МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

**НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Отчет по лабораторной работе №2

по курсу «Защита информации»

**Выполнил:** студент 4-го курса гр. 17208

Гафиятуллин А.Р

Новосибирск, 2020

Оглавление

[1. ЦЕЛИ РАБОТЫ 3](#_Toc56885275)

[2. ЗАДАЧИ 3](#_Toc56885276)

[3. ХОД РАБОТЫ 3](#_Toc56885277)

[3.1 Сканирование сети с помощью веб-интерфейса Сканер-ВС 4](#_Toc56885278)

[3.2 Информация об исследуемых хостах 4](#_Toc56885279)

[3.3 Информация об открытых портах 4](#_Toc56885280)

[3.4 Определение версий работающих сервисов 4](#_Toc56885281)

[3.5 Построение топологии сети 4](#_Toc56885282)

[3.6 Сканирование Metasploitable 2 с помощью веб-интерфейса Сканер-ВС 4](#_Toc56885283)

[3.7 Отчет по результатам сканирования уязвимостей 4](#_Toc56885284)

[3.8 Подбор паролей сервисов ftp и smb 4](#_Toc56885285)

[4. ВЫВОДЫ 4](#_Toc56885286)

# ЦЕЛИ РАБОТЫ

1. изучить процесс сканирования портов;
2. изучить принцип работы сканеров безопасности;
3. провести сетевой аудит паролей Metasploitable 2.

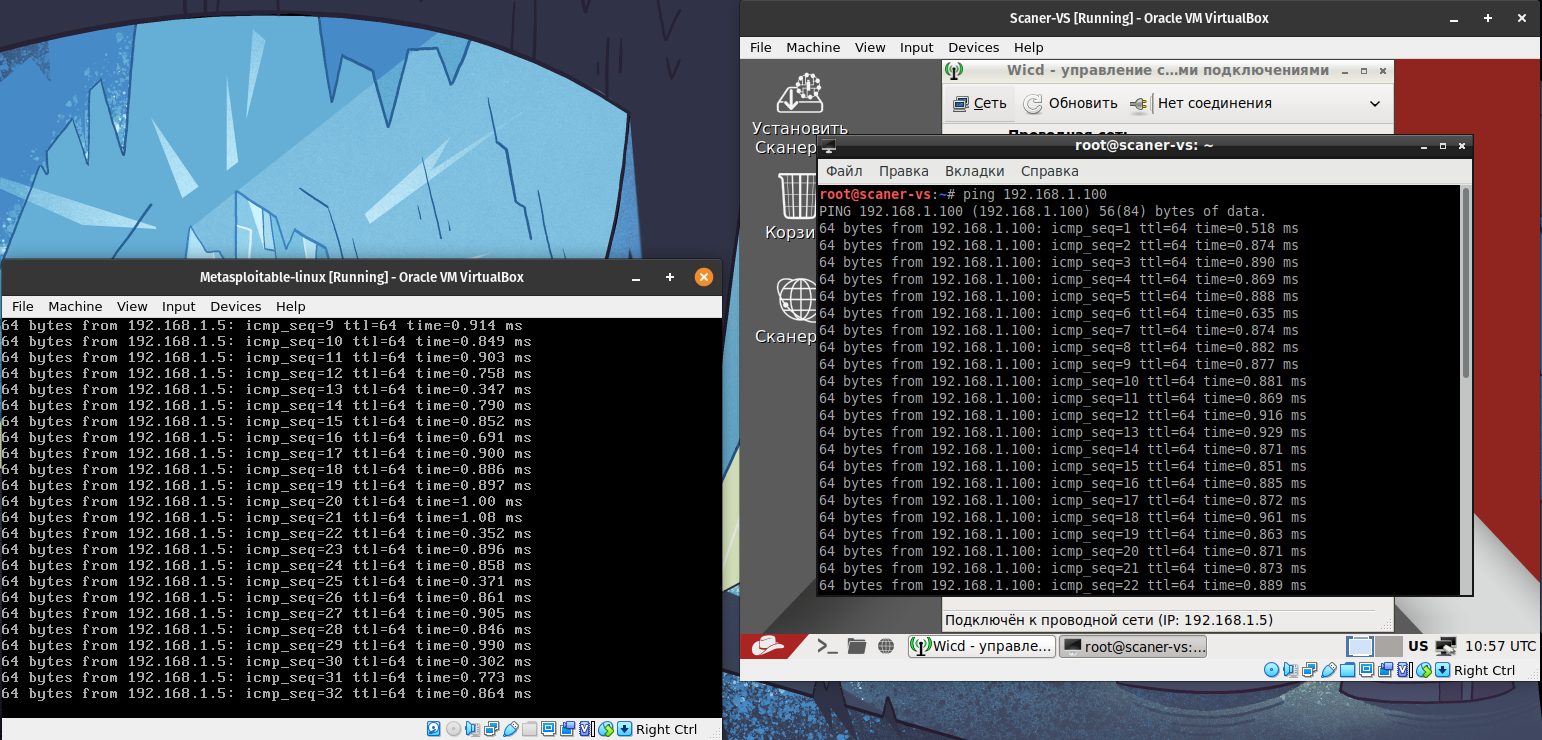
# ЗАДАЧИ

1. провести сканирование сети с помощью веб-интерфейса Сканер-ВС (фаза Поиск целей);
2. определить открытые порты;
3. определить версию операционной системы;
4. провести сканирование Metasploitable 2 с определением версий работающих сервисов;
5. построить топологию тестовой сети;
6. провести сканирование Metasploitable 2 с помощью веб-интерфейса Сканер-ВС (фаза Поиск уязвимостей);
7. сформировать отчет по результатам сканирования уязвимостей;
8. провести подбор паролей сервисов ftp и smb (фаза Эксплуатация).

# ХОД РАБОТЫ

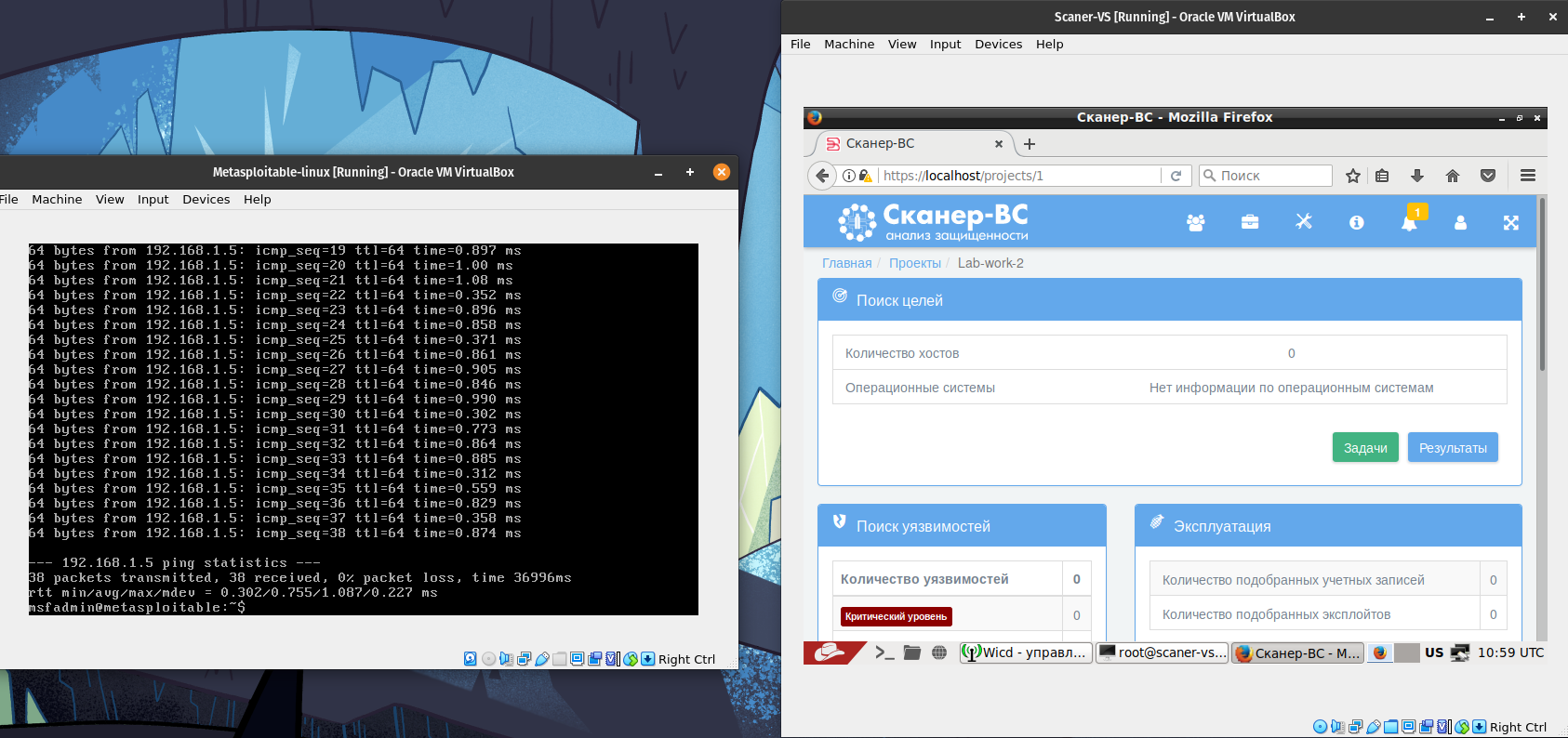
Проверим доступность друг до друга узлов тестовой сети.

Рисунок 1. Проверка доступности узлов сети друг до друга с помощью команды ping.



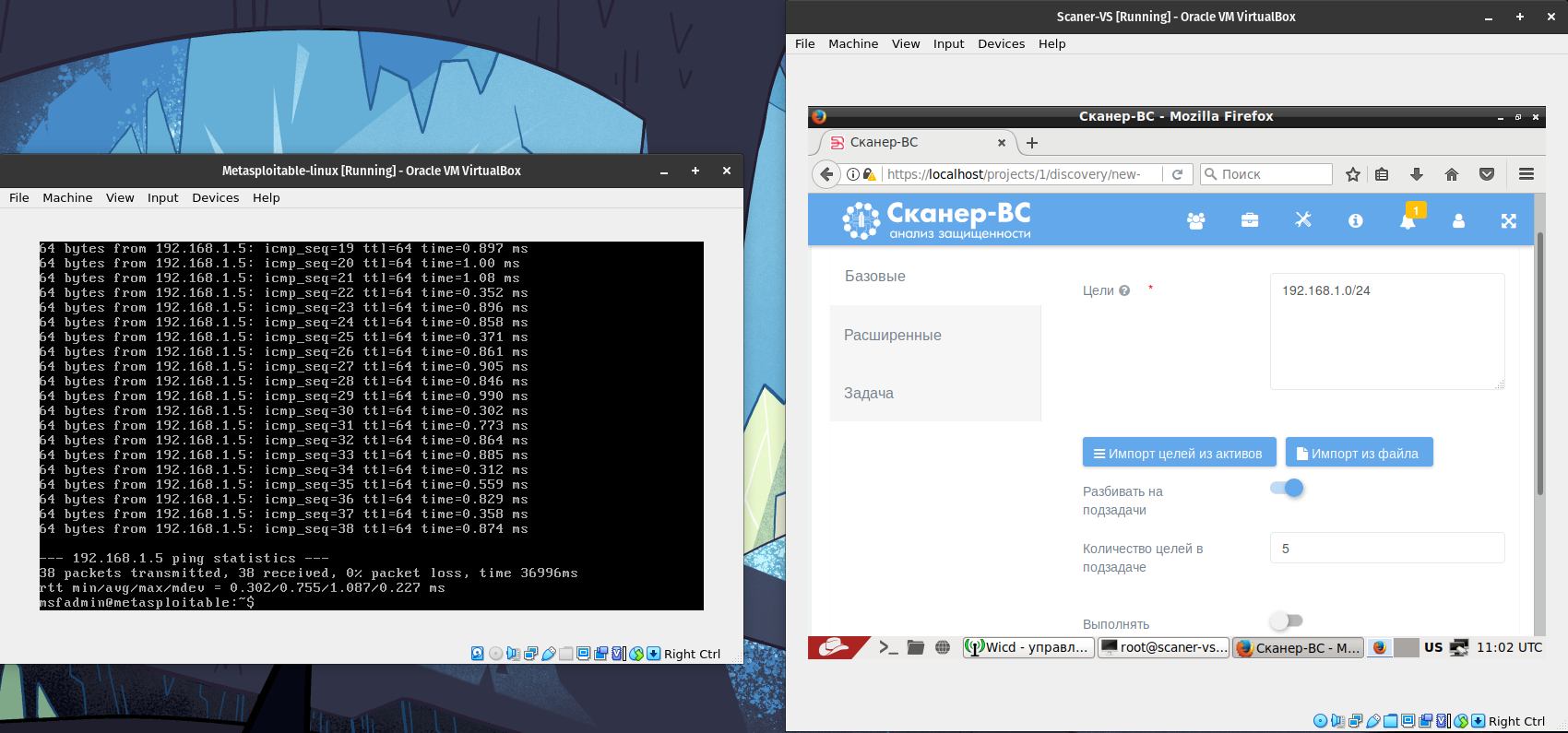
## Сканирование сети с помощью веб-интерфейса Сканер-ВС

Рисунок 2. Веб-интерфейс Сканер-ВС.



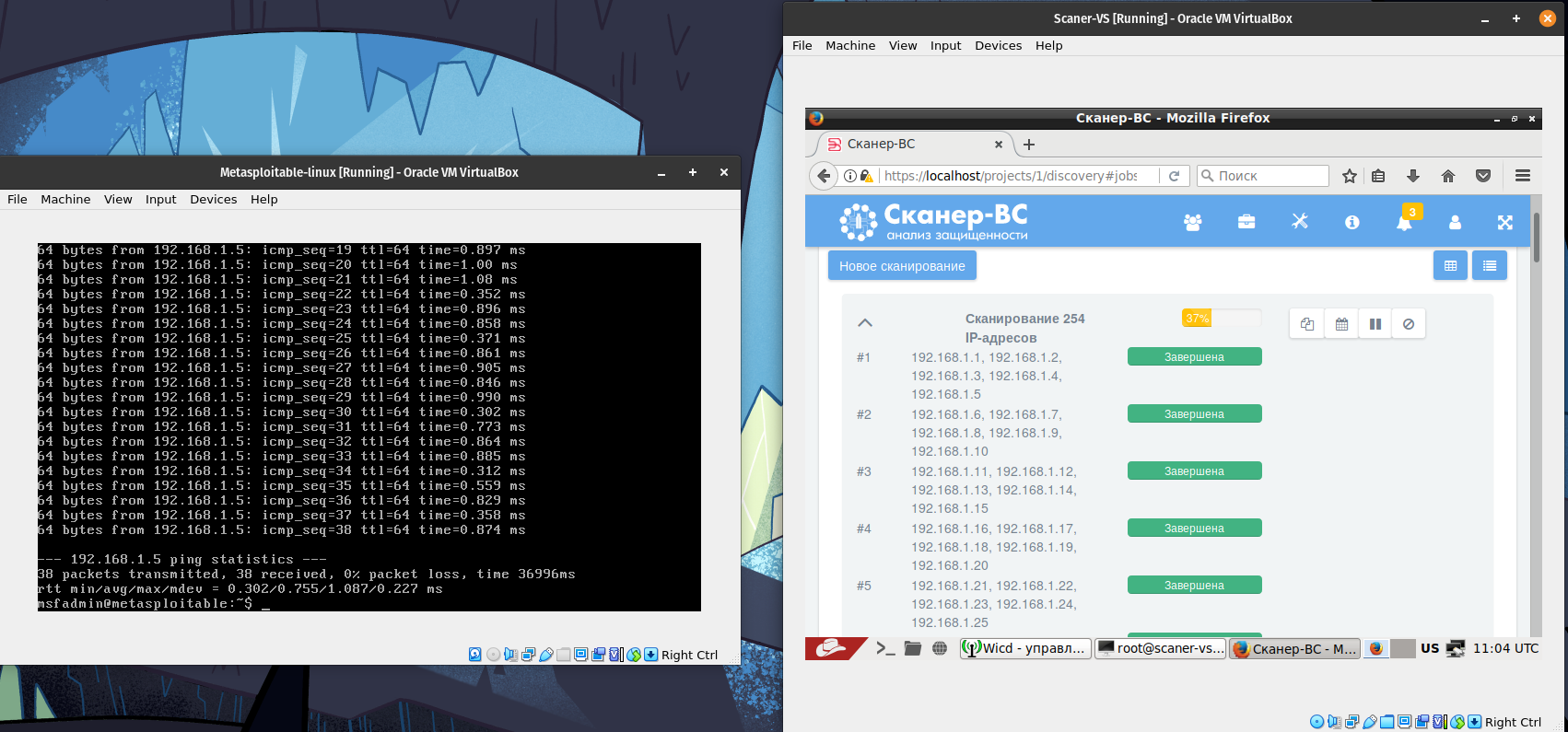
Создание нового сканирования подсети.

Рисунок 3. Создание нового сканирования подсети 192.168.1.0/24 с «Разбивкой на подзадачи».



Процесс сканирования подсети.

Рисунок 4. Процесс сканирования подсети 192.168.1.0/24.



## Информация об исследуемых хостах

На вкладке «Хосты» доступна информация об исследуемых хостах.

Рисунок 5. Информация об исследуемых хостах.

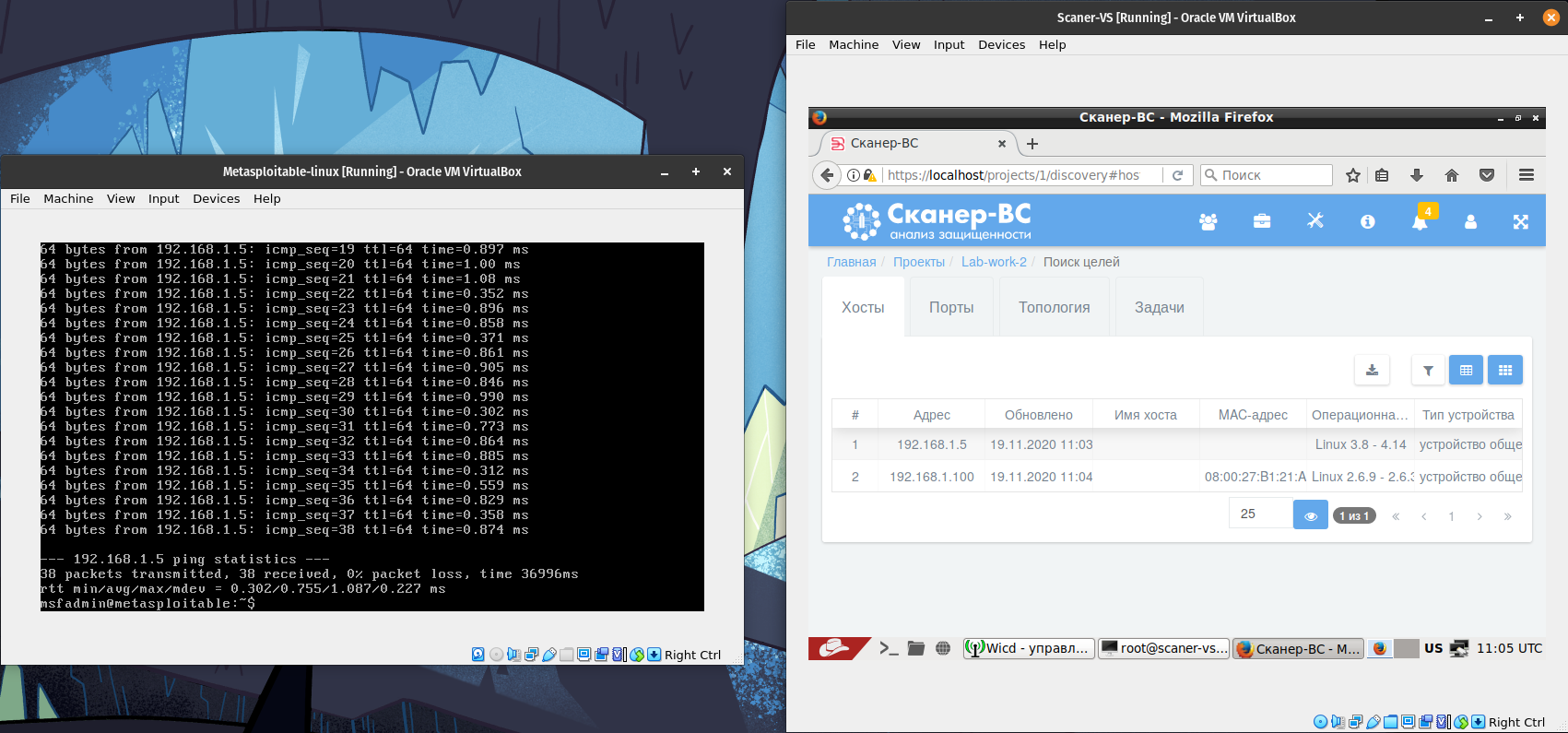


Таблица 1. Информация об исследуемых хостах и их операционных системах.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Адрес | Имя хоста | MAC-адрес | Операционная система | Тип устройства |
| 192.168.1.5 |  |  | Linux 3.8 - 4.14 | устройство общего назначения |
| 192.168.1.100 |  | 08:00:27:B1:21:A5 | Linux 2.6.9 - 2.6.33 | устройство общего назначения |

## Информация об открытых портах

На вкладке «Порты» доступна информация об открытых портах.

Рисунок 6. Информация об открытых портах.

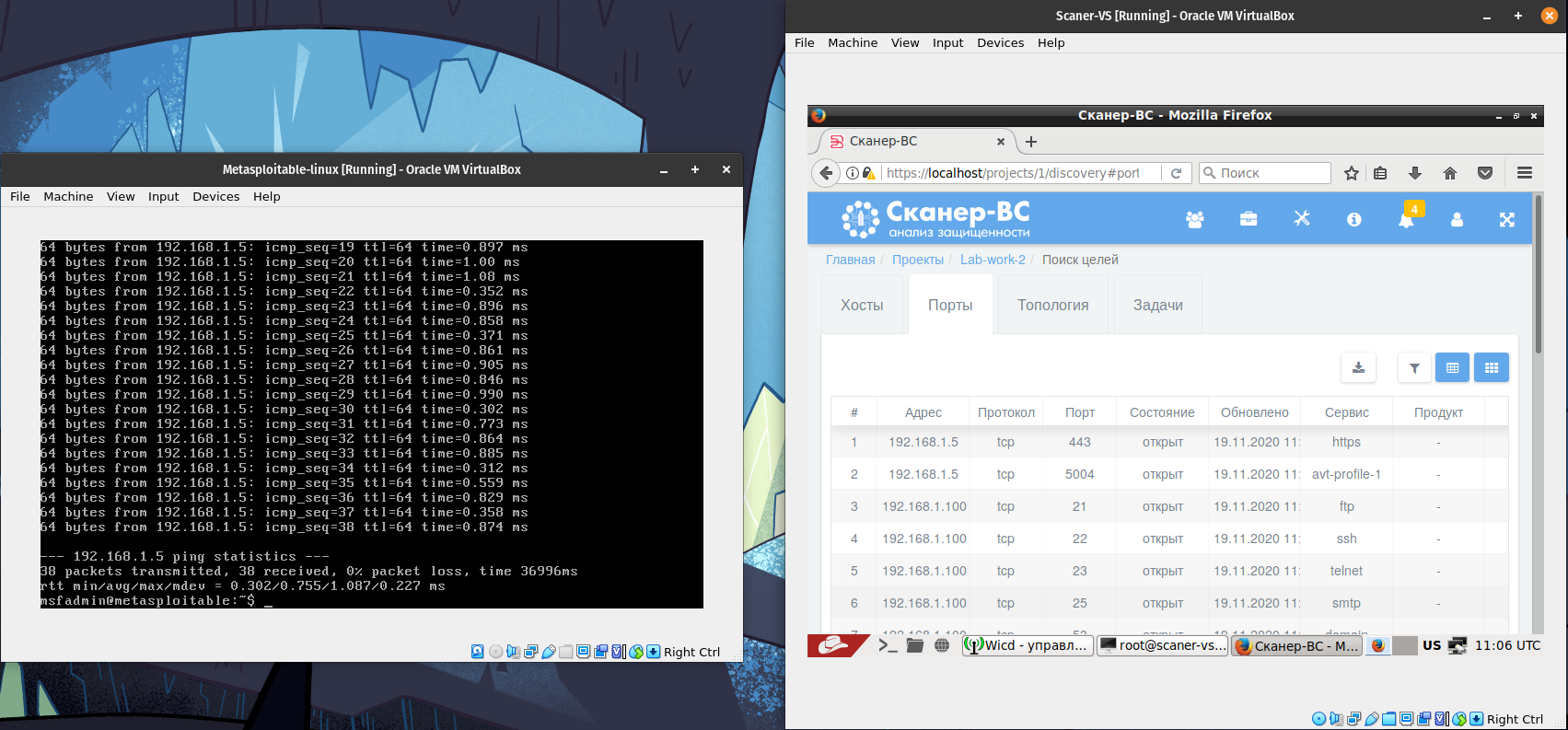


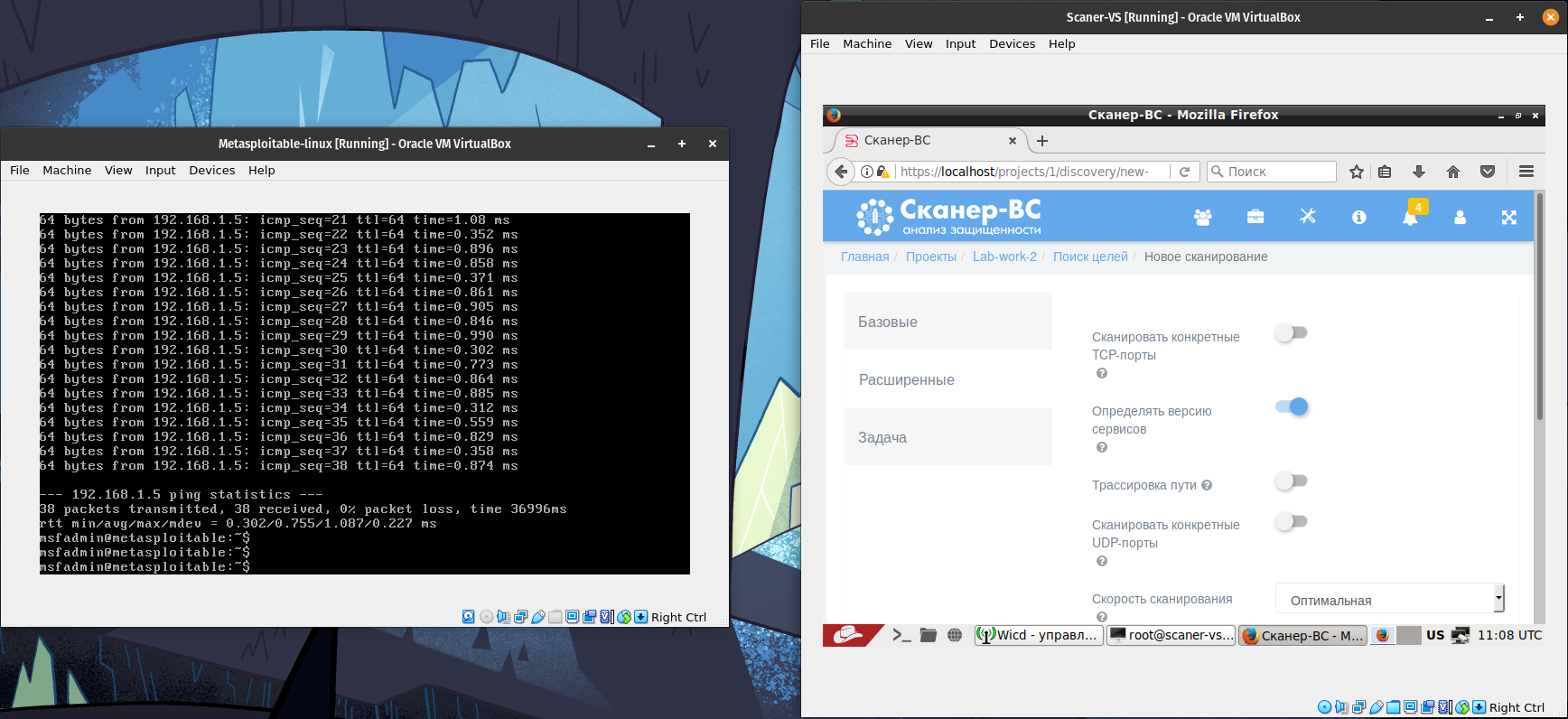
Таблица 2. Информация об открытых портах.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Адрес | Порт | Протокол | Состояние | Сервис |
| 192.168.1.5 | 443 | tcp | открыт | https |
| 192.168.1.5 | 5004 | tcp | открыт | avt-profile-1 |
| 192.168.1.100 | 21 | tcp | открыт | ftp |
| 192.168.1.100 | 22 | tcp | открыт | ssh |
| 192.168.1.100 | 23 | tcp | открыт | telnet |
| 192.168.1.100 | 25 | tcp | открыт | smtp |
| 192.168.1.100 | 53 | tcp | открыт | domain |
| 192.168.1.100 | 80 | tcp | открыт | http |
| 192.168.1.100 | 111 | tcp | открыт | rpcbind |
| 192.168.1.100 | 139 | tcp | открыт | netbios-ssn |
| 192.168.1.100 | 445 | tcp | открыт | netbios-ssn |
| 192.168.1.100 | 512 | tcp | открыт | exec |
| 192.168.1.100 | 513 | tcp | открыт | login |
| 192.168.1.100 | 514 | tcp | открыт | shell |
| 192.168.1.100 | 1099 | tcp | открыт | rmiregistry |
| 192.168.1.100 | 1524 | tcp | открыт | bindshell |
| 192.168.1.100 | 2049 | tcp | открыт | nfs |
| 192.168.1.100 | 2121 | tcp | открыт | ftp |
| 192.168.1.100 | 3306 | tcp | открыт | mysql |
| 192.168.1.100 | 5432 | tcp | открыт | postgresql |
| 192.168.1.100 | 5900 | tcp | открыт | vnc |
| 192.168.1.100 | 6000 | tcp | открыт | X11 |
| 192.168.1.100 | 6667 | tcp | открыт | irc |
| 192.168.1.100 | 8009 | tcp | открыт | ajp13 |
| 192.168.1.100 | 8180 | tcp | открыт | http |

## Определение версий работающих сервисов

Для определения работающих версий сервисов изменим «Расширенные» параметры сканирования.

Рисунок 7. Изменение параметров сканирования для определения версий работающих сервисов.



Проведем сканирование и получим результаты на вкладке «Порты».

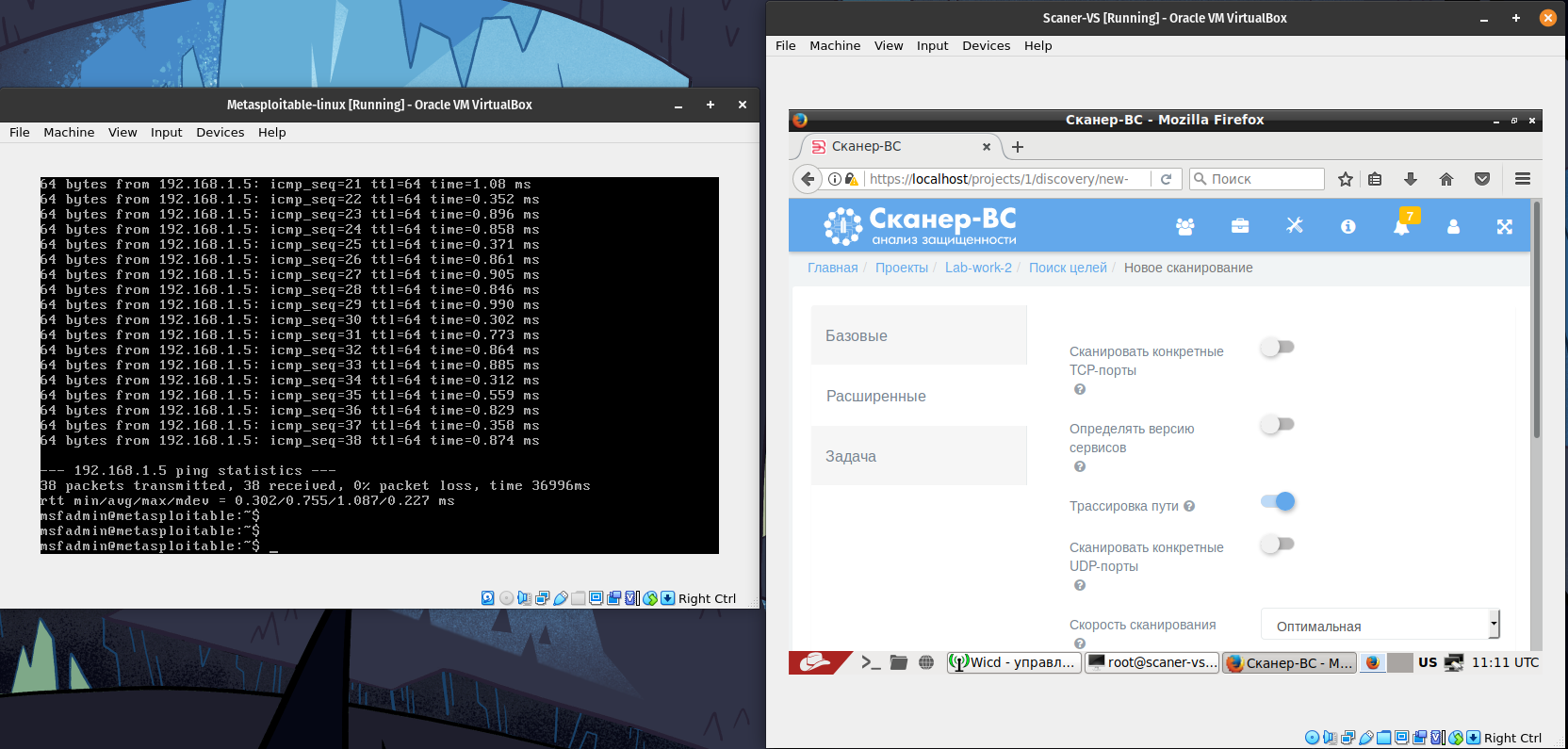
Таблица 3. Информация об открытых портах с версиями работающих сервисов.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Адрес | Порт | Протокол | Состояние | Сервис | Продукт | Версия |
| 192.168.1.5 | 443 | tcp | открыт | https | - | - |
| 192.168.1.5 | 5004 | tcp | открыт | avt-profile-1 | - | - |
| 192.168.1.100 | 21 | tcp | открыт | ftp | vsftpd | 2.3.4 |
| 192.168.1.100 | 22 | tcp | открыт | ssh | OpenSSH | 4.7p1 Debian 8ubuntu1 |
| 192.168.1.100 | 23 | tcp | открыт | telnet | Linux telnetd | - |
| 192.168.1.100 | 25 | tcp | открыт | smtp | Postfix smtpd | - |
| 192.168.1.100 | 53 | tcp | открыт | domain | ISC BIND | 9.4.2 |
| 192.168.1.100 | 80 | tcp | открыт | http | Apache httpd | 2.2.8 |
| 192.168.1.100 | 111 | tcp | открыт | rpcbind | - | 2 |
| 192.168.1.100 | 139 | tcp | открыт | netbios-ssn | Samba smbd | 3.X - 4.X |
| 192.168.1.100 | 445 | tcp | открыт | netbios-ssn | Samba smbd | 3.X - 4.X |
| 192.168.1.100 | 512 | tcp | открыт | exec | netkit-rsh rexecd | - |
| 192.168.1.100 | 513 | tcp | открыт | login | OpenBSD or Solaris rlogind | - |
| 192.168.1.100 | 514 | tcp | открыт | shell | Netkit rshd | - |
| 192.168.1.100 | 1099 | tcp | открыт | rmiregistry | GNU Classpath grmiregistry | - |
| 192.168.1.100 | 1524 | tcp | открыт | bindshell | Metasploitable root shell | - |
| 192.168.1.100 | 2049 | tcp | открыт | nfs | - | 2-4 |
| 192.168.1.100 | 2121 | tcp | открыт | ftp | ProFTPD | 1.3.1 |
| 192.168.1.100 | 3306 | tcp | открыт | mysql | MySQL | 5.0.51a-3ubuntu5 |
| 192.168.1.100 | 5432 | tcp | открыт | postgresql | PostgreSQL DB | 8.3.0 - 8.3.7 |
| 192.168.1.100 | 5900 | tcp | открыт | vnc | VNC | - |
| 192.168.1.100 | 6000 | tcp | открыт | X11 | - | - |
| 192.168.1.100 | 6667 | tcp | открыт | irc | UnrealIRCd | - |
| 192.168.1.100 | 8009 | tcp | открыт | ajp13 | Apache Jserv | - |
| 192.168.1.100 | 8180 | tcp | открыт | http | Apache Tomcat/Coyote JSP engine | 1.1 |

## Построение топологии сети

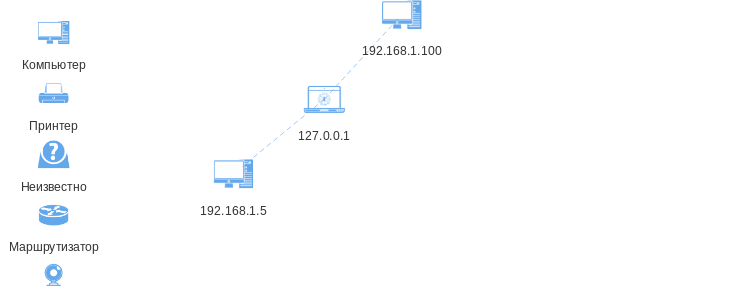
В «Расширенных» настройках сканирования выберем пункт «Трассировка пути».

Рисунок 8. Пункт «Трассировка пути» «Расширенных» настроек сканирования.



После завершения сканирования на вкладке «Топология» появится топология исследуемой сети.

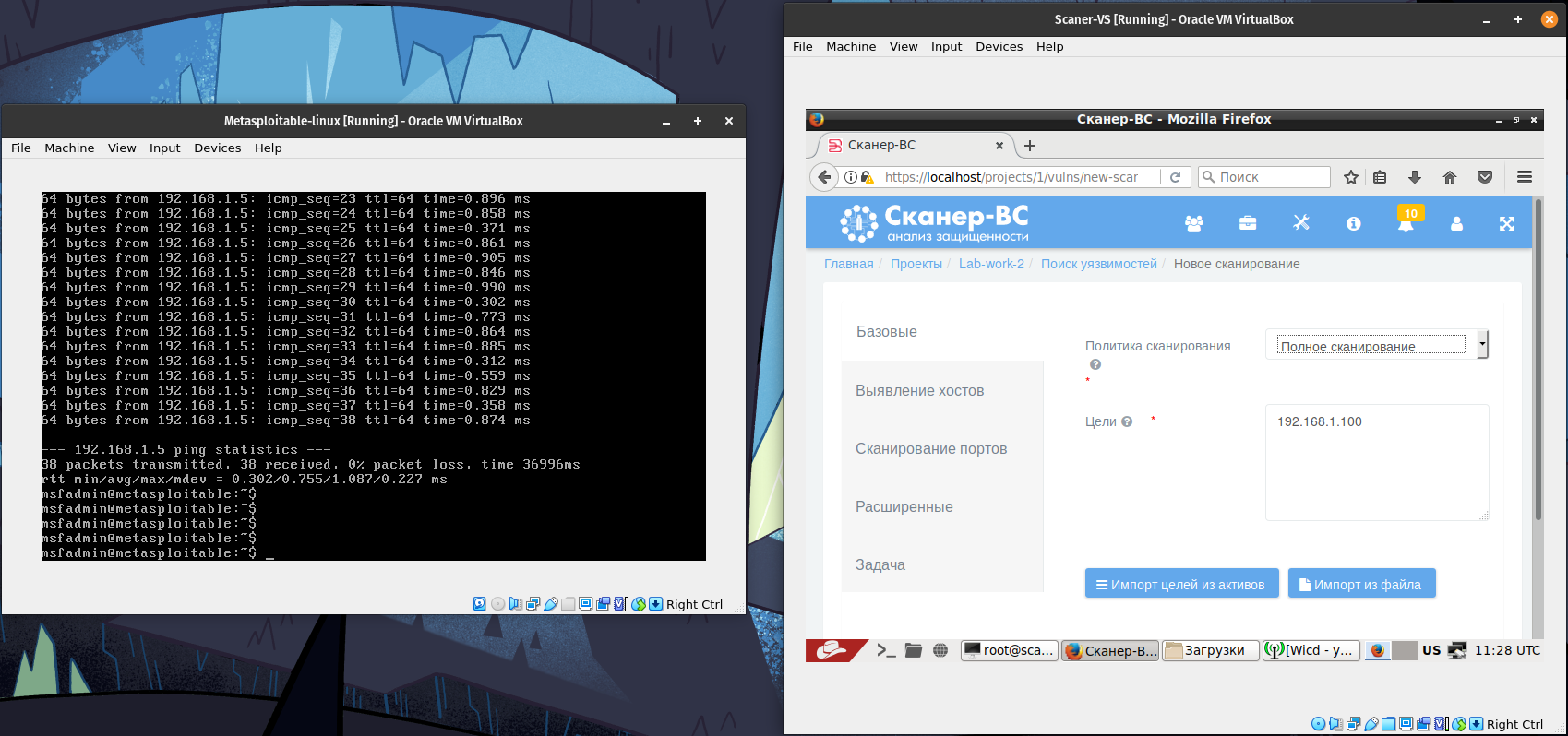
Рисунок 9. Топология сети.



## Сканирование Metasploitable 2 с помощью веб-интерфейса Сканер-ВС

Выберем для полного сканирования уязвимостей узел с адресом 192.168.1.100

Рисунок 10. Выбор узла для полного сканирования.



## Отчет по результатам сканирования уязвимостей

По завершению сканирования были выявлены уязвимости, перечисленные в Файле 1 (не копирован в текст отчета ввиду громоздкости таблицы).

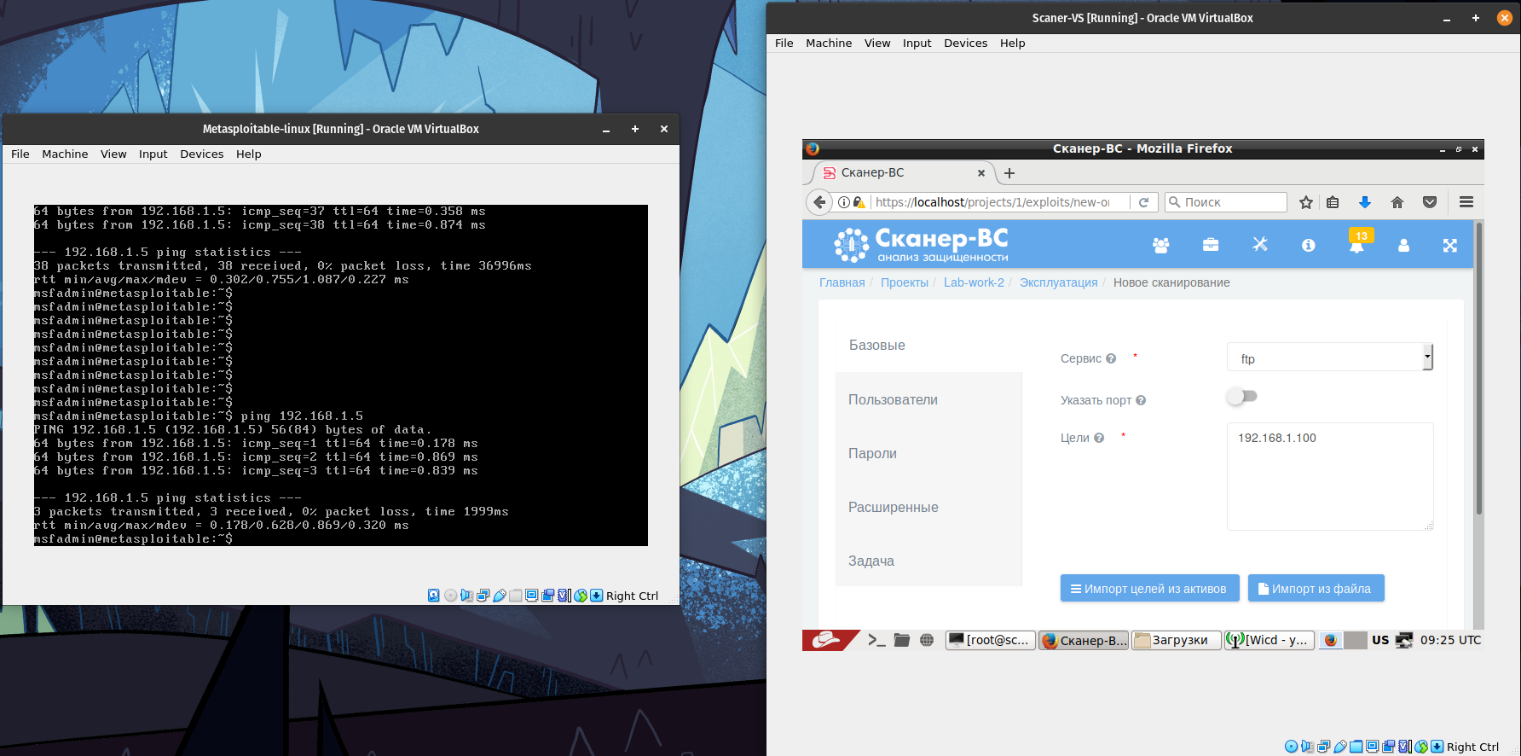
Файл 1. Выявленные уязвимости.



## Подбор паролей сервисов ftp и smb

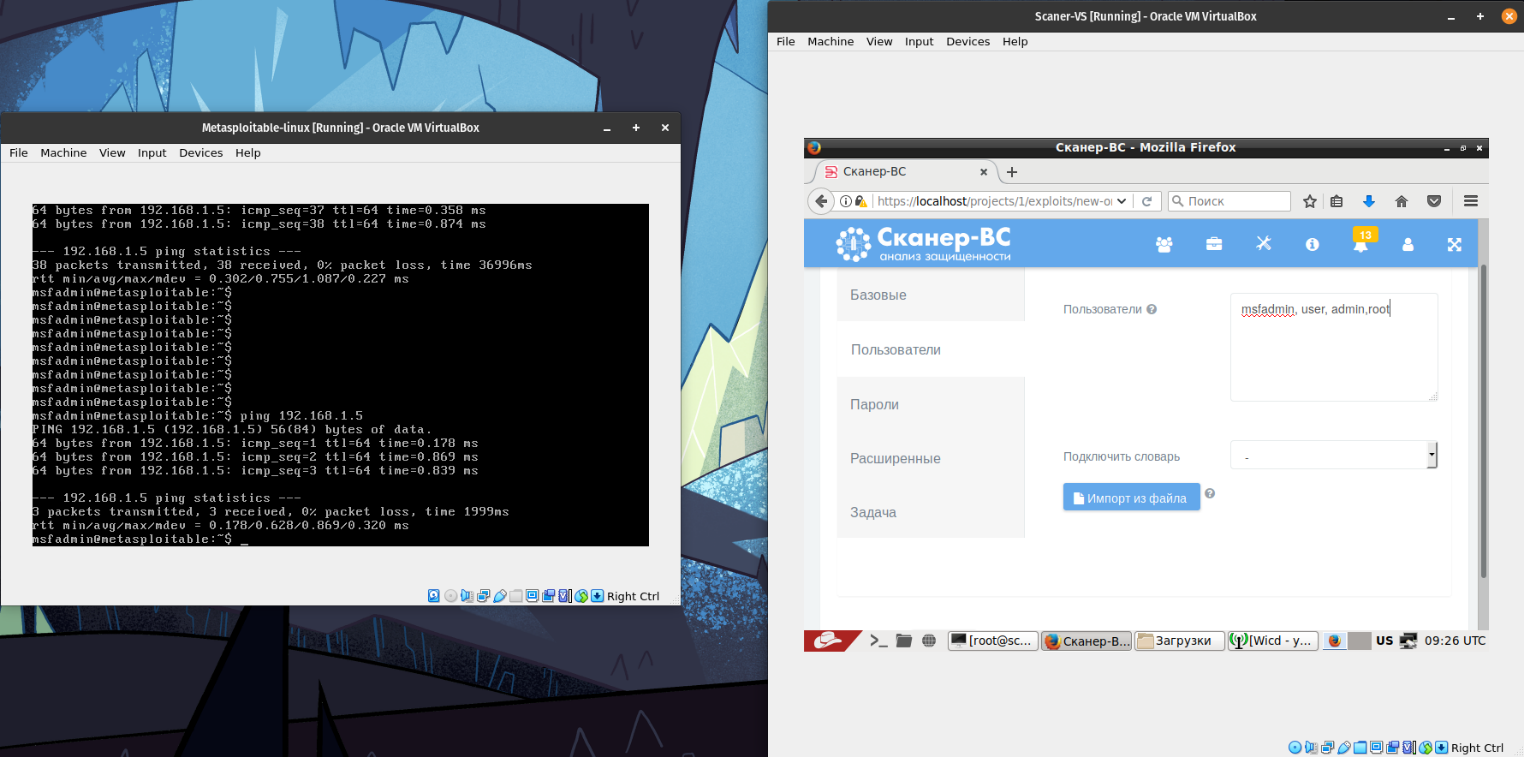
Выберем сервис ftp на хосте 192.168.1.100 для подбора паролей.

Рисунок 11. Выбор сервиса и хоста для подбора паролей.



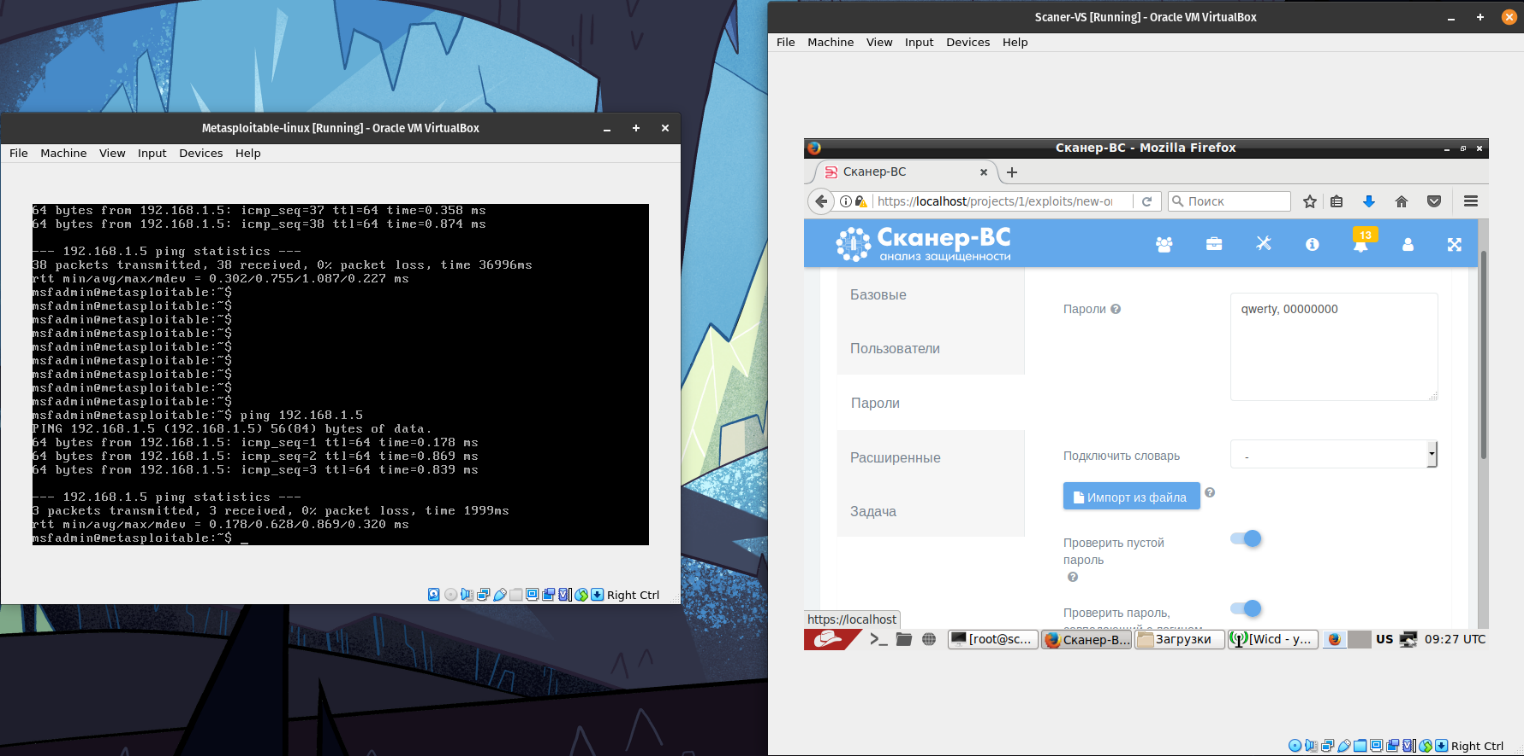
Выберем пользователей для подбора паролей на вкладке «Пользователи».

Рисунок 12. Выбор пользователей для подбора паролей.



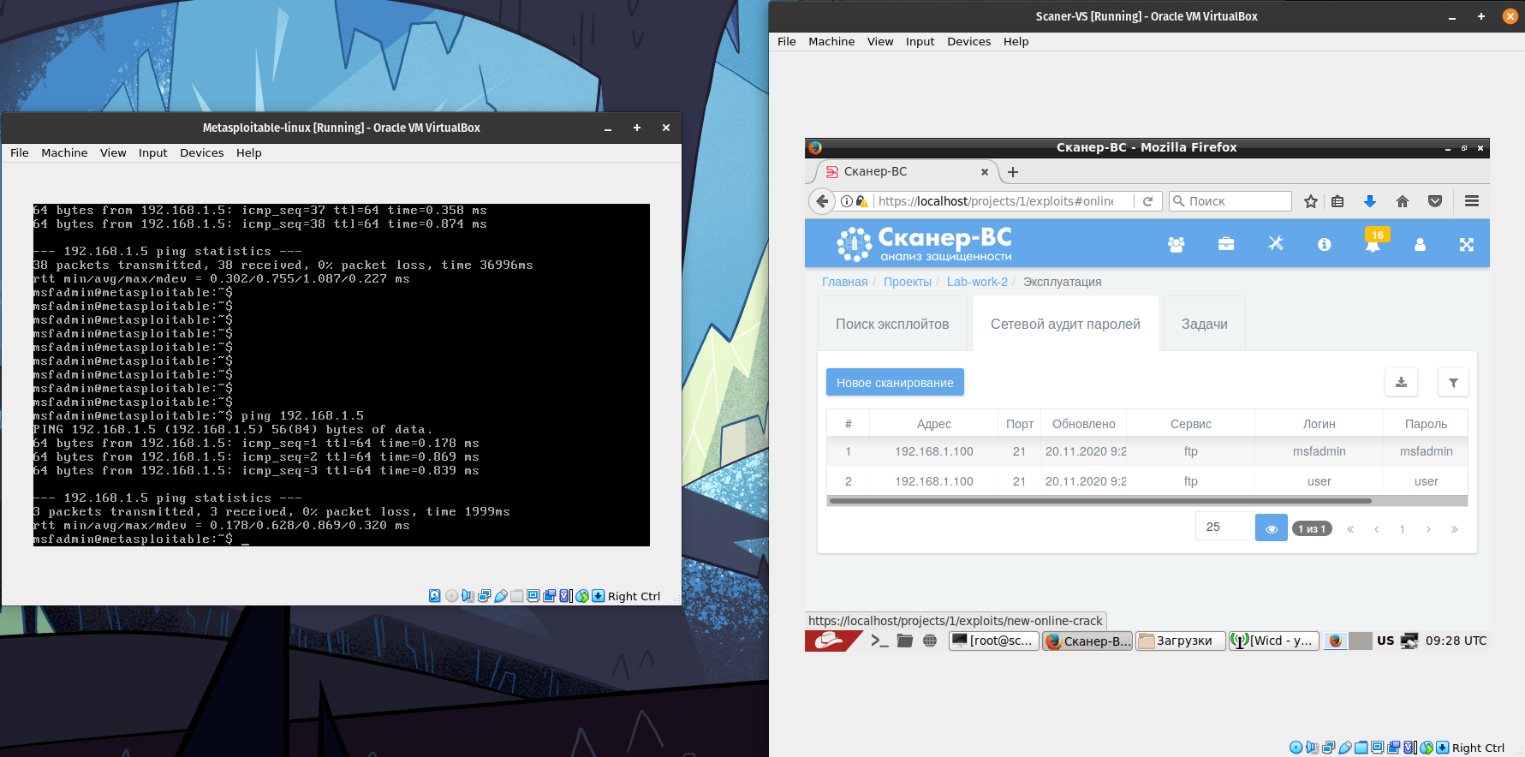
Добавим пароли для проверки, а также укажем проверку пустого пароля и пароля, совпадающего с логином во вкладке «Пароли».

Рисунок 13. Выбор паролей для проверки.



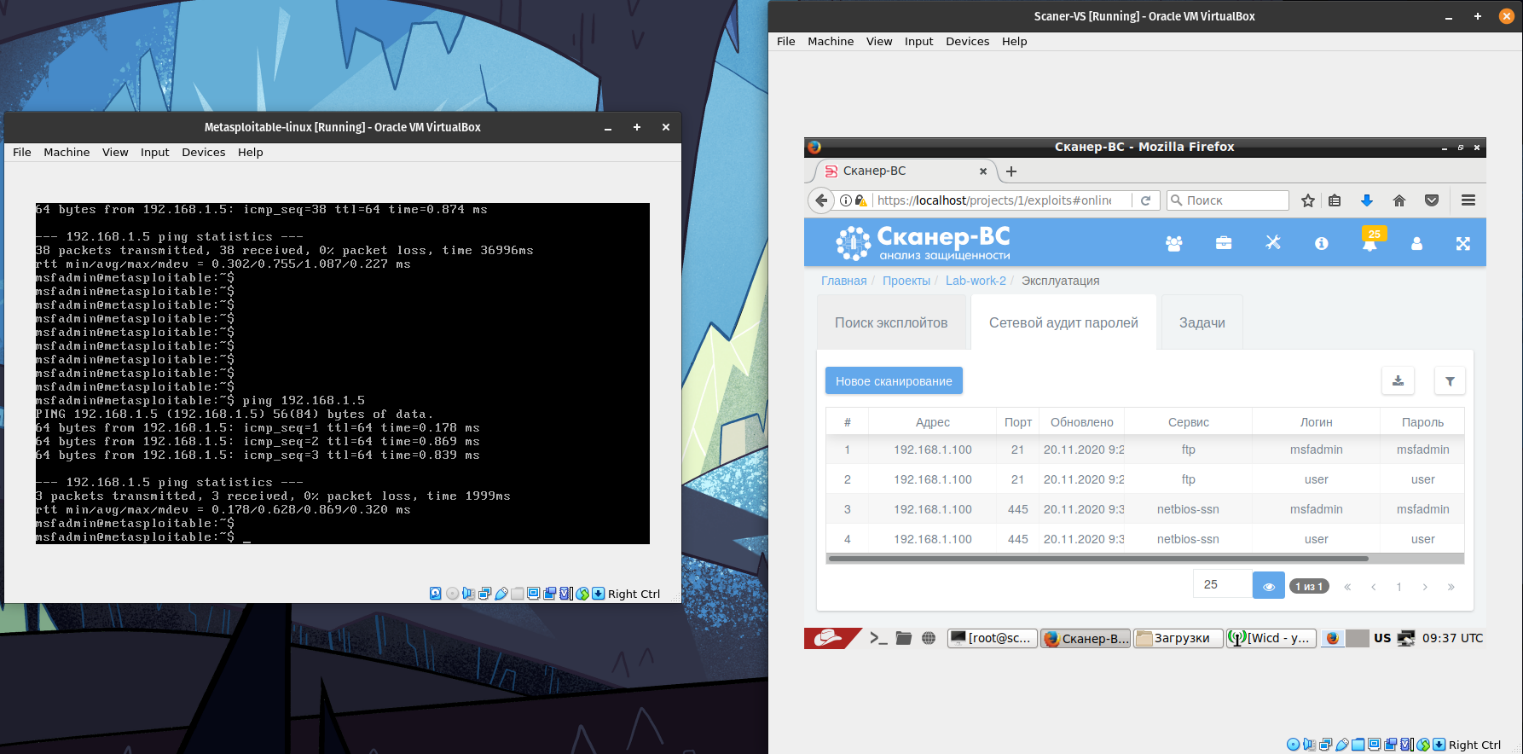
После сканирования во вкладке «Сетевой аудит паролей» появятся подобранные комбинации.

Рисунок 14. Подобранные пароли для сервиса ftp.



Аналогичные действия проведем для сервиса smb.

Рисунок 15. Подобранные пароли для сервисов ftp и smb.



# ВЫВОДЫ

1. Изучили процесс сканирования портов;
2. Изучили принципы работы сканеров безопасности;
3. Провели сетевой аудит паролей Metasploitable 2.