ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»

Д. М. Созиев

Информационная безопасность и непрерывность бизнеса

Учебно-методическое пособие по проведению лабораторных и практических работ

СПб ГУТ)))

Санкт-Петербург
2016

УДК 004.77
ББК 20
Б 20

Рецензент
кандидат экономических наук,
доцент кафедры информационных технологий в экономике
(СПбГУТ) *М. Б. Вольфсон*

Рекомендовано к печати редакционно-издательским советом СПбГУТ

Созиев Д. М.

Б 20 Информационная безопасность и непрерывность бизнеса : учебно-методическое пособие по проведению лабораторных и практических работ / Д. М. Созиев ; СПбГУТ. – СПб., 2016 – 32 с.

Написано в соответствии с программой дисциплины «Методы обеспечения непрерывности бизнеса». Целью издания является знакомство студентов с основными угрозами информационной безопасности и непрерывности бизнеса.

Предназначено для подготовки бакалавров по направлениям «Менеджмент» (080200) и «Бизнес-информатика» (080500).

УДК 004.77
ББК 20

ВВЕДЕНИЕ

Учебно-методическое пособие разработано для студентов, проходящих обучение по программам подготовки бакалавров по направлениям «Менеджмент» (080200) и «Бизнес-информатика» (080500) в соответствии с учебной программой по курсу дисциплины «Методы обеспечения непрерывности бизнеса».. Учебный материал предназначен для знакомства с основными мугрозами информационной безопасности и основными методами защиты против них , а также для получения практики выполнения базовых операций в по защите информационной среды предприятия. Пособие содержит методические указания по выполнению трех лабораторно-практических работ в компьютерных классах и полностью учитывает особенности учебно-лабораторной и программно-аппаратной базы факультета экономики и управления СПбГУТ.

По результатам выполнения приведённых в пособии заданий каждый студент составляет индивидуальный отчёт в формате MS Office, содержащий:

- Титульный лист с указанием названия работы, номера группы, фамилии, имени и отчества автора.
- Результаты в виде таблиц, расчётов, скриншотов или приложений.
- Выводы
- Список использованной литературы

Файлы отчёта и приложений с результатами выполнения задания посылаются с электронным письмом по адресу: soziev@fem-sut.spb.ru. В теме письма обязательно надо указать группу, фамилию автора и номер задания. Например: ЭМ21 Иванов К.И. 1.

1. Сбор информации из открытых источников.

Цель работы.

Целью работы является сбор информации при помощи поисковых систем, социальных сетей и специальных сайтов.

Общие сведения

Для сбора информации в пассивном режиме злоумышленник может использозовать интернет для сбора информации. .

Все последующие задания выполняются при помощи стандартных програм операционной системы Windows. Овладение возможностями этой системы представляется не только необходимым для успешного прохождения курса, но и полезным для решения повседневных задач, а может быть, и в будущей трудовой деятельности.

Задание

1. Использование сервиса Whois, DNS
   1.1. Найдите информацию о регистрации доменов rt.ru; sut.ru; fem-sut.spb.ru, yandex.ru, google.com.
   1.2. Найдите IP адреса сайтов www указанных в предыдущем задании. Определите кому принадлежат эти адреса.
   1.3. Найдите информацию о почтовых серверах: sut.ru; fem-sut.spb.ru; yandex.ru, gmail.com.
   1.4. Попытайтесь найти все сайты в зоне домена sut.ru или fem-sut.spb.ru
2. Использование Архива Archive.org.
   2.1. Найди те каким образом выглядели сайты www.sut.ru; www.fem-sut.spb.ru и www.lenta.ru 1 месяц назд.
   2.2. То же самое 2 года назад
   2.3. То же самое 5 года назад
3. Использование файла Robots.txt
   3.1. Определите что не индексируется поисковиками для сайтов www.fem-sut.spb.ru, www.sut.ru
   3.2. То же самое для сайтов мобильных операторов megafon.ru , beeline.ru, mts.ru
   3.3. То же самое для сайтов соц. сетей facebook.com, vk.com, twitter.com, linkedin.com, hh.com.
4. Поиск информации о сотрудниках компании
   4.1. Найдите при помощи соц сетей информацию о сотрудниках компании Yandex, Microsoft, Мегафон, МТС.

4.2. Найдите резюме при помощи сайтов superjob.ru, linkedin.com. При необходимости заведите себе аккаунт электронной почты и зарегистрируйтесь, не используйте свой аккаунт электронной почты.
4.3. Составте досье на компанию, в котором должна быть указана информация о сайте, электронной почте сотрудников,
4.4. Отправьте приветсвенное письмо с пжеланием хорошего рабочего дня сотруднику компании, электронную почту которого вы обнаружите, напрямую используя SMTP сервер компании.

5. Сбор информации о человеке.
   5.1. Постарайтесь составить досье на человека используя поисковые системы, сайты соц сетей , twitter и т.п. Досье должно описывать человека, род его занятий увлечения, географическое положение.

6. Поиск при помощи google.com
   6.1. Поиск при помощи директивы allinurl:, постарайтесь найти файлы которые могут содержать пароли или информацию об аккакунтах.
   6.2. Поиск при помощи директивы site: проделайте тот же самый поиск для конкретного сайта или домена.
   6.3. Поиск “Index of /admin”, “Index of /cgi-bin”, “Index of users”
   6.4. Поиск при помощи директивы filetype:
7. Использование online-tools http://www.dirk-loss.de/onlinetools.htm
   7.1. Используйте онлайн утилиты для выплнения запросов DNS, PING
   7.2. Попробуйте использовать доступные утилиты, исследуйте информацию полученную при их помощи.

Рекомендации

К заданию 1:
http://www.ripn.net/nic/whois/index.html
http://ru.wikipedia.org/wiki/WHOIS
Nic.ru
Утилита nslookup
http://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%B8%D1%81%D1%8C_MX
К заданию 2:
Archive.org
К заданию 3:
http://ru.wikipedia.org/wiki/Robots.txt
К заданию 4:
Vk.com
Facebook.com

К заданию 5:
Goofle.com, Yandex.ru, Bing.com
Linkedin.com, superjob.com
Twitter.com

2. Сбор информации с использованием специальных инструментов

Цель работы.

Целью работы является получение опыта сбора информацию о уязвимостях приложений при помощи специальных инструментов.

Общие сведения

Поскольку обнаружение уязвимостей является важным этапом подготовки изащиты от атак студет должен уметь использовать инструменты для определения уязвимостей. Настоящее задание знакомит с основными такими инструментами.

Задание

1. Использование сервиса Shodan : http://shodanhq.com
   1.1. Найдите сервеера которые используют веб сервер IIS.
   1.2. Найдите сервера которые используют CMS Joomla, на территории России.
   1.3. Найдите сервеа которые используют IOS Cisco.
   1.4. Найдите сервера использующие ос ESX
   1.5. Сервера на оборудовании D-Link
2. Использование инструмента DNSWALK в составе BackTrack 5.
   2.1. С помощью интрумента просканируйте зону fem-sut.spb.ru
   2.2. С помощью интрумента просканируйте зону fem-sut.spb.ru
   2.3. С помощью интрумента просканируйте зону yandex.ru
3. Сканирование локальной сети при помощи инструмента Autoscan в составе BackTrack 5.
   3.1. Просканируйте локальную сеть и идетифицируйте все хосты в ней.
   3.2. Использование Zenmap
   3.3. Просканируйте несколько хостов в локальной сети
   3.4. Просканируйте несколько хостов найденых при помощи shodan
4. Использование Nessus (Login:root, password: toor: https://backtrack5ip:8834)
   4.1. Просканируйте собственную мащшину на уязвимости
   4.2. Просканируйте хосты локальной сети на уязвимости
   4.3. Просканируйте сайт www.fem-sut.spb.ru на наличие уязвимостей.
   4.4. Просканируйте сайт www.sut.ru на уязвимости
5. Использование Open-VAS
   5.1. Проделай те те же самые действия что и в предыдущем пункте.
6. Использование Grendel Scan для сканирования уязвимостей вебсайтов.
   6.1. Просканируйте fem-sut.spb.ru

6.2. Просканируйте сайты найденые рании при использовании Shodan.

Рекомендации

К заданию 1:
http://www.shodanhq.com/help/faq
Пример использования http://www.xakep.ru/post/55017/default.asp
К заданию 2:
http://www.youtube.com/watch?v=i-KMGQvDOUcК заданию 3:
К заданию 3:
http://www.backtrack-linux.org/wiki/index.php/Autoscan
К заданию 4:
http://ru.wikipedia.org/wiki/Zenmap
http://ru.wikipedia.org/wiki/nmap
http://compiling.ru/security/nmap/
К заданию 5
http://ru.wikipedia.org/wiki/Nessus
К заданию 6
http://www.backtrack-linux.org/wiki/index.php/OpenVas#Installing_OpenVAS
http://www.openvas.org/
К заданию 7
http://securitytube-tools.net/index.php?title=Grendel_Scan
http://en.wikipedia.org/wiki/Nikto_Web_Scanner
http://www.securitylab.ru/software/233415.php

3. Использование инструментов снифинга и перехвата

Цель работы.

Целью работы является получение навыков перехвата и анализа трафика.

Общие сведения

Безопасность при передаче трафика является одним из важнейших условий защищенной и непрерыной работы ИТ инфраструткуры. Задание знакомит студента с возможностями по перехвату трафика и средствами защиты от такого воздействия.

Задание

1. Использование Wireshark . При помощи Wireshark перехватите трафик который исходит из ващего хоста на другие компьютеры.
    a. Протокол Http: откройте браузер и отправьте поисковый запрос.
    b. Протокол Http: откройте сайт социальной сети и напишите несколько сообщений.
    c. Протокол Http: откройте сайт социальной сети и загрузите файл формата word или txt.
    d. Протокол smtp отправьте пиьмо пользователю при помощи протокола telnet.
    e. Протокол DNS отправьте запрос на разрешение адроеса сайта fem-sut.spb.ru.
2. Использование Wireshark.
    a. Найдите MAC адреса соседних компьютеров
    b. Найдите MAC адрес маршрутизатора.
3. Использованиес
    a. При помощи утилиты перехватите трафик соседнего компьютера из задания 1.
4. Использование Cain and Abel
    a. Перехватите трафик при вводе пароля на сайт соц сети
    b. Перехватите траффик при вводе пароля в систему электронной почты.

Рекомендации

1. К заданию 1:

a. http://www.wireshark.com

2. К заданию 2:
    a. http://ru.wikipedia.org/wiki/ARP:
3. К заданию 3:
    a. http://en.wikipedia.org/wiki/Ettercap_(computing)
4. К заданию 4:

СОДЕРЖАНИЕ