимодействующие между собой, как раз и призваны модели сетей. Модели сетей позволяют правильно организовать взаимодействие как абонентам внутри одной сети, так и самым разным сетям на различных уровнях. В настоящее время наибольшее распространение получила так называемая эталонная модель обмена информацией открытой системы OSI (Open System Interchange). Под термином «открытая система» понимается не замкнутая в себе система, имеющая возможность взаимодействия с какими-то другими системами (в отличие от закрытой системы).

Обращаясь к истории создания иерархической модели, скажу, что модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго) все производители сетевых продуктов. Модель OSI не лишена ряда недостатков, присущих универсальным моделям, а именно она громоздка, избыточна и не слишком гибка. В результате реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций, то есть возможны устройства, сочетающие в себе функционал различных уровней. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети и, соответственно, как лучше ее защищать. Все сетевые функции в модели разделены на 7 уровней. При этом вышестоящие уровни выполняют более сложные, глобальные задачи, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. В идеале каждый уровень взаимодействует только с теми, которые находятся рядом с ним (выше и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, например веб-браузеру, нижний – непосредственной передаче сигналов по каналу связи.

Данные, которые следует передать по сети, на пути от верхнего (седьмого) уровня приложений до нижнего (первого) физического

проходят процесс инкапсуляции, то есть каждый нижеследующий уровень не только производит обработку данных, приходящих с более высокого уровня, но и снабжает их своим заголовком, а также добавляет к нему служебную информацию. Такой процесс обрастания служебной информацией продолжается до последнего (физического) уровня. На физическом уровне вся эта многооболочечная конструкция передается по кабелю приемнику. Там происходит обратный процесс – декапсуляция, то есть при передаче на вышестоящий уровень убирается одна из оболочек. Верхнего, седьмого уровня достигают уже данные, освобожденные от всех оболочек, то есть от всей служебной информации нижестоящих уровней. При этом каждый уровень принимающего абонента производит обработку данных, полученных с нижеследующего уровня, в соответствии с убираемой им служебной информацией.

В тех случаях, когда на пути между абонентами в сети включаются некие промежуточные устройства (например, концентраторы, коммутаторы, маршрутизаторы), то и они тоже могут выполнять функции, входящие в нижние уровни модели OSI. Чем больше сложность промежуточного устройства, тем больше уровней оно захватывает. В случае если между получателем и отправителем присутствует межсетевой экран, будут обработаны все семь уровней иерархической модели. Но любое промежуточное устройство должно принимать и возвращать информацию на нижнем, физическом уровне. Все внутренние преобразования данных должны производиться дважды и в противоположных направлениях. Промежуточные сетевые устройства, в отличие от полноценных абонентов (например, компьютеров), работают только на нижних уровнях и к тому же выполняют двустороннее преобразование.

Теперь поговорим подробнее о функциях разных уровней.

1.1.1. Прикладной (7) уровень (Application Layer)

Это уровень приложений, который обеспечивает услуги, непосредственно поддерживающие приложения пользователя. Примером таких приложений являются: программные средства передачи файлов (FTP), доступа к базам данных (клиенты баз дланных), средства электронной почты (Microsoft Outlook), служба регистрации на сервере (RADIUS). Этот уровень фактически управляет всеми остальными шестью уровнями. Примером может являться работа с таблицами Excel, когда пользователь сохраняет файл на сетевой ресурс. В этом случае прикладной уровень обеспечивает перемещение файла с рабочего компьютера на сетевой диск прозрачно для пользователя.

1.1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ / МОДЕЛЬ OSI: УЧЕБНИК И ПРАКТИКУМ / ПОД ОБЩ. РЕД БИРЮКОВ А. А.-М.:ДМК ПРЕСС, 2012. – С. 26-28.

Цель дисциплины - формирование у студентов навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.