Методы и средства защиты информации
Описание лабораторных работ

асс. К. Д. Вылегжанина
<k.vilegzhanina@gmail.com>

27 апреля 2015 г.

Содержание

1 Система верстки TEX и расширения LATEX

1.1 Цель работы

Изучение принципов верстки TEX, создание первого отчета

1.2 Ход работы

Изучение

1. Создание минимального файла .tex в простом текстовом редакторе – преамбула, тело документа
2. Компиляция в командной строке – latex, xdvi, pdflatex
3. Оболочка TexMaker, Быстрый старт, Быстрая сборка
4. Создание титульного листа, нескольких разделов, списка, несложной формулы
5. Понятие классов документов, подключаемых пакетов
6. Верстка более сложных формул

Выполнение практического задания Созданение отчетов по лабораторным работам

1.3 Выводы

Описание преимуществ и недостатков в подходе практикуемом при верстке для системы TEX
Один абзац, выражающий впечатления от работы с TEX

1.4 Материалы

1. Не очень краткое введение
2. Конспект-справочник
3. `http://www.inp.nsk.su/~baldin/LaTeX/lurs.pdf`
4. Математика в LATEX

1.5 Инструменты

1. TeX для Windows ProTeXt
2. TeXmaker

2 Система контроля версий Git

2.1 Цель работы

Изучить систему контроля версий Git, освоить основные приемы работы с ней.

2.2 Ход работы

1. Изучить справку для основных команд
2. Получить содержимое репозитория
3. Добавить новую папку и первого файла под контроль версий
4. Зафиксировать изменения в локальном репозитории
5. Внести изменения в файл и просмотреть различия
6. Отменить локальные изменения
7. Внести изменения в файл и просмотреть различия
8. Зафиксировать изменения в локальном репозитории, зафиксировать изменения в центральном репозитории
9. Получить изменения из центрального репозитория
10. Поэкспериментировать с ветками

2.3 Выводы

Описать свои впечатления от работы с распределенной системой контроля версий, описать преимущества такой системы.

2.4 Материалы

1. Документация по Git
2. Он-лайн курс быстрому началу работы с Git
3. Он-лайн курс по ветвлению в Git
4. "Pro Git" книга Scott Chacon доступная для чтения

2.5 Инструменты

Система контроля версий Git

3 Программа для шифрования и подписи GPG, пакет Gpg4win

3.1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

3.2 Ход работы

1. Изучить документацию, запустить графическую оболочку Kleopatra
2. Создать ключевую пару OpenPGP (File → New Certificate)
3. Экспортировать сетрификат (File → Export Certificate)
4. Поставить ЭЦП на файл (File → Sign/Encrypt Files)
5. Получить чужой сертификат из репозитория (например `https://github.com/vilegzhanina/InfoSecCourse2015/tree/master/%D0%9E%D1%82%D1%87%D0%B5%D1%82%D1%8B/01_LaTeX_Git_GPG`), файл с данными и файл с сигнатурой (подписью)
6. Импортировать сертификат, подписать его
7. Проверить подпись
8. Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой-либо текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись

9. Предыдущий пункт наоборот
10. Используя GNU Privacy handbook (ссылка в материалах) потренироваться в использовании gpg через интерфейс командной строки, без использования графических оболочек.

3.3 Выводы

3.4 Материалы

1. GnuPG.org
2. GNU Privacy handbook
3. Документация по Ggp4win

3.5 Инструменты

Gpg4win - пакет для Windows содержащий утилиту gpg и набор графических оболочек GPA и Kleopatra

4 Утилита для исследования сети и сканер портов Nmap

4.1 Цель работы

4.2 Ход работы

Определить набор и версии сервисов запущенных на компьютере в диапазоне адресов

1. Провести поиск активных хостов
2. Определить открытые порты
3. Определить версии сервисов
4. Изучить файлы `nmap-services`, `nmap-os-db`, `nmap-service-probes`
5. Добавить новую сигнатуру службы в файл `nmap-service-probes` (для этого создать минимальный tcp server, добиться, чтобы при сканировании nmap указывал для него название и версию)

6. Сохранить вывод утилиты в формате xml

7. Исследовать различные этапы и режимы работы nmap с использованием утилиты Wireshark

Просканировать виртуальную машину Metasploitable2 используя `db_nmap` из состава metasploit-framework

Выбрать пять записей из файла nmap-service-probes и описать их работу Выбрать один скрипт из состава Nmap и описать его работу

4.3 Выводы

4.4 Материалы

1. Документация по Nmap

2. Описание файла nmap-service-probes

3. Описание движка сценариев

4.5 Инструменты

1. Утилита для исследования сети и сканер портов Nmap

2. Дистрибутив Kali linux, в составе которого утилиты Nmap, Wireshark, а также metasploit-framework

5 Инструмент тестов на проникновение Metasploit

5.1 Цель работы

5.2 Ход работы

Изучение

1. Используя документацию изучить базовые понятия - `auxiliary`, `payload`, `exploit`, `shellcode`, `nop`, `encoder`

2. Запустить `msfconsole`, узнать список допустимых команд (`help`)

3. Базовые команды `search` (поиск по имени, типу, автору и др.), `info`, `load`, `use`

4. Команды по работе с эксплойтом

5. Команды по работе с БД
6. GUI оболочка Armitage
7. GUI веб-клиент

Практическое задание Описать последовательность действий для выполения следующих задач:

1. Подключиться к VNC-серверу, получить доступ к консоли
2. Получить список директорий в общем доступе по протоколу SMB
3. Получить консоль используя уязвимость в vsftpd
4. Получить консоль используя уязвимость в irc
5. Armitage Hail Mary

Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит

5.3 Выводы

5.4 Материалы

1. Metasploit Unleashed

5.5 Инструменты

1. Дистрибутив Kali linux, в составе которого утилиты Nmap, Wireshark, а также metasploit-framework

6 Набор инструментов для аудита беспроводных сетей AirCrack

6.1 Цель работы

Изучить основные возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK и WEP.

6.2 Ход работы

Изучение

1. Изучить документацию по основным утилитам пакета – `airmon-ng`, `airodump-ng`, `aireplay-ng`, `aircrack-ng`.
2. Запустить режим мониторинга на беспроводном интерфейсе
3. Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать

Практическое задание Проделать следующие действия по взлому WPA2 PSK сети (описание по ссылке "Руководство по взлому WPA"в материалах)

1. Запустить режим мониторинга на беспроводном интерфейсе
2. Запустить сбор трафика для получения аутентификационных сообщений
3. Если аутентификаций в сети не происходит в разумный промежуток времени, произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений
4. Произвести взлом используя словарь паролей

Опциональное задание Произвести взлом сети WEP (описание по ссылке "Руководство по взлому WEP"в материалах)

6.3 Выводы

6.4 Материалы

1. Обзор утилит AirCrack
2. Airmon-ng - включение режима мониторинга на беспроводных сетевых картах
3. Airodump-ng - захват пакетов из беспроводной сети
4. Aireplay-ng - генерация трафика
5. Aircrack-ng - утилита взлома WEP/WPA

6. Руководство по взлому WPA с использованием AirCrack
7. Руководство по взлому WEP с использованием AirCrack

6.5 Инструменты

1. Дистрибутив Kali linux, в составе которого набор инструментов AirCrack

7 Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs – SSL Server Test

7.1 Цель работы

7.2 Ход работы

Изучение

1. Изучить лучшие практики по развертыванию SSL/TLS
2. Изучить основные уязвимости и атаки на SSL последнего времени – POODLE, HeartBleed

Практическое задание Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst – изучить отчеты, интерпретировать результаты в разделе Summary

Выбрать для анализа интернет-домен защищенный SSL-шифрованием (старайтесь выбрать что-то достаточно известное, но не слишком очевидное), проделать следующие шаги:

1. Интерпретировать результаты в разделе Summary
2. Расшифровать все аббревиатуры шифров в разделе Configuration
3. Прокомментировать большинство позиций в разделе Protocol Details
4. Сделать итоговый вывод о реализации SSL на заданном домене

7.3 Выводы

7.4 Материалы

1. Описание лучших практик по развертыванию SSL/TLS
2. HeartBleed
3. Атака POODLE на TLS
4. Атака POODLE на SSL3

7.5 Инструменты

1. Qualys SSL Labs – SSL Server Test

8 Проект OWASP WebGoat

8.1 Цель работы

8.2 Ход работы

Изучение

1. Изучить описания десяти самых распространенных веб-уязвимости согласно рейтингу OWASP

Практическое задание Запустить уязвимое приложение WebGoat. Запустить сканер безопасности ZAP. Запустить инструмент Mantra, настроить его для использования ZAP в качестве прокси-сервера

1. Недостатки контроля доступа
2. Безопасность AJAX
3. Недостатки аутентификации
4. Переполнение буфера
5. Качество кода
6. Многопоточность
7. Межсайтовое выполнение сценариев

8. Неправильная обработка ошибок
9. Недостатки приводящие к осуществлению инъекций (SQL и прочее)
10. Отказ в обслуживании
11. Небезопасное сетевое взаимодействие
12. Небезопасная конфигурация
13. Небезопасное хранилище
14. Исполнение злонамеренного кода
15. Подделка параметров
16. Недостатки управление сессией
17. Безопасность веб-сервисов

8.3 Выводы

8.4 Материалы

1. OWASP WebGoat Project
2. OWASP Top Ten Project

8.5 Инструменты

1. Уязвимое приложение WebGoat
2. OWASP Mantra – набор инструментов для аудита веб-приложения на основе браузера
3. OWASP ZAP – сканер безопасности веб-приложений
4. Telerik Fiddler – отладочный прокси