ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ

Дисциплина: Сети и телекоммуникации

Работу выполнила: Белорукова Елизавета Игоревна

Студентка 3 курса ИВТ 1 подгруппа

Лабораторная работа №1

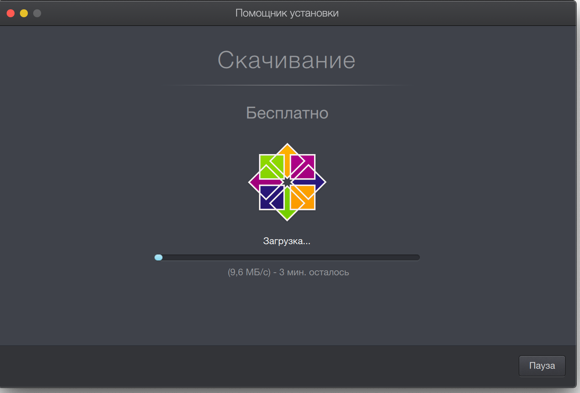
Тема: ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ МАШИН ДЛЯ ИЗУЧЕНИЯ

СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ ОПЕРАЦИОННЫХ СИСТЕМ

Цель работы: изучение сетевого взаимодействия операционных систем, устанавливаемых в виртуальную машину Microsoft Virtual PC 2007.

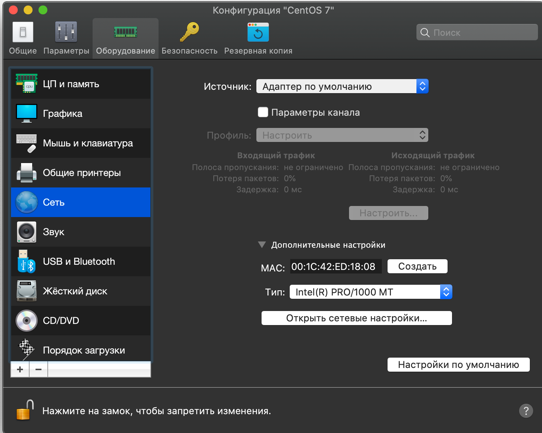
Задание: На лабораторной работе необходимо установить на компьютер Virtual PC 2007, создать две новых виртуальных машины, установить операционные системы Windows Server 2003 и Linux (по указанию преподавателя) и проверить сетевое взаимодействие виртуальных машин.





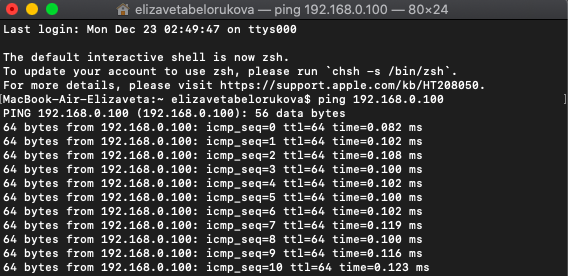
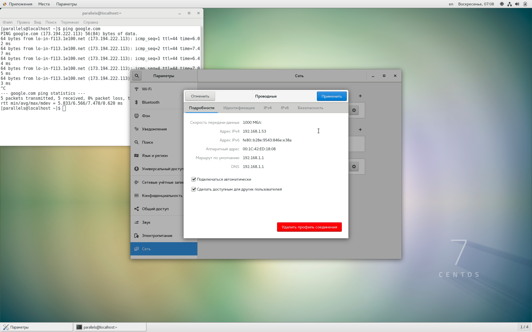
Настройка сетевого окружения в ВМ.

Универсальный способ - подключить “Сетевой мост”, который сразу же предоставляет доступ к общей сети(глобальной), через физическую машину. в этом пункте, нужно определить наиболее подходящий адаптер, и поставить галочку “Подключить кабель”.



Чтобы пропинговать нашу машину через физ.машину, нужно установить адаптер локальной сети - “Внутренняя сеть”.

Определяем , какой ip адрес присвоен ВМ, после чего посылаем пинг с физической машины на этот ip



Лабораторная работа №2

Тема: УПРАВЛЕНИЕ ПОЛИТИКОЙ БЕЗОПАСНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

Цель работы: освоения средств администратора и аудитора операционной системы Windows.

**Аудит (ГОСТ Р 53114-2008)-**

Систематический независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

**Политика безопасности (ГОСТ Р 53114-2008)** - Формальное изложение правил поведения, процедур, практических приёмов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Примечание: Политики должны содержать:

1. предмет, основные цели и задачи политики безопасности;

2. условия применения политики безопасности и возможные ограничения;

3. описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;

4. права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации:

5. порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

**Журнал аудита - (audit log):** Хронологическая последовательность записей аудита, каждая из которых содержит данные об определенном событии

**Электронная цифровая подпись (ЭЦП)** – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа ЭЦП, а также установить отсутствие искажения информации в электронном документе.

Действие приложения, такое как авторизация или использование цифровой подписи, является функцией Выполнить, a ID события ее идентифицирует.

**Какие события безопасности должны фиксироваться в журнале аудита?**

Служба журнала событий записывает события приложений, системные события и события безопасности в окне просмотра событий, например, Вход в систему, Управление учетной записью, Доступ к службе каталогов, Доступ к объектам, Изменения политики, Использования привилегий, Отслеживание процессов, Системных событий, Событий входа в систему.

**Какие параметры определяют политику аудита?**

Аудит событий входа в систему по учетной записи, Аудит управления учетными записями, Аудит доступа к службе каталогов, Аудит событий входа в систему, Аудит доступа к объектам, Аудит изменения политики, Аудит использования привилегий, Аудит отслеживания процессов, Аудит системных событий

**Целесообразно ли с точки зрения безопасности компьютерной системы (КС) разрешать анонимный доступ к ее информационным ресурсам?**

Нет. Если предоставить доступ к инф. ресурсам, то можно нарушить не только работу компьютерной системы, но и сохранность данных, хранящихся на КС.

**Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя?**

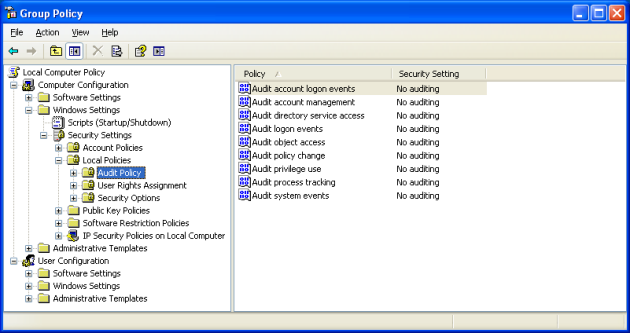
В зашифрованном виде, ключ к расшифровке передается отдельно (на флешке, например).

**Нужно ли ограничивать права пользователей по запуску прикладных программ?**

Да, для обеспечения безопасности.

Применение Аудита Windows для отслеживания деятельности пользователей

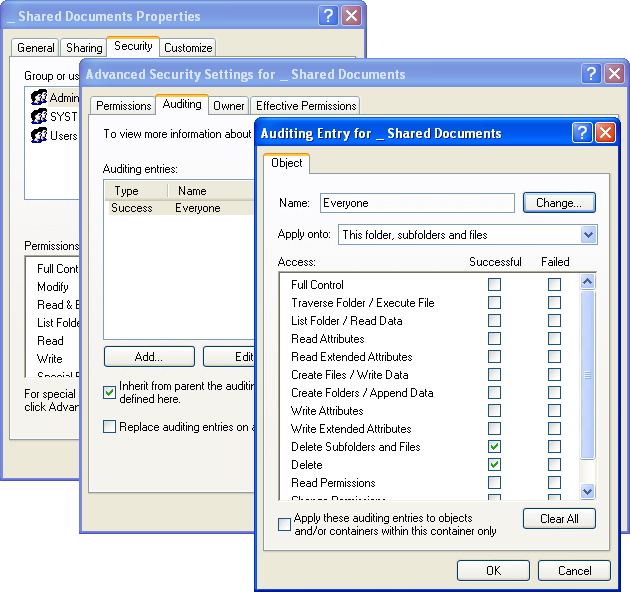
Для включения аудита зайдите с правами администратора в компьютер, предоставляющий доступ к общим документам, и выполните команду **Start**→**Run**→**gpedit.msc.** В разделе Computer Configuration раскройте папку **Windows Settings → Security Settings → Local Policies → Audit Policies:**

[](http://windowsntlv.files.wordpress.com/2011/08/audit_policy.png)

Дважды щёлкните по политике **Audit object access (Аудит доступа к объектам)** и выберите галочку **Success.** Этот параметр включает механизм слежения за успешным доступом к файлам и реестру. Действительно, ведь нас интересуют только удавшиеся попытки удаления файлов или папок. Включите Аудит только на компьютерах, непосредственно на которых хранятся отслеживаемые объекты.

        Простого включения политики Аудита недостаточно, мы также должны указать, доступ к каким именно папкам требуется отслеживать. Обычно такими объектами являются папки общих (разделяемых) документов и папки с производственными программами или базами данных (бухгалтерия, склад и т.п.) — то есть, ресурсы, с которыми работают несколько человек.

        Заранее угадать, кто именно удалит файл, невозможно, поэтому слежение и указывается за Всеми (Everyone). Удавшиеся попытки удаления отслеживаемых объектов любым пользователем будут заноситься в журнал. Вызовите свойства требуемой папки (если таких папок несколько, то всех их по очереди) и на закладке **Security (Безопасность) → Advanced (Дополнительно) → Auditing (Аудит)** добавьте слежение за субъектом **Everyone (Все),** его успешными попытками доступа **Delete (Удаление)** и **Delete Subfolders and Files (Удаление подкаталогов и файлов):**

[](http://windowsntlv.files.wordpress.com/2011/08/audit_files.png)

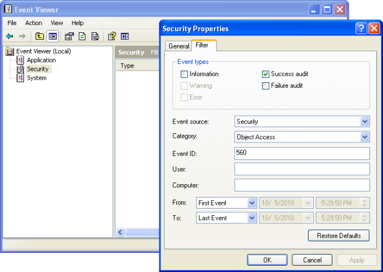
        Событий может журналироваться довольно много, поэтому также следует отрегулировать размер журнала **Security (Безопасность)**, в который они будут записываться. Для  
этого выполните команду **Start → Run → eventvwr.msc.** В появившемся окне вызовите свойства журнала Security и укажите следующие параметры:

* Maximum Log Size = **65536 KB** (для рабочих станций) или **262144 KB** (для серверов)
* Overwrite events as needed.

        На самом деле, указанные цифры не являются гарантированно точными, а подбираются опытным путём для каждого конкретного случая.

 Нажмите **Start → Run → eventvwr.msc** и откройте для просмотра журнал **Security (Безопасность).**Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щёлкнув правой кнопкой по журналу Security, выберите команду **View → Filter** и отфильтруйте просмотр по следующим критериям:

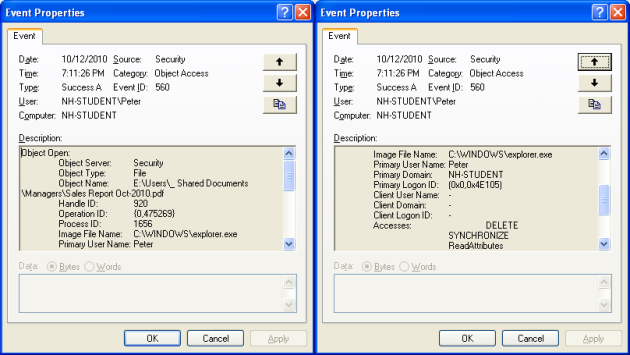
* Event Source:Security;
* Category:         Object Access;
* Event Types:      Success Audit;
* Event ID:         560;

**[](http://windowsntlv.files.wordpress.com/2011/08/audit_events2003.png)**

Просмотрите список отфильтрованных событий, обращая внимание на следующие поля внутри каждой записи:

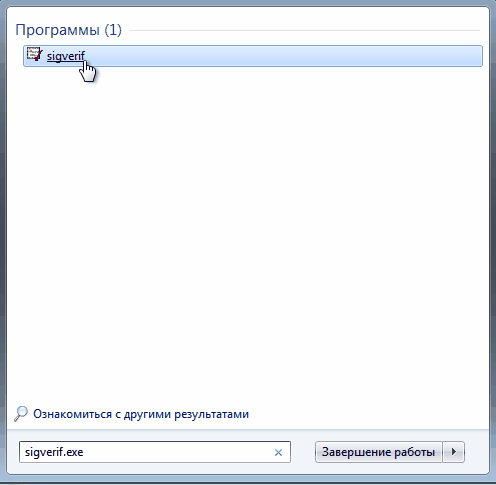
* **Object Name.** Название искомой папки или  файла;
* **Image File Name.** Имя программы, с помощью которой удалили файл;
* **Accesses.** Набор запрашиваемых прав.

Программа может запрашивать у системы сразу несколько типов доступа — например, **Delete+Synchronize**или **Delete+Read\_Control.** Значимым для нас правом является **Delete.**

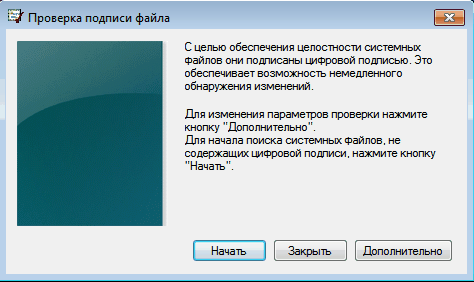
**[](http://windowsntlv.files.wordpress.com/2011/08/audit_details2003.png)**

### Проверка цифровой подписи

В Windows 7 для проверки цифровой подписи есть специальная утилита sigverif.exe. Для ее запуска нужно в поисковой строке меню Пуск набрать sigverif.exe и нажать Ввод

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig1.gif)

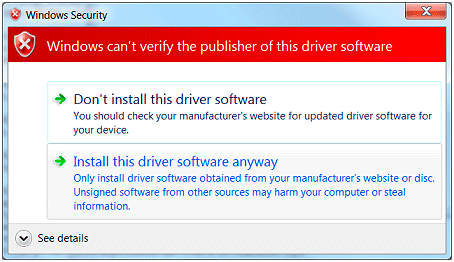
В окне программы жмем начать, и она автоматически проверяет системные файлы на наличие подписей.

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig2.gif)

Результат проверки сохраняется в текстовый файл sigverif.txt. Хранится он в папке Общие документы, также его можно посмотреть прямо из окна программы, щелкнув по кнопке Дополнительно.

### Отключение проверки цифровой подписи

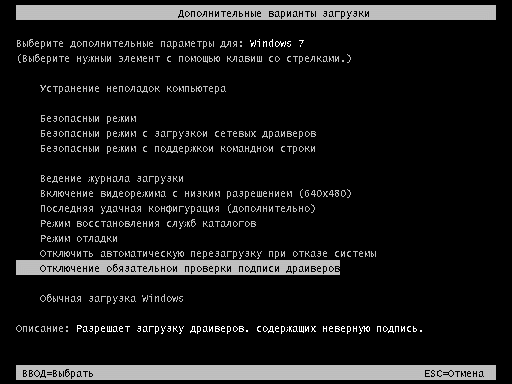
В Windows 7 требования к устанавливаемым драйверам существенно ужесточены, и любой устанавливаемый драйвер должен иметь цифровую подпись, проверенную и сертифицированную Microsoft. Перед загрузкой и установкой драйвера устройства Windows проверит его цифровую подпись, и если драйвер не подписан, выдаст предупреждение

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig7.gif)

Можно это предупреждение проигнорировать и установить драйвер, однако работать он не будет все равно. При установке неподписанного драйвера в диспетчере устройств данное устройство будет помечено восклицательным знаком и содержать сообщение об ошибке.

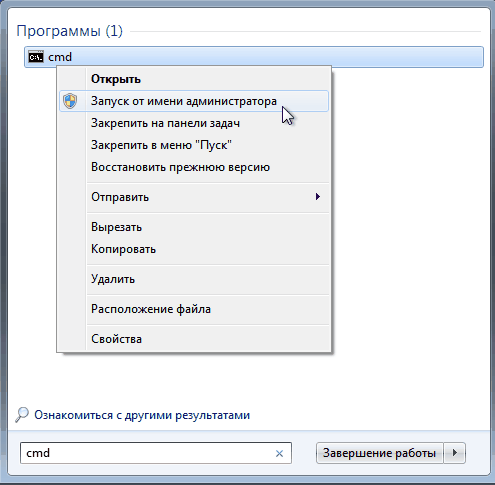
Политика проверки цифровой подписи драйверов призвана улучшить надежность и стабильность операционной системы, но иногда возникает необходимость установить неподписанный драйвер. К счастью, в Windows 7 можно отключить проверку цифровой подписи. Для этого есть несколько способов:

Отключить поверку цифровой подписи драйверов при загрузке через загрузочное меню. Для этого при загрузке ОС жмем клавишу F8. Для загрузки без проверки цифровых подписей нужно выбрать пункт «Отключение обязательной проверки подписи драйверов»

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig5.gif)

Дальше можно загружаться и устанавливать необходимые драйвера. Однако данный режим предназначен исключительно для тестирования и при следующей загрузке в обычном режиме установленный драйвер работать не будет.

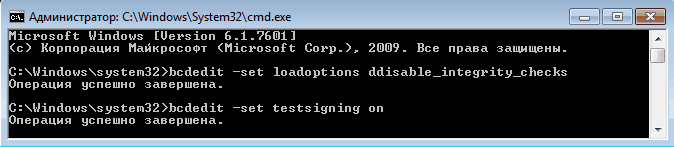
Для постоянной загрузки в тестовом режиме можно воспользоваться утилитой командной строки bcdedit. Для этого открываем командную строку с правами администратора

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig8.gif)

И последовательно вводим 2 команды:

bcdedit -set loadoptions DDISABLED\_INTEGRITY\_CHECKS

bcdedit  -set TESTSIGNING ON

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig9.gif)

После выполнения каждой команды должно появиться сообщение об успешном выполнении.  Теперь можно перезагрузить компьютер и установить необходимые драйвера.

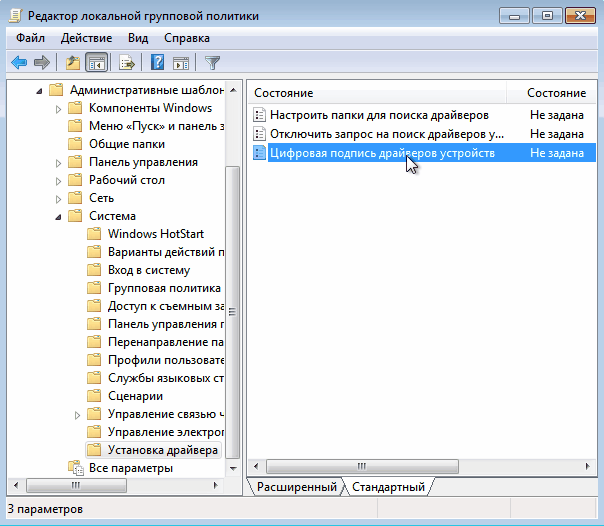
Для отключения тестового режима нужно ввести в командной строке команды:

bcdedit -set loadoptions ENABLE\_INTEGRITY\_CHECKS

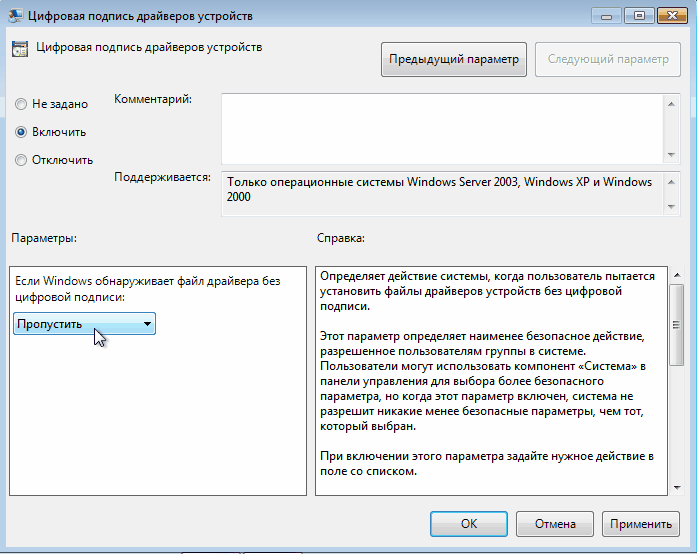
bsdedit -set loadoptions TESTSIGNING ON

**Важно**: если выдается сообщение о том, что команда неизвестна, то вместо дефиса (-) ключи можно писать через слеш (/).

Ну и наконец можно просто отключить проверку цифровых подписей драйверов через групповую политику. Для запуска оснастки групповой политики вводим в меню Пуск в строке поиска команду gpedit.msc и жмем Ввод. В меню политик идем в Конфигурация пользователя\Административные шаблоны\Система\Установка драйверов и выбираем политику «Цифровая подпись драйверов устройств».

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig10.gif)

В появившемся окне включаем политику и указываем параметр пропустить в качестве действия системы при обнаружении неподписанных драйверов.

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig11.gif)

После перезагрузки политика применится и можно будет загружать и устанавливать любые, в том числе и неподписанные драйвера.

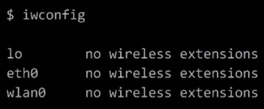
Лабораторная работа №3

Тема: АНАЛИЗ УСТОЙЧИВОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ WEP И WPA-TKIP

Цель работы: анализ устойчивости ко взлому и уязвимостей протоколов шифрования WEP и WPA-TKIP, изучение признаков атак, направленных на взлом Wi-Fi сети, определение параметров сети, необходимых для обеспечения ее безопасности.

**WEP**

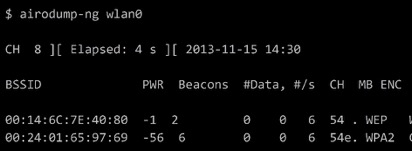
1. Узнаем имя беспроводного интерфейса с помощью iwconfig



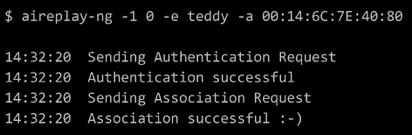
1. Запускаем интерфейс в режиме мониторинга



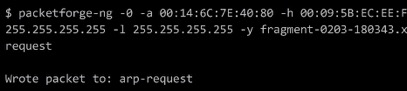
1. Выбираем сеть для атаки среди доступных



1. Используем aircrack-ng, чтобы произвести авторизацию



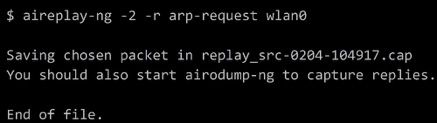
1. Получаем PRGA в новой консоли
2. Получили. xor файл. Генерируем пакет для инъекции



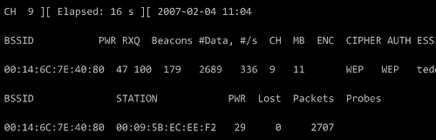
1. В новой консоли:



1. В консоли, где сгенерировали пакет – начинаем инъекцию



1. Вывод в третьей консоли:



1. Запускаем aircrack-ng для получения WEP ключа

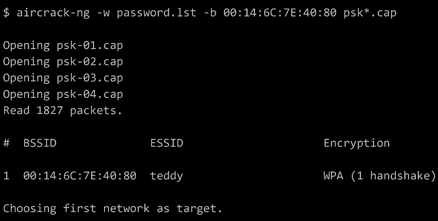


**WPA-PSK**

1. Повторяем пункты 1-3 прошлого эксперимента
2. Используем aireplay-ng для деаутентификации клиентов



1. Запускаем aircrack-ng для взлома ключа пре-авторизации



1. Результат



**Какой алгоритм лежит в основе шифрования WEP? Какой уровень защиты должно было обеспечить шифрование WEP? Обеспечивается ли этот уровень на данный момент?**

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

Как и любая другая система безопасности на основе паролей, надежность WEP зависит от длины и состава ключа, а также частоты его смены. Первый серьезный недостаток – применение статического ключа – за относительно небольшое время ключ можно подобрать перебором. И второй недостаток WEP-шифрования – самосинхронизация для каждого сообщения, поскольку вектор инициализации передается незашифрованным текстом с каждым пакетом и через небольшой промежуток времени он повторяется. В результате протокол шифрования WEP на основе алгоритма RC4 в настоящее время не является стойким.

**Какого размера могут быть ключи при использовании шифрования WEP? Из каких частей они состоят?**

Ключи состоят из статической составляющей от 40 до 104 бит и с дополнительной случайной динамической составляющей (вектором инициализации) размером 24 бит; в результате шифрование данных производилось на ключе размером от 64 до 128 бит.

**Какие пакеты необходимо перехватывать, чтобы иметь возможность определить ключ WEP?**

Необходимо перехватить векторы инициализации (динамическая часть).

**В чем заключается основная уязвимость шифрования WEP?**

Уязвимости его настолько серьезны, что позволяют взломать ключ и подключиться к защищенной сети за считанные минуты. Основные уязвимости WEP связаны с малой длиной IV, примитивном алгоритме получения per-packet key, уязвимостями самого RC4 алгоритма и его потоковой природой.

Какое главное отличие шифрования WPA от WEP?

WPA шифрует данные каждого клиента отдельно.

**Какой тип шифрования WPA в настоящее время уязвим для взлома?**

WPA-PSK.

**Какое условие является обязательным при взломе WPA-PSK? Для чего оно необходимо?**

Нужно чтобы был подключен как минимум один клиент к точке доступа. Так как нам нужно перехватить “пакет-рукопожатия” для последующего перебора.

**По какому методу осуществляется подбор WPA-PSK ключа?**

Атака происходит путем перебора паролей по словарю.

**От чего самым непосредственным образом зависит успешность подбора ключа?**

Подбор ключа WPA-PSK будет успешным только в том случае, если он будет присутствовать в словаре, по которому ведется перебор.

**Может ли WPA-PSK обеспечить надежную защиту информации?**

Да, если грамотно подобрать пароль.

Лабораторная работа №4

Тема: ИЗУЧЕНИЕ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы: - освоение программных средств защиты информации PGP, предназначенных для:

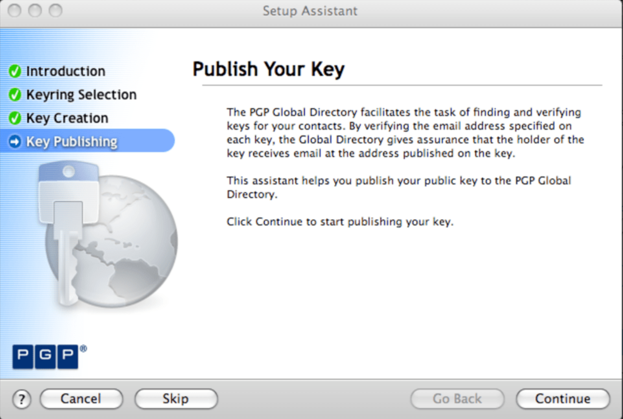
- шифрования конфиденциальных информационных ресурсов;

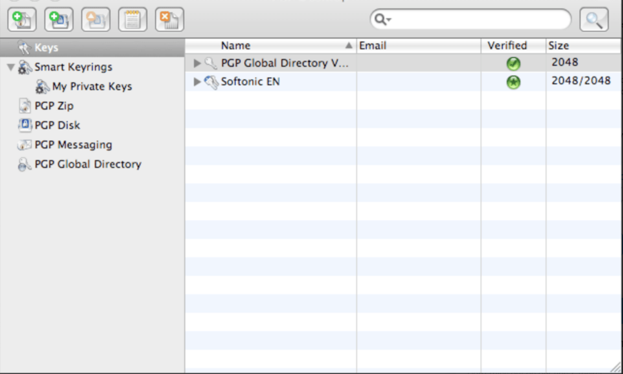
- обеспечения целостности информационных ресурсов с помощью механизма;

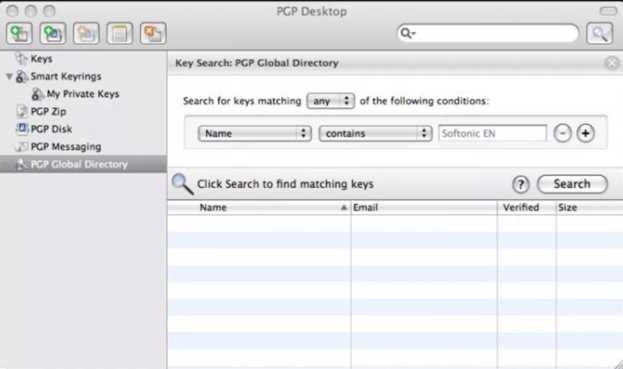
- электронной цифровой подписи;

- надежного уничтожения остаточной конфиденциальной информации;

- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

****

****

****

**Как обеспечивается случайность выбираемых криптографических ключей в системе PGP?**

Компонент PGP, ответственный за выдачу случайных чисел, называется генератором (истинно) случайных чисел (ГСЧ), в противовес так называемым ГПСЧ, алгоритмам, генерирующим детерминированный поток, похожий на случайные данные. ГСЧ использует гибридный подход: он обращается к внешним источникам для обеспечения непредсказуемости и использует функцию хэширования, чтобы сгладить отклонения.

**Как и где хранится секретный ключ пользователя в системе PGP?**

Секретные ключи хранятся в виде "сертификатов ключей", которые включают в себя идентификатор пользователя владельца ключа (обычно это имя пользователя), временную метку, которая указывает время генерации пары ключей, и собственно ключи. Сертификаты секретных ключей — секретные. Каждый секретный ключ также шифруется с отдельным паролем. Файл ключей, или каталог ключей ("кольцо с ключами" — "keyring") содержит один или несколько таких сертификатов. В каталогах секретных ключей хранятся сертификаты секретных ключей.

**Как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере.?**

Сохранением его резервной копии.

**Какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение?**

1. **Файл ключа,** введите расположение файла PGP ключа, который будет использоваться для шифрования файлов. Если оставить это поле пустым, действия файла шифрования PGP используется файл, укажите в папки Keyring поля. Файлы могут иметь любое расширение имени файла, но \*.asc является стандартным.
2. **Папка Keyring,** введите расположение папки, содержащей keyring, который будет использоваться для шифрования файлов. Файл открытого keyring (\*.pkr) могут быть переименованы с расширением \*.gpg.
3. **Пользователь,** введите имя пользователя, который был указан при создании ключа шифрования. Это поле является обязательным.
4. **COMMENT,** введите комментарий, который был указан при создании ключа шифрования. Если это поле был завершен, когда был создан ключ шифрования, необходимо предоставить эти сведения при использовании этого действия.
5. **Электронная почта,** введите адрес электронной почты, который был указан при создании ключа шифрования. Это поле является обязательным.

**Как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP;**

Генерируется ГСЧ, хранится в самом зашифрованном файле.

**Как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей?**

Отправить свой открытый ключ на публично доступный сервер ключей, с которого этот ключ смогут получить другие пользователи.

**Изменяется ли и как размер файла после его шифрования?**

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения.

**Какие функции по управлению криптографическими ключами пользователей предоставляет администратору программа PGP?**

С помощью команд строчного интерфейса ее пользователь может выполнять все базовые криптографические функции, а именно:

1. генерацию пары из закрытого/открытого ключа;
2. шифрование файла с помощью открытого ключа любого пользователя PGP (в том числе своего);
3. расшифровку файла с помощью своего закрытого ключа;
4. наложение цифровой подписи с помощью своего закрытого ключа на файл (аутентификация файла) или на открытый ключ другого пользователя (сертификация ключа);
5. проверку (верификацию) своей подписи или подписи другого пользователя с помощью его открытого ключа.