**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 | | | 3 | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-20 | | | | | | | |
| ФИО: | Ахтямов В.И. | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2022г. | |
| Оценка: |  | | | | | | | |

Москва, 2022г.

**Этапы выполнения** лабораторной работы:

**I. Подготовка к выполнению лабораторной работы**

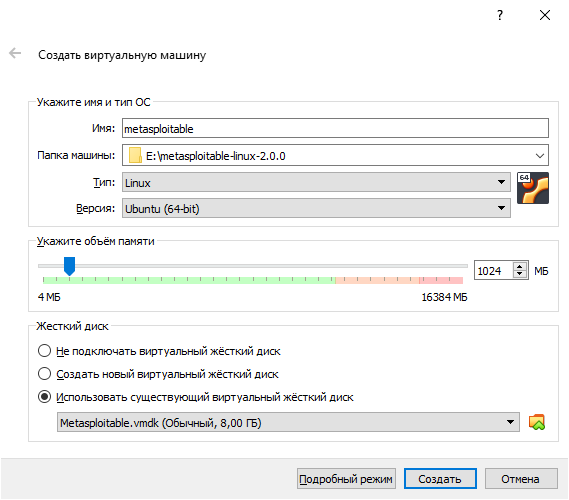
1. Скачать исследуемый дистрибутив Metasploitable

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

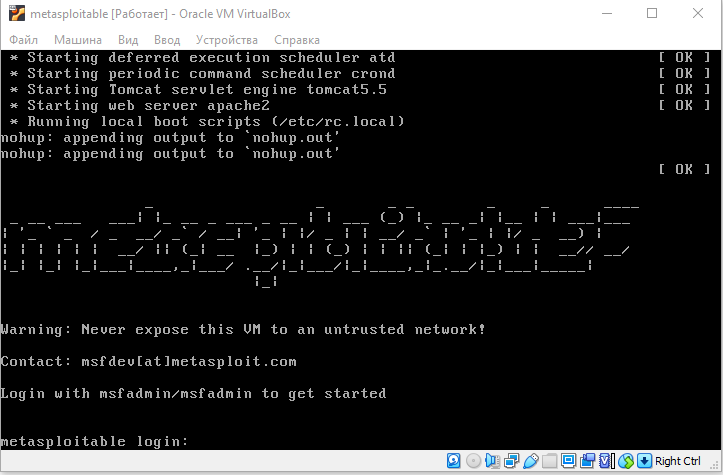
2. Распаковать архив

3. Запустить Oracle VirtualBox

4. Выбрать Машина – Создать

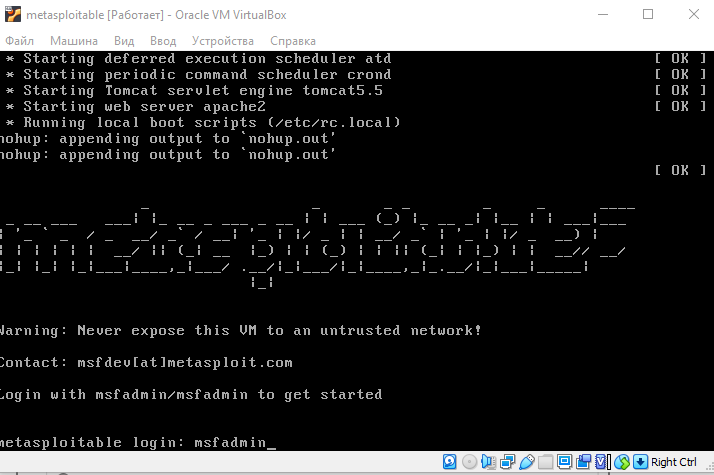


6. Запустить виртуальную машину



**Изучение базовых команд управления**

1. Ввести логин и пароль msfadmin/msfadmin



2. Ознакомиться с

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

Благодаря этому сайту удалось ознакомились с утилитой поиска aptituide и его возможности по работе с пакетами

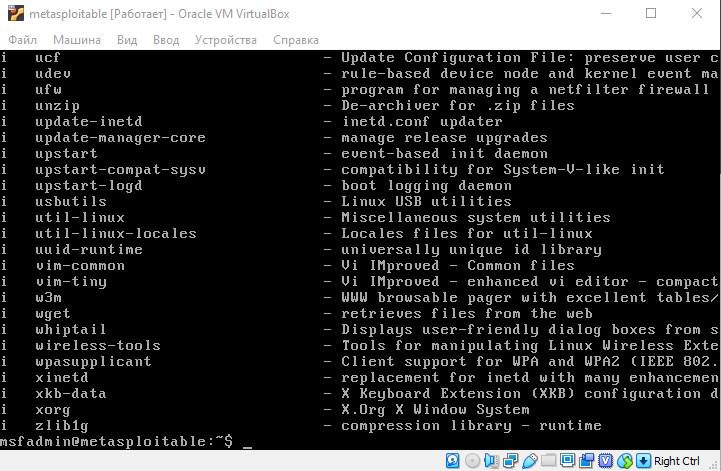
3. Выполнить команду

aptitude search '~i!~M'

Данная команда осуществляет поиск и выводит список пакетов

Флаг M - выводит пакеты, которые были установлены автоматически.

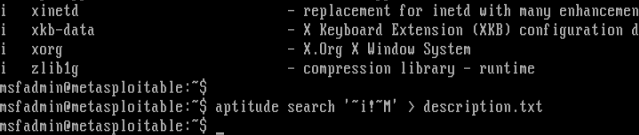
Флаг I - выводит установленные пакеты.



4. Выполнить команду

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

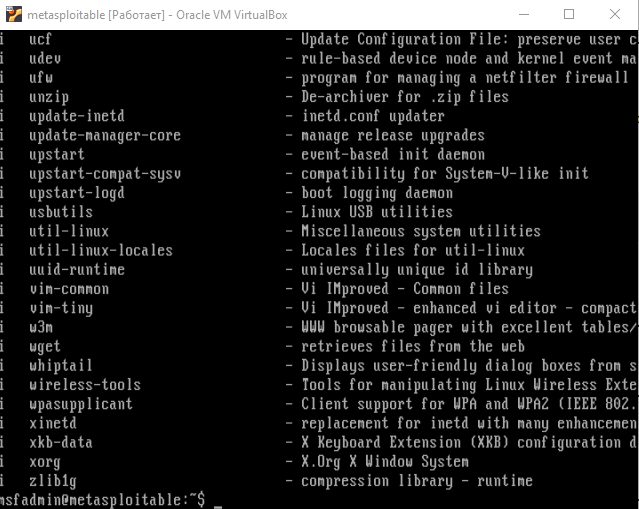
В результате этой команды мы сохранили листинг пакетов в текстовый файл



5. Убедиться в успехе командой

cat description.txt

Команда cat выводит содержимое файла в терминал



**III. Формирование отчетного документа**

1. Ознакомиться с

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

В этом разделе описывается, как настроить содержимое и формат списка пакетов, строки состояния и строки заголовка, а также вывод файла [aptitude search](https://www.debian.org/doc/manuals/aptitude/rn01re01.en.html" \l "cmdlineSearch).

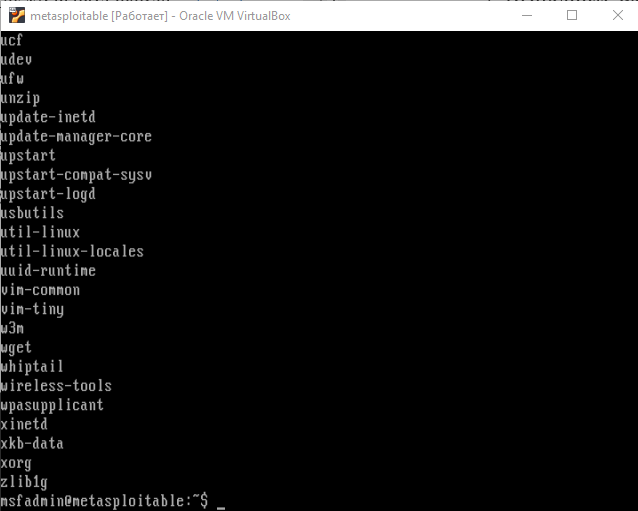
Формат каждого из этих местоположений определяется « строкой формата » . Строка формата — это строка текста, содержащая %-escape-символы, такие как %p, %S, и т. д. Результирующий вывод создается путем взятия текста и замены символов %-escape в соответствии с их значениями

Данный ресурс используется для удобного вывода информации о пакетах

2. Выполнить команды

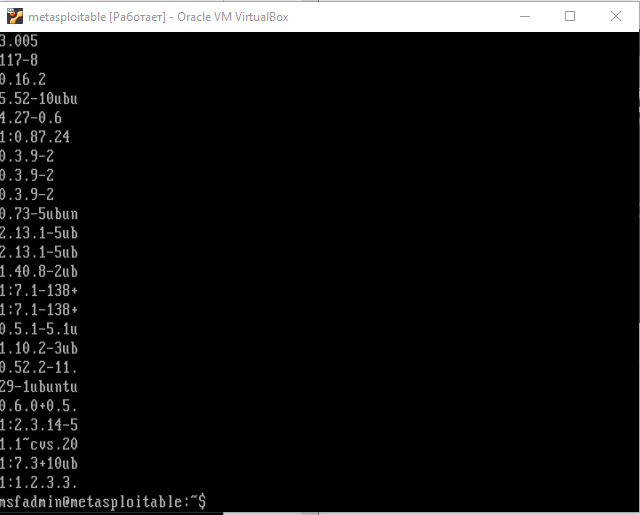
aptitude search '~i!~M' -F '%p'

%p - Выводит имя пакета. Когда пакет отображается в контексте дерева, имя пакета будет иметь отступ, если это возможно, в соответствии с его глубиной в дереве.

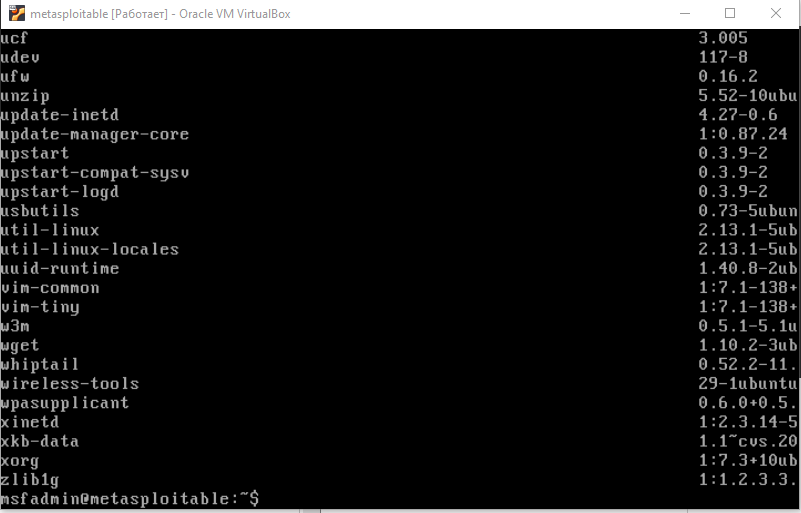


aptitude search '~i!~M' -F '%v'

%v - Выводит текущую установленную версию пакета или <none>если пакет в данный момент не установлен.



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



3. Понять различия между ними

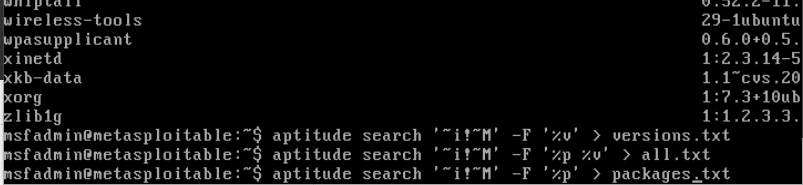
Различие между ними заключается в виде выводимой информации – название пакета или утилиты, название-номер версии, и название вместе с номером версии.

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

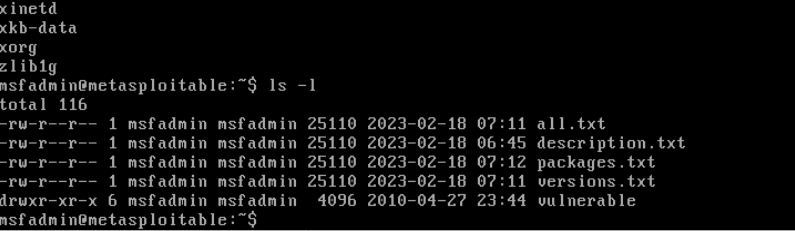
cat packages.txt

cat versions.txt

cat all.txt

6. Убедиться в наличии всех файлов

ls –l



m

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

1. Создать папку и переместить туда файлы

mkdir data

Данная команда создает директорию

mv all.txt data

Данная команда перемещает файл в директорию

mv description.txt data

mv packages.txt data

mv versions.txt data

cd data

Данная команда позволяет перейти в директорию

ls –l

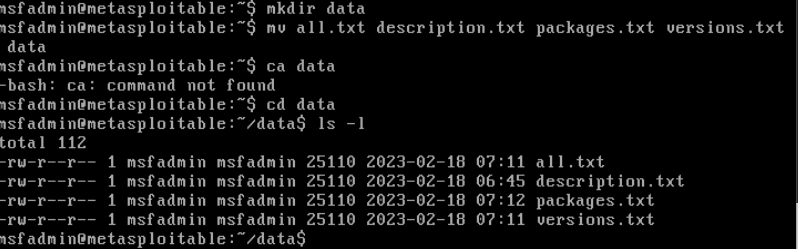
cd ..

Данная команда позволяет перейти на одну дтректорию выше

2. Создать архив с файлами

tar –zcvf data.tar.gz data

ls –l

tar

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

1. **Перечень изученных команд**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование команды** | **Назначение команды** |
|  | aptitude search '~i!~M' | Данная команда осуществляет поиск и выводит список пакетов  Флаг M - выводит пакеты, которые были установлены автоматически.  Флаг I - выводит установленные пакеты. |
|  | ptitude search '~i!~M' > description.txt | В результате этой команды мы сохранили листинг пакетов в текстовый файл |
|  | cat description.txt | Команда cat выводит содержимое файла в терминал |
| 4 | aptitude search '~i!~M' -F '%p' | %p - Выводит имя пакета. Когда пакет отображается в контексте дерева, имя пакета будет иметь отступ, если это возможно, в соответствии с его глубиной в дереве |
| 5 | aptitude search '~i!~M' -F '%v' | %v - Выводит текущую установленную версию пакета или <none>если пакет в данный момент не установлен. |
| 6 | aptitude search '~i!~M' -F '%p %v' | Выводит текущую установленную версию пакета и название пакета |
| 7 | mkdir data | Данная команда создает директорию |
| 8 | mv description.txt data  cd data | Данная команда перемещает файл в директорию  Данная команда позволяет перейти в директорию |
| 9 | cd .. | Данная команда позволяет перейти на одну дтректорию выше |
| 10 | tar –zcvf data.tar.gz data | Создать архив с файлами |

**V. Выполнение анализа полученных результатов**

|  |  |  |  |
| --- | --- | --- | --- |
| Имя пакета | Версия | CVE | CVSS Score |
| Apache2 | 2.2.8-1 | CVE-2016-4975 | 4.3 |
|  |  | CVE-2014-0231 | 5.0 |
|  |  | CVE-2013-5704 | 5.0 |
|  |  | CVE-2012-4558 | 4.3 |
|  |  | CVE-2012-3499 | 4.3 |
| bash | 5.0 | CVE-2019-18276 | 7.2 |
|  | 4.4 | CVE-2019-9924 | 7.2 |
|  | 4,4 | CVE-2017-5932 | 4.6 |
| Curl | 7.24.0 | CVE-2012-0036 | 7.5 |
|  | 7.20.0 | CVE-2010-3842 | 5.8 |
|  | 7.19.7 | CVE-2010-0734 | 6.8 |
| Firefox-3.0 | 3.0.5 | CVE-2009-0071 | 7.2 |
|  | 3.0.8 | CVE-2009-1232 | 5.8 |
|  | 3.0.1 | CVE-2008-4582 | 6.4 |
| mysql-server | 7.83.1 | CVE-2022-27778 | 5.8 |
|  | 17.3.1 | CVE-2022-21824 | 6.4 |
| postgresql-8.3 | 7.3 | CVE-2021-21704 | 4.3 |
|  | 7.2 | CVE-2020-7066 | 4.3 |
|  | 7.2 | CVE-2020-7062 | 4.3 |
| python2.5 | 2.5.2 | CVE-2008-1887 | 7.2 |
|  | 2.5 | CVE-2008-1721 | 5.4 |
|  | 2.5 | CVE-2008-2316 | 4.3 |
| samba | 6.14 | CVE-2022-29869 | 4.3 |
|  | 6.14 | CVE-2022-27239 | 7.2 |
|  | 4.15 | CVE-2021-44142 | 9.0 |
| tomcat5.5 | 5.5 | CVE-2008-0128 | 3,4 |
|  | 5.5 | CVE-2007-5461 | 4.3 |
|  | 5.5 | CVE-2007-3386 | 6.8 |
| wget | 1.12.1 | CVE-2021-31879 | 5.8 |
|  | 1.20.1 | CVE-2019-5953 | 7.5 |
|  | 1.20.1 | CVE-2018-20483 | 2.1 |
|  | 1.19.2 | CVE-2017-13090 | 9.3 |

**Результаты оценки уязвимостей виртуальной машины**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя пакета | Версия | CVE | CVSS Score | Наличие эксплойта |
| Apache2 | 2.2.8-1 | CVE-2016-4975 | 4.3 | - |
|  |  | CVE-2014-0231 | 5.0 | - |
|  |  | CVE-2013-5704 | 5.0 | - |
|  |  | CVE-2012-4558 | 4.3 | - |
|  |  | CVE-2012-3499 | 4.3 | - |
| bash | 5.0 | CVE-2019-18276 | 7.2 | - |
|  | 4.4 | CVE-2019-9924 | 7.2 | - |
|  | 4,4 | CVE-2017-5932 | 4.6 | - |
| Curl | 7.24.0 | CVE-2012-0036 | 7.5 | - |
|  | 7.20.0 | CVE-2010-3842 | 5.8 | - |
|  | 7.19.7 | CVE-2010-0734 | 6.8 | - |
| Firefox-3.0 | 3.0.5 | CVE-2009-0071 | 7.2 | - |
|  | 3.0.8 | CVE-2009-1232 | 5.8 | - |
|  | 3.0.1 | CVE-2008-4582 | 6.4 | - |
| mysql-server | 7.83.1 | CVE-2022-27778 | 5.8 | - |
|  | 17.3.1 | CVE-2022-21824 | 6.4 | - |
| postgresql-8.3 | 7.3 | CVE-2021-21704 | 4.3 | - |
|  | 7.2 | CVE-2020-7066 | 4.3 | - |
|  | 7.2 | CVE-2020-7062 | 4.3 | - |
| python2.5 | 2.5.2 | CVE-2008-1887 | 7.2 | - |
|  | 2.5 | CVE-2008-1721 | 5.4 | - |
|  | 2.5 | CVE-2008-2316 | 4.3 | - |
| samba | 6.14 | CVE-2022-29869 | 4.3 | - |
|  | 6.14 | CVE-2022-27239 | 7.2 | - |
|  | 4.15 | CVE-2021-44142 | 9.0 | - |
| tomcat5.5 | 5.5 | CVE-2008-0128 | 3,4 | - |
|  | 5.5 | CVE-2007-5461 | 4.3 | - |
|  | 5.5 | CVE-2007-3386 | 6.8 | - |
| wget | 1.12.1 | CVE-2021-31879 | 5.8 | - |
|  | 1.20.1 | CVE-2019-5953 | 7.5 | - |
|  | 1.20.1 | CVE-2018-20483 | 2.1 | - |
|  | 1.19.2 | CVE-2017-13090 | 9.3 | - |

Вывод

В данной лабораторной работе мы ознакомились с дистрибутивом Metasploitable2, посмотрели какие пакеты были в нем установлены, посмотрели версии данных утилит, попробовали ознакомится с базовыми командами.

Далее мы ознакомились с базой данных CVE при помощи сайта cvedetails и vpn, в данном сайте представлена информация о уязвимостях, которые присутствуют в установленных пакетах.

Далее мы попробовали поискать на найденные уязвимости наличие эксплойтов, но в основном выложенных эксплойты не были найдены, по крайней мере на сайте exploit.db.