Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.02.2021 16:43:08
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_____»_____2017 г.

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

Методические указания по выполнению самостоятельных работ
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» И.В. Калуцкий

Безопасность сетей ЭВМ [Текст]: методические рекомендации по выполнению самостоятельных работ/ Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 14 с.: ил. 3. – Библиогр.: с. 14.

Содержат сведения по вопросам самостоятельных работ безопасности сетей ЭВМ. Указывается порядок выполнения самостоятельных работ, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,81. Уч.-изд. л. 0,74. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

Самостоятельная работа №1 – Сетевая аутентификация

К базовым технологиям безопасности относятся аутентификация, авторизация, аудит, технология защищенного канала.

Аутентификация предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Доказательством аутентичности может служить знание аутентифицируемым некоего общего для обеих сторон слова (пароля) или факта, владение некоторым уникальным предметом или демонстрация уникальных биохарактеристик. Чаще всего для доказательства идентичности используются пароли. Существует достаточно физиологических признаков, однозначно указывающих на конкретного человека. К ним относятся: отпечатки рук и ног, зубы, ферменты, динамика дыхания, черты лица и т.д. Для аутентификации терминальных пользователей автоматизированных систем наиболее приемлемыми считаются отпечатки пальцев, геометрия рук, голос, личная подпись.

Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором.

Аудит – это фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.

Технология защищенного канала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например, через Интернет. Защищенный канал обеспечивает выполнение трех основных функций:

· взаимную аутентификацию абонентов при установлении соединения,

· защиту передаваемых по каналу сообщений от несанкционированного доступа,

· подтверждение целостности поступающих по каналу сообщений.

Совокупность защищенных каналов, созданных предприятием в публичной сети для объединения своих филиалов, часто называют виртуальной частной сетью (Virtual Private Network, VPN).

Существует очень большое количество технологий аутентификации, и все они обладают разной степенью удобства и надежности.

Рассмотрим основные методы аутентификации по принципу нарастающей сложности. Начнем с самого простого и общеизвестного метода - аутентификация по паролю. Поскольку данная технология, как правило, используется без изменения параметров в течение длительного времени (неделя, месяц, год - в зависимости от политик безопасности предприятия), то она получила название "аутентификация по многоразовым паролям".

Учетные записи пользователей современных операционных систем включают в себя службу аутентификации, которая может хранить простейший идентификатор (login) и пароль (password) пользователя в своей

базе данных. При попытке логического входа в сеть пользователь набирает свой пароль, который поступает в службу аутентификации. По итогам сравнения пары login/password с эталонным значением из базы данных учетных записей пользователей пользователь может успешно пройти процедуру простейшей аутентификации и авторизоваться в информационной системе. В зависимости от степени защищенности в рамках эволюционного развития операционных систем Windows компанией Microsoft использовались протоколы LAN Manager (LM), NT LAN Manager (NTLM), NT LAN Manager версии 2 (NTLM v2) и Kerberos.

Для организации удаленного доступа пользователей к защищенным информационным ресурсам были разработаны достаточно надежные схемы с применением одноразовых паролей (OTP – One Time Password). Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Одноразовый пароль действителен только для одного входа в систему. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от внешних угроз. Известно четыре метода аутентификации с применением технологии OTP:

· использование механизма временных меток на основе системы единого времени;

· применение общего пароля для легального пользователя и проверяющего списка случайных паролей и надежного механизма их синхронизации;

· использование общего пароля для пользователя и проверяющего генератора псевдослучайных чисел с одним и тем же начальным значением;

· применение фиксированного числа случайных (псевдослучайных) последовательностей, скопированных на носители в виде скретч-карт.

В качестве примера решений OTP можно привести линейку RSA SecurID, ActivCard Token, комбинированный USB-ключ Aladdin eToken NG-OTP. В частности, одной из распространенных аппаратных реализаций одноразовых паролей является технология SecurID, предлагаемая компанией RSA Security. Она основана на специальных калькуляторах — токенах, которые каждую минуту генерируют новый код. В токен встроена батарейка, заряда которой хватает на 3 – 5 лет, после чего токен нужно менять. Аутентификация с помощью SecurID интегрирована в сотни приложений, а недавно при поддержке Microsoft она была встроена в операционную систему Windows. Впрочем, имеются реализации "в железе" и другие алгоритмы генерации одноразовых паролей. Например, можно генерировать пароль по событию — нажатию клавиши на устройстве. Такое решение предлагает компания Secure Computing в виде продукта Safeword. Аппаратную реализацию технологии "запрос-ответ" продает корпорация CryptoCard. Имеются даже универсальные аппаратные реализации, которые позволяют перепрограммировать токены. В частности, решения,

выпускаемые компанией VASCO, допускают реализацию нескольких десятков алгоритмов аутентификации с помощью одноразовых паролей. В целом технология OTP основана на использовании двухфакторных схем аутентификации и может быть классифицирована как усиленная технология аутентификации.

Под аутентификацией информации в компьютерных системах понимают установление подлинности данных, полученных по сети, исключительно на основе информации, содержащейся в полученном сообщении.

Если конечной целью шифрования информации является обеспечение защиты от несанкционированного ознакомления с этой информацией, то конечной целью аутентификации информации является обеспечение защиты участников информационного обмена от навязывания ложной информации. Концепция аутентификации в широком смысле предусматривает установление подлинности информации как при условии наличия взаимного доверия между участниками обмена, так и при его отсутствии.

В компьютерных системах выделяют два вида аутентификации информации:

1. аутентификация хранящихся массивов данных и программ – установление того факта, что данные не подвергались модификации;

2. аутентификация сообщений – установление подлинности полученного сообщения, в том числе решение вопроса об авторстве этого сообщения и установление факта приема.

Аутентификация с применением цифровых сертификатов является альтернативой использованию паролей и особенно эффективно в сетях с очень большим числом пользователей. В таких обстоятельствах процедура предварительной регистрации пользователей, связанная с назначением и хранением их паролей, становится крайне обременительной, опасной или просто нереализуемой. При использовании сертификатов сеть, которая дает пользователю доступ к своим ресурсам, не хранит никакой информации о своих пользователях – они ее предоставляют сами в своих запросах в виде сертификатов, удостоверяющих личность пользователей. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем.

Сертификат является аналогом пропуска и выдается по запросам специальными сертифицирующими центрами при выполнении определенных условий. Сертификат представляет собой электронную форму, в которой содержится следующая информация:

· Открытый ключ владельца данного сертификата;

· Сведения о владельце сертификата (имя, адрес электронной почты, наименование организации, в которой он работает и т.д.)

· Наименование сертифицирующей организации, выдавшей данный сертификат.

Сертификат содержит электронную подпись сертифицирующей организации – это зашифрованные закрытым ключом этой организации данные, содержащиеся в сертификате.

Контрольные вопросы:

1) Что называют сетевой аутентификацией?
2) Что такое авторизация?
3) Перечислите объекты воздействия в информационных системах.
4) Что входит в задачи межсетевых экранов?
5) Что называют контролируемой зоной?

Тест по самостоятельной работе №1:

1. Невозможность получения сервиса законным пользователем называется:
   A) DoS-атакой
   B) Replay-атакой
   C) Атакой «man-in-the-middle»
2. Криптоанализ – это процесс, при котором
   A) Зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение
   B) Зная одну или несколько пар (незашифрованное сообщение, зашифрованное сообщение), пытаются узнать ключ
   C) Изменяют передаваемое зашифрованное сообщение
3. В алгоритмах симметричного шифрования используются только следующие операции:
   A) Операции перестановки и сдвига
   B) S-box и побитовое исключающее или (XOR)
   C) Любые из перечисленных выше операций, а также многие другие
4. Атака «man in the middle» является
   A) Пассивной
   B) Активной
   C) Может быть как активной, так и пассивной
5. Мастер-ключ используется для:
   A) Шифрования ключа сессии
   B) Шифрования прикладных данных

C) Шифрования как ключа сессии, так и прикладных данных

6. Модификация передаваемого сообщения называется:
   A) DoS-атакой
   B) Replay-атакой
   C) Атакой «man-in-the-middle»
7. Аутентификация – это
   A) Невозможность несанкционированного доступа к данным
   B) Подтверждение того, что информация получена из законного источника законным получателем
   C) Невозможность несанкционированного просмотра и модификации информации
8. Что из перечисленного относится к механизмам безопасности ?
   A) Хэш-функции
   B) Целостность сообщения
   C) Алгоритмы симметричного шифрования
   D) невозможность отказа от полученного сообщения
9. Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется:
   A) Аутентификацией
   B) Целостностью
   C) Конфиденциальностью
10. При односторонней аутентификации осуществляется аутентификация:
   A) Отправителя
   B) Получателя
   C) KDC

Самостоятельная работа №2 – Подсистема аутентификации

Аутентификация (установление подлинности) (Authentication) — процедура проверки принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности (чаще всего, логина и пароля). Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает).

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

набор символов (пароль, секретный ключ, персональный идентификатор и т.п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);

физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Как уже упоминалось ранее, существует множество технологий, призванных повысить сетевую безопасность, и все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки.

Под аутентификацией подразумевается аутентификация пользователя или конечного устройства (хост клиента, сервер, коммутатор, маршрутизатор, межсетевой экран и т.д.) и его местоположения с последующей авторизацией пользователей и конечных устройств. Целостность данных включает такие области, как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных.

Аутентификация в стандарте IEEE 802.11 (Рис.2.1.) ориентирована на аутентификацию клиентского устройства радиодоступа, а не конкретного клиента как пользователя сетевых ресурсов. Процесс аутентификации клиента беспроводной локальной сети IEEE 802.11 и состоит из следующих этапов:

1. Клиент посылает кадр (фрейм) запроса Probe Request во все радиоканалы.

2. Каждая точка радиодоступа (Access Point, AP), в зоне радиуса действия которой находится клиент, посылает в ответ фрейм Probe Response.

3. Клиент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию Authentication Request.

4. Точка радиодоступа посылает подтверждение аутентификации Authentication Reply.

5. В случае успешной аутентификации клиент посылает точке доступа запрос на соединение (ассоциирование) Association Request.

6. Точка доступа посылает в ответ фрейм подтверждения ассоциации Association Response.

7. Клиент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

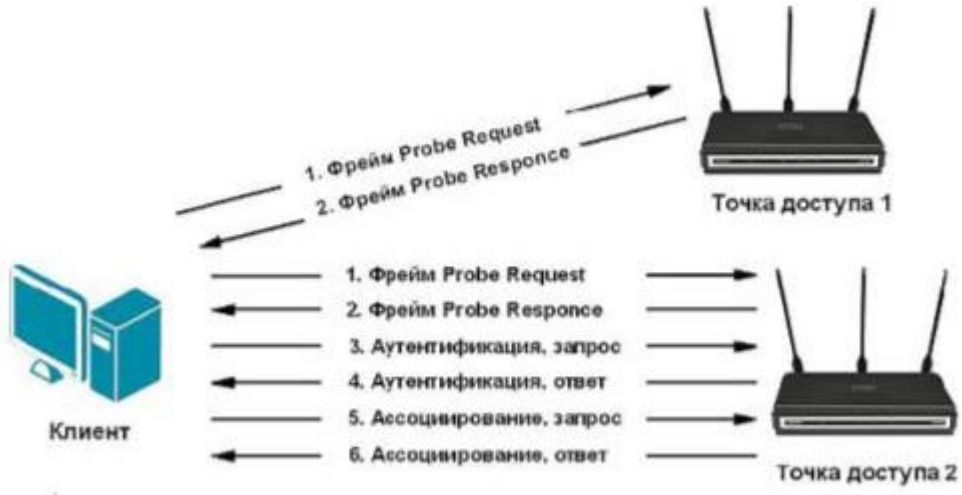


Рис. 2.1. Аутентификация по стандарту 802.11

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Процесс аутентификации с общим ключом аналогичен процессу открытой аутентификации, отличаясь тем, что данный метод требует настройки статического ключа шифрования WEP, идентичного на клиентском устройстве (беспроводной адаптер) и на беспроводной точке доступа.

Аутентификация клиента по его MAC-адресу поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса клиента либо со списком разрешенных (или запрещенных) адресов клиентов, внесенным в MAC-таблицу точки доступа, либо с помощью внешнего сервера аутентификации (рис. 2.2). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних пользователей.

2.2 Аутентификация с помощью внешнего сервера

Открытая аутентификация не позволяет точке доступа определить, разрешен ли клиенту доступ к сети или нет. Это становится уязвимым местом в системе безопасности в том случае, если в беспроводной локальной сети не используется так называемое WEP-шифрование. В случаях, когда использование WEP-шифрования не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Интернет-шлюзов.

Стандарт IEEE 802.11 требует передачи MAC-адресов клиента и точки радиодоступа в открытом виде. В результате этого в беспроводной сети, использующей аутентификацию по MAC-адресу, злоумышленник может обмануть метод аутентификации путём подмены своего MAC-адреса на разрешенный.

Первым стандартом шифрования данных в беспроводных сетях стал протокол WEP (Wired Equivalent Privacy). Шифрование осуществляется с помощью 40 или 104-битного ключа (поточное шифрование с использованием алгоритма RC4 на статическом ключе) и дополнительной динамической составляющей размером 24 бита, называемой вектором инициализации (Initialization Vector, IV).

Процедура WEP-шифрования выглядит следующим образом. Первоначально передаваемые в пакете данные проверяются на целостность (алгоритм CRC-32) для получения значения контроля целостности (Integrity CheckValue, ICV), добавляемого в конец исходного сообщения. Далее генерируется 24-битный вектор инициализации (IV), а к нему добавляется статический (40- или 104-битный) секретный ключ. Полученный таким образом 64- или 128-битный ключ и является исходным ключом для генерации псевдослучайного числа, которое используется для шифрования данных. Далее данные смешиваются (шифруются) с помощью логической операции XOR с псевдослучайной ключевой последовательностью, а вектор инициализации добавляется в служебное поле кадра.

Рис. 2.3 Формат WEP-кадра

Как и любая другая система безопасности на основе паролей, надежность WEP зависит от длины и состава ключа, а также частоты его смены. Первый серьезный недостаток – применение статического ключа – за относительно небольшое время ключ можно подобрать перебором. И второй недостаток WEP-шифрования – самосинхронизация для каждого сообщения,

поскольку вектор инициализации передается незашифрованным текстом с каждым пакетом и через небольшой промежуток времени он повторяется. В результате протокол шифрования WEP на основе алгоритма RC4 в настоящее время не является стойким.

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях — конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

методы, использующие постоянные (многократно используемые) пароли;

методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) — специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

1) пассивные (карточки с памятью);
2) активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двукомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100% идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти

методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Биометрические системы идентификации, доступные в настоящее время или находящиеся в стадии разработки, включают системы доступа по отпечатку пальца, аромату, ДНК, форме уха, геометрии лица, температуре кожи лица, клавиатурному почерку, отпечатку ладони, рисунку вен ладони, структуре сетчатки глаза, рисунку радужной оболочки глаза, подписи и голосу.

Аутентификация по отпечаткам пальцев. Эта биометрическая технология, вполне вероятно, в будущем будет использоваться наиболее широко. Преимущества средств доступа по отпечатку пальца - простота использования, удобство и надежность. Весь процесс идентификации осуществляется довольно быстро и не требует особых усилий от пользователей. Вероятность ошибки при идентификации пользователя намного меньше в сравнении с другими биометрическими методами. Кроме того, устройство идентификации по отпечатку пальца достаточно компактно - в настоящее время уже производятся подобные системы размером меньше колоды карт.

Аутентификация по радужной оболочке глаза. Преимущество сканирования радужной оболочки состоит в том, что образец пятен на радужной оболочке находится на поверхности глаза, и от пользователя не требуется специальных усилий - фактически видеоизображение глаза может быть отсканировано на расстоянии метра, что делает возможным использование таких сканеров в банкоматах. Идентифицирующие параметры могут сканироваться и кодироваться, в том числе, и у людей с ослабленным зрением, но неповрежденной радужной оболочкой. Катаракта - повреждение хрусталика глаза, которое находится позади радужной оболочки, также никоим образом не влияет на процесс сканирования радужной оболочки.

Аутентификация по сетчатке глаза. Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Сканеры для сетчатки глаза получили большое распространение в сверхсекретных системах контроля доступа, так как эти средства аутентификации характеризуются одним из самых низких процентов отказа в доступе зарегистрированным пользователям и почти нулевым процентом ошибочного доступа. Однако такая болезнь глаз, как катаракта, может отрицательно воздействовать на качество получаемого изображения и увеличивать ошибки системы.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий

аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Контрольные вопросы:

1) Чем определяется стойкость подсистемы идентификации и аутентификации?

2) Перечислить минимальные требования к выбору пароля.

3) Перечислить минимальные требования к подсистеме парольной аутентификации.

4) Как определить вероятность подбора пароля злоумышленником в течении срока его действия?

5) Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Тест по самостоятельной работе №2:

1. Аутентификация – это
   A) Невозможность несанкционированного доступа к данным
   B) Подтверждение того, что информация получена из законного источника законным получателем
   C) Невозможность несанкционированного просмотра и модификации информации
2. Выберите команду, позволяющую вывести список сетевых имен работающих в данный момент компьютеров Вашей сети:
   A) Net computer
   B) Net view
   C) Net config
   D) Net group
3. Укажите, кто входит в группу пользователей Все в операционной системе Windows:
   A) Все пользователи локальной сети;
   B) Все пользователи сети предприятия;
   C) Все зарегистрированные в операционной системе пользователи.

4. Какой из сетевых компонентов Windows отвечает за адресацию узлов сети на сетевом уровне?

A) Адаптер;

B) Сетевой протокол;

C) Клиент;

D) Служба

5. Какой из сетевых компонентов Windows обеспечивает возможность предоставления ним сетевых ресурсов?

A) Адаптер;

B) Сетевой протокол;

C) Клиент;

D) Служба

6. Выберите типы доступа для сетевых дисков и папок, определяемых в операционной системе Windows:

A) Чтение;

B) Чтение и выполнение;

C) Изменение;

D) Запись;

E) Полный доступ;

F) Просмотр;

G) Список содержимого папки.

7. Выберите соответствие названий и определений сетевых компонентов Windows, приведенных в списке:

A) Адаптер;

B) Протокол;

C) Клиент;

D) Служба

8. Укажите вводимую в окне командной строки команду, отображающую IP-адрес компьютера, работающего под операционной системой Windows:

A) Cmd;

B) Net;

C) Ipconfig;

D) Netstat.

9. Укажите преимущества использования компьютерных сетей:

A) Возможность оперативной коммуникации между участниками сети и оперативного доступа к информации;

B) Возможность совместного использования аппаратных ресурсов;

C) Возможность практически безграничного увеличения вычислительной производительности систем;

D) Возможность организации совместной работы путем разделения прикладных программ и файлов;

E) Упрощение конфигурирования и пользования операционными системами и пользовательскими программами;

F) Возможность централизованного управления данными и программами.

10. Выберите ресурсы, выделяемые операционной системой сетевому адаптеру:

A) MAC-адрес адаптера;

B) Порт ввода-вывода (I/O port);

C) Полоса пропускания канала;

D) Запрос прерывания IRQ;

E) Диапазон адресов памяти адаптера.

Самостоятельная работа №3 – Функции межсетевых экранов, профили защиты

Межсетевым экраном называют особый программный продукт, используемый для защиты определенных частей компьютерной сети организации. Применяя межсетевой экран, можно разделить компьютерную сеть на две части и задать правила фильтрации пакетов данных при переходе из одной части в другую. Наиболее часто эта граница проводится между корпоративной сетью компании и сетью Интернет. Межсетевой экран также называют брандмауэром или файрволом (firewall). Исторически применение файрволов стало одним из первых способов защиты корпоративных сетей предприятий. В настоящее время использование сетевого экрана является одним из основных правил защиты сети.

Для осуществления функций контроля межсетевого доступа файрвол должен находится между защищаемой сетью компании и потенциально враждебной внешней сетью. При этом все операции по передаче данных между этими сетями должны реализовываться только через него. Межсетевой экран дает возможность решить, как правило, две основных задачи:

- контроль и ограничение доступа из внешних источников к внутренним ресурсам сети. Ограничение доступа необходимо при подключении к корпоративной сети компании клиентов и партнеров, а также при попытках несанкционированного доступа со стороны злоумышленников.
- ограничение доступа пользователей внутренней сети к внешним ресурсам данных. Как правило, это ресурсы, не имеющие прямого отношения к выполнению сотрудниками рабочих функций.

Межсетевой экран способен выполнять большое количество разных функций по обеспечению информационной безопасности. В основном, его функционал зависит от поставленных перед ним администратором сети задач.

Смысл фильтрации потоков информации состоит в выборочном пропускании через брандмауэр случайных пакетов данных. Определение потенциально опасной информации основывается на загружаемых в файрвол правилах, которые, в свою очередь, определяются политикой безопасности, принятой в данной компании. Правила, загружаемые в файрвол, обозначают как набор фильтров, каждый из которых отвечает за определенный критерий отбора.

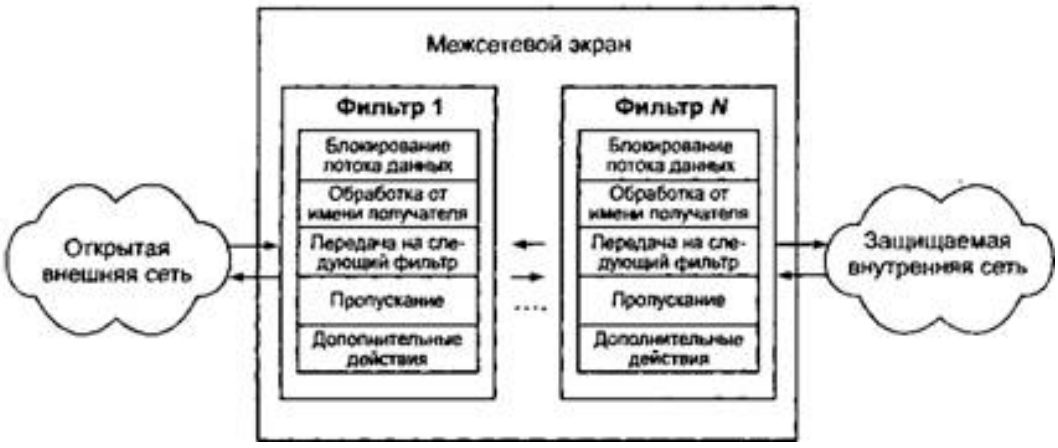


Рис. 3.1. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем:

1) анализа информации по заданным в интерпретируемых правилах критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

2) принятия на основе интерпретируемых правил одного из следующих решений:

• не пропустить данные;
• обработать данные от имени получателя и возвратить результат отправителю;
• передать данные на следующий фильтр для продолжения анализа;
• пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например, преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

• разрешение или запрещение дальнейшей передачи данных;
• выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:
• служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
• непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
• внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень

модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

Таким образом, при выполнении файрволом функций посредничества, при необходимости доступа из одной части сети в другую, первоначально создается соединение с программой-посредником, которая проверяет допустимость запрошенного взаимодействия и, при его допустимости, уже сама устанавливает соединение с нужным ресурсом. Далее, обмен информацией осуществляется только через эту программу-посредник. Создание такого механизма взаимодействия ресурсов дает возможность решить целый ряд задач: проверка подлинности передаваемых данных, фильтрация потока информации – поиск вирусов, шпионов и т. д., кэширование данных.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:
• проверку подлинности передаваемых данных;
• фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
• разграничение доступа к ресурсам внутренней сети;
• разграничение доступа к ресурсам внешней сети;
• кэширование данных, запрашиваемых из внешней сети;
• идентификацию и аутентификацию пользователей;
• трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
• регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Программы-посредники могут осуществлять проверку подлинности получаемых и передаваемых данных. Это актуально не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Программы-посредники могут выполнять разграничение доступа к ресурсам внутренней или внешней сети, используя результаты идентификации и аутентификации пользователей при их обращении к МЭ.

Способы разграничения доступа к ресурсам внутренней сети практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы.

При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:
• разрешение доступа только по заданным адресам во внешней сети;
• фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
• накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:
• экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
• универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов, или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных и, если какой-либо объект не соответствует заданным критериям, то либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например, обезвреживает обнаруженные компьютерные вирусы. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN (Virtual Private Network), например, безопасно объединять несколько локальных сетей, подключенных к Internet, в одну виртуальную сеть.

Помимо выполнения фильтрации трафика и функций посредничества некоторые МЭ позволяют реализовывать другие, не менее важные функции, без которых обеспечение защиты периметра внутренней сети было бы неполным.

Идентификация и аутентификация пользователей. Кроме разрешения или запрещения допуска различных приложений в сеть, МЭ могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым МЭ.

Прежде чем пользователю будет предоставлено право использования какого-либо сервиса, необходимо убедиться, что он действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции МЭ. Авторизация пользователя обычно рассматривается в контексте аутентификации — как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности — пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Internet произошли отчасти из-за уязвимости традиционных многоразовых паролей. Злоумышленники могут наблюдать за каналами в сети Internet и перехватывать передающиеся в них открытым текстом пароли, поэтому такая схема аутентификации считается неэффективной. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде (рис. 3.2). Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов.

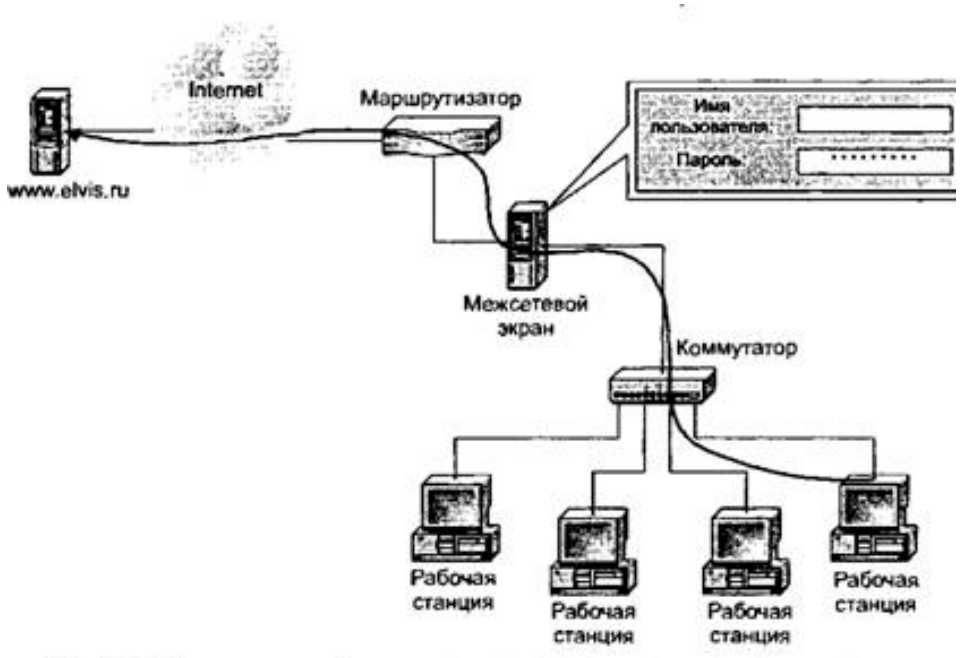


Рис. 3.2. Схема аутентификации пользователя по предъявляемому паролю

Требования к безопасности конкретных средств и информационных систем устанавливаются на основании угроз, которые уже есть или

прогнозируются, в соответствии с политикой безопасности и условий применения этих средств(систем). Требования, которые являются общими для некоторого типа продуктов или информационных систем, можно объединить в структуру, называемую профилем защиты. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" **профиль защиты (ПЗ)** - это независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

Продукт ИТ - совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ.

Изделие ИТ - обобщенный термин для продуктов и систем ИТ.

ПЗ не регламентирует, каким образом должны быть выполнены данные требования, тем самым предоставляя возможность разработчику системы защиты самостоятельно выбирать средства защиты. ПЗ может применяться либо к определенному классу продуктов, например, операционным системам или межсетевым экранам, и к совокупности продуктов, образующих систему информационной технологии. Использование профилей защиты преследует три основные задачи:

1. стандартизация наборов требований к информационным продуктам;
2. оценка безопасности;
3. проведение сравнительного анализа уровней безопасности различных изделий ИТ.

ПЗ подлежат оценке, регистрации и сертификации в соответствии с руководящими документами ФСТЭК России.

Разработчиком ПЗ может быть, как юридическое, так и физическое лицо.

ПЗ должен содержать:

потребности пользователя изделия ИТ в обеспечении информационной безопасности;

описание среды безопасности изделия ИТ – обоснованность применения данного ИТ с учетом угроз среды, политики безопасности и пр.

цели безопасности изделия ИТ- то есть что должно быть сделано в результате использования данного ИТ;

функциональные требования к безопасности и требования доверия к безопасности. Функциональные требования отображают то, что должно выполнять ИТ и его среда, а требования доверия к безопасности отображают степень уверенности в функционале данного ИТ. Совокупность этих требований должна обеспечить достижение целей безопасности;

обоснование достаточности выдвинутых требований.

Контрольные вопросы:

1) Что такое межсетевой экран?
2) Каковы функции межсетевого экрана?
3) В чем состоит фильтрация информационных потоков?
4) Перечислите проблемы безопасности межсетевых экранов.
5) Какие бывают типы межсетевых экранов?

Тест по самостоятельной работе №3:

1. При разработке политики безопасности главное, что должен определить собственник информационных активов:
   A) Атаки, которые возможны на информационные ценности.
   B) Множество файлов, доступ к которым должен быть запрещен.
   C) Множество сервисов, которые не должны быть доступны посторонним.
   D) Информационные ценности, безопасность которых следует обеспечивать.
2. Что из перечисленного может не являться уязвимостью:
   A) Ошибка в настройках межсетевого экрана.
   B) Ошибка в настройках маршрутизации.
   C) Ошибка в программном обеспечении.
   D) Слабое место в системе, с использованием которого может быть осуществлена атака.
3. Сервис безопасности – это
   A) Сервис, который обеспечивает взаимодействие с вышестоящей организацией.
   B) Сервис, который предотвращает несанкционированный доступ к файлам и программам.
   C) Сервис, который обеспечивает задаваемую политикой безопасность информационных систем и/или передаваемых данных.
   D) Сервис, который определяет осуществление атаки.
4. Что не относится к понятию «оборона в глубину»:
   A) Использование нескольких взаимосвязанных между собой технологий.
   B) Использование аппаратных средств разных производителей.
   C) Использование нескольких коммутаторов.
   D) Использование нескольких межсетевых экранов.
5. Риск – это
   A) Невозможность ликвидировать все уязвимости в информационной системе.

B) Невозможность исправить все ошибки в программном обеспечении.
C) Вероятность того, что в системе остались неизвестные уязвимости.
D) Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.

6. Повторное использование перехваченного ранее сообщения называется
   A) DDoS-атакой.
   B) Replay-атакой.
   C) Атакой «man-in-the-middle».
   D) DoS-атакой.
7. Что не относится к DoS-атаке:
   A) Выполнение незаконного проникновения в систему.
   B) Определение топологии сети.
   C) Попытка монополизировать сетевое соединение.
   D) Попытка исчерпать какие-либо ресурсы на целевой системе.
8. Что не относится к атаке «man in the middle»:
   A) Исчерпание ресурсов на целевой системе.
   B) Выполнение незаконного проникновения в систему.
   C) Просмотр передаваемых данных.
   D) Изменение передаваемых данных.
9. Что не относится к пассивной атаке:
   A) Изменение передаваемых данных.
   B) Просмотр передаваемых данных.
   C) Выполнение незаконного проникновения в систему.
   D) Изучение топологии сети.
10. Атаки сканирования могут определять:
    A) Топологию целевой сети.
    B) ПО сервера, которое выполняется на хостах.
    C) Типы сетевого трафика, пропускаемые межсетевым экраном.
    D) Номера версий для всего обнаруженного ПО.
    E) Операционные системы, которые выполняются на хостах.

Самостоятельная работа №4 – Типы межсетевых экранов

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика. Из материала следующих разделов вы увидите, что степень обеспечиваемой этими устройствами защиты зависит от того, каким образом они применены и настроены.

Сетевой/межсетевой экран (МСЭ) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов по различным протоколам в соответствии с заданными правилами.

Основной задачей межсетевого экрана является защита компьютерных сетей и/или отдельных узлов от несанкционированного доступа. Иногда межсетевые экраны называют **фильтрами**, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Для того чтобы эффективно обеспечивать безопасность сети, межсетевой экран отслеживает и управляет всем потоком данных, проходящим через него. Для принятия управляющих решений для TCP/IP-сервисов (то есть передавать, блокировать или отмечать в журнале попытки установления соединений) межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений.

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: дать ему возможность пройти или нет. Для того чтобы межсетевой экран мог осуществить эту операцию, ему необходимо определить набор правил фильтрации. Решение о том, фильтровать ли с помощью межсетевого экрана пакеты данных, связанные с конкретными протоколами и адресами, зависит от принятой в защищаемой сети политики безопасности. По сути, межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности. Политика сетевой безопасности каждой организации должна включать (кроме всего прочего) две составляющие: политика доступа к сетевым сервисам и политика реализации межсетевых экранов.

Однако недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений – главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное

из прошлого потока данных), так и состояние приложения (полученное из других приложений).

Таким образом, управляющие решения требуют, чтобы межсетевой экран имел доступ, возможность анализа и использования следующих факторов:

• информации о соединениях – информация от всех семи уровней (модели OSI) в пакете;

• истории соединений – информация, полученная от предыдущих соединений;

• состоянии уровня приложения – информация о состоянии соединения, полученная из других приложений;

• манипулировании информацией – вычисление разнообразных выражений, основанных на всех вышеперечисленных факторах

При использовании межсетевого экрана прикладного уровня все соединения проходят через него (см. рис. 4.1). Как показано на рисунке, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

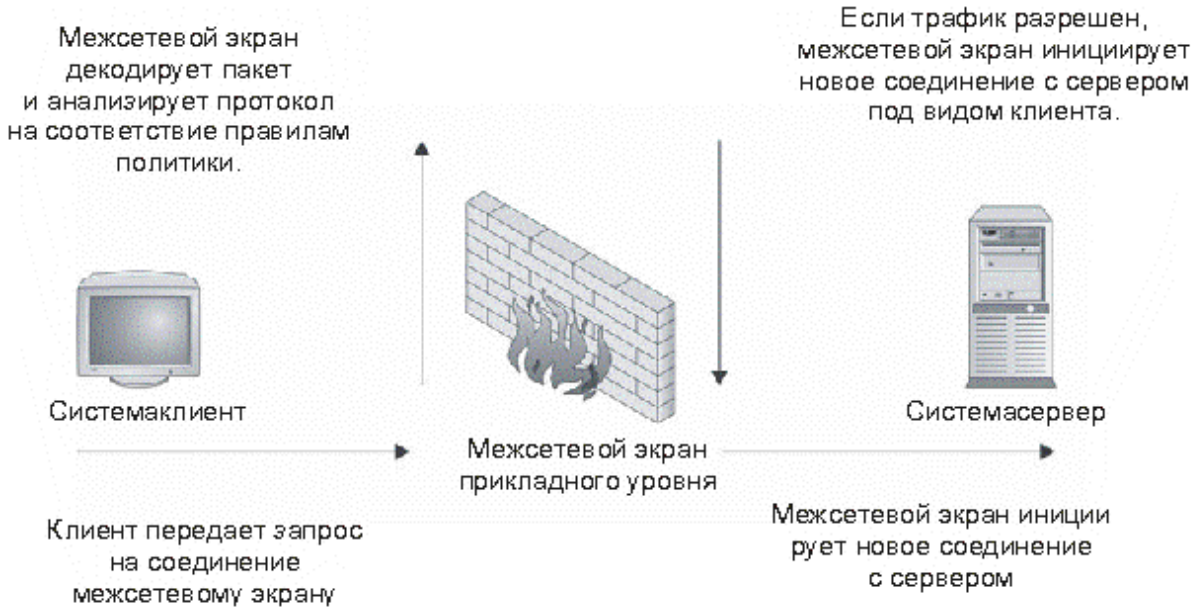


Рис. 4.1. Соединения модуля доступа межсетевого экрана прикладного уровня

Различают несколько типов межсетевых экранов в зависимости от следующих характеристик:

• обеспечивает ли экран соединение между одним узлом и сетью или между двумя, или более различными сетями;

• происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели OSI;

• отслеживаются ли состояния активных соединений или нет. В зависимости от охвата контролируемых потоков данных межсетевые экраны подразделяются на:

• традиционный сетевой (или межсетевой) экран – программа (или неотъемлемая часть операционной системы) на шлюзе или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями;

• персональный межсетевой экран – программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

В зависимости от уровня OSI, на котором происходит контроль доступа, сетевые экраны могут работать на:

• сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;

• сеансовом уровне (также известные, как stateful), когда отслеживаются сеансы между приложениями и не пропускаются пакеты, нарушающие спецификации TCP/IP, часто используемые в злонамеренных операциях – сканирование ресурсов, взломы через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных;

• прикладном уровне (или уровне приложений), когда фильтрация производится на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Фильтрация входящих и исходящих пакетов осуществляется на основе информации, содержащейся в следующих полях TCP- и IP-заголовков пакетов: IP-адрес отправителя; IP-адрес получателя; порт отправителя; порт получателя.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются ненадежными.

К преимуществам такой фильтрации относится:

• сравнительно невысокая стоимость;

• гибкость в определении правил фильтрации;

• небольшая задержка при прохождении пакетов.

Недостатки:

• не собирает фрагментированные пакеты;

• нет возможности отслеживать взаимосвязи (соединения) между пакетами.?

Контрольные вопросы:

1) Выделите два основных типа межсетевых экранов.
2) Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
3) Является ли один из типов межсетевых экранов более безопасным, нежели другой?
4) Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
5) В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
6) Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
7) Что должен обеспечивать межсетевой экран для проверки состояния?
8) При каком условии межсетевой экран прикладного уровня может называться гибридным?
9) Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
10) Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

Тест по самостоятельной работе №4:

1. Информация - это:
   A) Знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в результате физического или умственного опыта
   B) Известия, новости, факты, данные
   C) Сведения, полученные при исследовании, изучении или обучении
   D) Команды или символы представления данных (в системах связи или в компьютере)
2. Аутентификация личности в компьютерных системах может быть реализована при помощи:
   A) Паспорта
   B) Пароля

C) биометрической системы

D) смарт-карты

3. Межсетевой экран - это:

A) Устройство управления доступом, защищающее внутренние сети от внешних атак

B) Устройство кэширования сетевого трафика

C) Устройство маршрутизации трафика

4. Какие параметры могут использоваться в биометрических системах?

A) Отпечатки сетчатки/радужной оболочки

B) Паспорт

C) Отпечатки пальцев

5. Система управления доступом

A) Защищает от внутренних пользователей

B) Ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему

C) Предотвращает атаку через разрешенный канал связи.

6. Основные достоинства парольной аутентификации:

A) Простота реализации

B) Низкая стоимость внедрения

C) Высокая надежность

7. Какие преимущества имеет аппаратная реализация VPN?

A) Скорость

B) Дешевизна

D) Безопасность

8. К основным категориям атак относятся:

A) Атаки прохода

B) Атаки трансформации

D) Атаки на отказ в обслуживании

9. Какие методы используют хакеры при проведении социального инжиниринга?

A) Умение вести телефонную беседу

B) Скрытое сканирование портов

C) Подбор паролей методом перебора

10 . Где лучше размещать VPN сервер?

A) в DMZ интернета, вместе с остальными серверами

B) в отдельной DMZ

C) во внутренней сети компании

Самостоятельная работа №5 – Основные компоненты межсетевых экранов, схемы подключения

Межсетевой экран (МЭ) - это средство защиты информации, осуществляющее анализ и фильтрацию проходящих через него сетевых пакетов. В зависимости от установленных правил, МЭ пропускает или уничтожает пакеты, разрешая или запрещая таким образом сетевые соединения. МЭ является классическим средством защиты периметра компьютерной сети: он устанавливается на границе между внутренней (защищаемой) и внешней (потенциально опасной) сетями и контролирует соединения между узлами этих сетей. Но бывают и другие схемы подключения, которые будут рассмотрены ниже.

Английский термин, используемый для обозначения МЭ - firewall. Поэтому в литературе межсетевые экраны иногда также называют файервол или брандмауэр (немецкий термин, аналог firewall).

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- порт отправителя;
- порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать

эффективные правила фильтрации, их возможности останутся ограниченными.

Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- отсутствует аутентификация на пользовательском уровне.

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например, 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом АСК и содержащий число на единицу большее, чем в принятом пакете (в нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например, 700, а клиент подтверждает его получение передачей пакета АСК, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и АСК, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Обнаружив сетевой сеанс, шлюз приложений останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Для достижения более высокого уровня безопасности и гибкости шлюзы уровня приложений и фильтрующие маршрутизаторы могут быть объединены в межсетевом экране.

Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь

входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

Одним из важных элементов концепции межсетевых экранов является аутентификация, то есть пользователь получает право воспользоваться тем или иным сервисом только после того, как будет установлено, что он действительно тот, за кого себя выдает. При этом считается, что сервис для данного пользователя разрешен.

При получении запроса на использование сервиса от имени какого-либо пользователя межсетевой экран проверяет, какой способ аутентификации определен для данного субъекта, и передает управление серверу аутентификации. После получения положительного ответа от сервера аутентификации межсетевой экран осуществляет запрашиваемое пользователем соединение. Как правило, большинство коммерческих межсетевых экранов поддерживает несколько различных схем аутентификации, предоставляя администратору сетевой безопасности возможность сделать выбор наиболее приемлемой в сложившихся условиях схемы.

Рассмотрим теперь вопросы, связанные с установкой МЭ.
Ниже представлены типовые схемы подключения МЭ. В первом случае (рис. 5.1a), МЭ устанавливается после маршрутизатора и защищает всю внутреннюю сеть. Такая схема применяется, если требования в области защиты от несанкционированного межсетевого доступа примерно одинаковы для всех узлов внутренней сети. Например, "разрешать соединения, устанавливаемые из внутренней сети во внешнюю, и пресекать попытки подключения из внешней сети во внутреннюю". В том случае, если требования для разных узлов различны (например, нужно разместить почтовый сервер, к которому могут подключаться "извне"), подобная схема установки межсетевого экрана не является достаточно безопасной. Если в нашем примере нарушитель, в результате реализации сетевой атаки, получит контроль над указанным почтовым сервером, через него он может получить доступ и к другим узлам внутренней сети.

В подобных случаях иногда перед МЭ создается открытый сегмент сети предприятия (рис. 5.1b), а МЭ защищает остальную внутреннюю *сеть*. Недостаток данной схемы заключается в том, что подключения к узлам открытого сегмента МЭ не контролирует.

Более предпочтительным в данном случае является использование МЭ с тремя сетевыми интерфейсами (рис. 5.1c). В этом случае, МЭ конфигурируется таким образом, чтобы правила доступа во внутреннюю сеть были более строгими, чем в открытый сегмент. В то же время, и те, и другие соединения могут контролироваться МЭ. Открытый сегмент в этом случае иногда называется "демилитаризованной зоной" - DMZ.

Еще более надежной считается схема, в которой для защиты сети с *DMZ* задействуются два независимо конфигурируемых МЭ (рис. 5.1d). В этом случае, МЭ 2 реализует более жесткий набор правил фильтрации *по* сравнению с МЭ1. И даже успешная атака на первый МЭ не сделает внутреннюю сеть беззащитной.

В последнее время стал широко использоваться вариант установки программного МЭ непосредственно на защищаемый компьютер. Иногда такой МЭ называют "персональным". Подобная схема позволяет защититься от угроз, исходящих не только из внешней сети, но из внутренней.

Типовые схемы подключения межсетевых экранов (Рисунок 5):

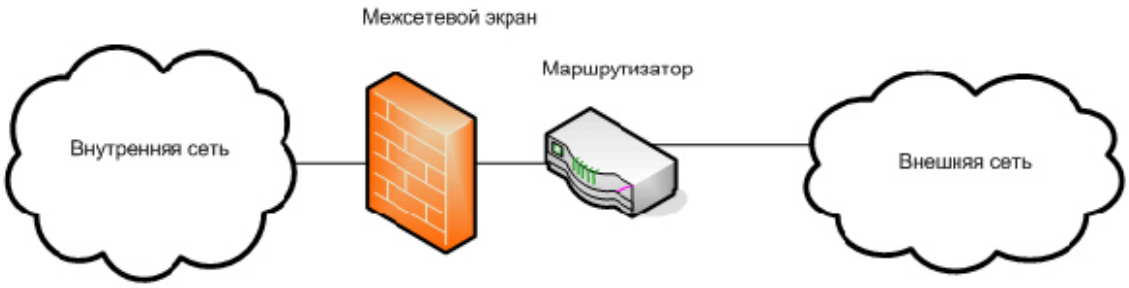


Рис. 5.1a - подключение межсетевого экрана с двумя сетевыми интерфейсами для "единообразной" защиты локальной сети

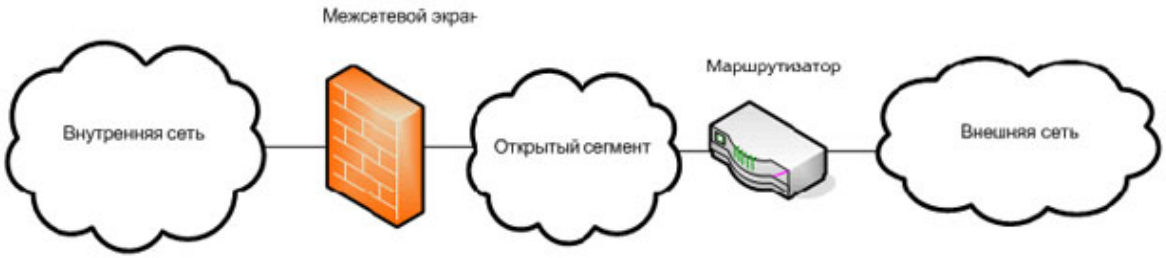


Рис. 5.1b - подключение межсетевого экрана с двумя сетевыми интерфейсами при выделении открытого сегмента внутренней сети

Рис. 5.1c - подключение межсетевого экрана с тремя сетевыми интерфейсами для защиты внутренней сети и ее открытого сегмента

Рис. 5.1d - подключение двух межсетевых экранов для защиты внутренней сети и ее открытого сегмента

Контрольные вопросы:

1) В чем заключается механизм межсетевого экранирования?
2) Дайте определение межсетевого экрана.
3) Принцип функционирования межсетевых экранов с фильтрацией пакетов.
4) На уровне каких протоколов работает «шлюз сеансового уровня»?
5) В чем особенность межсетевых экранов экспертного уровня?

Тест по самостоятельной работе №5:

1. При удаленном администрировании необходимо:

   А) Разрешать доступ только из локальной сети

B) Разрешать доступ только из демилитаризованной зоны

C) Использовать безопасные протоколы

2. Выберите правильное утверждение:

A) Для web сервера всегда следует использовать специальные appliances

B) Для web-сервера всегда следует удалять или запрещать не требуемые web серверу сетевые сервисы

C) Для web-сервера всегда следует использовать Trusted OC

3. Зонный файл содержит:

A) Логи name-сервера

B) Конфигурационные опции

C) Ресурсные записи

4. Активным содержимым на стороне клиента являются:

A) Интерактивные элементы, обрабатываемые клиентом (web-браузером)

B) Интерактивные элементы HTML, с помощью которых сервер может получать информацию клиента

C) Интерактивные элементы, создающие HTML страницы на стороне сервера

5. Управление доступом в пакетном фильтре осуществляется на основании:

A) Порта источника

B) Порта назначения

C) Типа трафика

6. Действие может быть:

A) Наследовано из родительского контекста

B) Задано по умолчанию

C) Указано для каждого правила

7. При DIGEST-аутентификации в качестве аутентификатора используется:

A) Пароль пользователя

B) Сертификат сервера

C) Пароль сервера

D) Сертификат пользователя

8. Основное назначение firewall'a состоит в том, чтобы:

A) Защитить хосты и сети от использования существующих уязвимостей в стеке протоколов TCP/IP

B) Обнаружить проникновение в локальную сеть

C) Обеспечить полную безопасность локальной сети

9. Обычно в ПО web-сервера имеются следующие файлы, содержащие логи:

A) Transfer Log, Error Log

B) Info Log, Error Log

C) Agent Log, Referrer Log

10. При использовании IDS:

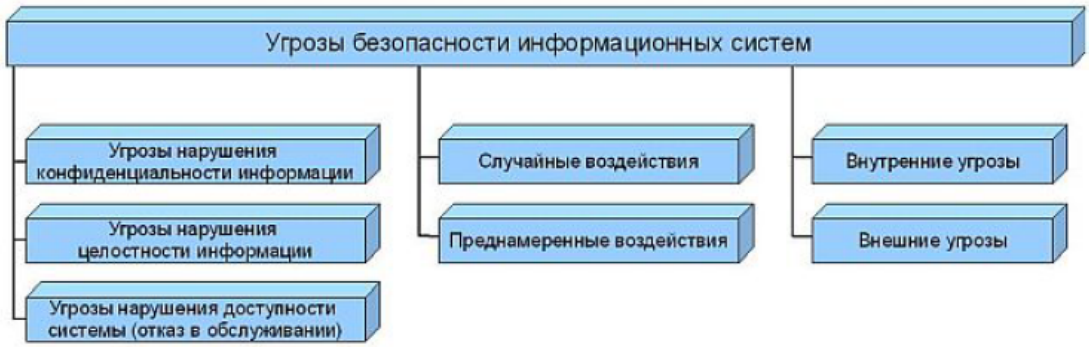
A) Возрастает возможность определения преамбулы атаки

B) Возрастает возможность фильтрования трафика

C) Возрастает возможность раскрытия осуществленной атаки

Самостоятельная работа №6 – Программные и аппаратные средства криптографической защиты

Угрозы безопасности информационных систем классифицируются по нескольким признакам (рис. 6.1).



6.1 Классификация угроз информационной безопасности

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциальной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. Несанкционированный доступ к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, копирование этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством сети передачи данных, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации. Целостность информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи). Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется авторизованными пользователями с обоснованной целью.

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам.

Причины случайных воздействий:

• аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;

• ошибки в программном обеспечении;

• ошибки в работе обслуживающего персонала и пользователей;

• помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет место так называемый "человеческий фактор", когда человек не умышленно, по ошибке, совершает действия, приводящие к разглашению конфиденциальной информации или к нарушению доступности информационной системы. Большую долю конфиденциальной информации злоумышленник (конкурент) может получить при несоблюдении работниками-пользователями компьютерных сетей элементарных правил защиты информации. Это может проявиться, например, в примитивности паролей или в том, что сложный пароль пользователь хранит на бумажном носителе на видном месте или же записывает в текстовый файл на жестком диске и пр. Утечка конфиденциальной информации может происходить при использовании незащищенных каналов связи, например, по телефонному соединению.

Под внешними угрозами безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

• атаки из внешней сети (например, Интернет), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;

• распространение вредоносного программного обеспечения;

• нежелательные рассылки (спам);

• воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;

• перехват информации с использованием радиоприемных устройств;

• воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;

• воздействие на персонал предприятия с целью получения конфиденциальной информации.

В современном мире, когда стало возможным применять сервисы и службы с использованием информационной коммуникационной среды (электронные платежи, Интернет-магазины, электронные очереди и т.п.), многократно увеличивается риск именно внешних угроз.

Как правило, несанкционированный доступ, перехват, хищение информации, передаваемой по каналам связи, проводится средствами технической разведки, такими как радиоприемные устройства, средства съема акустической информации, системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций, средства съема информации с кабелей связи и другие.

Вредоносное программное обеспечение и, прежде всего, компьютерные вирусы представляют очень серьезную опасность для информационных систем. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. В то же время чрезмерное преувеличение угрозы вирусов негативно влияет на использование всех возможностей компьютерной сети. Знание механизмов действия вредоносного программного обеспечения (ПО), методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и нанесения вреда машинам и информации.

О наличии вредоносного ПО в системе пользователь может судить по следующим признакам:

• появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств;

• явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе;

• неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств компьютерной системы – увеличение времени обработки той или иной информации (т.н. "задумчивость" ПК), необоснованное уменьшение свободного объёма на дисковых носителях, отказ выполнять программы-сканеры вирусной активности, "зависания" системы и т.п.;

• рассылка писем, которые пользователем не отправлялись, по электронной почте.

Вредоносная программа (Malware, malicious software – злонамеренное программное обеспечение) – это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стало то, что технологии детектирования систем антивирусных компаний отличаются друг от друга и, как следствие, невозможно унифицировать результаты проверки разными антивирусными программами. Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов. Последним значительным проектом подобного рода было создание стандарта CME (Common Malware Enumeration), суть которого заключается в присвоении одинаковым детектируемым объектам единого уникального идентификатора.

Контрольные вопросы:

1) Какие свойства присущи информации?

2) Дайте понятие объекта защиты информации.

3) Что относят к информационным процессам?

4) Что понимают под информационной системой?

5) Что называют информационными ресурсами?

6) Что понимают под угрозой информации, дайте понятие искусственных и естественных угроз, приведите примеры.

7) Что составляет основу политики безопасности?

8) Сделайте сравнительный анализ избирательной и полномочной политики безопасности.

9) Проанализируйте механизмы и свойства защиты информации.

Тест по самостоятельной работе №6:

1. Аутентификация – это
   A) Невозможность несанкционированного просмотра и модификации информации
   B) Невозможность несанкционированного доступа к данным
   C) Подтверждение того, что информация получена из законного источника законным получателем

2. Политика безопасности – это

A) Только множество критериев, в основе которых лежат сервисы безопасности

B) Как административные меры, так и множество критериев для сервисов безопасности

C) Только совокупность административных мер, которые определяют порядок прохода в компьютерные классы

3. Под DoS-атакой понимается:

A) Повторное использование переданного ранее сообщения

B) Модификация передаваемого сообщения

D) Модификация передаваемого сообщения

4. Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется:

A) Целостностью
B) Аутентификацией
D) Конфиденциальностью

5. В таблице кодировки ASCII+ печатные и управляющие символы занимают:

A) Последние 128 позиций таблицы
B) Все 256 символов таблицы
C) Последние 127 позиций таблицы
D) Первые 128 позиций таблицы
E) Первые 127 позиций таблицы

6. Бит определяет информацию:

A) В ответе на вопрос "да" или "нет"
B) Которая может быть представлена любым целым числом
C) Содержащуюся в 8 байтах

7. Когда в криптографии стало использоваться асимметричное шифрование?

A) В первой половине XIX;
B) В первой половине XX;
C) Во второй половине XX
D) Во второй половине XIX;

8. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?

A) Ключ
B) Алгоритм
C) Протокол
D) Шифр

9. Выберите правильное определение термина «криптография»

A) Криптография изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации
B) Криптография изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
C) Криптография – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи
D) Криптография – это наука о преодолении криптографической защиты информации

10. Что из перечисленного может не являться уязвимостью:

A) Ошибка в настройках межсетевого экрана.
B) Ошибка в настройках маршрутизации.
C) Ошибка в программном обеспечении.
D) Слабое место в системе, с использованием которого может быть осуществлена атака.

Самостоятельная работа №7 – Критерии оценки защищенности криптографических модулей

В федеральном стандарте США FIPS 140-2 "Требования безопасности для криптографических модулей" под криптографическим модулем понимается набор аппаратных и/или программных (в том числе встроенных) компонентов, реализующих утвержденные функции безопасности (включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию) и заключенных в пределах явно определенного, непрерывного периметра.

В стандарте FIPS 140-2 рассматриваются криптографические модули, предназначенные для защиты информации ограниченного доступа, не являющейся секретной, т. е. речь идет о промышленных изделиях, представляющих интерес для основной массы организаций. Наличие подобного модуля – необходимое условие обеспечения защищенности сколько-нибудь развитой информационной системы, однако, чтобы выполнять предназначенную ему роль, сам модуль также нуждается в защите, как собственными средствами, так и средствами окружения (например, операционной системы).

Согласно стандарту, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

- применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа;
- обеспечение защиты модуля от несанкционированного использования и нештатных методов эксплуатации;
- предотвращение несанкционированного раскрытия содержимого модуля (криптографических ключей и других данных, критичных для безопасности);
- предотвращение несанкционированной и не обнаруживаемой модификации модуля и криптографических алгоритмов, в том числе несанкционированной модификации, подмены, вставки и удаления криптографических ключей и других данных, критичных для безопасности;
- обеспечение отображения (индикации) режима работы (состояния) модуля;
- обеспечение доверия тому, что модуль функционирует должным образом при работе в утвержденном режиме;
- обнаружение ошибок в функционировании модуля и предотвращение компрометации информации ограниченного доступа и данных модуля, критичных для безопасности вследствие подобных ошибок.

Из перечисленных целей вытекают требования безопасности, относящиеся к этапам проектирования и реализации модуля и разделенные в стандарте на одиннадцать групп:

- спецификация криптографического модуля;
- требования к портам и интерфейсам модуля;
- роли, сервисы и аутентификация;
- конечно-автоматная модель;
- физическая безопасность;
- эксплуатационное окружение;
- управление криптографическими ключами;
- электромагнитная совместимость;
- самотестирование;
- доверие проектированию;
- сдерживание прочих атак.

Спецификация модуля включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности.

Среди портов и интерфейсов модуля должны быть выделены обязательные и дополнительные. Следует специфицировать все интерфейсы, а также все маршруты входных и выходных данных. Кроме того, порты для незащищенных параметров, критичных для безопасности, должны быть логически отделены от других портов.

Среди ролей и сервисов необходимо провести логическое разделение на обязательные и дополнительные, обеспечить персональную или ролевую аутентификацию.

Модель в виде конечного автомата должна описывать деление на обязательные и дополнительные состояния.

Меры физической самозащиты модуля включают замки, защитные кожухи, сохраняющие свидетельства вторжений пломбы, средства оперативного выявления и реагирования на попытки вторжений, меры по противодействию атакам, основанным на использовании нештатных внешних условий.

В число поддерживаемых механизмов управления ключами должны входить генерация случайных чисел, распределение ввод/вывод, хранение и обнуление ключей.

На требованиях электромагнитной совместимости мы останавливаться не будем.

При включении питания и при выполнении определенных условий необходимо выполнение тестов криптографических алгоритмов, контроль целостности программного обеспечения, проверки критичных функций.

Меры доверия проектированию должны включать конфигурационное управление, процедуры безопасной установки, генерации и распространения. Следует подготовить функциональную спецификацию, при реализации использовать язык высокого уровня, продемонстрировать соответствие проекта и политики, снабдить пользователей соответствующими руководствами.

Наконец, предусматриваются меры по сдерживанию атак, для которых пока нет стандартизованных требований.

К первому (самому слабому) уровню применяется минимальный набор требований безопасности, которым удовлетворяет, например, шифрующая плата для персонального компьютера. Программные компоненты соответствующих модулей могут выполняться на универсальных вычислительных системах с несертифицированной ОС.

На втором уровне требуются:

- ролевая аутентификация;
- замки на съемных оболочках и дверцах, защитные покрытия и пломбы, сохраняющие свидетельства вторжений;
- использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго.

К третьему уровню предъявляются следующие дополнительные требования:

- отделение портов и интерфейсов, применяемых для нешифрованного ввода/вывода криптографических ключей и других данных, критичных для безопасности;
- персональная аутентификация с проверкой допустимости принятия определенных ролей;
- наличие средств оперативного выявления и реагирования на попытки вторжений (к примеру, микросхемы, обеспечивающие обнуление критичных данных модуля при попытке вскрыть корпус);
- использование ОС, сертифицированных на соответствие определенным профилям защиты с оценочным уровнем доверия не ниже третьего и поддержкой доверенного маршрута.

Четвертый уровень самый сильный. Его требования предусматривают полный спектр мер физической защиты, включая меры по противодействию атакам, берущим на вооружение нештатные внешние условия (электрические или температурные). Операционная система должна соответствовать оценочному уровню доверия не ниже четвертого.

Далее будут детально рассмотрены наиболее содержательные группы требований. Здесь же обратим внимание на параллель с профилем защиты для смарт-карт, общность целого ряда целей, предположений и требований безопасности для криптографических модулей и смарт-карт (что, разумеется,

вполне естественно). На наш взгляд, сравнительный анализ этого профиля и стандарта FIPS140-2 позволяет в полной мере оценить достоинства "Общих критериев" и ассоциированных спецификаций, высокую степень их полноты и систематичности. Конечно, "Общие критерии" можно критиковать, их нужно развивать и совершенствовать, но перевод стандарта FIPS 140-2 на рельсы "Общих критериев", несомненно, повысил бы его качество.

Контрольные вопросы:

1) Наиболее значимыми нормативными документами в области информационной безопасности являются?
2) Что включает в себя методика анализа защищённости?
3) Какие спецификации (шаблоны) для конфигурации наиболее распространенных системных программных средств известны?
4) Что определяют спецификации 1 и 2 уровней?

Тест по самостоятельной работе №7:

1. Атаки, влияющие на доступность и надежность сайта, называются:
   A) Denial of Service
   B) DoS
   C) атаками на отказ в обслуживании
   D) DsO
   E) Down Service
2. Термин, описывающий данный тип атаки, он основан на управлении личностью человека для достижения своей цели:
   A) Cracking
   B) Hacking
   C) Physical attack
   D) Social engineering
   E) Denial of Service
3. Червь Red Code появился в:
   A) Китае
   B) России
   C) Бразилии
   D) Японии
   E) Индии
4. Мотивами хакеров являются:
   A) высказывание своего политического мнения
   B) любопытство
   C) уклонение от финансовой ответственности
   D) желание заявить о себе
5. Обеспечение безопасности включает в себя следующие основные задачи:
   A) Обнаружение
   B) Реагирование

C) Предотвращение

6. К атакам на содержимое и информацию можно отнести:
   A) Нарушение конфиденциальности
   B) Повреждение отображаемого на веб-сайте содержимого
   C) Мошенничество
   D) Удаление файлов
7. Проникновение посредством незаконной аутентификации в одной учетной записи для перемещения финансовых средств в другую учетную запись - это следующий тип атаки:
   A) Аннулирование транзакции
   B) Маскарад
   C) Взлом таблиц маршрутизаторов
   D) Мошенничество
8. Они защищают внутренние ресурсы, маскируя реальные IP-адреса компьютеров и блокируя попытки доступа к сети, инициированные извне, если только внешний пользователь не является законным и авторизованным сотрудником организации:
   A) Firewalls
   B) Брандмауэры
   C) Маршрутизаторы
   D) Сетевые экраны
9. Атаки, направленные не на конкретную организацию, а на большое число потенциальных жертв - это:
   A) Атаки широкого диапазона действия
   B) Атаки узконаправленного действия
   C) Универсальные атаки
10 К методологии хакерства можно отнести:
   A) Случайный поиск или разведка для определения жертв
   B) Сбор базовых сведений
   C) Выполнение эксплоита
   D) Создание перечня параметров
   E) Сокрытие действий
   F) Зондирование

Самостоятельная работа №8 – Построение VPN

Интернет все чаще используется в качестве средства коммуникации между компьютерами, поскольку он предлагает эффективную и недорогую связь. Однако Интернет является сетью общего пользования и для того чтобы обеспечивать безопасную коммуникацию через него необходим некий механизм, удовлетворяющий как минимум следующим задачам:

• конфиденциальность информации;

• целостность данных;

• доступность информации;

Этим требованиям удовлетворяет механизм, названный VPN (Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет) с использованием средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

Создание VPN не требует дополнительных инвестиций и позволяет отказаться от использования выделенных линий. В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: хост-хост, хост-сеть и сеть-сеть.

Для наглядности представим следующий пример: предприятие имеет несколько территориально отдаленных филиалов и "мобильных" сотрудников, работающих дома или в разъезде. Необходимо объединить всех сотрудников предприятия в единую сеть. Самый простой способ – это поставить модемы в каждом филиале и организовывать связь по мере необходимости. Такое решение, однако, не всегда удобно и выгодно – порой нужна постоянная связь и большая пропускная способность. Для этого придется либо прокладывать выделенную линию между филиалами, либо арендовать их. И то и другое довольно дорого. И здесь в качестве альтернативы при построении единой защищенной сети можно применять VPN-подключения всех филиалов фирмы через Интернет и настройку VPN-средств на хостах сети.

VPN-соединение всегда состоит из канала типа точка-точка, также известного под названием туннель. Туннель создаётся в незащищённой сети, в качестве которой чаще всего выступает Интернет.

Технология виртуальных частных сетей (VPN — Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

1. шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
2. экранирования (с использованием межсетевых экранов);
3. туннелирования.

Сущность технологии VPN заключается в следующем (рисунок 8.1).

Рис. 6.4. VPN-соединение типа сеть-сеть

Рисунок 8.1. Соединение типа хост-сеть

На все компьютеры, имеющие выход в Интернет (вместо Интернет может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

1. анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

2. вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
3. пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
4. формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

- из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);
- согласно настройкам, выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);
- после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Контрольные вопросы:

1) Для каких целей используется программное обеспечение *VIPNET OFFICE?*

2) Каковы функции ViPNet Manager?

3) Каковы функции ViPNet Координатор?

4) Каковы функции ViPNet Клиент?

5) Какие сервисные функции предоставляет пакет ViPNet OFFICE?

Тест по самостоятельной работе №8:

1. Выберите верные утверждения:
   A) Применение терминального доступа характеризуется снижением затрат на содержание серверов
   B) Применение терминального доступа характеризуется снижением затрат на содержание рабочих станций
   C) Применение терминального доступа характеризуется снижением общего уровня безопасности
2. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   C) Безопасность
3. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента
4. Выберите верные утверждения:
   A) x86 архитектура изначально не была предназначена для использования решений виртуализации
   B) При использовании виртуализации реальная архитектура решения соответствует структуре представления
   C) При использовании виртуализации реальная архитектура решения не скрывается от пользователя
5. Решение задачи консолидации вычислительных ресурсов обеспечивается использованием:
   A) Терминального доступа
   B) Веб – приложений
   C) Виртуализации
6. Виртуализация характеризуется:
   A) Высокой мобильностью пользователей
   B) Сокрытием реальной архитектуры решения от пользователя
   C) Возможностью запуска нескольких ОС на одном компьютере
7. Выберите верные утверждения:
   A) Всякая платформа виртуализации поддерживает виртуализацию всего аппаратного обеспечения

B) Виртуальные машины поддерживают эмуляцию устройств

C) Виртуальная машина может быть перенесена с одного хоста на другой

8. Внутренняя виртуализация сети:

A) Объединение нескольких виртуальных сетей в одну

B) Объединение в единую сеть виртуальных и физических машин

C) Создание виртуальной сети между несколькими виртуальными машинами одного хоста

9. Процесс интеллектуальной балансировки нагрузки является частью:

A) Виртуализации сети

B) Виртуализации ОС

C) Виртуализации серверов приложений

10. Атаки, направленные не на конкретную организацию, а на большое число потенциальных жертв - это:

A) Атаки широкого диапазона действия

B) Атаки узконаправленного действия

C) Универсальные атаки

Самостоятельная работа №9 – Туннелирование в VPN

Туннелирование (от англ. tunnelling — «прокладка туннеля») в компьютерных сетях — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Туннелирование представляет собой метод построения сетей, при котором один сетевой протокол инкапсулируется в другой. От обычных многоуровневых сетевых моделей (таких как OSI или TCP/IP) туннелирование отличается тем, что инкапсулируемый протокол относится к тому же или более низкому уровню, чем используемый в качестве тоннеля.

Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт» для обеспечения конфиденциальности и целостности всей передаваемой порции, включая служебные поля. Туннелирование может применяться на сетевом и на прикладном уровнях. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети (VPN). Туннелирование обычно применяется для согласования транспортных протоколов либо для создания защищённого соединения между узлами сети.

В процессе инкапсуляции (туннелирования) принимают участие следующие типы протоколов:

транспортируемый протокол;

несущий протокол;

протокол инкапсуляции.

Протокол транзитной сети является несущим, а протокол объединяемых сетей — транспортируемым. Пакеты транспортируемого протокола помещаются в поле данных пакетов несущего протокола с помощью протокола инкапсуляции. Пакеты-«пассажиры» не обрабатываются при транспортировке по транзитной сети никаким образом. Инкапсуляцию выполняет пограничное устройство (маршрутизатор или шлюз), которое находится на границе между исходной и транзитной сетями.

Туннель может быть использован, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию. При этом пограничные маршрутизаторы, которые подключают объединяемые сети к транзитной, упаковывают пакеты транспортного протокола объединяемых сетей в пакеты транспортного протокола транзитной сети. Второй пограничный маршрутизатор выполняет обратную операцию.

Обычно туннелирование приводит к более простым и быстрым решениям по сравнению с трансляцией, так как решает более частную задачу, не обеспечивая взаимодействия с узлами транзитной сети.

Основными компонентами туннеля являются:

инициатор туннеля;

маршрутизируемая сеть;

туннельный коммутатор;

один или несколько туннельных терминаторов.

Инициатор туннеля встраивает (инкапсулирует) пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Несмотря на то, что все передаваемые по туннелю пакеты являются пакетами IP, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть и сетью, отличной от Internet. Терминатор туннеля выполняет процесс, который является обратным инкапсуляции — он удаляет новые заголовки и направляет каждый исходный пакет в локальный стек протоколов или адресату в локальной сети. Инкапсуляция сама по себе никак не влияет на защищенность пакетов сообщений, передаваемых по туннелю VPN. Но инкапсуляция даёт возможность полной криптографической защиты инкапсулируемых пакетов. Конфиденциальность инкапсулируемых пакетов обеспечивается путём их криптографического закрытия, т. е. зашифровывания, а целостность и подлинность — путём формирования цифровой подписи.

Для организации создания туннелей VPN используется технология туннелирования. Суть туннелирования состоит в том, чтобы инкапсулировать, т. е. «упаковать», передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от НСД или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по открытой сети.

Контрольные вопросы:

1) Каким образом сети VPN обеспечивают безопасную передачу пакетов?

2) Назовите виды VPN-соединений.

3) Перечислите достоинства и недостатки протоколов PPTP и L2TP.

4) Что такое RADIUS?

Тест по самостоятельной работе №9:

1. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   C) Безопасность
2. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента
3. Выберите верные утверждения:
   A) Всякая платформа виртуализации поддерживает виртуализацию всего аппаратного обеспечения
   B) Виртуальные машины поддерживают эмуляцию устройств
   C) Виртуальная машина может быть перенесена с одного хоста на другой
4. Внутренняя виртуализация сети:
   A) Объединение нескольких виртуальных сетей в одну
   B) Объединение в единую сеть виртуальных и физических машин
   C) Создание виртуальной сети между несколькими виртуальными машинами одного хоста
5. Процесс интеллектуальной балансировки нагрузки является частью:
   A) Виртуализации сети
   B) Виртуализации ОС
   C) Виртуализации серверов приложений
6. Виртуализация блоков является частью:
   A) виртуализации серверов
   B) виртуализации систем хранения
   C) виртуализации ОС
7. Свойствами цифровой информации являются:
   A) Длительный поиск
   B) Отчуждаемость
   C) Невоспроизводимость
8. К причинам снижения количества информационных атак можно отнести

A) Упрощение методов организации атак

B) Небольшое число объектов атаки

C) Возрастание числа обнаруживаемых уязвимостей систем

9. К основным составляющим безопасности информации, как правило, относят:

A) Полезность

B) Целостность

C) Подлинность

10. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:

A) Повторяемый

B) Узкоспециализированный

C) Наличие определенного процесса

D) Управляемый

Самостоятельная работа №10 – Политики безопасности для VPN

Защита информации в понимании VPN включает в себя кодирование, подтверждение подлинности и контроль доступа. Кодирование подразумевает шифрование передаваемой через VPN информации. Прочитать полученные данные может лишь обладатель ключа к шифру.

Наиболее часто используемыми в VPN-решениях алгоритмами кодирования в наше время являются DES, Triple DES и различные реализации AES. Степень защищенности алгоритмов, подходы к выбору наиболее оптимального из них – это тоже отдельная тема, которую мы не в состоянии обсудить.

Подтверждение подлинности включает в себя проверку целостности данных и идентификацию лиц и объектов, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных на сегодня – MD5 и SHA1.

Идентификация - это процесс удостоверения того, что объект действительно является тем, за кого/что он себя выдает. Здесь, помимо традиционных схем имя - пароль, все более и более активно используются системы сертификатов и специальных серверов для их проверки - CA (Certification Authorities). Такие серверы являются, как правило, частью систем PKI (Public Key Infrastructure). Популярные ныне PKI, например, Verisign или Entrust, могут обслуживать сертификаты и идентифицировать их держателей по протоколам HTTP и LDAP (X.509). Кроме того, для идентификации могут быть использованы биометрия, неизменяемые характеристики оборудования (например, MAC-адреса) или специальные идентификационные комплексы (Tacacs, Radius).

Контроль трафика подразумевает определение и управление приоритетами использования пропускной полосы VPN. С его помощью мы можем установить различные пропускные полосы для сетевых приложений и сервисов в зависимости от степени их важности.

EFS использует архитектуру Windows CryptoAPI. В ее основе лежит технология шифрования с открытым ключом. Для шифрования каждого файла случайным образом генерируется ключ шифрования файла. При этом для шифрования файла может применяться любой симметричный алгоритм шифрования. В настоящее же время в EFS используется один алгоритм, это DESX, являющийся специальной модификацией широко распространенного стандарта DES.

Ключи шифрования EFS хранятся в резидентном пуле памяти (сама EFS расположена в ядре Windows 2000), что исключает несанкционированный доступ к ним через файл подкачки.

Все, что от вас требуется для шифрования файла, — это установить атрибут шифрования “encrypt contents to secure data” в папке, где вы хотите хранить зашифрованные данные. Файлы прозрачно шифруются по мере записи на диск и расшифровываются во время считывания с диска. В результате вы можете шифровать файлы ваших пользователей в их каталогах, находящихся на сервере, работающем под управлением Windows 2000, даже если ваши пользователи все еще работают с определенными системами, которые не обеспечивают реальную безопасность данных, например с Windows 95.

EFS обеспечивает встроенную поддержку восстановления данных на тот случай, если потребуется их расшифровать, но, по каким-либо причинам, это не может быть выполнено обычным. По умолчанию, EFS автоматически сгенерирует ключ восстановления, установит сертификат доступа в учетной записи администратора и сохранит его при первом входе в систему.

Таким образом, администратор становится так называемым агентом восстановления, и сможет расшифровать любой файл в системе.

Контрольные вопросы:

1)Что включает в себя защита информации в понимании VPN?

2)Что такое идентификация?

3) Как осуществляется шифрование данных?

4) Что лежит в основе технологии шифрования с открытым ключом?

Тест по самостоятельной работе №10:

1. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   C) Безопасность
2. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:
   A) Повторяемый
   B) Узкоспециализированный
   C) Наличие определенного процесса
   D) Управляемый
3. Свойствами цифровой информации являются:
   A) Длительный поиск
   B) Отчуждаемость

C) Невоспроизводимость

4. К причинам снижения количества информационных атак можно отнести
   A) Упрощение методов организации атак
   B) Небольшое число объектов атаки
   C) Возрастание числа обнаруживаемых уязвимостей систем
5. К основным составляющим безопасности информации, как правило, относят:
   A) Полезность
   B) Целостность
   C) Подлинность
6. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:
   A) Повторяемый
   B) Узкоспециализированный
   C) Наличие определенного процесса
   D) Управляемый
7. Выберите верные утверждения:
   A) Применение терминального доступа характеризуется снижением затрат на содержание серверов
   B) Применение терминального доступа характеризуется снижением затрат на содержание рабочих станций
   C) Применение терминального доступа характеризуется снижением общего уровня безопасности
8. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента
9. Выберите верные утверждения:
   A) x86 архитектура изначально не была предназначена для использования решений виртуализации
   B) При использовании виртуализации реальная архитектура решения соответствует структуре представления
   C) При использовании виртуализации реальная архитектура решения не скрывается от пользователя
10. Атаки, направленные не на конкретную организацию, а на большое число потенциальных жертв - это:
    A) Атаки широкого диапазона действия

B) Атаки узконаправленного действия
C) Универсальные атаки

Самостоятельная работа №11 – Стандартные протоколы построения VPN

Для построения VPN используются протоколы следующих уровней:

- канального;

- сетевого;

- транспортного.

К протоколам канального уровня относятся

- PPTP (Point to Point Tunneling Protocol) - инкапсулирует IP - пакеты для передачи по сети. Позволяет передавать через туннель пакеты PPP.

- L2TP (Layer 2 Tunneling Protocol) - позволяет передавать через туннель пакеты SLIP и PPP. Позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay.

- MPLS (Multiprotocol Label Switching) - механизм передачи данных, эмулирующий свойства различных сетей. был разработан с целью обеспечения универсальной службы передачи данных как для клиентов сетей с коммутацией каналов, так и сетей с коммутацией пакетов. С помощью MPLS можно передавать трафик самой разной природы, такой как IP-пакеты, ATM, SONET и кадры Ethernet.

К протоколам сетевого уровня относятся:

- IPSec - согласованный набор открытых стандартов. Ядром IPSec являются три протокола:

· AH (Authentication Header) - гарантирует целостность и аутентичность данных.

· ESP (Encapsulating Security Payload) - шифрует передаваемые данные, обеспечивая их конфиденциальность, поддерживает средства аутентификации и обеспечения целостности данных.

· IKE (Internet Key Exchange) - решает задачу автоматического предоставления конечным пользователям защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования.

К протоколам транспортного уровня относятся:

- SSL/TLS (Secure Socket Layer/Transport Layer Security) - реализует шифрование и аутентификацию между транспортными уровнями приемника и передатчика. Применяется для защиты TCP - трафика, не может применяться для UDP.

Контрольные вопросы:

1)Может ли шифрование полностью защитить данные, передаваемые через VPN.

2) С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

3) Какие протоколы используются для построения VPN?

4) К протоколам канального уровня относятся?

5) К протоколам сетевого уровня относятся?

6) К протоколам транспортного уровня относятся?

Тест по самостоятельной работе №11:

1. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   C) Безопасность
2. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента
3. Выберите верные утверждения:
   A) x86 архитектура изначально не была предназначена для использования решений виртуализации
   B) При использовании виртуализации реальная архитектура решения соответствует структуре представления
   C) При использовании виртуализации реальная архитектура решения не скрывается от пользователя
5. Виртуализация блоков является частью:
   A) Виртуализации серверов
   B) Виртуализации систем хранения
   C) Виртуализации ОС
6. Свойствами цифровой информации являются:
   A) Длительный поиск
   B) Отчуждаемость

C) Невоспроизводимость

7. К причинам снижения количества информационных атак можно отнести
   A) Упрощение методов организации атак
   B) Небольшое число объектов атаки
   C) Возрастание числа обнаруживаемых уязвимостей систем
8. К основным составляющим безопасности информации, как правило, относят:
   A) Полезность
   B) Целостность
   C) Подлинность
9. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:
   A) Повторяемый
   B) Узкоспециализированный
   C) Наличие определенного процесса
   D) Управляемый

10. Что из перечисленного может не являться уязвимостью:
    A) Ошибка в настройках межсетевого экрана.
    B) Ошибка в настройках маршрутизации.
    C) Ошибка в программном обеспечении.
    D) Слабое место в системе, с использованием которого может быть осуществлена атака.

Самостоятельная работа №12 – Проблемы и уязвимости VPN

Термин Virtual Private Network, то есть виртуальная частная сеть, приобрел в последнее время широкую известность, поскольку с помощью VPN можно в принципе обойти блокировку сайтов. Впрочем, переоценивать возможности этой технологии не стоит — у нее есть свои проблемы и уязвимости, к тому же законодатели собираются ввести запрет на пользование услугами VPN от иностранных компаний.

Приватность VPN обычно достигается шифрованием, при этом применяемые криптографические методы обеспечивают такую защиту, чтобы посторонние не могли ни прочитать сообщение, ни установить источник передачи. Однако, для того чтобы посмотреть данные в зашифрованном соединении, хакерам вовсе необязательно взламывать алгоритм шифрования.

Каждый клиент использует VPN для решения определенных задач. С помощью этой технологии к сети центрального офиса подключаются удаленные филиалы, дистанционные рабочие места или мобильные сотрудники. Банки могут предоставлять услуги доступа к платежным сервисам, обеспечивая безопасность по VPN, а операторы — предлагать услуги защищенного соединения своим клиентам. Но массовую популярность технология VPN приобрела после создания реестра запрещенных сайтов и ограничения доступа к ним.

Услуги VPN обхода блокировки сайтов предоставляют в основном иностранные компании. В этом случае канал между клиентом и оператором шифруется, чтобы не было понятно, к какому сайту запрашивается доступ, а само подключение выполняется с иностранного IP, принадлежащего оператору. Чаще всего для этого используется Tor — тогда маршрутизатор оператора, который должен заблокировать трафик, не может определить конечного получателя и отправителя пакета.

В зависимости от цели использования VPN, можно выделить следующие основные угрозы.

Man-in-the-middle (MITM) — «шпион посредине». Это атака на VPN, при которой злоумышленник вклинивается в канал шифрования между отправителем и получателем, создавая два отдельных шифрованных соединения. Обычно такая атака осуществляется в момент обмена ключами шифрования: злоумышленник перехватывает их и навязывает обеим общающимся сторонам свои ключи. При использовании SSL и сертификатов ему достаточно встроиться в цепочку доверия браузера.

Например, именно так перехватываются SSL-VPN правительствами США, Японии и Китая, поскольку сертификаты правительственных центров этих стран находятся в числе доверенных в большинстве браузеров. Методика перехвата зашифрованного соединения при этом следующая: в инфраструктуре DNS соответствующей страны для сайтов, которые нужно прослушивать, указываются IP-адреса правительственного центра. Когда

клиент пытается обратиться к подконтрольному сайту, ему возвращаются адреса правительственного центра.

Поскольку используемый сертификат признается как доверенный, клиент полагает, что соединение защищено. Далее уже правительственный центр расшифровывает трафик, протоколирует его, вновь зашифровывает и пересылает на соответствующий сайт. В результате клиент может и не знать, что взаимодействует с серверами перечисленных правительств, считая, что взаимодействует с требуемым ему сайтом.

Примерно по такой схеме, например, работает Большой китайский межсетевой экран. В отношении правительств США и Японии нет данных о таком способе прослушки, однако среди доверенных сертификатов есть в том числе и правительственные центры сертификации указанных стран.

Identity Theft — кража личности. В организациях, где VPN используется для защиты доступа к корпоративным ресурсам, у злоумышленников появляется возможность проникновения внутрь сети с помощью аутентификационной информации легальных пользователей. Ее можно получить путем перехвата паролей в результате атаки MITM или MITB. Подключившись к корпоративному шлюзу и создав защищенное соединение, злоумышленник может действовать от имени сотрудника компании и получить расширенные полномочия и доступ к внутренней структуре сети, которая не всегда сегментирована и дополнительно укреплена.

Фактически такое использование VPN позволяет проникнуть сквозь защищенный периметр компании. Именно поэтому и говорят о размывании защитного периметра: часть удаленных устройств находится на неподконтрольной администратору территории, и что с ними происходит — неизвестно. Во избежание компрометации нужны механизмы, которые позволяли бы осуществлять строгую аутентификацию пользователей независимо от того, какие устройства они выбирают для работы. В частности, для решения этой задачи предлагаются специальные аппаратные идентификаторы

Решения для реализации VPN уже достаточно зрелые. Стоит отметить, что они поддерживались еще первым поколением межсетевых экранов. Однако новые технологии, в частности WebRTC или DNS-атаки, порождают новые угрозы, поэтому, даже если вы давно используете VPN, следует регулярно заново оценивать вероятность тех или иных рисков и при обнаружении опасности внедрять решения, которые обеспечат надежную защиту.

Контрольные вопросы:

1) Что такое Virtual Private Network?
2) Основные угрозы использования VPN?
3) В чем заключается атака Man-in-the-middle?
4) В чем заключается атака Identity Theft ?

Тест по самостоятельной работе №12:

1. Выберите верные утверждения:
   A) При использовании терминального доступа осложняется процесс контроля лицензий на ПО
   B) Терминальный доступ подразумевает выполнение всех вычислительных задач на удаленном мощном компьютере
   C) Применение терминального доступа характеризуется снижением затрат на содержание серверов, при увеличении затрат на содержание рабочих станций
2. Выберите верные утверждения:
   A) Веб - приложение не зависит от ОС клиента
   B) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне сервера
   C) Требования веб - приложений к аппаратному обеспечению ограничиваются требованиями ОС и браузера
3. Выберите верные утверждения:
   A) Виртуализация на основе x86 платформ началась с решений виртуализации серверов
   B) При использовании виртуализации реальная архитектура решения скрыта от пользователя
   C) x86 архитектура проектировалась с учетом возможности использования решений виртуализации
4. Наибольшую мобильность сотрудников подразумевает использование решений:
   A) Терминального доступа
   B) Виртуализации
   C) Веб – приложений
5. Веб - приложения характеризуются:
   A) Высокой мобильностью пользователей
   B) Низкими требованиями к аппаратному и программному обеспечению клиента
   C) Повышенной безопасностью персональных данных пользователей
6. Выберите верные утверждения:
   A) Виртуальные машины поддерживают эмуляцию устройств
   B) Всякая платформа виртуализации поддерживает виртуализацию всего аппаратного обеспечения
   C) Виртуальная машина может быть перенесена с одного хоста на другой
7. Использование программных решений в рамках изолированно виртуальной среды относится к:
   A) Виртуализации систем хранения
   B) Виртуализации приложений
   C) Виртуализации сети

8. Процесс интеллектуальной балансировки нагрузки является частью:
   A) Виртуализации ОС
   B) Виртуализации серверов приложений
   C) Виртуализации сети
9. Использование нескольких ОС на одном хосте обеспечивается
   A) Виртуализацией серверов приложений
   B) Виртуализацией приложений
10. Технология, обеспечивающая запуск нескольких ОС на одном хосте, при независимости ОС друг от друга и от аппаратных ресурсов:
   A) Паравиртуализация
   B) аппаратная виртуализация
   C) полная виртуализация

Самостоятельная работа №13 – Аудит и мониторинг информационной безопасности

Для организаций, компьютерные сети которых насчитывают не один десяток компьютеров, функционирующих под управлением различных ОС, на первое место выступает задача управления множеством разнообразных защитных механизмов в таких гетерогенных корпоративных сетях. Сложность сетевой инфраструктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности за пределами внимания администратора безопасности могут остаться многие угрозы. Поэтому необходимо осуществление регулярного аудита и постоянного мониторинга безопасности ИС.

Аудит безопасности информационной системы

Понятие аудита безопасности. Аудит представляет собой независимую экспертизу отдельных областей функционирования предприятия. Одной из составляющих аудита предприятия является аудит безопасности его ИС.

В настоящее время актуальность аудита безопасности ИС резко возросла. Это связано с увеличением зависимости организаций от информации и ИС. Возросла уязвимость ИС за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема ПО. Расширился спектр угроз для ИС из-за активного использования предприятиями открытых глобальных сетей для передачи сообщений и транзакций.

Аудит безопасности ИС дает возможность руководителям и сотрудникам организаций получить ответы на вопросы:
• как оптимально использовать существующую ИС при развитии бизнеса;
• как решаются вопросы безопасности и контроля доступа;
• как установить единую систему управления и мониторинга ИС;
• когда и как необходимо провести модернизацию оборудования и ПО;
• как минимизировать риски при размещении конфиденциальной информации в ИС организации, а также наметить пути решения обнаруженных проблем.

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Достоверную и обоснованную информацию можно получить, только рассматривая все взаимосвязи между проблемами. Проведение аудита позволяет оценить текущую безопасность ИС, оценить риски, прогнозировать и управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности информационных ресурсов организации.

Цели проведения аудита безопасности ИС:
• оценка текущего уровня защищенности ИС;
• локализация узких мест в системе защиты ИС;
• анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
• выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;
• оценка соответствия ИС существующим стандартам в области информационной безопасности.

В число дополнительных задач аудита ИС могут также входить выработка рекомендаций по совершенствованию политики безопасности организации и постановка задач для ИТ персонала, касающихся обеспечения защиты информации.

Проведение аудита безопасности информационных систем

Работы по аудиту безопасности ИС состоят из последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ аудита автоматизированной системы:
• инициирования процедуры аудита;
• сбора информации аудита;
• анализа данных аудита;
• выработки рекомендаций;
• подготовки аудиторского отчета.

Аудиторский отчет является основным результатом проведения аудита. Отчет должен содержать описание целей проведения аудита, характеристику обследуемой ИС, результаты анализа данных аудита, выводы, содержащие оценку уровня защищенности АС или соответствия ее требованиям стандартов, и рекомендации по устранению существующих недостатков и совершенствованию системы защиты.

Мониторинг безопасности системы

Функции мониторинга безопасности ИС выполняют средства анализа защищенности и средства обнаружения атак. Средства анализа защищенности исследуют настройки элементов защиты ОС на рабочих станциях и серверах, БД. Они исследуют топологию сети, ищут незащищенные или неправильные сетевые соединения, анализируют настройки МЭ.

В функции системы управления безопасностью входит выработка рекомендаций администратору по устранению обнаруженных уязвимостей в сетях, приложениях или иных компонентах ИС организации.

Использование модели адаптивного управления безопасностью сети дает возможность контролировать практически все угрозы и своевременно реагировать на них, позволяя не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к их появлению.

Контрольные вопросы:

1) Что такое аудит безопасности?
2) На какие вопросы отвечает аудит безопасности?
3) Какие функции выполняет мониторинг безопасности?
4) Для чего используется модели адаптивного управления безопасности сети?

Тест по самостоятельной работе №13:

1. Базирующаяся в Сан-Франциско ассоциация профессионалов информационной безопасности:
   A) NIPC
   B) ИКБ
   C) ФБР
   D) CERT
   E) CSI
2. Назначение Национального центра по защите инфраструктур (NIPC, National Infrastructure Protection Center), размещенного в штаб-квартире ФБР:
   A) главный правительственный механизм для борьбы с кибератаками на национальные инфраструктуры и ответа на них
   B) выработать методы по оценке, улучшению и поддержке безопасности и выживаемости сетевых систем
   C) предоставляет широкий выбор информационных и образовательных программ в помощь по защите информационных активов корпораций и правительственных организаций.
   D) работа с интернет-сообществом по обнаружению и разрешению инцидентов компьютерной безопасности
3. Какие компоненты входят в ИТ-инфраструктуру?
   A) устройства специального назначения (принтеры, сканеры и т. п.)
   B) пользователи ПК и персонал организации
   C) ИТ-менеджеры
   D) устройства резервного копирования (накопители на магнитных лентах, ленточные автоматы и хранилища)
   E) устройства безопасности (например, прокси или брандмауэры)
4. Под термином (подставит нужное) подразумевается любая информация, потеря, неправильное использование, несанкционированный доступ или модификация которой могли бы неблагоприятно повлиять на

национальные интересы, или на проведение федеральных программ, или же на частную жизнь граждан
   A) "секретная информация" (определена приказом президента или актом конгресса как секретная в интересах национальной безопасности или внешней политики)
   B) "защищаемая информация"
   C) "недоступная информация"
   D) "важная информация"
   E) "публичная информация"
5. Принцип необходимого знания:
   A) стратегия защиты информации, при которой пользователь получает доступ к секретной и сверхсекретной информации, если он имеет на это право
   B) стратегия защиты информации, при которой пользователь получает доступ только к внутренней информации организации
   C) стратегия защиты информации, при которой пользователь получает доступ только к тем данным, которые непосредственно необходимы ему для выполнения конкретно данной работы
   D) стратегия защиты информации, при которой пользователь не получает доступ к конфиденциальной информации
   E) стратегия защиты информации, при которой пользователь получает доступ к любым не секретным данным по запросу
6. Что включает в себя понятие целостности данных?
   A) это состояние, в котором информация сохраняется неизменной во время ее передачи
   B) то состояние, в котором информация сохраняется неизменной во время ее извлечения
   C) сохранение информации для ее использования по назначению
   D) это состояние, при котором данные остаются такими же, какими были в оригинале, и ни случайно, ни преднамеренно не модифицируются, не изменяются и не уничтожаются
   E) гарантия того, что информация не была раскрыта неавторизированным персонам, процессам или устройствам
7. Что относится к понятию конфиденциальности информации
   A) контролирование доступа к информации посредством механизмов безопасности
   B) гарантия того, что информация не была раскрыта неавторизированным персонам, процессам или устройствам
   C) сохранение информации для ее использования по назначению
8. Симметричное шифрование получило свое название из того факта, что
   A) один и тот же алгоритм используется как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного
   B) один и тот же ключ используется как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного
   C) в алгоритме шифрования используются четные числа

9. К факторам надежности симметричного ключа относятся:
   A) длина пароля и его сложность
   B) размер пространства ключа
   C) степень рандомизации входящего и выходящего сообщений при шифровании
   D) сложность хэш-функции
10. В чем заключается особенность гибридного алгоритма?
   A) использование симметричного ключа для шифрования данных, а асимметричного для шифрования самого симметричного ключа
   B) одновременное использование симметричного и асимметричного ключа для шифрования данных
   C) использование симметричного ключа для шифрования ключа, а асимметричного для шифрования самого данных

Самостоятельная работа №14 – **Классификация систем анализа защищенности**

Защищенность является одним из важнейших показателей эффективности функционирования АС, наряду с такими показателями как надежность, отказоустойчивость, производительность и т.п.

Под защищенностью АС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.

Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность. На практике всегда существует большое количество неподдающихся точной оценке возможных путей осуществления угроз безопасности в отношении ресурсов АС. В идеале каждый путь осуществления угрозы должен быть перекрыт со ответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность АС. Вторым фактором является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода либо преодоления. Третьим фактором является вели чина ущерба, наносимого владельцу АС в случае успешного осуществления угроз безопасности. На практике получение точных значений приведенных характеристик затруднено, т. к. понятия угрозы, ущерба и сопротивляемости механизма защиты трудноформализуемы. Например, оценку ущерба в результате НСД к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Оценка степе ни сопротивляемости механизмов защиты всегда является субъективной. Описанный в настоящей работе подход позволяет получать качественные оценки уровня защищенности АС путем сопоставления свойств и параметров АС с многократно опробованными на практике и стандартизированными критерия ми оценки защищенности.

Нормативная база анализа защищенности.

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются:

1. Общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408).

2. Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799). Кроме этого, в нашей стране первостепенное значение имеют Руководящие

документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

Методика анализа защищенности.

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике. Типовая методика включает использование следующих методов:

• Изучение исходных данных по АС;

• Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;

• Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;

• Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;

• Сканирование внешних сетевых адресов ЛВС из сети Интернет;

• Сканирование ресурсов ЛВС изнутри;

• Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств. Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

Средства анализа защищенности.

Арсенал программных средств, используемых для анализа защищенности АС достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступа ют коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами. Удобным и мощным средством анализа защищенности ОС является рассматриваемый ни же, свободно распространяемый программный продукт CIS Windows 2000 Level I Scoring Tool, а также аналогичные средства разработчиков ОС, предоставляемые

бесплатно, такие как ASET для ОС Solaris или MBSA (Microsoft Security Baseline Analyzer) для ОС Windows 2000. Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, свое временность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. (Управление агентами осуществляется по сети программой менеджером.) Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной ба зе данных. Администратор управляет менеджера ми при помощи графической консоли, позволяю щей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агента ми, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попы ток сетевого вторжения в АС. Для этих целей при меняются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средства ми анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга. Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более

простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

Контрольные вопросы:

1) Какими факторами определяется уровень защищенности компьютерных систем от угроз безопасности

2) Что используют современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации?

3) Какие Вам известны спецификации (Security Benchmarks)?

4) Что такое защищённость АС?

Тест по самостоятельной работе №14:

1. Что в сфере информационной безопасности принято считать риском?
   A) Характеристику, которая делает возможным возникновение угрозы
   B) Потенциальную возможность понести убытки из-за нарушения безопасности информационной системы
   C) Потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней
2. На какие ресурсы может быть направлена угроза?
   A) На любые виды ресурсов (информационный, аппаратный, программный и т.д.)
   B) Только на аппаратные ресурсы
   C) Только на информационные ресурсы
3. Что представляет собой система с полным перекрытием?
   A) Система, в которой обеспечивается селективная безопасность
   B) Система, в которой ведется учет всех вторжений, блокируются только вредоносные проникновения
   C) Система, в которой имеются средства защиты на каждый возможный путь проникновения
4. Какие из перечисленных характеристик не входят в систему обеспечения безопасности Клементса: O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов?
   A) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов
   B) P- набор креативных функций; Z - набор виндикативных инструментов

C) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций

5. Какое из перечисленных требований доверия к безопасности не является справедливым?
   A) К анализу уязвимостей
   B) Верификации контента
   C) К технологии разработки и тестированию
6. Какой из перечисленных классов функциональных требований включает требования кодирования информации?
   A) Класс криптографической поддержки (криптографической защиты)
   B) Класс приватности (конфиденциальности)"
   C) Класс защиты функций безопасности объекта
7. Что представляет собой событие - триггер?
   A) Это одна из разновидностей атак на сервер
   B) Событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска
   C) Событие, увеличивающее время отклика web – сервера
8. Что формируют потенциальные злоумышленные действия по отношению к объектам?
   A) Набор угроз ИБ
   B) Шаблоны мер потенциального противодействия
   C) Вероятностный набор действий по подавлению угроз
9. Может ли анализ угроз каким-то образом помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня?
   A) Да
   B) Нет
10. Чем определяется высокая стойкость системы?
   A) Уровнем стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения
   B) Уровнем стойкости функции безопасности объекта оценки, на котором обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения
   C) Уровнем стойкости, при котором обеспечивается защита от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения

Самостоятельная работа №15 – Критерии выбора сканеров безопасности

Сканер безопасности – это программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей. Основными пользователями таких систем являются профессионалы: администраторы, специалисты по безопасности и т.д. Простые пользователи тоже могут использовать сканеры безопасности, но информация, выдаваемая такими программами, как правило специфична, что ограничивает возможности ее использования неподготовленным человеком. Сканеры безопасности облегчают работу специалистов, сокращая суммарно потраченное время на поиск уязвимостей.

I. Использование сканера безопасности начинается с планирования развёртывания и собственно развёртывания. Поэтому первая группа критериев касается архитектуры сканеров безопасности, взаимодействия их компонентов, инсталляции, управления.

Вариант пробной версии. Прежде чем приобретать продукт, имеет смысл оценить его, скачав пробную версию.

Наличие аппаратно-программного варианта. В области средств защиты в последнее время наметилась устойчивая тенденция перехода от чисто программных реализаций к программно-аппаратным. Программно-аппаратный вариант продукта включает в себя:

1.Аппаратное обеспечение (компьютер с чётко описанной спецификацией).

2.Установленная и настроенная операционная система (ОС). Обычно это «усечённый» вариант ОС Linux.

3.Собственно сам продукт, в данном случае, сканер безопасности.

Это даёт следующие преимущества:

•Выигрыш по времени (устройство готово к работе сразу после приобретения)

•Надёжность (исключение из используемой ОС ненужных функций)

•Снижение затрат на внедрение, поддержку, обучение и т. п.

И если для межсетевых экранов и систем обнаружения атак программно-аппаратные решения – теперь уже не редкость, то для сканеров безопасности — это направление только-только начинает вырисовываться.

Платформа. В случае выбора в пользу программно-аппаратного решения не возникает вопросов ни по выбору аппаратуры, ни по выбору ОС (и это одно из преимуществ такого решения). Но, поскольку в области сканеров безопасности пока что преобладают программные решения, возникает вопрос выбора ОС. Задача эта тривиальна и не требует подробного рассмотрения (достаточно изучить системные требования).

Наличие распределённой архитектуры.

Это, пожалуй, самый главный параметр данной группы. Система анализа защищённости может иметь распределённую архитектуру, в этом случае она состоит как минимум из двух типов компонентов:

•Агент (сервер)

•Консоль (клиент)

Собственно, сканером при этом является серверная часть (агент). Наличие распределённой архитектуры добавляет гибкость и масштабируемость при размещении сканера безопасности в корпоративной сети, особенно в большой, территориально-распределённой. Довольно часто сканирование приходится проводить с разных «точек зрения», например, демилитаризованную зону можно сканировать как снаружи (через межсетевой экран), так и непосредственно из её сегмента. Возникают ситуации, когда для проведения сканирования «ноутбук» со сканерами безопасности «путешествует» от филиала к филиалу. Часто само перемещение компьютера со сканером и его подключение – целая проблема, не столько техническая, сколько организационная (получение разрешения на доступ в серверную и т. п.). Решением в данном случае следует считать наличие у сканера распределённой архитектуры.

Это настолько важный критерий, что следует остановиться на его описании несколько подробнее. Прежде всего, этот критерий важен для большой сети. Сканирование огромного числа узлов, сканирование с разных точек зрения с последующим сравнением результатов – здесь вряд ли удастся обойтись одним ноутбуком со сканером.

Наличие распределённой архитектуры и централизованного управления – довольно значительное преимущество. Следующие несколько критериев относятся к сканерам, имеющим распределённую архитектуру.

В случае распределённой архитектуры клиентская и серверная части взаимодействуют друг с другом по сети. На транспортном уровне для этого могут быть использованы протоколы TCP или UDP (для всех четырёх сравниваемых сканеров разработчиками был выбран протокол TCP).

На прикладном уровне может использоваться либо свой собственный протокол, либо стандартный.

Контрольные вопросы:

1) Для чего необходим сканер уязвимости?
2) Какие сканеры уязвимости Вы знаете?
3) Что включают в себя многофункциональные сканеры уязвимости?
4) Основные функции сканера Symantec Security Check?
5) Недостатки сканера Nessus?

Тест по самостоятельной работе №15:

1. К методологии хакерства можно отнести:
   A) Случайный поиск или разведка для определения жертв
   B) Сбор базовых сведений
   C) Выполнение эксплоита
   D) Создание перечня параметров
   E) Сокрытие действий
   F) Зондирование
2. Атаки, влияющие на доступность и надежность сайта, называются:
   A) Denial of Service
   B) DoS
   C) Атаками на отказ в обслуживании
   D) DsO
   E) Down Service
3. Мотивами хакеров являются:
   A) Высказывание своего политического мнения
   B) Любопытство
   C) Уклонение от финансовой ответственности
   D) Желание заявить о себе
4. Обеспечение безопасности включает в себя следующие основные задачи:
   A) Обнаружение
   B) Реагирование
   C) Предотвращение
5. К атакам на содержимое и информацию можно отнести:
   A) Нарушение конфиденциальности
   B) Повреждение отображаемого на веб-сайте содержимого
   C) Мошенничество
   D) Удаление файлов
6. Проникновение посредством незаконной аутентификации в одной учетной записи для перемещения финансовых средств в другую учетную запись - это следующий тип атаки:
   A) Аннулирование транзакции
   B) Маскарад
   C) Взлом таблиц маршрутизаторов
   D) Мошенничество
7. Они защищают внутренние ресурсы, маскируя реальные IP-адреса компьютеров и блокируя попытки доступа к сети, инициированные извне, если только внешний пользователь не является законным и авторизованным сотрудником организации:
   A) Firewalls
   B) Брандмауэры
   C) Маршрутизаторы

D) Сетевые экраны

8. Выберите верные утверждения:
   A) Применение терминального доступа характеризуется снижением затрат на содержание серверов
   B) Применение терминального доступа характеризуется снижением затрат на содержание рабочих станций
   C) Применение терминального доступа характеризуется снижением общего уровня безопасности
9. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   C) Безопасность
10. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента

Самостоятельная работа №16 – Методы отражений вторжений

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)

Обычно архитектура СОВ включает:

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы

- подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров

- хранилище, обеспечивающее накопление первичных событий и результатов анализа

- консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Существует несколько способов классификации СОВ в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой анализа для выявления подозрительной активности. Во многих простых СОВ все компоненты реализованы в виде одного модуля или устройства.

Виды систем обнаружения вторжений.

В сетевой СОВ, сенсоры расположены на важных для наблюдения точках сети, часто в демилитаризованной зоне, или на границе сети. Сенсор перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов. Протокольные СОВ используются для отслеживания трафика, нарушающего правила определенных протоколов либо синтаксис языка (например, SQL). В хостовых СОВ сенсор обычно является программным агентом, который ведет наблюдение за активностью хоста, на который установлен. Также существуют гибридные версии перечисленных видов СОВ.

Сетевая СОВ (Network-based IDS, NIDS) отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами.

Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к хабу или свитчу, настроенному на зеркалирование портов, либо сетевое TAP устройство. Примером сетевой СОВ является Snort.

Основанная на протоколе СОВ (Protocol-based IDS, PIDS) представляет собой систему (либо агента), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Для веб-сервера подобная СОВ обычно ведет наблюдение за HTTP и HTTPS протоколами. При использовании HTTPS СОВ должна располагаться на таком интерфейсе, чтобы просматривать HTTPS пакеты ещё до их шифрования и отправки в сеть.

Основанная на прикладных протоколах СОВ (Application Protocol-based IDS, APIDS) — это система (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов. Например, на веб-сервере с SQL базой данных СОВ будет отслеживать содержимое SQL команд, передаваемых на сервер.

Узловая СОВ (Host-based IDS, HIDS) — система (или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников. Примером является OSSEC.

Гибридная СОВ совмещает два и более подходов к разработке СОВ. Данные от агентов на хостах комбинируются с сетевой информацией для создания наиболее полного представления о безопасности сети. В качестве примера гибридной СОВ можно привести Prelude.

Существует два основных подхода к обнаружению вторжений:
1.Сигнатурный;
2.Поведенческий.

Сигнатурный анализ трафика в IDS очень похож на принцип работы многих антивирусов. Сетевой трафик анализируется и сравнивается с базой данных сигнатур, в которой хранится информация о вредоносных программах, если в трафике обнаруживается вредоносный объект, система оповещает об этом ответственное лицо.

Поведенческий анализ заключается в том, что включенная в сеть IDS исследует нормальное поведение и функционирование пользователей и приложений в сети, и затем, на основании построенной модели система обнаруживает некорректное и аномальное поведение пользователей либо приложений.

Контрольные вопросы:

1) Какие методы обнаружения Вам известны?
2) Преимущество способа обнаружения аномалий?
3) Какие атаки могут выполнять злоумышленники?
4) Могут ли сетевые системы обнаружения вторжений взаимодействовать с другими системами безопасности?

Тест по самостоятельной работе №16:

1. Акт проникновения в компьютерную систему или сеть - это:
   A) Физическая атака
   B) Социальный инжиниринг
   C) Крекинг
   D) Хакерство
2. Мотивами хакеров являются:
   A) Высказывание своего политического мнения
   B) Любопытство
   C) Уклонение от финансовой ответственности
   D) Желание заявить о себе
3. Обеспечение безопасности включает в себя следующие основные задачи:
   A) Обнаружение
   B) Реагирование
   C) Предотвращение
4. К атакам на содержимое и информацию можно отнести:
   A) Нарушение конфиденциальности
   B) Повреждение отображаемого на веб-сайте содержимого
   C) Мошенничество
   D) Удаление файлов
5. Проникновение посредством незаконной аутентификации в одной учетной записи для перемещения финансовых средств в другую учетную запись - это следующий тип атаки:
   A) аннулирование транзакции
   B) маскарад
   C) взлом таблиц маршрутизаторов
   D) мошенничество
6. Они защищают внутренние ресурсы, маскируя реальные IP-адреса компьютеров и блокируя попытки доступа к сети, инициированные извне, если только внешний пользователь не является законным и авторизованным сотрудником организации:
   A) Firewalls
   B) Брандмауэры

C) Маршрутизаторы
D) Сетевые экраны

7. Атаки, направленные не на конкретную организацию, а на большое число потенциальных жертв - это:
   A) Атаки широкого диапазона действия
   B) Атаки узконаправленного действия
   C) Универсальные атаки
8. К основным составляющим безопасности информации, как правило, относят:
   A) Полезность
   B) Целостность
   C) Подлинность
9. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:
   A) Повторяемый
   B) Узкоспециализированный
   C) наличие определенного процесса
   D) управляемый
10. Что из перечисленного может не являться уязвимостью:
   A) Ошибка в настройках межсетевого экрана.
   B) Ошибка в настройках маршрутизации.
   C) Ошибка в программном обеспечении.
   D) Слабое место в системе, с использованием которого может быть осуществлена атака.

Самостоятельная работа №17 – Основы построения систем обнаружения вторжений

Системы обнаружения вторжения (СОВ) – это системы, собирающие информацию из различных точек защищаемой компьютерной системы (вычислительной сети) и анализирующие эту информацию для выявления как попыток нарушения, так и реальных нарушений защиты (вторжений).

Системы обнаружения атак представляют собой инструменты управления защитой, которые:

- Собирают информацию от целого ряда системных источников.
- Анализируют эту информацию на предмет наличия шаблонов, отражающих злоупотребления или необычную деятельность.
- В некоторых случаях автоматически реагируют на обнаруженную деятельность.
- Генерируют отчет с результатами, полученными в течение процесса обнаружения.

До недавнего времени наиболее распространенной структурой СОВ была модель, предложенная Дороти Деннинг (D. Denning).

В современных системах обнаружения логически выделяют следующие основные элементы: подсистему сбора информации, подсистему анализа и модуль представления данных.

● **Подсистема сбора информации** используется для сбора первичной информации о работе защищаемой системы.

● **Подсистема анализа** (обнаружения) осуществляет поиск атак и вторжений в защищаемую систему.

● **Подсистема представления данных** (пользовательский интерфейс) позволяет пользователю(ям) СОВ следить за состоянием защищаемой системы.

Подсистема сбора информации аккумулирует данные о работе защищаемой системы. Для сбора информации используются автономные модули – датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы. Датчики в СОВ принято классифицировать по характеру собираемой информации. В соответствии с общей структурой информационных систем выделяют следующие типы:

● датчики приложений – данные о работе программного обеспечения защищаемой системы;

● датчики хоста – функционирование рабочей станции защищаемой системы;

● датчики сети – сбор данных для оценки сетевого трафика;

● межсетевые датчики – содержат характеристики данных, циркулирующих между сетями.

Система обнаружения вторжения может включать любую комбинацию из приведенных типов датчиков.

Подсистема анализа структурно состоит из одного или более модулей анализа – анализаторов. Наличие нескольких анализаторов требуется для повышения эффективности обнаружения. Каждый анализатор выполняет поиск атак или вторжений определенного типа. Входными данными для анализатора является информация из подсистемы сбора информации или от другого анализатора. Результат работы подсистемы – индикация о состоянии защищаемой системы. В случае, когда анализатор сообщает об обнаружении несанкционированных действий, на его выходе может появляться некоторая дополнительная информация. Обычно эта информация содержит выводы, подтверждающие факт наличия вторжения или атаки.

Подсистема представления данных необходима для информирования заинтересованных лиц о состоянии защищаемой системы. В некоторых системах предполагается наличие групп пользователей, каждая из которых контролирует определенные подсистемы защищаемой системы. Поэтому в таких СОВ применяется разграничение доступа, групповые политики, полномочия и т.д.

Контрольные вопросы:

1) Что такое системы обнаружения вторжения?
2) Основные элементы системы обнаружения?
3) Какие типы датчиков Вам известны?
4) Что такое анализатор?

Тест по самостоятельной работе №17:

1. Принцип необходимого знания:

A) Стратегия защиты информации, при которой пользователь получает доступ к секретной и сверхсекретной информации, если он имеет на это право
B) Стратегия защиты информации, при которой пользователь получает доступ только к внутренней информации организации
C) Стратегия защиты информации, при которой пользователь получает доступ только к тем данным, которые непосредственно необходимы ему для выполнения конкретно данной работы
D) Стратегия защиты информации, при которой пользователь не получает доступ к конфиденциальной информации
E) Стратегия защиты информации, при которой пользователь получает доступ к любым не секретным данным по запросу

2. Что включает в себя понятие целостности данных?
   A) Это состояние, в котором информация сохраняется неизменной во время ее передачи
   B) То состояние, в котором информация сохраняется неизменной во время ее извлечения
   C) Сохранение информации для ее использования по назначению
   D) Это состояние, при котором данные остаются такими же, какими были в оригинале, и ни случайно, ни преднамеренно не модифицируются, не изменяются и не уничтожаются
   E) Гарантия того, что информация не была раскрыта неавторизированным персонам, процессам или устройствам
3. Что относится к понятию конфиденциальности информации
   A) Контролирование доступа к информации посредством механизмов безопасности
   B) Гарантия того, что информация не была раскрыта неавторизированным персонам, процессам или устройствам
   C) Сохранение информации для ее использования по назначению
4. Симметричное шифрование получило свое название из того факта, что
   A) Один и тот же алгоритм используется как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного
   B) Один и тот же ключ используется как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного
   C) В алгоритме шифрования используются четные числа
5. К факторам надежности симметричного ключа относятся:
   A) Длина пароля и его сложность
   B) Размер пространства ключа
   C) Степень рандомизации входящего и выходящего сообщений при шифровании
   D) Сложность хэш-функции
6. В чем заключается особенность гибридного алгоритма?
   A) Использование симметричного ключа для шифрования данных, а асимметричного для шифрования самого симметричного ключа

B) Одновременное использование симметричного и асимметричного ключа для шифрования данных
C) Использование симметричного ключа для шифрования ключа, а асимметричного для шифрования самого данных

7. Система управления доступом
   A) Защищает от внутренних пользователей
   B) Ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему
   C) Предотвращает атаку через разрешенный канал связи.
8. Основные достоинства парольной аутентификации:
   A) Простота реализации
   B) Низкая стоимость внедрения
   C) Высокая надежность
9. Какие преимущества имеет аппаратная реализация VPN?
   A) Скорость
   B) Дешевизна
   D) Безопасность
10. К основным категориям атак относятся:
    A) Атаки прохода
    B) Атаки трансформации
    D) Атаки на отказ в обслуживании

Самостоятельная работа №18 – Многофункциональные устройства защиты от сетевых атак

Интернет, предоставляя множество возможностей, несет потенциальные угрозы. Системным администраторам приходится тратить много сил и времени на обеспечение безопасности сети.

При всех существующих рисках невозможно отказаться от использования веб-пространства, поэтому необходимо минимизировать риски. На помощь приходят многофункциональные устройства.

Они эффективно защищают от:

- DoS и DDoS атак (монопольного захвата сетевых ресурсов, в результате которого системы становятся недоступны);

- Сетевого вторжения (удаленного проникновения в сеть);

- Вирусов (компьютерных программ, разрушающих другие программы);

- Rootkit (программ, перехватывающих команды доступа к файлам, находящимся на жестком диске);

- Рекламного и шпионского ПО (программ, демонстрирующих рекламные баннеры при запуске);

- DNS Poisoning (перенаправления трафика на ресурсы, зараженные вредоносным ПО).

Сеть становится уязвимой при изменении структуры организации, ее расширении. В случаях, когда используются сложные сети, которые должны обеспечивать поддержку и развитие деловой активности компании, лучшим выбором для защиты от вредоносных атак станет эффективное UTM решение.

Термин был введен в 2004 году для обозначения универсальных устройств, предназначенных для защиты от увеличивающегося количества сетевых атак. С момента своего появления они привлекли к себе внимание, благодаря наличию нескольких модулей, простоте управления и развертывания. Если раньше они имели функции антивируса, DPI и firewall, то сегодня UTM устройства предоставляют значительно больше возможностей.

Особенности UTM

В условиях роста сетевых атак предприятиям необходимо использовать надежные и простые в управлении средства защиты для безопасного обмена данными. В сфере малого и среднего бизнеса, при отсутствии финансовой и технической возможности в развертывании разного рода систем, вопрос комплексной безопасности стоит достаточно остро.

В таких компаниях обычно не достает квалифицированных специалистов и использование многоуровневых унифицированных сетевых устройств защиты - Unified Threat Management, наиболее актуально. Они

представляют собой комплексы программных и аппаратных решений, совмещающих в себе функции разных устройств.

UTM решение включает следующий набор функций:

- Файервол с DPI (Deep Packet Inspection);
- Фильтр контента;
- Межсетевой экран;
- Virtual Private Network (VPN).

Устройства имеют возможность учитывать трафик, балансировать нагрузки и производить аутентификацию пользователей. Система обеспечивает стандартные функции межсетевого экранирования и контролирует, в каком состоянии находятся сетевые соединения.

С помощью устройств обеспечивают функциональность веб-шлюза безопасности с URL-фильтрацией, проверками на присутствие вредоносного трафика и контролем приложений. UTM решение эффективно противостоит сетевым вторжениям, позволяет организовать удаленный доступ с использованием VPN.

Применение устройств с единой консолью настроек способствует быстрому вводу в эксплуатацию, позволяет в будущем выполнять обновление и добавление новых функций. При этом стоимость UTM обычно меньше, чем цена нескольких приложений.

Затраты на безопасность должны быть соизмеримы со стоимостью возможного ущерба от реализации угроз. Если безопасности слишком много, то значительно усложняется пользование системой в целом. Нужно прийти к разумному компромиссу - достичь баланса между возможными угрозами для сетевой безопасности и уровнем защиты. Многофункциональные устройства UTM позволяют предприятиям среднего и малого бизнеса эффективно справляться с задачами информационной и сетевой безопасности.

Контрольные вопросы:

1) От чего защищают многофункциональные устройства?
2) Для чего ввели термин UTM решение?
3) Какие функции включает UTM решение?

Тест по самостоятельной работе №18:

1. Выберите верное утверждение:
   A) При использовании веб - приложений аппаратная архитектура скрыта от пользователя
   B) Логика выполнения веб - приложений всегда скрыта от пользователя
   C) Веб - приложение подразумевает выполнение всех вычислительных задач на стороне клиента

2. Выберите верные утверждения:
   A) Всякая платформа виртуализации поддерживает виртуализацию всего аппаратного обеспечения
   B) Виртуальные машины поддерживают эмуляцию устройств
   C) Виртуальная машина может быть перенесена с одного хоста на другой
3. Внутренняя виртуализация сети:
   A) Объединение нескольких виртуальных сетей в одну
   B) Объединение в единую сеть виртуальных и физических машин
   C) Создание виртуальной сети между несколькими виртуальными машинами одного хоста
4. Процесс интеллектуальной балансировки нагрузки является частью:
   A) Виртуализации сети
   B) Виртуализации ОС
   C) Виртуализации серверов приложений
5. Свойствами цифровой информации являются:
   A) Длительный поиск
   B) Отчуждаемость
   C) Невоспроизводимость
6. К причинам снижения количества информационных атак можно отнести
   A) Упрощение методов организации атак
   B) Небольшое число объектов атаки
   C) Возрастание числа обнаруживаемых уязвимостей систем
7. К основным составляющим безопасности информации, как правило, относят:
   A) Полезность
   B) Целостность
   C) Подлинность

8. Уровень зрелости управления рисками, при котором в организации разработан базовый процесс управления рисками:
   A) Повторяемый
   B) Узкоспециализированный
   C) Наличие определенного процесса
   D) Управляемый

9.Система управления доступом
   A) Защищает от внутренних пользователей
   B) Ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему

C) Предотвращает атаку через разрешенный канал связи.

10. К основным категориям атак относятся:

A) Атаки прохода

B) Атаки трансформации

D) Атаки на отказ в обслуживании

Список контрольных вопросов:

1) Что называют сетевой аутентификацией?
2) Что такое авторизация?
3) Перечислите объекты воздействия в информационных системах.
4) Что входит в задачи межсетевых экранов?
5) Что называют контролируемой зоной?
6) Чем определяется стойкость подсистемы идентификации и аутентификации?
7) Перечислить минимальные требования к выбору пароля.
8) Перечислить минимальные требования к подсистеме парольной аутентификации.
9) Как определить вероятность подбора пароля злоумышленником в течении срока его действия?
10) Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?
11) Что такое межсетевой экран?
12) Каковы функции межсетевого экрана?
13) В чем состоит фильтрация информационных потоков?
14) Перечислите проблемы безопасности межсетевых экранов.
15) Какие бывают типы межсетевых экранов?
16) Выделите два основных типа межсетевых экранов.
17) Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
18) Является ли один из типов межсетевых экранов более безопасным, нежели другой?
19) Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
20) В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
21) Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
22) Что должен обеспечивать межсетевой экран для проверки состояния?
23) При каком условии межсетевой экран прикладного уровня может называться гибридным?
24) Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?

25) Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

26) В чем заключается механизм межсетевого экранирования?

27) Дайте определение межсетевого экрана.

28) Принцип функционирования межсетевых экранов с фильтрацией пакетов.

29) На уровне каких протоколов работает «шлюз сеансового уровня»?

30) В чем особенность межсетевых экранов экспертного уровня?

31) Какие свойства присущи информации?
32) Дайте понятие объекта защиты информации.
33) Что относят к информационным процессам?
34) Что понимают под информационной системой?
35) Что называют информационными ресурсами?
36) Что понимают под угрозой информации, дайте понятие искусственных и естественных угроз, приведите примеры.
37) Что составляет основу политики безопасности?
38) Сделайте сравнительный анализ избирательной и полномочной политики безопасности.
39) Проанализируйте механизмы и свойства защиты информации.
40) Наиболее значимыми нормативными документами в области информационной безопасности являются?
41) Что включает в себя методика анализа защищённости?
42) Какие спецификации (шаблоны) для конфигурации наиболее распространенных системных программных средств известны?
43) Что определяют спецификации 1 и 2 уровней?
44) Для каких целей используется программное обеспечение VIPNET OFFICE*?*
45) Каковы функции ViPNet Manager?
46) Каковы функции ViPNet Координатор?
47) Каковы функции ViPNet Клиент?
48) Какие сервисные функции предоставляет пакет ViPNet OFFICE?

49) Каким образом сети VPN обеспечивают безопасную передачу пакетов?

50) Назовите виды VPN-соединений.

51) Перечислите достоинства и недостатки протоколов PPTP и L2TP.

52) Что такое RADIUS?

53) Что включает в себя защита информации в понимании VPN?
54) Что такое идентификация?
55) Как осуществляется шифрование данных?
56) Что лежит в основе технологии шифрования с открытым ключом?

57) Может ли шифрование полностью защитить данные, передаваемые через VPN.
58) С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
59) Какие протоколы используются для построения VPN?
60) К протоколам канального уровня относятся?
61) К протоколам сетевого уровня относятся?
62) К протоколам транспортного уровня относятся?
63) Что такое Virtual Private Network?
64) Основные угрозы использования VPN?
65) В чем заключается атака Man-in-the-middle**?**
66) В чем заключается атака Identity Theft?
67) Что такое аудит безопасности?
68) На какие вопросы отвечает аудит безопасности?
69) Какие функции выполняет мониторинг безопасности?
70) Для чего используется модели адаптивного управления безопасности сети?
71) Какими факторами определяется уровень защищенности компьютерных систем от угроз безопасности
72) Что используют современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации?
73) Какие Вам известны спецификации (Security Benchmarks)?
74) Для чего необходим сканер уязвимости?
75) Какие сканеры уязвимости Вы знаете?
76) Что включают в себя многофункциональные сканеры уязвимости?
77) Основные функции сканера Symantec Security Check?
78) Недостатки сканера Nessus?

79) Какие методы обнаружения Вам известны?
80) Преимущество способа обнаружения аномалий?
81) Какие атаки могут выполнять злоумышленники?

82) Могут ли сетевые системы обнаружения вторжений взаимодействовать с другими системами безопасности?

83) Что такое системы обнаружения вторжения?

84) Основные элементы системы обнаружения?

85) Какие типы датчиков Вам известны?

86) Что такое анализатор?

87)

88) От чего защищают многофункциональные устройства?

89) Для чего ввели термин UTM решение?

90) Какие функции включает UTM решение?

Список литературы:

1. В.Г. Олифер, Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2006 - 672с.

2. Е. А. Богданова. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие. - Москва : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.

3. Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. Телекоммуникационные системы и сети [Текст] : учебное пособие / - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1 : Современные технологии. - 2013. - 620 с.

4. Под общ. ред. А. В. Пролетарского. Технологии коммутации и маршрутизации в локальных компьютерных сетях [Текст] : учебное пособие / - Москва : Изд - во МГТУ им. Н. Э. Баумана, 2013. – 389 с.