МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение   
высшего образования

**«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

П.В. МЫТАРЕВ

**Практикум по дисциплине   
«Информационная безопасность»**

Ульяновск

УлГТУ

2016

**УДК 004.9 : 338(076)**

**ББК 32.973.26 – 018.2я73**

|  |  |
| --- | --- |
| К69  К69 | Рекомендовано научно-методической комиссией факультета информационных систем и технологий в качестве практикума.  **Корунова, Надежда Владимировна**   Практикум по дисциплине «Информационная безопасность»/ П. В. Мытарев. – Ульяновск : УлГТУ, 2016. – 32  с.  Практикум адресован студентам для выполнения и оформления лабораторных работ по дисциплине «Информационная безопасность». Рекомендации и требования к лабораторным работам разработаны в соответствии с рабочими программами дисциплин. Предназначены для студентов, обучающихся по направлению 09.03.03 Прикладная информатика, 09.03.04 «Программная инженерия».  Работа подготовлена на кафедре «Информационные системы». |

**УДК 004.9 : 338(076)**

**ББК 32.973.26 – 018.2я73**

© Мытарев П.В., 2016

© Оформление. УлГТУ, 2016

СОДЕРЖАНИЕ

[Лабораторная работа №1 4](#_Toc4163885)

[Лабораторная работа №2 9](#_Toc4163886)

[Лабораторная работа №3 10](#_Toc4163887)

## Лабораторная работа №1

Разработка программы разграничения полномочий пользователей на основе парольной аутентификации c использованием встроенных криптопровайдеров.

**Цель работы:** научиться использовать механизмы встроенных криптопровайдеров.

**Содержание задания**

1. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя.
2. В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):
3. смена пароля администратора (при правильном вводе старого пароля);
4. просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу;
5. добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины);
6. блокирование возможности работы пользователя с заданным именем;
7. включение или отключение ограничений на выбираемые пользователем пароли (в соответствии с индивидуальным заданием, определяемым номером варианта);
8. завершение работы с программой.
9. В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть заблокированы.
10. После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘\*’.
11. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.
12. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.
13. При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода.
14. Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого пароля, завершения работы с программой (при первом входе данного пользователя) или отказа от смены пароля.
15. Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой, а также включении или отключении ограничений на выбираемые пароли должна сохраняться в специальном файле. При первом запуске программы этот файл должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль.
16. Файл с учетными данными зарегистрированных пользователей должен быть защищен криптографическими средствами от несанкционированного доступа.
17. При запуске программы файл с учетными данными должен расшифровываться во временный файл (или в файл в оперативной памяти), который после завершения работы программы должен быть снова зашифрован для отражения возможных изменений в учетных записях пользователей. «Старое» содержимое файла учетных записей при этом стирается.
18. После ввода парольной фразы при запуске программы, генерации ключа расшифрования и расшифрования файла с учетными данными зарегистрированных пользователей правильность введенной парольной фразы определяется по наличию в расшифрованном файле учетной записи администратора программы.
19. При вводе неправильной парольной фразы или отказе от ее ввода работа программы должна завершаться с выдачей соответствующего сообщения.
20. Временный файл на диске с расшифрованными учетными данными после завершения работы программы удаляется.
21. Варианты использования алгоритмов шифрования и хеширования выбираются в соответствии с выданным преподавателем заданием.
22. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.
23. Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию.
24. Отчет по лабораторной работе должен содержать листинги программы с подробными комментариями, скрин-шоты экранов, описание структуры файла паролей, подробное описание функций, связанных с шифрованием, описание мест хранения зашифрованных данных, в т.ч. в момент их шифрования (расшифрования).

**Индивидуальные варианты заданий (ограничения на выбираемые пароли)**

1. Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя.
2. Наличие строчных и прописных букв.
3. Наличие букв и цифр.
4. Наличие букв и знаков препинания.
5. Наличие цифр и знаков препинания.
6. Наличие букв и знаков арифметических операций.
7. Наличие цифр и знаков арифметических операций.
8. Наличие латинских букв и символов кириллицы.
9. Наличие букв, цифр и знаков препинания.
10. Наличие латинских букв, символов кириллицы и цифр.
11. Наличие латинских букв, символов кириллицы и знаков препинания.
12. Наличие строчных и прописных букв, а также цифр.
13. Наличие строчных и прописных букв, а также знаков препинания.
14. Наличие строчных и прописных букв, а также знаков арифметических операций.
15. Наличие латинских букв, символов кириллицы и знаков арифметических операций.
16. Наличие букв, цифр и знаков арифметических операций.
17. Наличие букв, знаков препинания и знаков арифметических операций.
18. Наличие цифр, знаков препинания и знаков арифметических операций.
19. Отсутствие повторяющихся символов.
20. Чередование букв, цифр и снова букв.
21. Чередование букв, знаков препинания и снова букв.
22. Чередование цифр, букв и снова цифр.
23. Отсутствие подряд расположенных одинаковых символов.
24. Чередование цифр, знаков препинания и снова цифр.
25. Чередование цифр, знаков арифметических операций и снова цифр.
26. Несовпадение с именем пользователя.
27. Несовпадение с именем пользователя, записанным в обратном порядке.
28. Наличие строчных и прописных букв, цифр и знаков препинания.
29. Наличие строчных и прописных букв, цифр и знаков арифметических операций.
30. Несовпадение с датой в одном из форматов: дд/мм/гг, дд-мм-гг, дд.мм.гг.

Индивидуальные варианты заданий на использование криптографических методов

|  |  |  |  |
| --- | --- | --- | --- |
| № | Используемый режим шифрования алгоритма DES | Добавление к ключу случайного значения | Используемый алгоритм хеширования |
| **1** | 2 | 3 | 4 |
| **1** | ECB | Да | MD4 |
| **2** | CBC | Нет | MD5 |
| **3** | CFB | Да | SHA |
| **4** | OFB | Нет | MD4 |
| **5** | ECB | Да | MD5 |
| **6** | CBC | Нет | SHA |
| **7** | CFB | Да | MD4 |
| **8** | OFB | Нет | MD5 |
| **9** | ECB | Да | SHA |
| **10** | CBC | Нет | MD4 |
| **11** | CFB | Да | MD5 |
| **12** | OFB | Нет | SHA |
| **13** | ECB | Да | MD4 |
| **14** | CBC | Нет | MD5 |
| **15** | CFB | Да | SHA |
| **16** | OFB | Нет | MD4 |
| **17** | ECB | Да | MD5 |
| **18** | CBC | Нет | SHA |
| **19** | CFB | Да | MD4 |
| **20** | OFB | Нет | MD5 |
| **21** | ECB | Да | SHA |
| **22** | CBC | Нет | MD4 |
| **23** | CFB | Да | MD5 |
| **24** | OFB | Нет | SHA |

## Лабораторная работа №2

**Изучение криптографических алгоритмов**

**Цель работы:** изучить какой-либо конкретный криптографический алгоритм и реализовать его программными средствами.

Задание

1. Реализовать указанный преподавателем криптографический алгоритм.
2. Программа должна иметь интерфейс, в котором содержатся данные студента, вариант, справочная информация – алгоритм и его описание, возможности для сохранения и выбора обрабатываемого файла.
3. В случае шифрования пароль должен вводиться как с клавиатуры, так и из файла по выбору.
4. Отчет должен содержать вариант задания, блок-схему алгоритма, реализованного в программе, листинг программы с комментариями, расчет данных по одному циклу алгоритма.
5. Отчет и код программы с исполняемым кодом дополнительно представляются в электронном виде.
6. Обрабатываться должен файл любого формата, длиной не менее 1 кБ.
7. В случае шифрования в программе должна быть возможность выбора исходного файла и файла назначения как для шифрования, так и для расшифрования.
8. Для хэш-функций должны быть приведены результаты хэширования каких-либо значений, полученных в разрабатываемой программе, и результаты хэширования, рассчитанные на различных сайтах в сети «Интернет».
9. Ответить на вопросы преподавателя.

**Вопросы:**

1. Симметричные алгоритмы шифрования и их характеристики.
2. Асиметричные алгоритмы шифрования и их характеристики.
3. Реализация хэш-функций.
4. Реализация MAC.
5. Реализация ЭЦП.
6. Понятие слоя, раунда, S-box.
7. Как в ГОСТ 28147 осуществляется преобразование с помощью S-boxes. Что подается на вход и получается на выходе.

**Варианты:**

1. DES в режиме ECB (Electronic Codebook) электронный шифроблокнот.
2. DES в режиме CBC (Cipher Block Chaining) цепочка блоков.
3. DES в режиме CFB (Cipher Feedback) обратная связь по шифртексту.
4. DES в режиме OFB (Output Feedback) обратная связь по выходу.
5. Алгоритм ГОСТ 28147. Режим гаммирования.
6. Алгоритм ГОСТ 28147. Режим гаммирования с ОС.
7. Алгоритм ГОСТ 28147. Режим простой замены.
8. Алгоритм ГОСТ 28147. Имитовставка.
9. RSA.
10. Алгоритм Диффи-Хеллмана.
11. Хэш-функция MD5.
12. Хэш-функция SHA-1.

## Лабораторная работа №3

**Захват и анализ сетевого трафика**

**Цель работы:** ознакомление с программой «The Wireshark Network analyzer», которая представляет собой программный анализатор протоколов. Программа содержит следую­щие основные компоненты: фильтр захвата, буфер кадров, декодер протоко­лов, фильтр отображения захваченных кадров и модуль статистики с элемен­тами экспертной системы и обладает следующими возможностями:

* возможность захвата трафика в сетевых сегментах различных базовых технологий;
* возможность анализа большого числа протоколов;
* возможность экспорта и импорта файлов данных в формат распространен­ных анализаторов;
* мощная и удобная система поиска и фильтрации информации в буфере пакетов;
* наличие элементов экспертной системы;
* возможность сохранения на диск выделенного фрагмента пакета;
* наличие полезных утилит командной строки для осуществления захвата трафика и обработки сохраненных файлов.

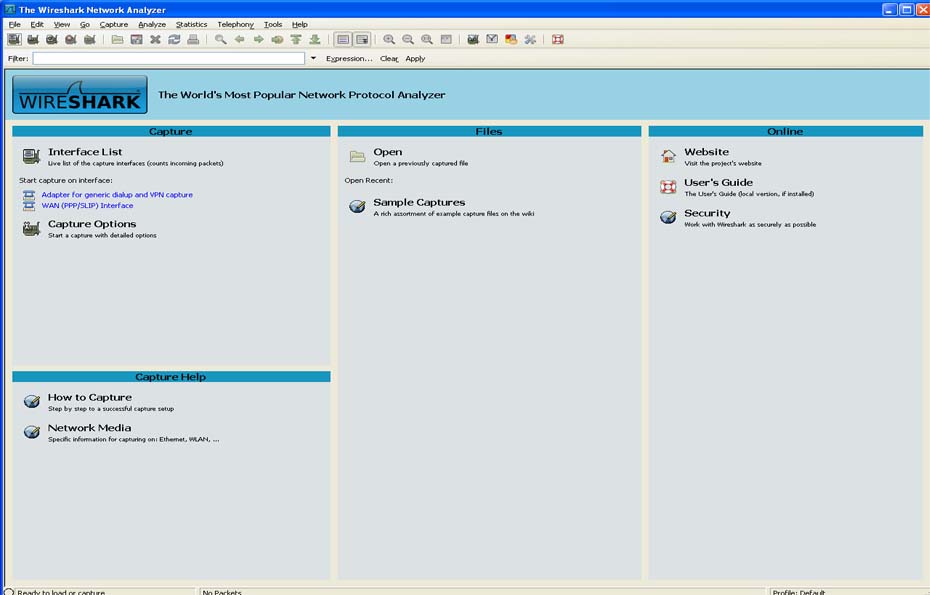


Рис.1 Основной экран программы.

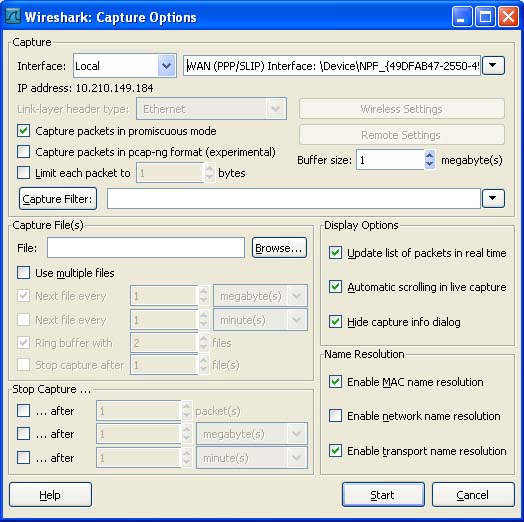


Рис. 2. Окно настроек параметров захвата.

После запуска программы Wireshark (Рис.1.) необходимо настроить некоторые параметры. Сначала необходимо открыть панель меню Capture => Options(Рис.2). На этой панели необходимо

установить следующие парамет­ры захвата кадров:

* Interface - сетевой адаптер;
* Buffer size - размер буфера захвата (по умолчанию 1 Мб);
* Capture packets in promiscuous mode - использование режима беспоря­дочного захвата, если флажок снят, то захватываться будут кадры, предназначенные для указанного сетевого интерфейса;
* Limit each packet to - запись только нескольких первых байт (определя­ется установленным значением параметра) каждого кадра;
* Capture Filter - фильтр захвата, предназначен для фильтрации кадров при записи, увеличивает нагрузку на процессор;
* Capture File(s) - файл захвата;
* Stop Capture - условия автоматического завершения захвата;
* Display Options - отображение пакетов в реальном времени и автомати­ческий скроллинг окна информации:
* Name Resolution - разрешение имен на физическом, сетевом и транс­портном уровнях.

Результат выполнения захвата кадра при выполнении команды «ping mail.ru» приведен на рис.3. На экране монитора в программе присутствует несколько панелей с отображением сетевых пакетов, записанных в буфер. Пользовательский интерфейс про­граммы содержит следующие компоненты:

* меню команд и панель инструментов:
* фильтр отображения пакетов:
* список пакетов в буфере;
* панель отображения декодера протоколов:
* панель отображения пакета в шестнадцатеричном коде и символах ASCII.

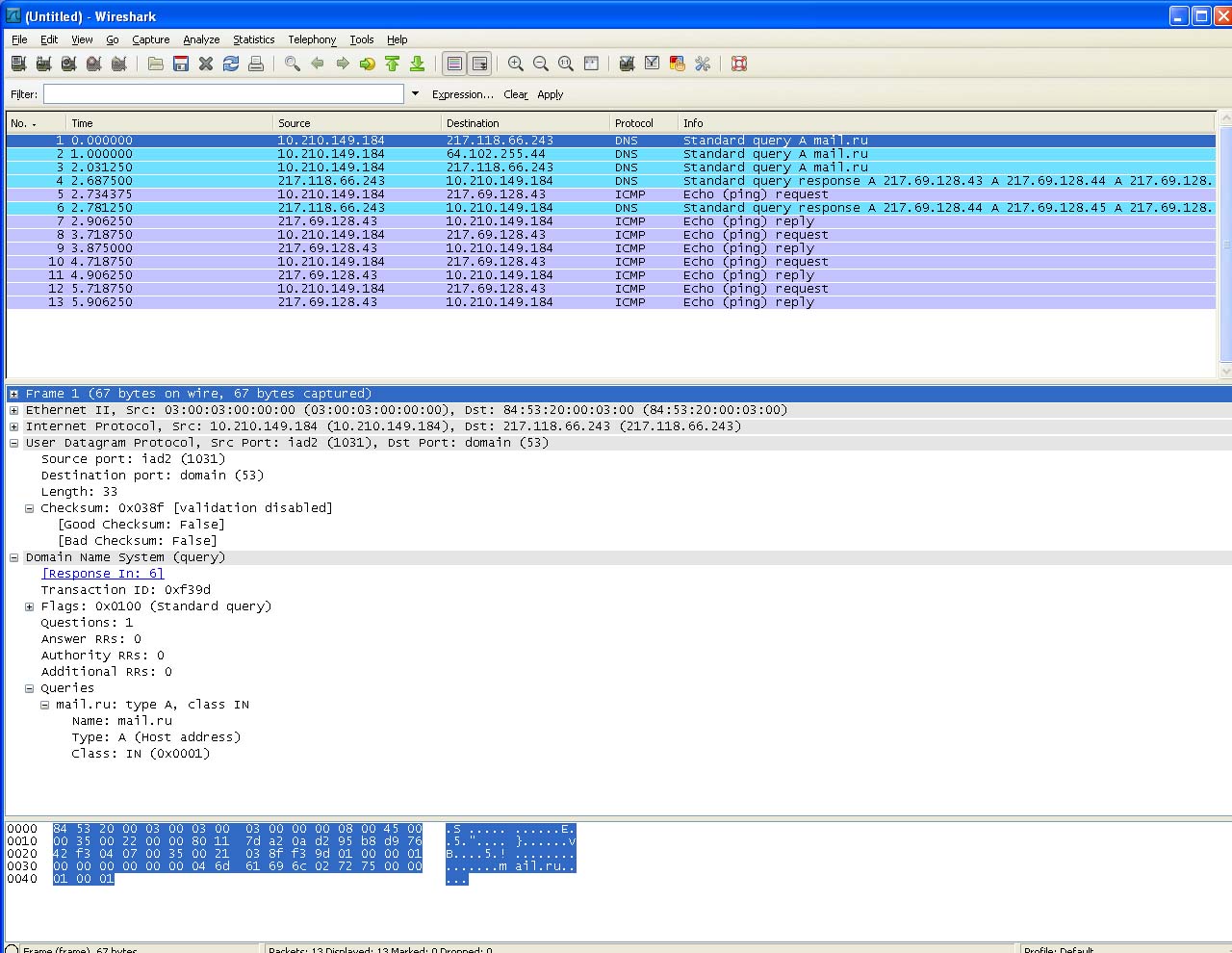


Рис.3. Результат захвата кадра при выполнении команды «ping mail.ru».

Панель со списком пакетов построчно отображает характеристики того или иного пакета (номер по порядку в буфере, время захвата, адреса источни­ка и получателя, тип протокола и общая информация о нем).

В поле Filter используется для фильтрации захваченных данных. Используемыми переменными являются поля заголовков протоколов. Можно создавать довольно сложные условия с использованием операторов “!=”, “==”, “<”, “>”, “>=”, “<=”, а также OR, AND, NOT(!). Например, условие TCP.Flags.SYN == 1 означает отбор всех кадров, в которых протокол TCP осуществляет запрос на установление соединения.

Поиск захваченных кадров можно осуществлять через меню Edit->Find Paket. Фильтр может содержать вышеописанные условия фильтрации, шестнадцатиричный код или данные типа «строка». Поиск может происходить в любой из трех областей – области пакетов, в области расшифровки протоколов пакета или непосредственно в пакете.

В настройках программы можно отключать показ выбранных протоколов с помощью пункта Analyze->Enabled Protocols.

**Задание**

1. Запустите программу «The Wireshark Network analyzer».
2. Выберите необходимый сетевой интерфейс.
3. Снимите флажок опции «Capture packets in promiscuous mode».
4. Чтобы начать процесс захвата нажми­те на кнопку «Start» (Рис.2) либо на соответствующий значок на панели управления.
5. В командной строке выполните команду ping на какой-либо хост.
6. После завершения команды ping остановите захват, нажав кнопку «Stop».
7. Проанализируйте результаты работы команды, содержимое экрана.
8. Загрузите в программу файл POP3.pcap. В этом файле находятся результаты связи по протоколу POP3 с почтовым сервером mail.ru для учетной записи test0073. Проанализируйте содержимое захваченных пакетов, определите пароль учетной записи. Найдите все пакеты, содержащие имя учетной записи. Отфильтруйте с помощью опции меню сеанс связи из общего потока. Отфильтруйте команду ping на сервер pop3.mail.ru.
9. Загрузите в программу файл SMTP.pcap. В этом файле находятся результаты связи по протоколу SMTP с почтовым сервером mail.ru для учетной записи test0073. Отфильтруйте с помощью опции меню сеанс связи из общего потока.
10. Включите захват кадров, среди захваченных кадров с помощью фильтра оставьте только ICMP-сообщения. Для этого можно в поле фильтр набрать ICMP и применить этот фильтр. Если после набора icmp набрать символ «.», то откроется окно с возможными вариантами дальнейшего выбора параметров второго уровня.
11. Дайте команду ping на какой-либо узел. Установите фильтр для выбора протокола ARP, в поле IP-адрес назначения которого присутствовал бы набранный IP-адрес.
12. Отберите кадры, содержащие в поле «Протокол» IP-протокола протокол ICMP, где адресом назначения является выбранный Вами адрес в команде ping.
13. Найдите все пакеты по строке «request» в области расшифровки протоколов.
14. Захватите кадры при копировании файла размером не менее 10кБ с ftp-сервера. Отключите протоколы, находящиеся выше протокола TCP, оставьте только протокол TCP. Проанализируйте, как изменились области, как фрагментировалась дейтаграмма, сколько TCP-сегментов получилось и какого размера.
15. Захватите кадры при копировании файла 111.txt с ftp-сервера из директории с заданием для данной лабораторной работы. Найдите в захваченных кадрах переданную структуру каталога, имя передаваемого файла, его содержимое.
16. Составьте условия отбора, чтобы определить количество TCP-соединений в захваченных кадрах.
17. Изучите пункт меню Analyze.
18. Откройте статистику сеансов TCP, выберите первый сеанс из меню Apply as Filter -> Selected -> A<->B.

РАЗРАБОТКА И УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ К ПРОЕКТУ:

практикум к выполнению   
лабораторных работ по дисциплине   
«Информационная безопасность»

Составитель МЫТАРЕВ Павел Владимирович

Усл. печ. л. 2

УлГТУ, 432027, г. Ульяновск, ул. Сев. Венец, д. 32.