ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.ДВ.06.02 Системы обнаружения вторжений

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

3.7 Практическое занятие № ПЗ-22-23 Обеспечение информационной безопасности в открытых системах. Принципы создания защищенных средств связи объектов в открытых системах

3.8 Практическое занятие № ПЗ-24-25 Политика безопасности открытых систем. Управление безопасностью открытых систем

1. 1 Лекция №__1-4__ (_8_ часов).

Тема: «Введение в предмет. Базовые понятия»

1.1.1 Вопросы лекции:

1. Основные понятия и определения.
2. Статистика вторжений на Web-ресурсы

1.1.2 Краткое содержание вопросов:

1. Основные понятия и определения.

Outlook Express

Приложение Microsoft Outlook Express - обычный клиент электронной почты и новостей интернета. Оно устанавливается по умолчанию в операционных системах Windows вместе с приложением Internet Explorer. Поскольку оно легко доступно, многие пользователи выбирают его для использования в качестве заданного по умолчанию почтового клиента. Поэтому, судебный эксперт должен быть готов к восстановлению электронной почты, сгенерированной из этой программы. В этом разделе описано, как судебный аналитик может использовать Outlook Express несколько отличным от обычного пользователя способом, чтобы помочь установить направление дальнейшего расследования.

Netscape Navigator/Communicator

Netscape Navigator и Communicator (http://www.netscape.com) имеют собственную версию почтовой программы, которая встречается так же часто, как Outlook Express. Подобно Outlook Express, файлы приложения Netscape, которые входят в почтовые папки, сохраняются в каталоге. Вместо простого импортирования, как мы делали в Outlook Express, или открытия файла, как это делается в Outlook, мы должны использовать более хитрое решение, чтобы получить доступ к электронной почтеNetscape.

Клиент службы America Online

Служба America Online (AOL) широко используется, особенно для доступа в интернет из дома. Поэтому использование клиента службы America Online для восстановления электронной почты заслуживает отдельного раздела в этой лекции.

Служба AOL, как правило, является наиболее трудной для восстановления из всех почтовых программ. Отчасти так происходит потому, что восстановление зависит от версии данных AOL, найденных на машине подозреваемого, та же самая версия должна быть установлена на судебном компьютере. Поскольку все расследования прошлого года, с которыми мы столкнулись, содержали улики в 5-й версии клиента службы AOL или выше, то мы сконцентрируемся на более новых методах восстановления электронной почты.

Служба AOL использует термин profile (профиль) для предоставления различных входов в систему и адресов электронной почты, которые используются с клиентом AOL. Каждый, кто совместно пользуется домашним компьютером в семье, имеет собственный профиль; таким способом электронная почта каждого пользователя сохраняется отдельно и конфиденциально. СлужбаAOL сохраняет всю информацию для каждого профиля в одном большом файле. Поскольку отдельным компьютером могут использоваться несколько профилей, вы должны восстановить каждый файл, чтобы получить полную картину деятельности, проделанной в интернете с определенного компьютера.

Клиенты службы America Online могут быть расположены на сайте http://www.aol.com, который содержит почти все когда-либо распространяемые версии. Клиенты свободно доступны для загрузки.

2. Статистика вторжений на Web-ресурсы

Mailbombing

Старейший вид атак. Значительно увеличивается трафик и количество присылаемых сообещний, что генерирует сбой в работе сервиса. Это вызывает паралич не только Вашей почты, но и работы самого почтового сервера. Эффективность таких атак в наши дни считается нулевой, поскольку теперь провайдер имеет возможность установитьограничение трафика от одного отправителя.

Переполнение буфера

Принцип этого вида атак - программные ошибки, при которых память нарушает свои же границы. Это, в свою очередь, вынуждает либо завершить процесс аварийно, либо выполнить произвольный бинарный код, где используется текущая учетная запись. Если учётная запись – администраторская, то данные действия разрешают получить полный доступ к системе.

Вирусы, трояны, почтовые черви, снифферы

Данный тип атак объединяет различные сторонние программы. Назначение и принцип действия такой программы может быть чрезвычайно разнообразным, поэтому нет смысла подробно останавливаться на каждой из них. Все эти программы объединяет то, что их главная цель - доступ и "заражение" системы.

Сетевая разведка

Данный тип атаки сам по себе не предусматривает какое-либо разрушительное действие. Разведка подразумевает лишь сбор информации злоумышленником – сканирование портов, запрос DNS, проверка защиты компьютера и проверка системы. Обычноразведка проводится перед серьёзной целенаправленной атакой.

Сниффинг пакетов

Принцип действия основан на особенностях работы сетевой карты. Пакеты, полученные ей, пересылаются на обработку, где с ними взаимодействют специальные приложения. В результате злоумышленник получает доступ не только к информация о структуре вычислительной системы, но и непосредственно передаваемая информация – пароли,сообщения и другие файлы.

IP-спуфинг

Тип атак на локальные сети, когда компьютер злоумышленника использует IP-адрес, входящий в данную локальную сеть. Атака возможна, если система безопасностипредусматривает идентификацию типа IP-адрес, исключая дополнительные условия.

Man-in-the-middle

Злоумышленник перехватывает канал связи между двумя приложениями, в результате чего получает доступ ко всей информации, идущей через данный канал. Цель атаки - не только кража, но и фальсификация информации. Примером такой атаки может служитьиспользование подобного приложения для мошенничества в онлайн-играх: информация об игровом событии, порождаемом клиентской частью, передаётся на сервер. На её пути ставится программа-перехватчик, которая изменяет информацию по желанию злоумышленника и отправляет на сервер вместо той, которую отправила программа-клиент игры.

Инъекция

Также довольно широкий тип атак, общий принцип которых - внедрение информационных систем со сторонними кусками программного кода в ход передачи данных, где код фактически не мешает работе приложения, но одновременно производит необходимое злоумышленнику действие.

Отказ в обслуживании

DoS (от англ. Denial of Service) — атака, имеющая своей целью заставить сервер не отвечать на запросы. Такой тип атаки не подразумевает непосредственно получение некоторой секретной информации, но используется для того, чтобы парализовать работу целевых сервисов. Например, некоторые программы из-за ошибок в своем коде могут

вызывать исключительные ситуации, и при отключении сервисов способны исполнять код, предоставленный злоумышленником или атаки лавинного типа, когда сервер не в состоянии обработать все входяще пакеты.

DDoS (от англ. Distributed Denial of Service — распределённая DoS) — подтип DoS атаки, имеющий ту же цель что и DoS, но производимой не с одного компьютера, а с нескольких компьютеров в сети. В данных типах атак используется либо возникновение ошибок, генерирущих отказ сервиса, либо срабатывание защиты, вызывающей блокированиеработы сервиса, а в результате также и отказ в обслуживании. DDoS используется там, где обычный DoS неэффективен. Для этого несколько компьютеров объединяются, и каждый производит DoS атаку на систему жертвы. Вместе это называется DDoS-атака.

Способы защиты от сетевых атак. Существует множество способов защиты от злоумышленников, в том числе антивирусы,фаерволлы, различные встроенные фильтры и пр. Самым же эффективным является профессионализм пользователя. Не следует открывать подозрительные сайты (ссылки), файлы в письмах от отправителя типа "таинственный незнакомец". Перед открытием вложений со знакомых адресов следует запрашивать подтверждение каким-либо иным, нежели почта, способом. Как правило, в этом могут помочь курсы повышения компьютерной квалицикации и грамотности, проводимые практически в любой организации. Это, впрочем, не заменит защитные механизмы и программы. Стоит помнить, что технология сетевых атак не стоит на месте и поэтому следует как можно чаще осуществлять обновление антивируса, а также проводить полные проверки компьютеров.

1. 2 Лекция № 5-9 (10 часов).

Тема: «Основные элементы технологий открытых информационных систем. Совместимость, переносимость и способность взаимодействовать открытых систем»

1.2.1 Вопросы лекции:

1. Проблемы обеспечения безопасности при удалённом доступе

2. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях

1.2.2 Краткое содержание вопросов:

1. **Проблемы обеспечения безопасности при удалённом доступе**

Обеспечение безопасности данных при удаленном доступе - проблема если и не номер один, то, по крайней мере, номер два, после проблемы обеспечения приемлемой для пользователей пропускной способности. А при активном использовании транспорта Internet она становится проблемой номер один.

Неотъемлемым свойством систем удаленного доступа является наличие глобальных связей. По своей природе глобальные связи, простирающиеся на много десятков и тысяч километров, не позволяют воспрепятствовать злонамеренному доступу к передаваемым по этим линиям данным. Нельзя дать никаких гарантий, что в некоторой, недоступной для контроля точке пространства, некто, используя, например, анализатор протокола, не подключится к передающей среде для захвата и последующего декодирования пакетов данных. Такая опасность одинаково присуща всем видам территориальных каналов связи и не связана с тем, используются ли собственные, арендуемые каналы связи или услуги общедоступных территориальных сетей, подобные Internet.

Однако использование общественных сетей (речь в основном идет об Internet) еще более усугубляет ситуацию, хотя бы потому, что в такой сети для доступа к корпоративным данным в распоряжении злоумышленника имеются более разнообразные и удобные средства, чем выход в чистое поле с анализатором протоколов. Кроме того, огромное число пользователей увеличивает вероятность попыток несанкционированного доступа.

Безопасная система - это система, которая, во-первых, надежно хранит информацию и всегда готова предоставить ее своим пользователям, а во-вторых, система, которая защищает эти данные от несанкционированного доступа.

Межсетевой экран (firewall, брандмауэр) - это устройство, как правило, представляющее собой универсальный компьютер с установленным на нем специальным программным обеспечением, который размещается между защищаемой (внутренней) сетью и внешними сетями, потенциальными источниками опасности. Межсетевой экран контролирует все информационные потоки между внутренней и внешними сетями, пропуская данные, в соответствии с заранее установленными правилами. Эти правила являются формализованным выражением политики безопасности, принятой на данном предприятии.

Межсетевые экраны базируются на двух основных приемах защиты:

пакетной фильтрации;

сервисах-посредниках (proxyservices).

Эти две функции можно использовать как по отдельности, так и в комбинации.

2. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях

1. К программно-аппаратным средствам обеспечения информационной безопасности средств связи в вычислительных сетях относятся:
2. программно-аппаратные шифраторы сетевого трафика;
3. методика Firewall, реализуемая на базе программно-аппаратных средств;
4. защищенные сетевые криптопротоколы;
5. программные средства обнаружения атак (IDS - Intrusion Detection Systems) (см. главу 9);
6. программные средства анализа защищенности (см. главу 9);
7. защищенные сетевые ОС.

Существует огромное количество литературы, посвященной средствам защиты для использования в сети Internet (за последние несколько лет практически в любом номере компьютерного журнала встречаются статьи на эту тему).

Эти средства мы опишем по возможности кратко, чтобы не повторять хорошо известную всем информацию. При этом мы преследуем следующие цели: во-первых, еще раз вернуться к мифу об "абсолютной защите", которую якобы обеспечивают системы Firewall; во-вторых, сравнить существующие версии криптопротоколов, применяемых в Internet, и дать оценку критическому, по сути, положению в этой области.

Методика Firewall

В общем случае методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети реализует следующие основные функции.

1. Многоуровневая фильтрация сетевого трафика

Фильтрация обычно происходит на четырех уровнях OSI:

1. Канальном (Ethernet).
2. Сетевом (IP).
3. Транспортном (TCP, UDP).
4. Прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика является основной функцией систем Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику в выделенном сегменте IP-сети, то есть, настроив соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной ОС, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к Firewall-фильтрации: в качестве субъектов взаимодействия будут выступать IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.

1. 3 Лекция № 10-13 (8 часов).

Тема: «Основные модели открытых систем. Интранет как открытая система»

1.3.1 Вопросы лекции:

1. Обнаружение факта проведения и причин возникновения сетевой атаки подручными средствами

2. Дидактическая единица: Общие сведения об IDS snort.

1.3.2 Краткое содержание вопросов:

1. **Обнаружение факта проведения и причин возникновения сетевой атаки подручными средствами**

Времена, когда для защиты хватало одного брандмауэра прошли. На сегодня предприятия реализуют мощные и огромные структурированные системы защиты, для ограничения предприятия от возможных угроз и рисков. С появлением таких атак, как атак на отказ в обслуживании (DDoS), адрес отправителя пакетов не может дать вам однозначный ответ, была ли против вас атака направленная или случайная. Нужно знать как реагировать на инцидент, а также как идентифицировать злоумышленника (Рис.1).

Выявить злоумышленника можно по следующим особенностям к действию:

1. реализует очевидные проколы
2. реализует неоднократные попытки на вхождение в сеть
3. пытается замести свои следы
4. реализует атаки в разное время

Средства обнаружения атак

Технология обнаружения атак должна справляться со следующим:

1. Распознавание популярных атак и предупреждение о них определенных лиц
2. Понимание непонятных источников данных об атаках
3. Возможность управления методами защиты не-специалистами в сфере безопасности
4. Контроль всех действий субъектов информационной сети (программ, пользователей и тд)
5. Освобождение или снижение функций персонала, который отвечает за безопасность, текущих рутинных операций по контролю

Зачастую системы обнаружения атак могут реализовывать функции, которые расширяют спектр их применения. К примеру:

1. Контроль эффективность межсетевых экранов. Можно расположить систему обнаружения после межсетевого экрана, что бы определить недостающих правил на межсетевом экране.
2. Контроль узлов сети с устаревшим ПО
3. Блокирование и контроль доступа к некоторым ресурсам Internet. Хоть они далеки от возможностей таких как сетевых экранов, но если нету денег на покупку сетевого экрана, можно расширить функции системы обнаружения атак
4. Контроль электронной почты. Системы могут отслеживать вирусы в письмах, а также анализировать содержимое входящих и исходящих писем

Лучшая реализация опыта и времени профессионалов в сфере информационной безопасности заключается в выявлении и устранениипричин реализации атак, а не обнаружение самих атак. Устранив причину, из-за которой возможна атака, сохранит многим временного ресурса и финансового.

2. Дидактическая единица: Общие сведения об IDS snort.

SNORT представляет собой систему IDS (Intrusion Detection System) с открытым исходным кодом, которая позволяет обнаружить любую подозрительную сетевую активность, сравнивая встроенные правила обнаружения вредоносного траффика с данными, проходящими по локальной сети организации. Фактически, так работает любой антивирус, но сходство на этом заканчивается, потому что предназначение у этих систем совершенно разное, очень важно правильно понимать цели и задачи систем IDS и не путать их с другими средствами защиты.

Система IDS предназначена для того, чтобы блокировать действия злоумышленника на стадии изучения вашей сети:

- обнаружить подозрительную сетевую активность,
- выявить известные инструменты для анализа и взлома сетей, используемые злоумышленником
- и при возможности воспрепятствовать противоправной деятельности.

Обычно эта задача не выполняется другими средствами, например, брандмауэром, который лишь ставит барьер на входе в локальную сеть. Антивирус отлавливает известные вирусные сигнатуры, но контроль за траффиком внутри локальной сети никак не осуществляется, а в большинстве организаций он вообще отсутствует.

Представьте, что одна из рабочих станций в локальной сети заражена новым, ранее неизвестным трояном. В этом случае, антивирусная программа не сможет его отследить и обезвредить, так как соответствующая сигнатура просто отсутствует в ее памяти. В то же время, все трояны нацелены на выполнение одной задачи – перехватить конфиденциальную информацию и отправить ее вирусописателю, а отправку конфиденциальной информации можно просто пресечь с помощью IDS SNORT. Сканирование сетевых ресурсов с целью выявления слабых мест сети также не пресекается ни антивирусом, ни брандмауэром, хотя это и важно, так как разведка никогда не проводится просто так, часто за этим следует нападение.

1. 4 Лекция № 14-17 (8 часа).

Тема: «Уязвимость открытых систем на примере интранета. Основные угрозы»

1.4.1 Вопросы лекции:

1. Значение IDS для решения задач поиска злоумышленников в собственной ЛВС

2. Классификация, средства и методы защиты от атак

1.4.2 Краткое содержание вопросов:

1. Значение IDS для решения задач поиска злоумышленников в собственной ЛВС

В повседневной деятельности рядового системного администратора в 99 процентах случаев не придется создавать сигнатуры самостоятельно. Зачем делать то, что уже сделано до тебя? Такая необходимость может возникнуть только в случае, если какая-либо неизвестная заранее атака была обнаружена самостоятельно и есть желание помочь обществу также защититься от этой атаки. В остальных же случаях сигнатуры обычно обновляются с официального сайта IDS Snort. От их актуальности немало зависит надежность всего комплекса системы безопасности. Постоянно обновлять сигнатуры вручную неудобно, кроме того, часто возникает ситуация, когда закомментированные или удаленные сигнатуры, которые не являются актуальными для конкретной системы или даже являются лишними, мешающими, восстанавливаются снова при первом же обновлении. С целью решения таких задач АндреасомОстлингом (Andreas Östling) была написана программа Oinkmaster. Это простой скрипт, написанный на языке программирования Perl и распространяемый на основании лицензии BSD. Он позволяет постоянно содержать сигнатуры в обновленном состоянии и при этом не удалять каждый раз ненужные сигнатуры вручную. Он также работает под различными операционными системами.

Выделим три основных шага, которые выполняет Oinkmaster при обновлении сигнатур.

1. Копирует архив правил Snort с официального сайта и помещает его во временную директорию.
2. Распаковывает этот архив и просматривает директорию rules, полученную из этого архива. Все полученные сигнатуры хранятся здесь. При этом он действует точно по правилам, заданным в своем конфигурационном файле. Обычно он открывает каждый файл правил, корректирует его, как считает необходимым, и сохраняет результаты проделанной работы. Все действия до сих пор происходят во временной директории.
3. После этого такие новые файлы проходят сравнение построчно с файлами правил, действующими сейчас. Если новое найденное правило не занесено в черный список (он задан в конфигурационном файле и содержит идентификаторы тех сигнатур, которые системный администратор считает неактуальными для своей системы), оно добавляется к действующим.

Oinkmaster может запускаться как вручную, так и с помощью демона cron, присутствующего во всех операционных системах и выполняющего задания согласно расписанию.

Acid – это аналитический инструмент, написанный на языке программирования PHP. Он проводит поиск в БД IDS и в результате несложных операций возвращает html-код, удобный для чтения человеком с помощью обычного браузера. Работает на многих операционных системах, поддерживающих PHP (Linux, *BSD, Microsoft Windows, Solaris). Acid был разработан Романом Денилью (Roman Danyliw), распространяется в открытых кодах согласно лицензии GPL.

Это очень удобная форма представления результатов работы всей системы обнаружения вторжений. Что интересно, она также предоставляет возможность отправки электронной почты в случае выполнения заданных условий. Работает с различными IDS и

идеально подходит для Snort. Системный администратор может просматривать состояние системы безопасности, находясь дома, в командировке или в любом другом месте, где есть доступ к Интернету. Веб-сервер может быть настроен так, чтобы при запросе страниц спрашивались логин и пароль. Возможна настройка Acid таким образом, чтобы сообщение системному администратору отправлялось при обнаружении, например, 50 атак. После получения такого сообщения системный администратор может зайти на веб-сервер и уже своими силами определить, была ли действительно система подвергнута нападению или же IDS просто выдала ложную тревогу.

Рассмотренная система реагирования на нарушения сетевой безопасности очень гибка благодаря тому, что отдельные ее элементы представлены в виде открытого исходного кода. Это означает, что специалист может вносить в нее такие тонкие изменения, которые характерны лишь для его конкретного случая. Данная система также хороша тем, что может применяться как в небольшой организации с сетью, состоящей из нескольких компьютеров, но требующей надежности в плане защиты информации. Ведь все рассмотренные программы могут быть установлены на одном единственном хосте. Также она может быть расширена до сколь угодно огромных размеров. Рассмотренный нами комплекс программ может быть настроен в виде распределенной системы, находящейся на нескольких хостах, и даже состоять из отдельных элементов, находящихся физически в разных сетях.

Конечно, если основная деятельность организации связана с обработкой огромнейших массивов информации и потоков данных, значимость защиты информации повышается на порядок. В таком случае возможно приобретение дорогого оборудования, такого как CISCO IDS. Продукты этой марки показали себя как непревзойденные на протяжении всего времени существования Интернета. Но они, кроме того, что дороги сами по себе, дороги также и в обслуживании. Для обеспечения их беспрерывной работы, нужно нанимать высокопрофессиональных специалистов. Рассмотренный же в данной статье вариант системы реагирования на нарушения сетевой безопасности дешев, гибок, прост в установке и настройке, а также считается очень надежным и стабильным средством. Об этом можно судить хотя бы по тому, что им пользуются миллионы специалистов информационной безопасности всего мира.

2. **Классификация, средства и методы защиты от атак**

1. По характеру воздействия
    - пассивное
    - активное

Пассивное воздействие на распределенную вычислительную систему - воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности.

Пассивное удаленное воздействие практически невозможно обнаружить.

Пример: прослушивание канала связи в сети.

2. По цели воздействия

нарушение конфиденциальности информации

нарушение целостности информации

нарушение работоспособности (доступности) системы

- При перехвате информации нарушается её конфиденциальность.
- Пример: прослушивание канала в сети.
- При искажении информации нарушается её целостность.

Пример: внедрение ложного объекта в РВС.

При нарушении работоспособности не происходит несанкционированного доступа, т.е. сохраняется целостность и конфиденциальность информации, однако доступ к ней легальных пользователей также невозможен.

Пример: отказ в обслуживании (DoS).

3. По условию начала осуществления воздействия

- Атака по запросу от атакуемого объекта
- Атака по наступлению ожидаемого события на атакуемом объекте
- Безусловная атака

В случае запроса атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия.

Инициатором осуществления начала атаки является атакуемый объект.

Пример: DNS- и ARP-запросы в стеке TCP/IP.

В случае наступления события, атакующий осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие.

Инициатором осуществления начала атаки является атакуемый объект.

Пример: прерывание сеанса работы пользователя с сервером в сетевых ОС без выдачи команды LOGOUT.

В случае безусловной атаки начало её осуществления безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. По наличию обратной связи с атакуемым объектом

- с обратной связью
- без обратной связи (однонаправленная атака)

Атака с обратной связью - атака, во время которой атакующий получает ответ от атакуемого объекта на часть своих действий. Эти ответы нужны, чтобы иметь возможность продолжить атаку и/или осуществлять её более эффективно, реагируя на изменения, происходящие на атакуемой системе.

Атака без обратной связи - атака, происходящая без реакции на поведение атакуемой системы.

Пример: отказ в обслуживании (DoS).

5. По расположению атакующего относительно атакуемого объекта

- внутрисегментное
- межсегментное

Внутрисегментная атака - атака, при которой субъект и объект атаки находятся внутри одного сегмента сети, где сегмент - есть физическое объединение станций с помощью коммуникационных устройств не выше канального уровня.

Межсегментная атака - атака, при которой субъект и объект атаки находятся в разных сегментах сети.

6. По количеству атакующих

- распределённая
- нераспределённая

Распределённая атака - атака, производимая двумя или более атакующими на одну и ту же вычислительную систему, объединёнными единым замыслом и во времени.

Нераспределённая атака проводится одним атакующим.

7. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

- физический
- канальный
- сетевой
- транспортный
- сеансовый
- представительный
- прикладной

1. 5 Лекция № 18-20 (6 часа).

Тема: «Уязвимость архитектуры клиент-сервер. Уязвимость открытых систем на примере интранета»

1.5.1 Вопросы лекции:

1. Идентификация и аутентификация

2. Ознакомление с криптографическими системами

3. Экранирование, анализ защищенности

1.5.2 Краткое содержание вопросов:

1. Идентификация и аутентификация

Основой любых систем защиты информационных систем являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. Напомним, что в качестве субъектов АС могут выступать как пользователи, так и процессы, а в качестве объектов АС – информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется идентификацией. Идентификация обеспечивает выполнение следующих функций:

- установление подлинности и определение полномочий субъекта при его допуске в систему,
- контролирование установленных полномочий в процессе сеанса работы;
- регистрация действий и др.

Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рис. 2.10. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

По контролируемому компоненту системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. Аутентификация партнеров по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация источника данных – это подтверждение подлинности источника отдельной порции данных.

По направленности аутентификация может быть односторонней (пользователь доказывает свою подлинность системе, например при входе в систему) и двусторонней (взаимной).

2. Ознакомление с криптографическими системами

На практике обычно используют два общих принципа шифрования: рассеивание и перемешивание. Рассеивание заключается в распространении влияния одного символа открытого текста на много символов шифр-текста: это позволяет скрыть статистические свойства открытого текста. Развитием этого принципа является распространение влияния одного символа ключа на много символов шифрограммы, что позволяет исключить восстановление ключа по частям. Перемешивание состоит в использовании таких шифрующих преобразований, которые исключают восстановление взаимосвязи статистических свойств открытого и шифрованного текста. Распространенный способ достижения хорошего рассеивания состоит в использовании составного шифра, который может быть реализован в виде некоторой последовательности простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемешивание. В качестве простых шифров чаще всего используют простые подстановки и перестановки. Одним из наилучших примеров криптоалгоритма, разработанного в соответствии с принципами рассеивания и перемешивания, может служить принятый в 1977 году Национальным бюро стандартов США стандарт шифрования данных DES. Несмотря на интенсивные и тща - тельные исследования алгоритма специалистами, пока не найдено уязвимых мест алгоритма, на основе которых можно было бы предложить метод криптоанализа, существенно лучший, чем полный перебор ключей. Общее мнение таково: DES - исключительно хороший шифр. В июле 1991 года введен в действие подобный отечественный криптоалгоритм ГОСТ 28147-89. В то же время блочные шифры обладают существенным недостатком - они размножают ошибки, возникающие в процессе передачи сообщения по каналу связи. Одиночная ошибка в шифр-тексте вызывает искажение примерно половины открытого текста при дешифровании. Это требует применения мощных кодов, исправляющих ошибки. [2] В блочном шифре из двух одинаковых блоков открытого текста получаются одинаковые блоки шифрованного текста. Избежать этого позволяют потоковые шифры, которые, в отличие от блочных, осуществляют поэлементное шифрование потока данных без задержки в криптосистемы. В общем случае каждый символ открытого текста шифруется, передается и дешифруется независимо от других символов. Иначе, шифрующее преобразование элемента открытого текста меняется от одного элемента к другому, в то время как для блочных шифров шифрующее преобразование каждого блока остается неизменным. Иногда символ открытого текста может шифроваться с учетом ограниченного числа предшествующих ему символов. Потоковые шифры основываются на псевдослучайных ключевых последовательностях - сгенерированных определенным образом последовательностях символов с заданными свойствами непредсказуемости (случайности) появления очередного символа. Генераторы ключевых последовательностей обычно базируются на комбинациях регистров сдвига и нелинейных булевых функциях. В качестве нелинейной булевой функции может использоваться криптоалгоритм DES, что соответствует применению DES в режиме обратной связи по выходу (OFB) лил обратной связи по шифртексту (CFB). Наибольший интерес представляет режим CFB, поскольку в ряде случаев режим OFB не обеспечивает требуемой секретности. Системы потокового шифрования близки к криптосистемам с одноразовым ключом, в которых размер ключа равен размеру шифруемого текста. При криптоанализе на основе известного открытого

текста стойкость системы определяется нелинейными булевыми функциями, что позволяет оценить криптостойкость системы на основе анализа вида используемых функций. Следовательно, потоковые шифры в отличие от других криптосистем обладают значительно большой анализируемой секретностью. Кроме того, в системах потокового шифрования не происходит размножения ошибок или оно ограничено. По этим причинам, а также ввиду высокой скорости обработки системы потокового шифрования вызывают большое доверие многих потребителей и специалистов. В криптосистемах с открытым ключом в алгоритмах шифрования идешифрования используются разные ключи, каждый из которых не может быть получен из другого (с приемлемыми затратами). Один ключ используется для шифрования, другой - для дешифрования. Основной принцип систем открытым ключом основывается на применении односторонних или необратимых функций и односторонних функций с лазейкой (потайным ходом). Вычисление ключей осуществляется получателем сообщений, который оставляет у себя тот ключ, который он будет потом использовать (то есть секретный ключ). [3] Другой ключ он высылает отправителю сообщений - открытый ключ - не опасаясь его огласки. Пользуясь этим открытым ключом, любой абонент может зашифровать текст и послать его получателю, который сгенерировал данный открытый ключ. Все используемые алгоритмы общедоступны. Важно то, что функции шифрования и дешифрования обратимы лишь тогда, когда они обеспечиваются строго взаимосвязанной парой ключей (открытого и секретного), а открытый ключ должен представлять собой необратимую функцию от секретного ключа. Подобным образом шифр-текст должен представлять собой необратимую функцию открытого текста, что в корне отличается от шифрования в системах с секретным ключом. Исследование необратимых функций проводилось в основном по следующим направлениям: дискретное возведение в степень - алгоритм DH (Диффи-Хелман), умножение простых чисел - алгоритм RSA (Райвест, Шамир, Адлеман), использование исправляющих ошибки кодов Гоппы, задачи NP-полноты, в частности криптоалгоритм Меркля и Хелмана на основе «задачи об укладке ранца», раскрытый Шамиром, и ряд других, оказавшихся легкораскрываемыми и бесперспективными. Первая система (DH) обеспечивает открытое распространение ключей, то есть позволяет отказаться от передачи секретных ключей, и по сегодняшний день считается одной из самых стойких и удобных систем с открытым ключом. Надежность второго метода (RSA) находится в прямой зависимости от сложности разложения больших чисел на множители. Если множители имеют длину порядка 100 десятичных цифр, то в наилучшем из известных способов разложения на множители необходимо порядка 100 млн. лет машинного времени, шифрование же и дешифрование требует порядка 1-2 с на блок. Задачи NP-полноты хорошо известны в комбинаторике и считаются в общем случае чрезвычайно сложными; однако построить соответствующий шифр оказывается весьма непросто. В системах с открытым ключом, так же как и в блочных шифрах, необходим большой размер шифруемого блока, хотя, возможно, и не больший, чем в алгоритме DES, что препятствует, наряду с низкой скоростью шифрования, использованию алгоритмов с открытым ключом в потоковых шифрах. [4] На сегодняшний день высокоэффективные системы с открытым ключом пока не найдены. Почти повсеместно принято ограничение использования криптосистем с открытым ключом - только для управления ключами и для цифровой подписи. Можно представить все существующие криптосистемы в виде диаграммы криптосистем.

Криптография известна с древнейших времен (достаточно вспомнить коды Цезаря) и до недавнего времени оставалась привилегией исключительно государственных и

военных учреждений. Ситуация рез - ко изменилась после публикации в 1949 году книги К. Шеннона «Работы по теории информации и кибернетике». Криптография стала объектом пристального внимания многих ученых. [1 принятие стандарта шифрования DES явилось мощным толчком к широкому применению шифрования в коммерческих системах. [5] Введение этого стандарта - отличный пример унификации и стандартизации средств защиты. Примером системного подхода к созданию единой крупномасштабной системы защиты информации является директива Министерства финансов США 1984 го - да, согласно которой все общественные и частные организации, ведущие дела с правительством США, обязаны внедрить процедуру шифрования DES; крупнейшие банки Citibank, Chase Manhattan Bank, Ma - nufaktures Hannover Trust, Bank of America, Security Pacific Bank также внедрили эту систему. Министерство энергетики США располагает более чем 30 действующими сетями, в которых используется алгоритм DES, Министерство юстиции устанавливает 20000 радиоустройств, располагающих средствами защиты на базе DES.

3. Экранирование, анализ защищенности

Говорить о том, что информационная безопасность (ИБ) стала частью корпоративной культуры, у нас в стране можно с большой натяжкой. Необходимость обеспечения ИБ осознали только крупные компании. Да и они до недавнего времени проблемы безопасности воспринимали исключительно как технические, связанные с внедрением межсетевых экранов, антивирусного программного обеспечения, средств обнаружения вторжений и виртуальных частных сетей.

На самом деле, по рекомендациям исследовательских фирм, от 60 до 80 % всех усилий по обеспечению безопасности следует направлять на разработку политики безопасности и сопутствующих ей документов. Почему? Потому, что политика безопасности является самым дешевым и одновременно самым эффективным средством обеспечения информационной безопасности (конечно, если ей следовать). Кроме того, если политика сформулирована, то она является и руководством по развитию и совершенствованию системы защиты.

Конкретные продукты и решения по информационной безопасности совершенствуются год от года, интегрируются между собой. Все это происходит так стремительно, что кажется будто недалек тот день, когда кто-нибудь предложит универсальный продукт для защиты любых информационных систем всеми доступными средствами. Это могло бы быть шуткой, если бы мы не наблюдали воочию, как усилия многих специализированных компаний "размазываются" в попытках создать универсальный продукт.

На мой взгляд, для потребителей была бы полезнее консолидация усилий нескольких производителей, направленных, например, на создание единой консоли управления.

Брандмауэры. Основные понятия

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами. Он является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Брандмауэр конфигурируется в соответствии с принятой в организации политикой контроля доступа к внутренней сети. Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

Брандмауэр с фильтрацией пакетов [packet-filtering firewall] - является маршрутизатором или компьютером, на котором работает программное

обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов (адреса отправителя и получателя, их номера портов и др.).

Брандмауэр экспертного уровня [stateful inspection firewall]- проверяет содержимое принимаемых пакетов на трех уровнях модели OSI - сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Создание брандмауэра относится к решению задачи ***экранирования***. Формальная постановка задачи **экранирования** состоит в следующем. Пусть имеется два множества информационных систем. **Экран** - это средство**разграничения доступа** клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков состоит в их **фильтрации**, возможно, с выполнением некоторых преобразований.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet (см. следующий раздел).

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Подчеркнем, что экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды - объектно-ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах экранирование станет одним из важнейших инструментов разграничения доступа к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Экранирование электронной почты описано в статье "Контроль над корпоративной электронной почтой: система "Дозор-Джет"" (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

1. 6 Лекция № 21-22 (4 часа).

Тема: «Уязвимости системных утилит, команд, сервисов. Уязвимости современных технологий программирования. Ошибки в ПО»

1.6.1 Вопросы лекции:

1. Виртуальные частные сети. Туннелирование

2. Сетевые уязвимости

1.6.2 Краткое содержание вопросов:

1. Виртуальные частные сети. Туннелирование

Виртуальные частные сети (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.

В этом случае решаются многие проблемы – филиалы могут располагаться где угодно по всему миру.

Опасность здесь заключается в том, что, во-первых, открытая сеть доступна для атак со стороны злоумышленников всего мира. Во-вторых, по Интернету все данные передаются в открытом виде, и злоумышленники, взломав сеть, будут обладать всей информацией, передаваемой по сети. И, в-третьих, данные могут быть не только перехвачены, но и заменены в процессе передачи через сеть. Злоумышленник может, например, нарушить целостность баз данных, действуя от имени клиентов одного из доверенных филиалов.

Чтобы этого не произошло, в решениях VPN используются такие средства, как шифрование данных для обеспечения целостности и конфиденциальности, аутентификация и авторизация для проверки прав пользователя и разрешения доступа к виртуальной частной 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.

Туннелирование (tunneling) или инкапсуляция (encapsulation) – это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в том виде, в котором он был сгенерирован хостом-отправителем, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Интернет). На конце туннеля кадры деинкапсулируются и передаются получателю. Как правило, туннель создается двумя пограничными устройствами, размещенными в точках входа в публичную сеть. Одним из явных достоинств туннелирования является то, что данная технология позволяет зашифровать исходный пакет целиком, включая заголовок, в котором могут находиться данные, содержащие информацию, которую злоумышленники используют для взлома сети (например, IP-адреса, количество подсетей и т.д.).

2. Сетевые уязвимости

Поскольку фактически все сетевые уровни содержат уязвимости, злонамеренные хакеры имеют изобилие возможностей для осуществления различных атак. Без создания надлежащей защиты любая часть любой сети может оказаться уязвимой для атак или другой несанкционированной деятельности. Угроза может исходить из широкого круга источников, включая профессиональных хакеров, конкурентов или даже собственных работников. Для определения наилучшего способа нейтрализации этих угроз и защиты сетей от осуществляемых атак, ИТ-менеджеры должны знать множество типов возможных атак и тот вред, который эти атаки могут нанести сетевой инфраструктуре вашей организации.

Вирусы и черви составляют подавляющее большинство хорошо известных атак. Вирус - это небольшой кусочек программного кода, присоединенный к легальной программе. Например, вирус может присоединить себя к таким программам, как программы табличных вычислений. Вирусы Melissa и "ILOVEYOU" попали в заголовки международных новостей вследствие того ущерба, который они вызвали. Червь - это небольшой кусочек программного кода, использующий "дыры" в безопасности для своего тиражирования. Копия червя сканирует сеть в поисках другого компьютера, имеющего определенную "дыру" в системе безопасности. Он копирует себя на новую машину через эту уязвимость, а затем начинает распространяться так же и с нее. W32/Blaster и

W32/Slammer - вот только два примера из получивших известность в последнее время червей.

Атака отказа в обслуживании (DoS, denial-of-service) генерирует фальшивые сетевые запросы с целью загрузки сетевых ресурсов и лишения других пользователей возможности их использования. DoS-атаки могут осуществляться на уровне сети с помощью посылки искусно подделанных пакетов, приводящих к отказу в работе сетевых соединений. Они могут также быть выполнены на уровне приложения, когда искусно подделанные команды приложения передаются программе, что приводит к ее чрезмерной загрузке или остановке работы. Атака может исходить из единственного источника (DoS) или быть распределенной между многими машинами (DdoS, distributed denial of service), предварительно подготовленными к этому. Эти неосведомленные компьютеры-соучастники, проводящие DoS-атаки, известны под именем "зомби". За работу "зомби" могут привлечь к судебной ответственности, даже если ваша организация не являлась инициатором атаки. Smurf, Trinoo, tribe flood network (TFN) и Slammer являются примерами DdoS-атак.

Исторически, атаки на пароль, в которых злоумышленник получает несанкционированный доступ к сети, являются наиболее распространенным типом атаки. Когда хакер "ломает" пароль законного пользователя, он получает доступ к его сетевым ресурсам. Хакер может легко получить пароль, потому что пользователи обычно выбирают простые слова или числа в качестве паролей, давая возможность хакеру использовать специальные программы для их методического перебора и угадывания. "Подслушивание" - другой способ получения пароля "жертвы", если сеть использует незащищенные удаленные соединения. Тщательно разработанные программы для "подслушивания" могут извлекать имя пользователя и его пароль в ходе сеанса входа в систему. Для получения доступа к паролям хакеры также используют технологии социального инжиниринга.

Переполнение буфера (buffer overflow) происходит в том случае, если программа или процесс пытаются использовать большее количество данных, чем объем буфера (область временного хранения данных), предназначенный для их хранения. В атаках переполнения буфера избыточные данные могут запускать код по желанию атакующего, например, получение прав пользователя root, позволяющих атакующему установить полный контроль над системой.

Скрипт-киддеры (script kiddy) используют широко распространенные программы или сценарии для случайного поиска уязвимостей через Интернет. Зачастую они слабо подготовлены в техническом отношении, но, к сожалению, представляют не меньшую угрозу, чем опытные хакеры.

Другая, часто остающаяся неразглашаемой угроза, исходит от своих сотрудников. Одно из исследований CSI говорит о том, что 45 процентов опрошенных респондентов регистрировали несанкционированный доступ со стороны собственных сотрудников. Эти злоумышленники обладают детальным знанием сети и вторгаются в нее со слабо-защищенной внутренней стороны (где брандмауэры теряют большую часть своей силы, а шифрование почти совсем не используется). Поэтому, внутренние злоупотребления остаются незамеченными и от них труднее всего защищаться.

1. 7 Лекция № 23-24 (4 часа).

Тема: «Обеспечение информационной безопасности в открытых системах. Принципы создания защищенных средств связи объектов в открытых системах»

1.7.1 Вопросы лекции:

1. Типы угроз

2. Классификация атак по основным механизмам реализации угроз

3. Сетевые сканеры

1.7.2 Краткое содержание вопросов:

1. Типы угроз

Фактически во многих случаях мы оказываемся "заложниками" современных технологий, зачастую не вполне понимая того, что эти технологии не являются в достаточной мере защищенными от вирусных и/или хакерских атак. Что работоспособность этих систем напрямую зависит от "эпидемиологической ситуации в компьютерном мире" в данный текущий момент времени, которая к тому же может измениться в любую минуту, как это уже происходило неоднократно. Что именно и каким образом происходит в современных компьютерных сетях, что угрожает нам в ближайшей перспективе, и что же нам следует делать в той ситуации, в которой оказалось современное компьютерное сообщество — ответы на эти и некоторые другие вопросы приведены в данной статье.

основные классы угроз

- вредное программное обеспечение;
- спам;
- глобальные сетевые атаки.

К первой категории относятся вирусные и троянские программы (включая сетевых червей), а также сетевые пакеты, которые используются в хакерских атаках. Ущерб, который наносится вредным программным обеспечением, можно классифицировать следующим образом:

Неавторизованный доступк персональной/корпоративной/государственной информации, т.е. ее уничтожение, изменение (включая намеренное искажение информации в злоумышленных целях), передача (отсылка, т.е. организация утечки информации, включая конфиденциальной/секретной).

Нештатное поведение программного обеспечения и железа,т.е. сбои и/или замедление работы компьютерных систем, зависания элементов систем, и т.п.

Использование вычислительных, дисковых и прочих ресурсовсистем в чужих интересах и/или в ущерб интересам владельца ресурсов.

Вторая категория угроз (спам) появилась значительно позднее, чем первая (вредоносные программы), однако по своей важности уверенно приближается к ней. Назойливость спама является далеко не единственной причиной, по которой к нему следует относиться как к отдельной категории современных угроз.

Спам — это:

Увеличение нагрузки на почтовые серверы,что влечет за собой неоправданное увеличение средств, вкладываемых в организацию инфраструктуры сетей, а также увеличение численности персонала, эти сети обслуживающего (если 50% писем — это спам, то 50% ваших почтовых серверов работают вхолостую, а системные администраторы, соответственно, вхолостую тратят часть своего рабочего времени).

Риск потери важной информациипо причине того, что она просто затерялась среди спама (если, например, 99 из 100 писем — это спам, то "заодно" уничтожится и нужное письмо).

Возможно, также, что письмо потеряется провайдером по причине того, что почтовый размер ящика переполнен спамом.

Пустая трата времени:для фильтрации спама сотрудники компаний (и домашние пользователи) тратят свое рабочее (и личное) время, доля которого возрастает с возрастанием доли спама в корреспонденции. Если к тому же оплата услуг провайдера ведется по размеру трафика, то возникает и прямой материальный ущерб — оплата

доставки заведомо ненужной принудительно навязываемой корреспонденции. Риск стать жертвой мошенников(привлечение к финансовым аферам или пирамидам), появление в почте нежелательной информации (если, например, домашний компьютер и почта используется также и детьми) и прочие подобные крупные, средние и мелкие неприятности.

Последняя (третья) категория угроз — это глобальные сетевые атаки, возникающие в результате запланированных действий хакера или группы хакеров, или как результат неконтролируемого распространения сетевых вирусов-червей. Сетевые атаки в компьютерных сетях являются, к счастью, пока достаточно редким событием, на которое особого внимания не обращают ни большинство экспертов по компьютерной безопасности, ни компьютерное сообщество в целом. Однако данная угроза существует реально, она является отдельным классом сетевых угроз, и к ней следует относиться со всей серьезностью, поскольку "успешная" глобальная сетевая атака (т.е. отказ каналов и/или центральных сетевых серверов) — это наихудшее из того, что может произойти в современных компьютерных сетях, как в локальных, так и в глобальных. Сетевые атаки приводят к следующимпоследствиям:

Отказ клиентских и серверных компонентов сетейпо причине перегрузки чрезмерным количеством запросов на обслуживание, т.е. запланированная или случайная DoS-атака (Denial of Service).

Заметное замедление работылокальных и глобальных сетей по причине перегрузки каналов, работа которых блокируется чрезмерным количеством передаваемых данных, т.е. "флудинг" (от flood) каналов передачи информации.

Заметный материальный ущербв тех случаях, когда оплата услуг провайдера ведется по размеру передаваемого и/или принимаемого трафика.

Говоря о сетевых атаках здесь и ниже подразумевается сеть "Интернет", как самая большая, наиболее популярная и наименее безопасная сеть. Хотя, в теории, возможны сетевые атаки в любых сетях (например, автомобильная пробка — это типичная "флуд"-атака на автомобильные дороги).

2. Классификация атак по основным механизмам реализации угроз

Проблема защиты ресурсов информационно-коммуникационных систем и сетей (ИКСМ), становится еще более актуальной в связи с развитием и распространением глобальных вычислительных сетей, территориально распределенных информационных комплексов и систем с удаленным управлением доступом к информационным ресурсам.

Весомым аргументом для повышения внимания к вопросам безопасности ИКСМ является бурное развитие программно-аппаратных методов и средств, способных скрытно существовать в системе и осуществлять потенциально любые несанкционированные действия (процессы), что препятствует нормальной работе пользователя и самой системы и непосредственно наносит вред свойствам информации (конфиденциальности, доступности, целостности).

Несмотря на разработку специальных программно-аппаратных средств защиты от воздействия угроз информационным ресурсам автоматизированных систем, количество новых методов реализации атак постоянно растет. Указанный влияние может быть реализовано технически или организационно, только в том случае, когда известна информация о принципах функционирования ИКСМ, ее структуру, программное обеспечение и т.д.

В настоящее время существует несколько классических определений понятия "атака" (вторжение, нападение) на информационную систему и ее ресурсы. Данный срок может определяться, как процедура вторжения, что приводит к нарушению политики безопасности или действие (процесс), что приводит к нарушению целостности, конфиденциальности и доступности информации системы. Однако, более

распространенная трактовка, непосредственно связано с термином «уязвимость», или «возможность реализации угрозы». Под атакой (attack, intrusion) на информационную систему, будем понимать действия (процессы) или последовательность связанных между собой действий нарушителя, которые приводят к реализации угроз информационным ресурсам ИКСМ, путем использования уязвимостей этой информационной системы.

Базовыми причинами нарушения функционирования информационной системы является сбои и отказы в работе информационной системы, которые частично или полностью препятствуют функционированию ИКСМ, возможностям доступа к информационным ресурсам и услугам системы. Кроме того, сбои и отказы в работе является одной из основных причин потери данных.

Существуют различные методы классификации атак. Например, деление на пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные.Однако, в данной статье, приведем более характерные типы атак на информационные системы и проведем их краткое описание реализации и определим характерные признаки.

Удаленное проникновение (remote penetration). Тип информационных атак, которые позволяют реализовать удаленное управление компьютером пользователя информационных ресурсов системы по сети на базе удаленного доступа. Примером такой программы является NetBus или BackOrifice.

Локальное проникновение (local penetration). Атака, приводящая к получению несанкционированного доступа к узлу ИКСМ, на котором она запущена. Примером такой программы является GetAdmin.

Удаленная отказ в обслуживании (remote denial of service). Атаки, которые позволяют нарушить функционирование информационной системы по условиям реализации ее услуг или имеют возможность котрольованного перезагрузки системы путем удаленного доступа.Примером такой атаки является Teardrop или trin00.

Локальная отказ в обслуживании (local denial of service). Атаки, позволяющие нарушить функционирование системы или перезагрузить систему, на которой они реализуются. В качестве примера такой атаки, можно привести использование несанкционированных апплетов, которые загружают центральный процессор бесконечным циклом, что делает невозможным обработку запросов других приложений.

Сетевые сканеры (network scanners). Программы, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки. Примером такой программы можно назвать систему nmap.

Сканеры уязвимостей (vulnerability scanners). Программы, осуществляющие поиск уязвимостей на узлах сети, могут быть использованы для реализации атак.Примеры: система SATAN или Shadow Security Scanner.

Взломщики паролей (password crackers). Программы, которые подбирают пароли авторизованных пользователей информационных ресурсов системы и ее услуг.Примером взломщика паролей может служить несанкционированное программное обеспечение: L0phtCrack для Windows или Crack для Unix.

Анализаторы протоколов (sniffers). Программы, которые "прослушивают" сетевой трафик. С помощью этих программ можно автоматически найти такую информацию, как идентификаторы и пароли пользователей, информацию о кредитных картах и т.д.Анализатором протоколов можно назвать программные продукты: Microsoft Network Monitor, NetXRay компании Network Associates или LanExplorer.

3. Сетевые сканеры

Поскольку системы на базе ОС Linux и BSD приобретают в последнее время все большую популярность, в этой публикации мы рассмотрим наиболее продвинутый сетевой сканер для операционных систем Linux — Nmap. Эта программа является одной

из наиболее распространенных в среде пользователей Linux и отличается мощным инструментарием и высокой скоростью работы.

Сетевой сканер Nmap появился в 1997 году для операционных систем на базе UNIX и продолжает совершенствоваться по сей день. От подобных программ для ОС на базе Windows он отличается мощным встроенным инструментарием, высокой скоростью работы, различными сопутствующими утилитами, разнообразными методами сканирования и популярность, поскольку практически любой дистрибутив Linux оснащен этим сканером сетевой безопасности. Однако, как и большинство узкоспециализированных программ для Linux, он не имеет доступной конечному пользователю оболочки и запускается из командной строки. Конечно, существуют дополнительные интерфейсы для управления этой утилитой, например такие, как Umit, Nmapfe, которые используют движок Nmap и выводят информацию в оконном режиме, а не в командной строке. Но все-таки эта утилита изначально разрабатывалась для работы в командной строке, а «навесные» утилиты увеличивают время работы и имеют массу недостатков по сравнению с оригиналом, в том числе и в стиле оформления. Кроме того, существует версия этой программы и для операционных систем на базе Windows. Так как методы работы и многие команды для обеих платформ идентичны, в данной статье будет рассмотрена версия Nmap 4.1 для Linux-систем. Поскольку Nmap входит практически в каждый дистрибутив Linux, для того чтобы просканировать сеть, не переставляя операционную систему, можно воспользоваться так называемыми LiveCD. Загрузочные диски такого типа не требуют установки и загружаются с CD/DVD-привода, при этом не нужно разбивать жесткий диск и создавать дополнительные разделы — жестким диском в этом случае служит часть оперативной памяти компьютера.

В настоящее время сетевые сканеры позволяют определять множество дополнительных параметров сканируемого компьютера. Nmap может определять большинство основных параметров сетевого адаптера: MAC-адрес, имя компьютера в домене, открытые порты, порты, закрытые брандмауэром, компанию — производителя чипсета сетевого адаптера исследуемого компьютера, версии ОС и служб. Отметим, что данные о MAC-адресах и о производителе чипсета можно получить только для компьютеров, которые находятся в той же подсети, что и сканирующий ПК. Чтобы оценить все достоинства этой программы, рассмотрим наиболее часто используемые при ее работе ключи.

Как уже говорилось, запуск Nmap производится из командной строки. При запуске программы без каких-либо ключей или с ключом Nmap -h (--help) либо без него на экран будет выведен список доступных ключей и задаваемых параметров

1. 8 Лекция № 25-26 (4 часа).

Тема: «Политика безопасности открытых систем. Управление безопасностью открытых систем»

1.8.1 Вопросы лекции:

1. Защита программ от изучения
2. Защита от разрушающих программных воздействий

1.8.2 Краткое содержание вопросов:

1. **Защита программ от изучения**

Запутывание кода

Наиболее часто встречающийся метод защиты ПО от исследования - обфускация, или запутывание кода. Под этим термином подразумевается приведение исполняемого кода к виду, сохраняющему функциональность программы, но затрудняющему анализ и понимание алгоритмов работы. Другими словами, запутывание так изменяет программу, что ее обратное преобразование будет экономически невыгодным (а физически очень трудновыполнимым). В основном этот способ защиты приложения используется для защиты программ от воссоздания исходного кода (декомпиляции) и незаконного использования, нарушения авторских прав программистов. Основная функция защиты программного обеспечения заключается не только в том, чтобы приложение нельзя было незаконно использовать, копировать или модифицировать, но и в том, чтобы не дать хакеру возможности изучить эту программу, применив излюбленный метод - пошаговый режим отладки. Тут уже может помочь нетипичное расположение стека (область памяти, где хранятся данные программы), его размер или варианты применения. Ведь при анализе с помощью специальных программ хакер может отбросить ненужный кусок кода или данных, в результате функционирование программы может оказаться невозможным или неправильным.

С помощью запутывания можно перемешать в программе куски кода или действия так, что логика работы становится совершенно непонятной. Кроме того, при запутывании могут вставляться новые куски неисполняемого (неиспользуемого) кода, а существующие блоки кода могут быть модифицированы таким образом, чтобы они использовались в нескольких частях программы одновременно.

Методы защиты от исследования

Иногда при защите программного продукта используется архивация данных программы, которые находятся в стеке. Для усложнения работы взломщиков в исполняемый код встраиваются "пустышки", которые выполняют некоторую сложную и на первый взгляд важную работу, но на самом деле не имеют никакого отношения к логике работы. Иногда используется такой метод, как "общая переменная", когда одна и та же переменная в разных частях алгоритма может употребляться для разных нужд (в разных функциях). Другой похожий метод - "разделяемая переменная" (для усложнения исследования программы одну переменную заменяют функцией от набора других переменных). В последнем случае при изменении одной из переменных, входящих в набор, меняется значение функции, а следовательно, и искомой переменной. Обычно в набор включают константы, другие переменные, адреса памяти, а также контрольные суммы отдельных блоков кода. Таким образом, меняя одну произвольную инструкцию в одном из блоков кода, можно повлиять на функциональность совершенно других частей программы. Также используется шифрование содержимого файлов данных, при котором защищенные файлы переносятся в защищенный контейнер. Особенностью защищенного контейнера является то, что к нему можно обращаться только из защищенного приложения.

В некоторых случаях применяется метод самогенерируемого кода, когда массив данных может быть сам по себе исполняемым кодом или смысловым текстом, но после некоторых операций он становится участком программы, выполняющим важные функции. Также используется полиморфный код, который при исполнении может изменять сам себя. Шифрование же позволяет изменить исполняемый код до полной неузнаваемости.

Используя защиту программного обеспечения от исследований, нужно иметь в виду, что лучше не только запутывать отдельные части кода, но и защищать всю программу целиком. Ведь защиту исполняемого кода можно дополнять другими видами защиты, например, при распространении приложения на дисках или через Интернет и т.п. Кроме того, защита кода должна быть максимально незаметной, замаскированной, запутывание не должно иметь регулярную структуру (иначе можно будет изучить

алгоритм запутывания и разработать программу, выполняющую обратные преобразования).

2. Защита от разрушающих программных воздействий

Важным моментом при использовании системы ЗИ является обеспечение потенциального невмешательства иных присутствующих в системе программ в процесс обработки информации компьютерной системой, работу системы ЗИ.

С помощью посторонних программ, присутствующих в компьютерной системе, злоумышленник может реализовать опосредованный несанкционированны доступ, то есть НСД, реализуемый злоумышленником не напрямую, а путем запуска в систему постороннего ПО – программных закладок, либо внедрения его на этапе проектирования АС. Можно выделить 3 вида разрушающих программных воздействий (программных воздействий, которые способны нарушить штатное функционирование АС).

Эти программы могут реализовать следующие функции:

скрывать признаки своего присутствия в оперативной среде

реализуют самодублирование и ассоциирование себя с другими программами. Самодублирование – процесс воспроизведения программой своего кода, который не обязательно совпадает с эталоном, но реализует те же самые функции. Под ассоциированием понимают внедрение программой своего кода в исполнительный код другой программы так, чтобы при неопределенных условиях управление передавалось этому РПВ.

способны разрушать код иных программ в оперативной памяти КС

способны переносить фрагменты информации из оперативной памяти в некие области внешней памяти, доступной злоумышленнику

имеют потенциальную возможность исказить либо подменить выводящуюся во внешнюю память информацию.

РПВ делятся на следующие классы:

Вирусы. Особенностью является направленность на самодублирование и деструктивные функции. Задача скрытия своего присутствия в ПА среде часто не ставится

Программные «черви» - РПВ, основной функцией которых является самодублирование путем распространения в сетях, используя уязвимости прикладных систем и сетевых сервисов.

«Троянские кони». Для этих программ не свойственно деструктивное воздействие. Данный класс РПВ часто относят к вирусам, однако, основной функцией РПВ данного класса, как правило, заключается в краже информации, например, номеров кредитных карт, либо в имитации сбоя ЭВМ, чтобы под видом ремонта злоумышленник мог получить к ней доступ. Основная особенность – ассоциирование либо выдача себя за часто используемое ПО либо сервисы.

Логические люки. РПВ, представляющее собой недекларируемую возможность, внедренную на этапе проектирования кода в исходные тексты программного обеспечения.

Программные закладки. Как правило, реализуют функции с 3 по 5, их действия могут быть направлены на кражу информации, либо отключение защитных функций.

Для того, чтобы РПВ получило управление, оно должно находится в оперативной памяти и активизироваться по некому общему для этого РПВ и прикладной программы, являющейся целью её воздействия, событию. Подобное событие называется активизирующим.

Если РПВ присутствует в ПА среде и загружено в оперативную память, то при отсутствии для него активизирующего события деструктивные особенности этого РПВ невозможны.

В качестве событий могут выступать прерывания, связанные с выполнением определенных действий, а часто действие, связанное с работой системы защиты, ввод с клавиатуры, прерывания по таймеру, операция с файлами и т.д.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Не предусмотрено РУП

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие №__1-4___ (_8_ часа).

Тема: «Инструментальные средства, помогающие расследовать деятельность, связанную с Интернет.»

3.1.1 Задание для работы:

1. Основные понятия и определения.
2. Статистика вторжений на Web-ререусры

3.1.2 Краткое описание проводимого занятия:

На этапе подготовки к практическому занятию студенты должны, используя учебную литературу и материалы лекций углубить свои знания по методам оценки уязвимости информации.

Во время проведения занятия Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое занятие, который представляет собой значения вероятностей РДik1 , PKij1 , PHijk1 , PИij1 для определения показателей уязвимости.

Студенты должны:

1. Вычислить значения базовых показателей уязвимости информации в соответствии с выражением.

2. Используя методику представленную выражениями вычислить значения показателей уязвимости.

3.1.3 Результаты и выводы:

Студент знакомится со статистикой вторжений на Web-ререусры, основными понятиями и определениями.

3.2 Практическое занятие №__5-8___ (_8_ часа).

Тема: «Основные понятия сетей TCP/IP. Виды сетевых адресов, сетевые протоколы, маршрутизация применительно к сетевым атакам. Аппаратура локальных сетей с точки зрения осуществления и предотвращения сетевых атак. Применение технологии виртуальных машин для моделирования сетевых атакПонятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры.

Понятие адаптивной безопасности и системы обнаружения атак. Особенности применения различных типов систем обнаружения атак. Особенности существующих свободно-распространяемых систем обнаружения атак.»

3.2.1 Задание для работы:

1. Проблемы обеспечения безопасности при удалённом доступе.
2. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.

3.2.2 Краткое описание проводимого занятия:

На этапе подготовки к практическому занятию студенты должны, используя учебную литературу и материалы лекций углубить свои знания по методам оценки уязвимости информации.

Во время проведения занятия Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое занятие, который представляет собой значения вероятностей РДikl , PKijl , PHijkl , PИijl для определения показателей уязвимости.

Студенты должны:

1 Определить наиболее опасную зону, категорию нарушителя, КНПИ.

2. Определить обобщенное значение показателя уязвимости ТКС

3.2.3 Результаты и выводы:

Студент знакомится с проблемами обеспечения безопасности при удалённом доступе и программно-аппаратными средствами обеспечения информационной безопасности в вычислительных сетях.

3.3 Практическое занятие №__9-12___ (_8_ часа).

Тема: «Атаки на основе подмены MAC-адреса. Методы защиты»

3.3.1 Задание для работы:

1 Обнаружение факта проведения и причин возникновения сетевой атаки подручными средствами
2 Дидактическая единица: Общие сведения об IDS snort.

3.3.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой. Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое

занятие, который представляет собой характеристики средств связи и средств радиоэлектронного противодействия.

Студенты должны:

1. Вычислить вероятность правильного обнаружения в зависимости от значений q при различных значениях базы сигнала и вероятности ложной тревоги в соответствии с методикой, построить соответствующие графические зависимости.

2. Для заданных исходных данных определить возможность перехвата сигнала разведприемником противника

3. Для заданных исходных данных определить возможность радиоэлектронного подавления линии радиосвязи противником

3.3.3 Результаты и выводы:

Студент знакомится с обнаружением факта проведения и причин возникновения сетевой атаки подручными средствами.

3.4 Практическое занятие №__13-16___ (_8_ часа).

Тема: «Атаки на основе подмены IP-адреса. Методы защиты. Синтаксис и механизм работы правил snort»

3.4.1 Задание для работы:

1. Значение IDS для решения задач поиска злоумышленников в собственной ЛВС.
2. Классификация, средства и методы защиты от атак.

3.4.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой. Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое занятие, который представляет собой характеристики средств связи и средств радиоэлектронного противодействия.

Студенты должны ответить на поставленные вопросы:

1. Дайте определение помехозащищенности.

2. Что такое помехоустойчивость и скрытность?

3. Перечислите основные меры по повышению помехозащищенности линии связи.

4. От чего зависит возможность радиоэлектронного подавления линии связи?

5. От чего зависит возможность перехвата сигнала средствами радиоразведки противника?

6. Дайте характеристику основным видам скрытности.

3.4.3 Результаты и выводы:

Студент знакомится со значением IDS для решения задач поиска злоумышленников в собственной ЛВС, классификацией, средствами и методами защиты от атак

3.5 Практическое занятие №__17-19___ (_6_ часа).

Тема: «Сравнительное тестирование персональных брандмауэров на предмет предоставляемого ими уровня защиты ПК от внешних сетевых атак»

3.5.1 Задание для работы:

1. Идентификация и аутентификация.
2. Ознакомление с криптографическими системами.
3. Экранирование, анализ защищенности.

3.5.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем студенты получают от преподавателя необходимую литературу [2-5] и самостоятельно, под руководством преподавателя, изучают средств защиты информации современных АС УВД «Альфа», «Синтез» и телекоммуникационных систем гражданской авиации, обращая внимание на методы, используемые для защиты информации и характеристики средств защиты информации

Студенты должны ответить на поставленные вопросы:

1 Что представляет собой комплекс программных средств защиты информации «Барьер-УВД2»? 2. Какие программно-аппаратные средства защиты информации, которые используются в комплексе средств защиты информации АС УВД «Синтез»?

3. Назовите основные характеристики средства защиты информации, которые используются в комплексе средств защиты информации АС УВД «Синтез».

4. Что представляет собой комплекс средств защиты информации «Сфера»?

3.5.3 Результаты и выводы:

Студент знакомится с идентификацией и аутентификацией,
экранированием, анализом защищенности

3.6 Практическое занятие №__20-21___ (_4_ часа).

Тема: «Синтаксиса и механизм работы правил регистрации и пропуска пакетов IDS snort, и возможностей динамических правил IDS snort»

3.6.1 Задание для работы:

1. Виртуальные частные сети. Туннелирование.

2. Сетевые уязвимости.

3.6.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем студенты получают от преподавателя необходимую литературу [2-5] и самостоятельно, под руководством преподавателя, изучают средств защиты информации современных АС УВД «Альфа», «Синтез» и телекоммуникационных систем гражданской авиации, обращая внимание на методы, используемые для защиты информации и характеристики средств защиты информации

Студенты должны ответить на поставленные вопросы:

1. Какие подсистемы входят в комплекс средств защиты информации «Сфера»?

2.Назовите основные методы, используемые для защиты информации вАС УВД «Альфа».

3. Как осуществляется настройка подсистем защиты информации комплекса «Сфера»?

4. Назовите состав персонала, обслуживающего комплекс средств защиты информации АС УВД «Альфа» и «Синтез» и их должностные обязанности

3.6.3 Результаты и выводы:

Студент знакомится с виртуальными частными сетями, туннелированием.

3.7 Практическое занятие №___22-23__ (_4_ часа).

Тема: «Знакомство с анализаторами сетевого трафика на примере Ethereal. Проведение служебного расследования деятельности, связанной с Интернет**»**

3.7.1 Задание для работы:

1. Типы угроз.
2. Классификация атак по основным механизмам реализации угроз.
3. Сетевые сканеры.

3.7.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на подгруппы. Для каждой подгруппы преподаватель определяет подсистему АС УВД (комплекс средств автоматизации (КСА) УВД, комплекс средств планирования использования воздушного пространства (КСА ПИВП), комплекс средств автоматизации аэродромных командно-диспетчерских пунктов (КСА АКДП), комплекс средств автоматизации метеорологического обеспечения (КСА МЕТЕО),

комплекс средств обеспечения справочной информацией (КОСИ)) и выдает необходимые для расчетов исходные данные.

Студенты должны:

1. Используя изложенную методику определить показатели актуальности угроз безопасности информации для заданной подсистемы АС УВД.

2. Сформулировать рекомендации по нейтрализации угроз информационной безопасности для заданной подсистемы АС УВД.

3. Определить схему построения защиты для заданной подсистемы АС УВД

3.7.3 Результаты и выводы:

Студент знакомится с типами угроз, классификацией атак по основным механизмам реализации угроз, сетевыми сканерами.

3.8 Практическое занятие №__24-25___ (_4_ часа).

Тема: «Средства анализа информационной безопасности компьютерных сетей»

3.8.1 Задание для работы:

1. Защита программ от изучения.
2. Защита от разрушающих программных воздействий.

3.8.2 Краткое описание проводимого занятия:

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на подгруппы. Для каждой подгруппы преподаватель определяет подсистему АС УВД (комплекс средств автоматизации (КСА) УВД, комплекс средств планирования использования воздушного пространства (КСА ПИВП), комплекс средств автоматизации аэродромных командно-диспетчерских пунктов (КСА АКДП), комплекс средств автоматизации метеорологического обеспечения (КСА МЕТЕО), комплекс средств обеспечения справочной информацией (КОСИ)) и выдает необходимые для расчетов исходные данные.

Студенты должны ответить на поставленные вопросы:

1. Сформулируйте общие положения методики расчета актуальности угроз информационной безопасности АС УВД.

2. Что является исходными данными при оценке актуальности угроз информационной безопасности в АС УВД?

3. Как определятся важность информации, циркулирующей в АС УВД?

3.8.3 Результаты и выводы:

Студент знакомится с защитой программ от изучения и защитой от разрушающих программных воздействий.