ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Факультет информационных технологий

Кафедра комплексного обеспечения информационной безопасности автоматизированных систем

КУРСОВОЙ ПРОЕКТ

по дисциплине «Безопасность вычислительных систем»

на тему: Проект защищенной беспроводной вычислительной сети.

 Выполнил студент 41 гр.

 КОИБАС Абакумов А.В.

 Проверил Галиев Р. Э.

Оренбург 2010

Содержание.

Введение\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.3

1. Разработка структуры сети\_\_\_\_­­­­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.5
	1. Архитектура сети\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.5
	2. Стандарты беспроводной сети\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.6
2. Настройка сетевых компонентов на сервере\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.8

 2.1 Установка и настройка DHCP**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**стр.8

 2.1.1 Установка службы DHCP на имеющийся сервер\_\_\_\_\_\_\_\_\_\_стр8

 2.1.2 Настройка службы DHCP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.9

 2.1.3 Создание новой области\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.10

 2.2 Установка служб IIS и FTP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.12

 2.2.1 Настройка службы FTP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.13

 2.3 Сервер терминалов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.15

 2.3.1 Открыть Подключение к удаленному рабочему столу\_\_\_\_\_\_стр.16

 2.3.2Создание подключения к удаленному рабочему столу\_\_\_\_\_\_стр.16

 2.4 Общий доступ к Интернету\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.17

 2.4.1 Настройка главного компьютера ICS\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.17

 2.4.2 Настройка клиента Windows\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.19

3. Анализ безопасности сети\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.21

 3.1 Угрозы в беспроводной сети\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.21

 3.2 Методы и средства защиты\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.29

Заключение.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.29

Список литературы.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_стр.30

Введение.

Основной задачей беспроводных сетей является обеспечение на определенной территории высокоскоростного локального доступа к сервисам и данным, обмен информацией между пользователями, находящимися в пределах данной территории.

Построение сетей Wi-Fi (IEEE 802.11) беспроводной передачи данных в настоящее время широко востребовано за счет массы преимуществ. Среди основных достоинств данной технологии наиболее привлекательны следующие:

- низкая стоимость оборудования;

- гибкость применения оборудования;

- высокая скорость передачи данных.

Благодаря отсутствию проводных подключений пользователи беспроводных Wi-Fi сетей обладают свободой передвижения, свободой выбора рабочих мест. Данная технология дает возможность наиболее рационального использования офисного пространства: сотрудники компании остаются мобильными, имея доступ ко всем необходимым данным и услугам.

Помимо прочих преимуществ, широкое распространение стандартов WLAN обеспечивает не только возможность работать в офисных помещениях и зданиях филиалов, но и обеспечивает мобильность сотрудников компании на время отъезда. Благодаря беспроводным сетям, во время командировки, отдыха в гостинице и нахождения в пути сотрудники смогут быть на связи в любую минуту. Эта же технология используется в публичных хот-спотах, которые устанавливаются в торговых и конференц-центрах, гостиницах, аэропортах, ресторанах и других общественных местах. Таким образом, за счет беспроводных сетей формируется экосистема, посредством которой обеспечивается защищенный мобильный доступ. У пользователей всегда есть возможность широкого использования информационных ресурсов не только в офисе компании, но и во время поездок на ближние и дальние расстояния.

Данная технология предоставляет возможность для работы целого ряда пользовательских приложений. Инфраструктура беспроводных сетей – это основа, на которой строится дальнейшее внедрение пользовательских приложений и обеспечивается поддержка ключевых для компании сервисов. К таким сервисам относятся сетевое управление, информационная безопасность и механизмы гарантии качества сервиса.

**1. Разработка структуры сети.**

**1.1 Архитектура сети**

Беспроводная сеть офиса содержит в себе как беспроводной сегмент сети, так и проводной сегмент.

 Беспроводная сеть включает в себя:

1. 80 компьютеров-клиентов;
2. 8 роутеров Wi-Fi;
3. Свич;
4. Сервер .

**1.2 Стандарты беспроводной сети.**

Технология Wi­Fi одна из самых перспективных на сегодняшний день в области компьютерной связи. Беспроводные сетевые технологи позволяют Вам, где бы Вы не находились, быть подключенными к сети и обмениваться данными. Технологией Wi-Fi называют один из форматов передачи цифровых данных по радиоканалам.

Wi-Fi сокращение от Wireless Fidelity - это логотип, который компания WECA использует для обозначения совместимости конкретного изделия с беспроводными сетями (WLAN). Термин введен Wi-Fi Alliance.
Все изделия проходят сложные тесты, и тем устройствам, которые отвечают требуемым стандартам взаимодействия (802.11), присваивается сертификат с правом на логотип Wi-Fi (Wi-Fi Certified).

Первоначально термин "Wi-Fi" использовался как обозначение стандарта 2.4GHz 802.11b, так же, как название "Ethernet" используется для обозначения стандарта IEEE 802.3. Альянс расширил использование термина, как обозначение возможности взаимодействия (interoperability) беспроводных локальных сетей.

WLAN- Сокращение от wireless local-area network- беспроводная локальная сеть. Иногда применяется сокращение LAWN. Тип локальной сети, при построении которой для связи между узлами вместо проводов используются высокочастотные радио волны.

IEEE 802.11 - семейство спецификаций, разработанных IEEE для беспроводных локальных сетей (wireless LAN). 802.11 задает спецификации интерфейса между беспроводным клиентом и базовой станцией или между двумя беспроводными клиентами. Спецификации представлены в 1997г.

Имеются следующие спецификации семейства 802.11:
**IEEE 802.11** -- применяется для беспроводных локальных сетей и обеспечивает передачу 1 или 2 Мбит/сек. (Mbps) в полосе 2.4 гигагерц (GHz) с использованием либо метода частотных скачков (FHSS), либо метода прямой последовательности(DSSS).

**IEEE 802.11a** -- расширение спецификации 802.11, применяется для беспроводных локальных сетей, и обеспечивает до 54 Мбит/сек (Mbps) в полосе 5 гигагерц (GHz). В спецификации 802.11a используется ортогональное частотное разделение сигналов и мультиплексирование вместо FHSS или DSSS.

**IEEE 802.11b** (известный также как 802.11 High Rate или Wi-Fi) -- расширение 802.11, обеспечивает 11 Мбит/сек (Mbps) (а также 5.5, 2 и 1 Мбит/сек.) в полосе 2.4 гигагерц (GHz). 802.11b использует толко DSSS.

**IEEE 802.11g** -- обеспечивает 20 (и более) Мбит/сек. (Mbps) в полосе 2.4 гигагерц (GHz).

**2. Настройка сетевых компонентов на сервере.**

**2.1 Установка и настройка DHCP.**

Перед настройкой службы DHCP ее необходимо установить на сервер. По умолчанию служба DHCP не устанавливается во время установки системы Windows Standard Server 2003 или Windows Enterprise Server 2003. Установку службы DHCP можно выполнить во время установки Windows Server 2003 или после нее.

**2.1.1 Установка службы DHCP на имеющийся сервер**

1. В меню **Пуск** выделите пункт **Панель управления** и выберите команду **Установка и удаление программ**.
2. В окне Установка и удаление программ выберите пункт **Установка компонентов Windows**.

1. В окне **«Мастер компонентов Windows»** из списка **Компоненты** выберите пункт **Сетевые службы** и нажмите кнопку **Состав**.
2. В окне **Сетевые службы** установите флажок **DHCP** и нажмите **OK**.
3. Для запуска программы установки щелкните кнопку **Далее** в мастере компонентов Windows. Если потребуется, вставьте в дисковод для чтения компакт-дисков или DVD-дисков установочный компакт-диск Windows Server 2003. Программа установки скопирует на компьютер файлы сервера DHCP и необходимых служебных программ.
4. После завершения работы программы установки нажмите кнопку **Готово**.

**2.1.2** **Настройка службы DHCP**

После установки и запуска службы DHCP необходимо создать область (диапазон допустимых IP-адресов, которые смогут использовать клиенты DHCP). Согласно рекомендациям корпорации Майкрософт у каждого сервера DHCP в сети должно быть по крайней мере по одной области, которая бы не пересекалась с областями других серверов DHCP в сети. В системе Windows Server 2003 серверы DHCP в домене Active Directory должны пройти авторизацию, чтобы случайные серверы DHCP не переходили в интерактивный режим. Любой сервер DHCP под управлением Windows Server 2003, не прошедший авторизацию, не будет работать с клиентами.

**2.1.3** **Создание новой области**

1. Нажмите кнопку **Пуск** и выберите последовательно пункты **Программы**, **Администрирование** и **DHCP**.
2. В дереве консоли щелкните правой кнопкой мыши сервер **DHCP**, для которого необходимо создать новую область DHCP, и выберите пункт **Создать область**.
3. В **Мастере создания новой области** нажмите кнопку **Далее**, а затем введите имя и описание области. Имя может выбираться произвольным образом, но оно должно отражать назначение данной области (например, можно указать имя «Адреса клиентов административного корпуса»). Нажмите кнопку **Далее**.
4. Введите диапазон адресов, входящих в область (например, можно использовать адреса от 192.168.10.1 до 192.168.10.254). Поскольку эти адреса будут присваиваться клиентам, они должны быть действительными внутри данной сети и не использоваться в данный момент. При необходимости можно ввести и использовать новую маску подсети. Нажмите кнопку **Далее**.
5. Введите IP-адреса, которые следует исключить из указанного диапазона (например, если некоторые из адресов, заданных в пункте 4, уже были статически присвоены некоторым компьютерам в сети). В большинстве случаев контроллеры доменов, веб-серверы, серверы DHCP, серверы DNS (Domain Name System) и другие серверы имеют статические IP-адреса. Нажмите кнопку **Далее**.
6. Введите срок действия аренды IP-адреса из данной области (дней, часов и минут). Он определяет время, в течение которого клиент может использовать выделенный адрес до его обновления. Нажмите кнопку **Далее** и выберите пункт **Да**, настроить эти параметры сейчас, если вам нужно продолжить работу мастера и настроить основные параметры DHCP. Нажмите кнопку **Далее**.
7. Введите IP-адрес основного шлюза, который должен использоваться клиентами при получении адреса из данной области. Нажмите Добавить для включения адреса шлюза по умолчанию в список и щелкните кнопку Далее.
8. Если в сети уже имеется сервер DNS, введите доменное имя вашей организации в поле Родительский домен. Введите имя сервера DNS и нажмите кнопку Сопоставить, чтобы проверить способность сервера DHCP установить связь с сервером DNS и определить его адрес. Нажмите кнопку Добавить, чтобы включить этот сервер в список серверов DNS, назначенных клиентам DHCP. Нажмите кнопку Далее и выполните те же действия еще раз, если в сети имеется сервер WINS (Windows Internet Naming Service), указав его имя и IP-адрес. Нажмите кнопку Далее.
9. Щелкните Да, я хочу активировать эту область сейчас, чтобы активировать область и разрешить выделение адресов из нее клиентам, и нажмите кнопку **Далее**.
10. Нажмите кнопку **Готово**.
11. В дереве консоли выделите имя сервера и выберите из меню Действия команду **Авторизовать**.

**2.2 Установка служб IIS и FTP**

Служба FTP зависит от служб IIS (Internet Information Services). Чтобы установить службы IIS и FTP, выполните следующие действия.

**Примечание**. В Windows Server 2003 служба FTP не устанавливается по умолчанию одновременно со службами IIS. Если службы IIS уже установлены, воспользуйтесь для установки службы FTP компонентом «Установка и удаление программ» панели управления.

1. В меню **Пуск** выберите пункт **Панель управления** и запустите компонент **Установка и удаление программ**.
2. Нажмите кнопку **Установка компонентов Windows**.
3. В списке **Компоненты** выберите пункт **Сервер приложений**, затем — **Службы IIS** (но не меняйте состояния флажка) и нажмите кнопку **Состав**.
4. Установите следующие флажки (если они не установлены):

**Общие файлы**

**Служба FTP**

**Диспетчер служб IIS**

1. Установите флажки других необходимых компонентов или служб и нажмите кнопку **ОК**.
2. Нажмите кнопку **Далее**.
3. В ответ на соответствующий запрос вставьте компакт-диск Windows Server 2003 или укажите путь к месту расположения файлов и нажмите кнопку **ОК**.
4. Нажмите кнопку **Готово**.

Службы IIS и FTP установлены. Перед началом использования службы FTP ее необходимо настроить.

 **2.2.1** **Настройка службы FTP**

Чтобы настроить службу FTP на прием анонимных подключений, выполните следующие действия:

1. Запустите **«Диспетчер служб IIS»** или **откройте оснастку IIS**.
2. Разверните компонент **имя\_сервера**, где имя\_сервера — имя сервера.
3. Разверните компонент Узлы FTP.
4. Щелкните правой кнопкой мыши элемент **FTP-узел по умолчанию** и выберите пункт **Свойства**.
5. Перейдите на вкладку **Учетные записи безопасности**.
6. Установите флажок **Разрешить анонимные подключения** (если он не установлен) и флажок **Разрешить только анонимные подключения**.

После установки флажка **Разрешить только анонимные подключения** служба FTP принимает только анонимные подключения (пользователи не смогут подключиться с помощью своих учетных данных).

1. Перейдите на вкладку **Основной каталог**.
2. Установите флажки **Чтение** и **Запись** в журнал (если они не установлены), снимите флажок **Запись** (если он установлен).
3. Нажмите кнопку **ОК**.
4. Закройте диспетчер служб IIS или оснастку IIS.

Сервер FTP готов принимать входящие запросы FTP. Скопируйте или переместите файлы, к которым следует открыть доступ, в папку публикации FTP. По умолчанию используется папка диск:\Inetpub\Ftproot, где диск — это диск, на котором установлены службы IIS.

**2.3 Сервер терминалов**

Сервер терминалов (Terminal Server). Позволяет множеству пользователей с помощью клиентского ПО Службы терминалов (Terminal Services) или Дистанционное управление рабочим столом (Remote Desktop) подключаться к приложениям и ресурсам сервера, например принтерам или дисковому пространству, как если бы эти ресурсы были установлены на их компьютерах. В отличие от Windows 2000, Windows Server 2003 предоставляет Дистанционное управление рабочим столом автоматически. Роли сервера терминалов требуются, только когда нужно размещать приложения для пользователей на сервере терминалов.

**2.3.1** **Открыть Подключение к удаленному рабочему столу.**

Чтобы открыть подключение к удаленному рабочему столу, нажмите кнопку **Пуск**, выберите пункт **Все программы**, выберите пункт **Стандартные**, выберите пункт **Связи** и выберите команду **Удаленный рабочий стол**.

 **2.3.2 Создание подключения к удаленному рабочему столу.**

1. В диалоговом окне **имя компьютера**, введите имя компьютера или IP-адрес сервера терминалов или компьютера, имеющего включено дистанционное управление рабочим столом.
2. Нажимаете кнопку **Подключение**.
3. В диалоговом окне **Вход в Windows** диалоговое окно введите имя пользователя, пароль и домен (при необходимости) и нажмите кнопку **OK.**

**2.4 Общий доступ к Интернету**

Общий доступ к Интернету (ICS) позволяет использовать Windows Server 2003 для подключения небольшой офисной сети или домашней сети через Интернет. Механизм ICS обеспечивает преобразование сетевых адресов (NAT), назначение IP-адресов и разрешение имен для всех компьютеров в небольшой сети.

Для установки ICS требуется следующее оборудование и программное обеспечение:

1. Цифровая абонентская линия (DSL) или кабельный модем, подключенный к поставщику услуг Интернета (ISP), а также активированную учетную запись DSL или кабельного интернета.
2. Два установленных сетевых адаптера.
3. Сеть, с уже настроенными TCP/IP.

**2.4.1 Настройка главного компьютера ICS**

На узловом компьютере ICS обеспечивает подключение через второй сетевой адаптер для существующей сети TCP/IP. Чтобы настроить главный компьютер ICS, необходимо войти в систему с помощью учетной записи члена группы «Администраторы».

1. Нажмите **Пуск**, затем **Панель управления** и выбирайте команду **Сетевые подключения.**
2. Далее нажимаете правой кнопкой мыши на **Подключение по локальной сети** (к которой подключен интернет) и переименуйте его в **Подключение к интернету.**
3. В диалоговом окне **Сетевые подключения**, отображаются два подключения: **Подключение к интернету** и **Подключение по локальной** **сети.**
4. Нажмите правой кнопкой мыши по **Подключение к Интернету** и выберите команду **Свойства**.
5. В «свойствах» перейдите на вкладку **Общие**, и убедиться что в компонентах отображены и выбраны **Клиент для сетей Microsoft** и **Протокол Интернета (TCP/IP)**.

1. Затем перейдите на вкладку **Дополнительно**, и напротив **«разрешить другим пользователям сети использовать подключение к Интернету данного компьютера»** установите флажок.

1. Далее нажимайте **OK** и возвращайтесь к рабочему столу.

 **2.4.2 Настройка клиента Windows**

Войдите в систему как член группы «Администраторы», чтобы настроить клиентов Windows, которые будут использовать подключение к Интернету.

1. Нажмите **Пуск**, затем **Панель управления** и выбирайте команду **Сетевые подключения.**
2. Далее нажимаете правой кнопкой мыши на **Подключение по локальной сети** и выберете **Свойства**
3. В «свойствах» перейдите на вкладку **Общие**, и убедиться что в компонентах отображены и выбраны **Клиент для сетей Microsoft** и **Протокол Интернета (TCP/IP)**.
4. Выбираете **Протокол интернета (TCP/IP)**, и нажимаете на кнопку **Свойства**
5. Во вкладке Общее устанавливаем флажки напротив **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически**

1. Затем нажимаете **OK** и возвращайтесь к рабочему столу

**3. Анализ безопасности сети**

* 1. **Угрозы в беспроводной сети.**

Итак, беспроводные технологии, работающие без физических и логических ограничений своих проводных аналогов, подвергают сетевую инфраструктуру и пользователей значительным угрозам. Для того чтобы понять, как обеспечить безопасное функционирование беспроводных сетей, давайте рассмотрим их подробнее.

Угроза первая – «чужаки»

«Чужаками» называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, зачастую в обход механизмов защиты, определенных корпоративной политикой безопасности. Чаще всего это те самые самовольно установленные точки доступа. Статистика по всему миру указывает на чужаков как на причину большинства взломов сетей организаций. Даже если организация не использует беспроводную связь и считает себя в результате такого запрета защищенной от беспроводных атак, внедренный (умышленно или нет) чужак с легкостью исправит это положение. Доступность и дешевизна устройств Wi-Fi привели к тому, что в США, например, практически каждая сеть с числом пользователей более 50 успела столкнуться с данным феноменом.

Помимо точек доступа, в роли чужака могут выступить домашний маршрутизатор с поддержкой Wi-Fi, программная точка доступа Soft AP, ноутбук с одновременно включенными проводным и беспроводным интерфейсами, сканер, проектор и т. п.

Угроза вторая – нефиксированная природа связи

Как уже отмечалось, беспроводные устройства не «привязаны» кабелем к розетке и могут менять точки подключения к сети прямо в процессе работы. К примеру, могут происходить «случайные ассоциации», когда ноутбук с Windows XP (достаточно доверительно относящейся ко всем беспроводным сетям) или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Такой механизм позволяет злоумышленникам «переключать на себя» ничего не подозревающего пользователя для последующего сканирования уязвимостей, фишинга или атак типа Man-in-The-Middle. Кроме того, если пользователь одновременно подключен и к проводной сети, то он становится удобной точкой входа, т. е. классическим чужаком.

Многие пользователи ноутбуков, оснащенных Wi-Fi и проводными интерфейсами и недовольные качеством работы проводной сети (медленно, администратор поставил фильтрацию URL, не работает ICQ), любят переключаться на ближайшие зоны доступа. Или ОС делает это для них автоматически в случае, например, отказа проводной сети. Излишне говорить, что в такой ситуации все старания ИТ-отдела по обеспечению сетевой безопасности остаются безрезультатными.

Сети ad-hoc – одноранговые соединения между беспроводными устройствами без участия ТД – позволяют быстро перебросить файл коллеге или распечатать нужный документ на принтере с картой Wi-Fi. Однако такой способ организации сети не поддерживает большинство необходимых методов обеспечения безопасности, предоставляя злоумышленникам легкий путь ко взлому компьютеров пользователей.

Угроза третья – уязвимости сетей и устройств

Некоторые сетевые устройства могут быть более уязвимы, чем другие: неправильно сконфигурированы, используют слабые ключи шифрования или методы аутентификации с известными уязвимостями. Неудивительно, что в первую очередь злоумышленники атакуют именно их. Отчеты аналитиков утверждают, что более 70% успешных взломов беспроводных сетей произошло именно в результате неправильной конфигурации точек доступа или клиентского ПО.

Некорректно сконфигурированные ТД. Одна-единственная некорректно сконфигурированная ТД (в т. ч. чужак) может послужить причиной взлома корпоративной сети. Настройки по умолчанию большинства ТД не включают аутентификацию или шифрование либо используют статические ключи, записанные в руководстве и потому общеизвестные. В сочетании с невысокой ценой этих устройств данный фактор значительно осложняет задачу слежения за целостностью конфигурации беспроводной инфраструктуры и уровнем ее защиты. Сотрудники организации могут самовольно приносить ТД и подключать их куда заблагорассудится. При этом маловероятно, что они уделят достаточно внимания их грамотной и безопасной конфигурации и согласуют свои действия с ИТ-отделом. Именно такие ТД и создают наибольшую угрозу проводным и беспроводным сетям.

Некорректно сконфигурированные беспроводные клиенты. Данная категория представляет угрозу еще большую, чем некорректно сконфигурированные ТД. Эти устройства буквально «приходят и уходят» с предприятия, часто они не конфигурируются специально с целью минимизации беспроводных угроз или довольствуются установками по умолчанию (которые не могут считаться безопасными). Такие устройства оказывают неоценимую помощь хакерам, обеспечивая удобную точку входа для сканирования сети и распространения в ней вредоносного ПО.

Взлом шифрования. Злоумышленникам давно доступны специальные средства для взлома сетей, основывающихся на стандарте шифрования WEP. Эти инструменты широко представлены в Интернете, и их применение не требует особых навыков. Они используют уязвимости алгоритма WEP, пассивно собирая статистику трафика в беспроводной сети до тех пор, пока полученных данных не окажется достаточно для восстановления ключа шифрования. С использованием последнего поколения средств взлома WEP, применяющих специальные методы инъекции трафика, срок «до тех пор» колеблется от 15 мин до 15 с. Совсем недавно были обнаружены первые, пока еще незначительные, уязвимости в TKIP, позволяющие расшифровывать и отправлять в защищенную сеть небольшие пакеты.

Угроза четвертая – новые угрозы и атаки

Беспроводные технологии породили новые способы реализации старых угроз, а также некоторые новые, доселе невозможные в проводных сетях. Во всех случаях бороться с атакующим стало гораздо тяжелее, так как невозможно ни отследить его физическое местоположение, ни изолировать от сети.

Разведка. Большинство традиционных атак начинаются с разведки, в результате которой злоумышленником определяются дальнейшие пути их развития. Для беспроводной разведки используются как средства сканирования беспроводных сетей (NetStumbler, Wellenreiter, встроенный клиент JC), так и средства сбора и анализа пакетов, ведь многие управляющие пакеты WLAN не зашифрованы. При этом очень сложно отличить станцию, собирающую информацию, от обычной, пытающейся получить авторизованный доступ к сети или от попытки случайной ассоциации.

Многие пробуют защитить свои сети путем сокрытия ее названия в маячках (Beacon), рассылаемых точками доступа, и отключения ответа на широковещательный запрос ESSID (Broadcast ESSID). Общепризнанно, что методов, относящихся к классу Security through Obscurity, недостаточно, поскольку атакующий все равно видит беспроводную сеть на определенном радиоканале, и ему остается лишь ждать первого авторизованного подключения, так как в его процессе в эфире передается ESSID в незашифрованном виде. После этого данная мера безопасности просто теряет смысл. Некоторые особенности беспроводного клиента Windows XP SP2 (поправленные в SP3) еще более усугубляли ситуацию, ведь клиент постоянно рассылал имя такой скрытой сети в эфир, пытаясь подключиться к ней. В результате злоумышленник не только получал имя сети, но и мог «подсадить» такого клиента на свою точку доступа.

Имперсонализация (Identity Theft). Имперсонализация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в последнем случае определить подлинность пользователя сложнее. Конечно, существуют SSID, и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и то и другое несложно подделать. А подделав, как минимум «откусить» часть пропускной способности сети, вставлять неправильные фреймы с целью нарушения авторизованных коммуникаций. Расколов же хоть чуть-чуть алгоритмы шифрования – устраивать атаки на структуру сети (например, ARP Poisoning, как в случае с недавно обнаруженной уязвимостью TKIP). Не говоря уже о взломе WEP, рассмотренном пунктом выше.

Существует ложное убеждение, что имперсонализация пользователя возможна только в случае MAC-аутентификации или применения статических ключей, что схемы на основе 802.1x, такие как LEAP, являются абсолютно безопасными. К сожалению, это не так, и уже сейчас доступен инструментарий для взлома, к примеру LEAP. Другие схемы, скажем EAP-TLS или PEAP, более надежны, но они не гарантируют устойчивости к комплексной атаке, использующей несколько факторов одновременно.

Отказы в обслуживании (Denial of Service, DoS). Задачей атаки «Отказ в обслуживании» является либо нарушение показателей качества функционирования сетевых услуг, либо полная ликвидация возможности доступа к ним для авторизованных пользователей. Для этого, к примеру, сеть может быть завалена «мусорными» пакетами (с неправильной контрольной суммой и т. д.), отправленными с легитимного адреса. В случае беспроводной сети отследить источник такой атаки без специального инструментария просто нельзя. Кроме того, есть возможность организовать DoS на физическом уровне, запустив достаточно мощный генератор помех в нужном частотном диапазоне.

Специализированные инструменты атакующего. Инструментарий атак на беспроводные сети широко доступен в Интернете и постоянно пополняется новыми средствами. Основными типами инструментов атакующего являются:

* средства разведки – сканирования сетей и определения их параметров, сбора и анализа трафика (Kismet, NetStumbler, AirMagnet, Ethereal, Wireshark со специальным модулем, THC-RUT);
* инструменты взлома шифрования (AirCrack, WEPWedgie, WEPCrack, WepAttack, AirSnort);
* инструменты взлома механизмов аутентификации для их обхода или получения параметров учетной записи доступа пользователя (ASLEAP, THC-LEAPCracker);
* инструменты организации отказов в обслуживании (WLANjack, hunter\_killer);
* сканеры уязвимостей (Nessus, xSpider);
* инструменты манипулирования беспроводными соединениями (HotSpotter, SoftAP, AirSnarf);
* традиционный инструментарий (SMAC, IRPAS, Ettercap, Cain & Abel, DSNIFF, IKEcrack).

Угроза пятая – утечки информации из проводной сети

Практически все беспроводные сети в какой-то момент соединяются с проводными. Соответственно, любая беспроводная ТД может быть использована как плацдарм для атаки. Но это еще не все: некоторые ошибки в их конфигурации в сочетании с ошибками конфигурации проводной сети могут открывать пути для утечек информации. Наиболее распространенный пример – ТД, работающие в режиме моста (Layer 2 Bridge), подключенные в плоскую сеть (или сеть с нарушениями сегментации VLAN) и передающие в эфир широковещательные пакеты из проводного сегмента, запросы ARP, DHCP, фреймы STP и т. п. Некоторые из этих данных могут быть полезными для организаций атак Man-in-The-Middle, различных Poisoning и DoS, да и просто разведки.

Другой распространенный сценарий основывается на особенностях реализации протоколов 802.11. В случае, когда на одной ТД настроены сразу несколько ESSID, широковещательный трафик будет распространяться сразу во все ESSID. В результате, если на одной точке настроены защищенная сеть и публичная зона доступа, злоумышленник, подключенный к последней, может, например, нарушить работу протоколов DHCP или ARP в защищенной сети. Это можно исправить, включив режим Multi-BSSID, он же Virtual AP, который поддерживается практически всеми производителями оборудования класса Enterprise (и мало кем из класса Consumer), но об этом нужно знать.

Угроза шестая – особенности функционирования беспроводных сетей

Некоторые особенности функционирования беспроводных сетей порождают дополнительные проблемы, способные влиять в целом на их доступность, производительность, безопасность и стоимость эксплуатации. Для грамотного решения этих проблем требуются специальный инструментарий поддержки и эксплуатации, специальные механизмы администрирования и мониторинга, не реализованные в традиционном инструментарии управления беспроводными сетями.

Активность в нерабочее время. К беспроводным сетям можно подключиться в любом месте в зоне их покрытия и в любое время. Из-за этого многие организации ограничивают доступность беспроводных сетей в своих офисах исключительно рабочими часами (вплоть до физического отключения ТД). В свете сказанного естественно предположить, что всякая беспроводная активность в сети в нерабочее время должна считаться подозрительной и подлежать расследованию.

Скорости. ТД, разрешающие подключения на низких скоростях, имеют бoльшую зону покрытия. Таким образом, они предоставляют дополнительную возможность удаленного взлома. Если в офисной сети, где все работают на скоростях 24/36/54 Мб/с, вдруг появляется соединение на 1 или 2 Мб/с, это может быть сигналом, что кто-то пытается пробиться в сеть с улицы.

Помехи. Качество работы беспроводной сети зависит от многих факторов. Наиболее ярким примером являются помехи, значительно снижающие пропускную способность и количество поддерживаемых клиентов, вплоть до полной невозможности использования сети. Источником помех может быть любое устройство, излучающее сигнал достаточной мощности в том же частотном диапазоне, что и ТД. С другой стороны, злоумышленники могут использовать помехи для организации DoS-атаки на сеть.

Помимо помех, существуют другие аспекты, влияющие на качество связи в беспроводных сетях – неверно сконфигурированный клиент или сбоящая антенна ТД могут создавать проблемы как на физическом, так и на канальном уровне, приводя к ухудшению качества обслуживания остальных клиентов сети.

* 1. **Методы и средства защиты.**

Стандартами беспроводных сетей предусмотрено несколько механизмов обеспечения безопасности:

* режим аутентификации и шифрования данных по протоколу WEP (Wired Equivalent Privacy);
* режим аутентификации и шифрования данных по протоколу WPA (Wi-Fi Protected Access);
* фильтрация по MAC-адресам;
* использование режима скрытого идентификатора сети.

Протокол WEP

Все современные беспроводные устройства (точки доступа, беспроводные адаптеры и маршрутизаторы) поддерживают протокол безопасности WEP, который был изначально заложен в спецификацию беспроводных сетей IEEE 802.11.

Протокол WEP позволяет шифровать поток передаваемых данных на основе алгоритма RC4 с ключом размером 64 или 128 бит. Некоторые устройства поддерживают также ключи в 152, 256 и 512 бит, однако это скорее исключение из правил. Ключи имеют так называемую статическую составляющую длиной 40 и 104 бит соответственно для 64- и 128-битных ключей, а также дополнительную динамическую составляющую размером 24 бита, называемую вектором инициализации (Initialization Vector, IV).

На простейшем уровне процедура WEP-шифрования выглядит следующим образом.

Первоначально передаваемые в пакете данные проверяются на целостность (алгоритм CRC-32), после чего контрольная сумма (integrity check value, ICV) добавляется в служебное поле заголовка пакета. Далее генерируется 24-битный вектор инициализации (IV), к которому добавляется статический (40- или 104-битный) секретный ключ. Полученный таким образом 64- или 128-битный ключ и является исходным ключом для генерации псевдослучайного числа, используемого для шифрования данных. Далее данные смешиваются (шифруются) с помощью логической операции XOR с псевдослучайной ключевой последовательностью, а вектор инициализации добавляется в служебное поле кадра.

На приемной стороне данные могут быть расшифрованы, поскольку вместе с данными передается информация о векторе инициализации, а статическая составляющая ключа хранится у пользователя, которому передаются данные.

Протокол WEP предусматривает два способа аутентификации пользователей: Open System (открытая) и Shared Key (общий ключ). При использовании открытой аутентификации собственно никакой аутентификации не происходит, то есть получить доступ в беспроводную сеть может любой пользователь. Однако даже в случае открытой системы допускается применение WEP-шифрования данных.

Протокол WPA

В 2003 году был представлен еще один стандарт безопасности — WPA, главной особенностью которого является технология динамической генерации ключей шифрования данных, построенная на базе протокола TKIP (Temporal Key Integrity Protocol), представляющего собой дальнейшее развитие алгоритма шифрования RC4. По протоколу TKIP сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей. В протоколе TKIP предусмотрена генерация нового, 128-битного ключа для каждого передаваемого пакета. Кроме того, контрольные криптографические суммы в WPA рассчитываются по новому методу — MIC (Message Integrity Code). В каждый кадр здесь помещается специальный восьмибайтный код целостности сообщения, проверка которого позволяет отражать атаки с применением подложных пакетов. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом.

Помимо этого протокол WPA поддерживает шифрование по усовершенствованному стандарту AES (Advanced Encryption Standard), который отличается более стойким, по сравнению с протоколами WEP и TKIP, криптоалгоритмом.

При развертывании беспроводных сетей в домашних условиях или в небольших офисах обычно используется вариант протокола безопасности WPA на основе общих ключей — WPA-PSK (Pre Shared Key). В дальнейшем мы будем рассматривать только вариант WPA, не касаясь вариантов протокола WPA, ориентированных на корпоративные сети, где авторизация пользователей проводится на отдельном RADIUS-сервере.

При использовании WPA в настройках точки доступа и профилях беспроводного соединения клиентов указывается пароль длиной от 8 до 63 символов.

Фильтрация MAC-адресов

Фильтрация MAC-адресов, которая поддерживается всеми современными точками доступа и беспроводными маршрутизаторами, хотя и не является составной частью стандарта 802.11, тем не менее, как считается, позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках точки доступа создается таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети.

Режим скрытого идентификатора сети SSID

Еще одна мера предосторожности, которую часто используют в беспроводных сетях, — это режим скрытого идентификатора сети. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. При попытке пользователя войти в сеть драйвер беспроводного адаптера прежде сканирует эфир на предмет наличия в ней беспроводных сетей. В случае использования режима скрытого идентификатора (как правило, этот режим называется Hide SSID) сеть не отображается в списке доступных и подключиться к ней можно, только если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

Заключение.

Распространенность беспроводных технологий в наше время ставит под угрозу и те сети, где они уже применяются, и те, где никогда не должны использоваться. Традиционные средства защиты бессильны против принципиально новых классов беспроводных угроз. При этом ситуация осложняется тем, что необходимо защищать также и своих пользователей (которые могут находиться и вдали от офиса), не нарушая при этом функционирования сетей соседей, каким бы подозрительным оно не выглядело. Тем не менее существуют методы защиты от подобных угроз как беспроводных, так и проводных сетей и пользователей, позволяющие уверенно и безопасно развертывать и использовать беспроводные сети.

Список литературы:

1. Шетка Петр «Microsoft Windows Server 2003» Практическое руководство по настройке сети. СПБ: Наука и техника, 2006
2. <http://support.microsoft.com/?ln=ru>
3. <http://www.insotel.ru/article.php?id=206>