МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** «Инженерно-экономический институт»

(название факультета/института)

**Кафедра** «Безопасности и информационных технологий»

(название кафедры)

**Лабораторная работа № 1**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Исследование сервисов уязвимой виртуальной машины с применением CVE

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

**Исследование сервисов уязвимой виртуальной машины с применением CVE**

**Цель**: ознакомление с базами данных уязвимостей

**Задачи**:

1. Понять, как работают сканеры уязвимостей, на упрощенной модели

2. Ознакомиться с базой данных CVE

3. Ознакомиться с базой данных Exploit DB для оценки текущего состояния защищенности компьютерной системы

**Этапы выполнения** лабораторной работы:

**I. Подготовка к выполнению лабораторной работы**

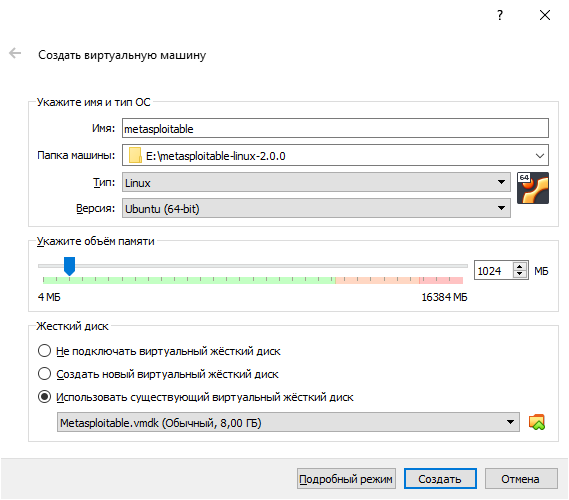
1. Скачать исследуемый дистрибутив Metasploitable

<https://sourceforge.net/projects/metasploitable/>

2. Распаковать архив

3. Запустить Oracle VirtualBox

4. Выбрать Машина – Создать



6. Запустить виртуальную машину

**II. Изучение базовых команд управления**

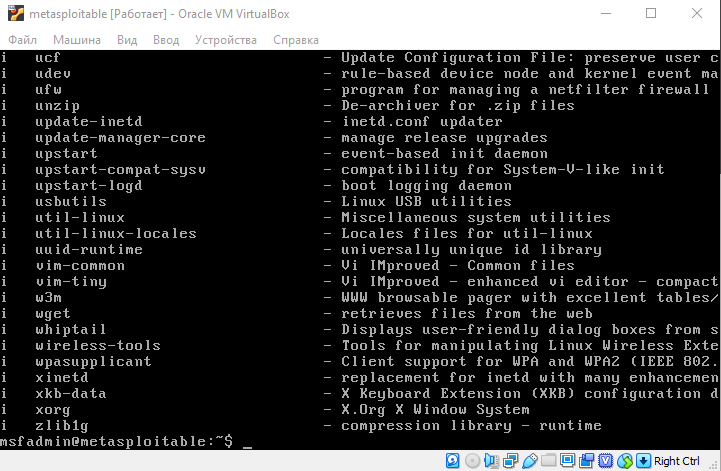
1. Ввести логин и пароль msfadmin/msfadmin

2. Ознакомиться с

<https://www.debian.org/doc/manuals/aptitude/ch02s04s05.en.html>

3. Выполнить команду

aptitude search '~i!~M'



4. Выполнить команду

aptitude search '~i!~M' > description.txt

5. Убедиться в успехе командой

cat description.txt

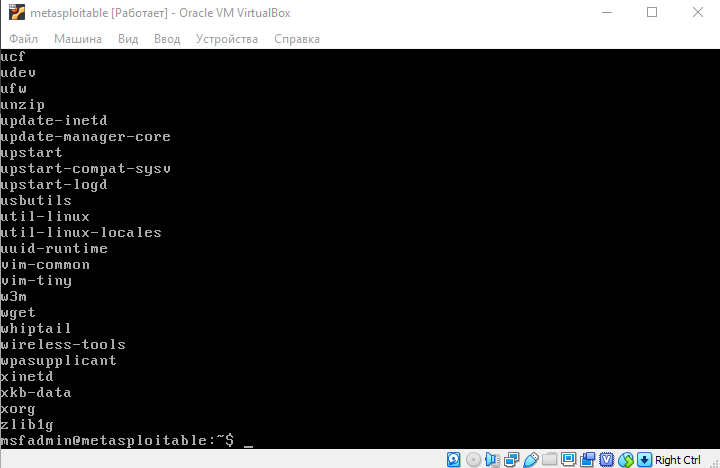
**III. Формирование отчетного документа**

1. Ознакомиться с

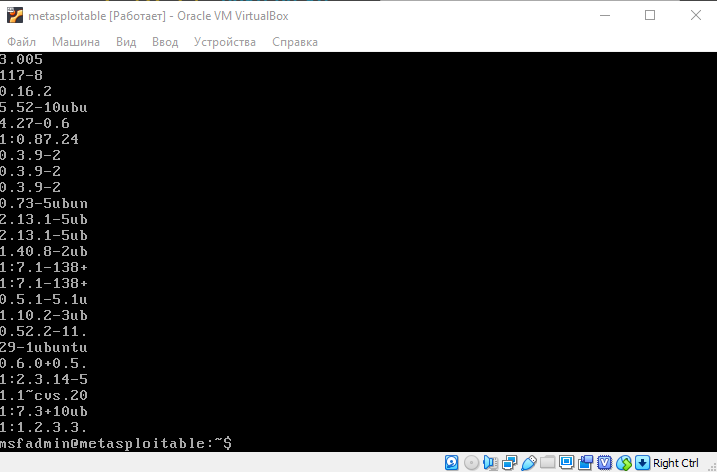
<https://www.debian.org/doc/manuals/aptitude/ch02s05s01.en.html>

2. Выполнить команды

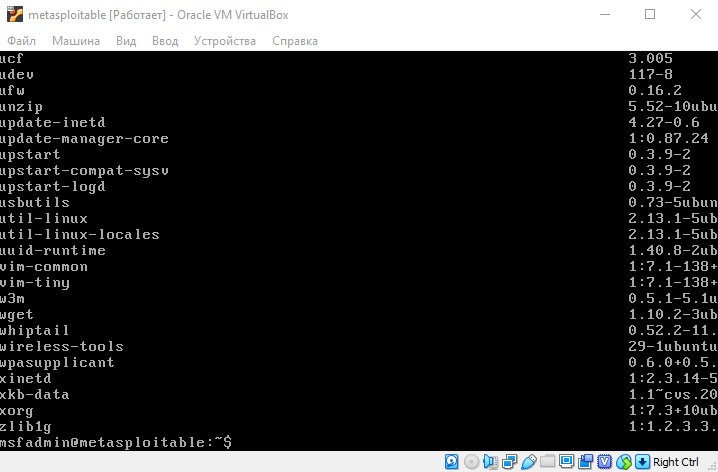
aptitude search '~i!~M' -F '%p'



aptitude search '~i!~M' -F '%v'



aptitude search '~i!~M' -F '%p %v'



3. Понять различия между ними

4. Сохранить результаты в файлы

aptitude search '~i!~M' -F '%p' > packages.txt

aptitude search '~i!~M' -F '%v' > versions.txt

aptitude search '~i!~M' -F '%p %v' > all.txt

5. Убедиться в успешности

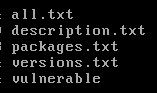
cat packages.txt

cat versions.txt

cat all.txt

6. Убедиться в наличии всех файлов

ls –l



**IV. Загрузка отчетного файла из виртуальной машины**

1. Создать папку и переместить туда файлы

mkdir data

mv all.txt data

mv description.txt data

mv packages.txt data

mv versions.txt data

cd data

ls –l

cd ..

2. Создать архив с файлами

tar –zcvf data.tar.gz data

ls -l

3. Загрузить файлы для дальнейшего анализа

curl -F "file=@data.tar.gz" <http://file.io>



4. Скачать собранные данные по ссылке, указанной в поле link

5. Распаковать скачанный архив

6. Выключить виртуальную машину

sudo shutdown –h now

Пароль - msfadmin

**V. Выполнение анализа полученных результатов**

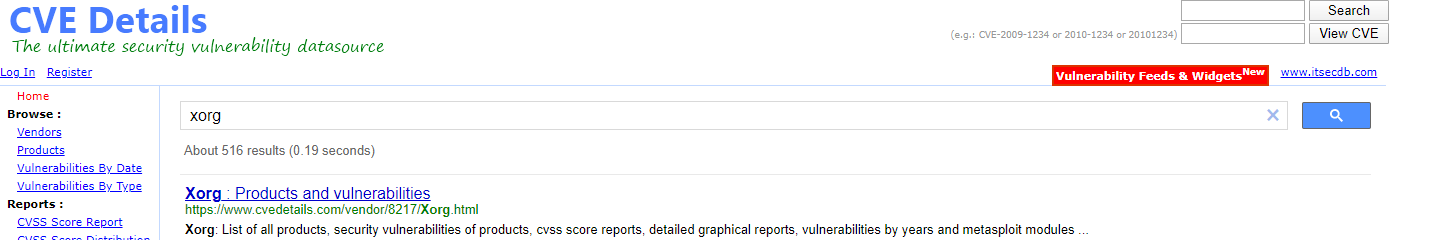
Для дальнейшего рассмотрения предлагаются следующие пакеты

* apache2
* bash
* curl
* firefox-3.0
* mysql-server
* postgresql-8.3
* python2.5
* samba
* tomcat5.5
* wget

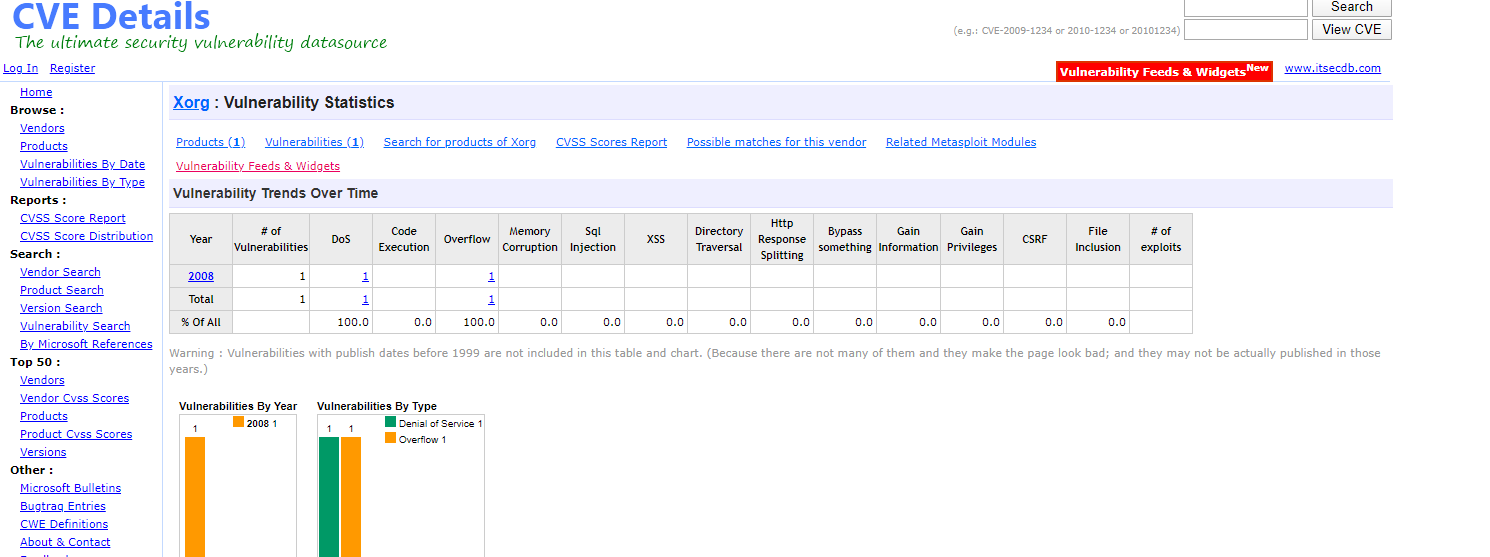
1. Открыть <https://www.cvedetails.com/>

2. Через поиск можно найти информацию о каждом приложении

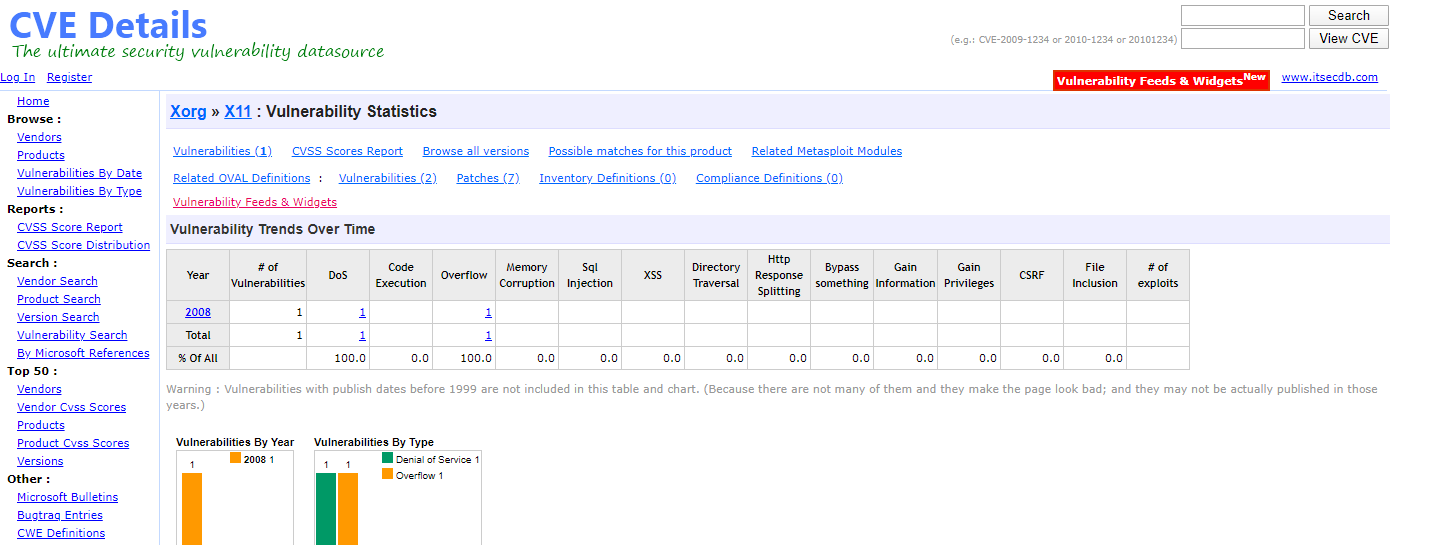
Например, xorg:



При переходе по ссылке открывается страница вендора:



Необходимо выбрать Products и открыть нужный



В Browse all versions можно выбрать необходимую версию



По ссылке Vulnerablities находится список уязвимостей с идентификаторами, которым подвержено данное приложение данной версии

Отчёт предлагается оформлять в виде таблицы

|  |  |  |  |
| --- | --- | --- | --- |
| Имя пакета | Версия | CVE | CVSS Score |
|  |  |  |  |

1. Открыть <https://www.exploit-db.com/search>

2. Используя поле CVE, определить наличие эксплойтов для каждой уязвимости

3. Оформить результаты в виде

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя пакета | Версия | CVE | CVSS Score | Наличие эксплойта |
|  |  |  |  |  |

**Отчёт по результатам выполнения лабораторной работы**

**Титульный лист:**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** Инженерно-экономический институт

(название факультета/института)

**Кафедра** Безопасности и информационных технологий»

(название кафедры)

**Отчет по лабораторной работе № 1**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Исследование сервисов уязвимой виртуальной машины с применением CVE

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

Москва, 201\_г.

**Результаты выполнения лабораторной работы**

1. **Перечень изученных команд**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование команды** | **Назначение команды** |
|  | aptitude search '~i!~M' |  |
|  |  |  |
|  |  |  |
| … |  |  |

1. **Результаты оценки уязвимостей виртуальной машины**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Имя пакета** | **Версия** | **CVE** | **CVSS Score** | **Наличие эксплойта** |
|  |  |  |  |  |

1. **Результат попытки автоматизации процесса поиска уязвимостей**

Для автоматизации работы с браузером используется <https://selenium.dev/>

1. **Вывод и краткие рекомендации по повышению уровня защищенности на основе полученных результатов**