

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ №7

по дисциплине «Программные и аппаратные средства защиты информации»

«Использование сканеров безопасности»

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 21 июня 2023 г.

Преподаватель:

Перов А. А.

«__» _____ 2023 г.

Москва, 2023

Содержание

1	Цель работы	3
2	Ход работы	3
2.1	Создание ВМ	3
2.2	Лабораторная работа 1. Сканирование портов	5
2.3	Лабораторная работа 2. Поиск уязвимостей	12
2.4	Лабораторная работа 3. Сетевой аудит паролей	14
2.5	Лабораторная работа 4. Поиск подходящих эксплойтов	18
3	Выводы о проделанной работе	21
	Приложение А. Отчёт	22

1 Цель работы

Цель: освоение основ анализа защищённости сетевого компьютера с использованием пассивных и активных методов.

2 Ход работы

2.1 Создание ВМ

Для выполнения работы используются две виртуальные машины, на одну из которых устанавливается Сканер-ВС, а на другую — тестовая уязвимая операционная система Metasploitable. (Рисунок 1).

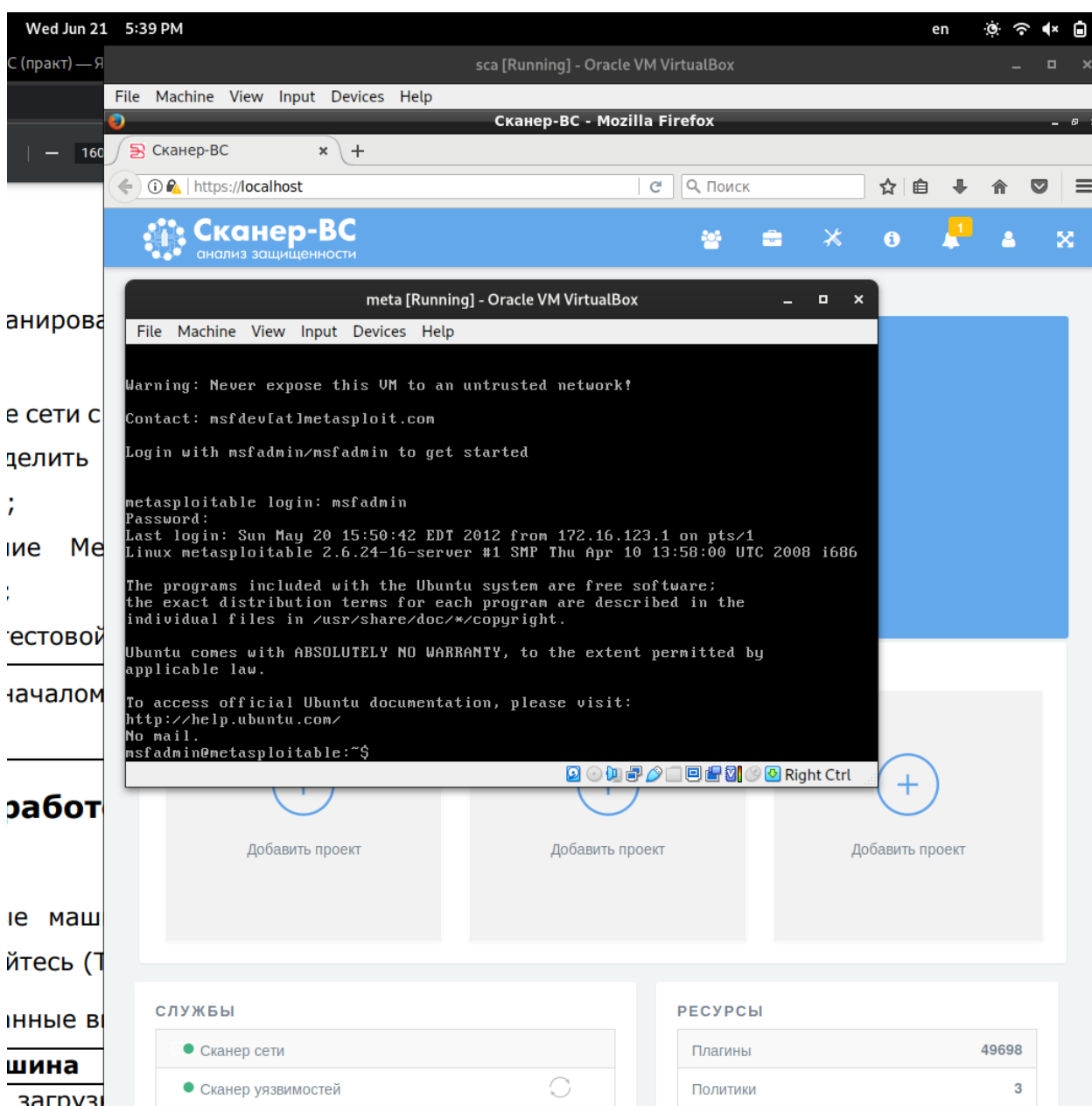


Рисунок 1 – Создание ВМ

Проверим настройки сети. У метасплота адрес 192.168.56.102, у сканера — .103 (Рисунок 2).

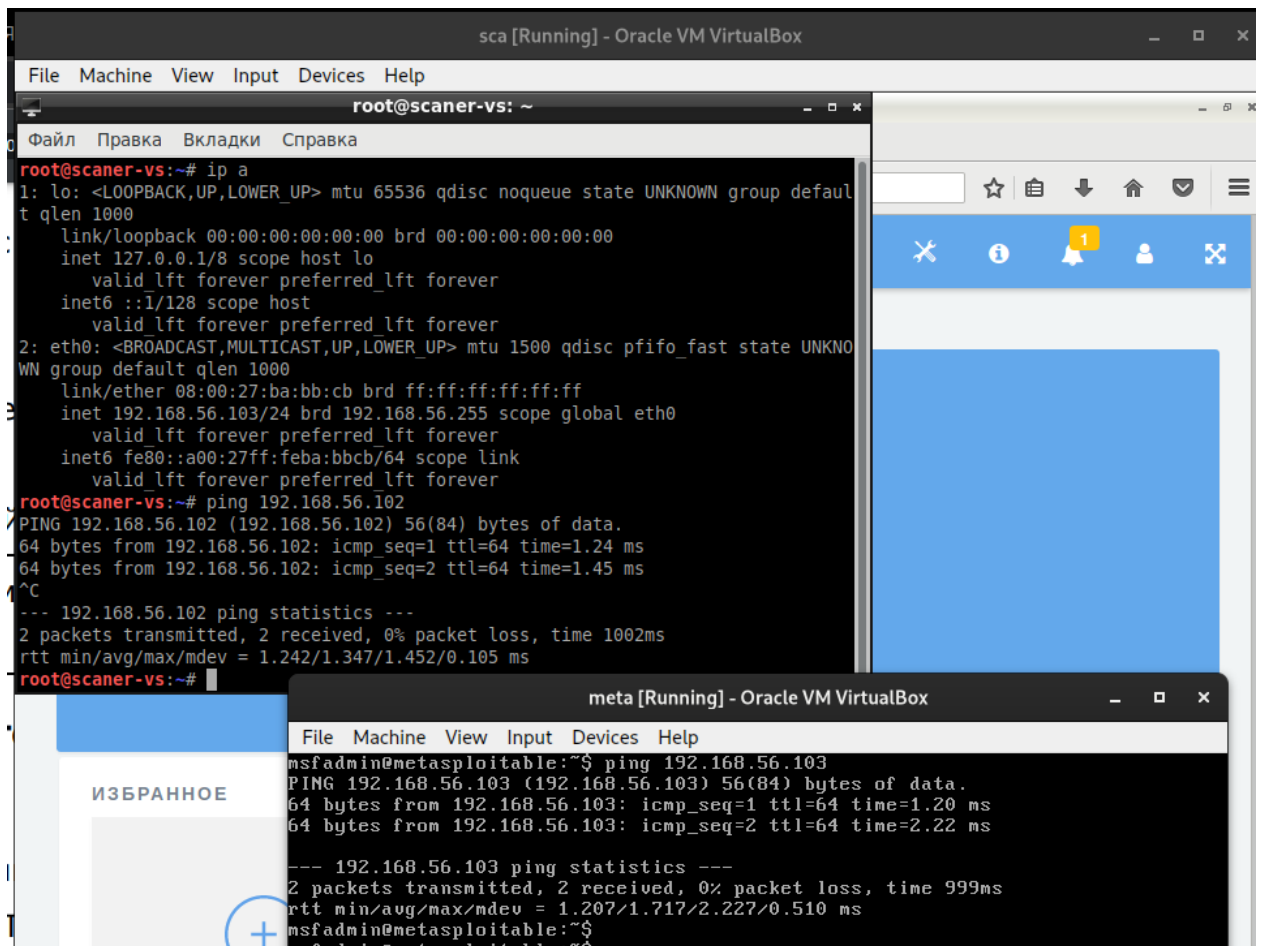


Рисунок 2 – Адреса ВМ

2.2 Лабораторная работа 1. Сканирование портов

В этой работе изучим процесс сканирования портов. Для этого создадим новый проект и добавим задачу (Рисунок 3). В качестве цели зададим подсеть.

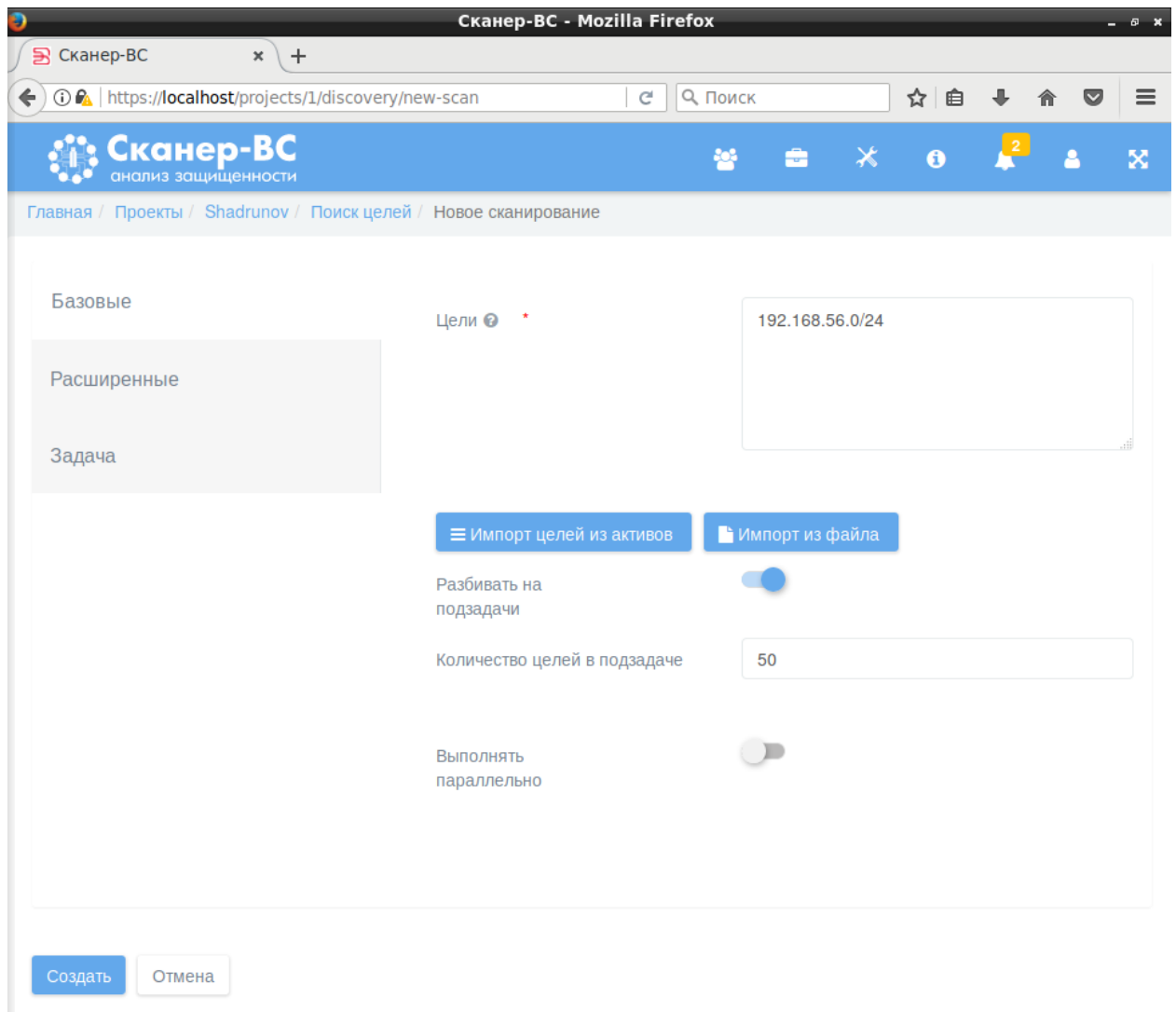


Рисунок 3 – Новая задача

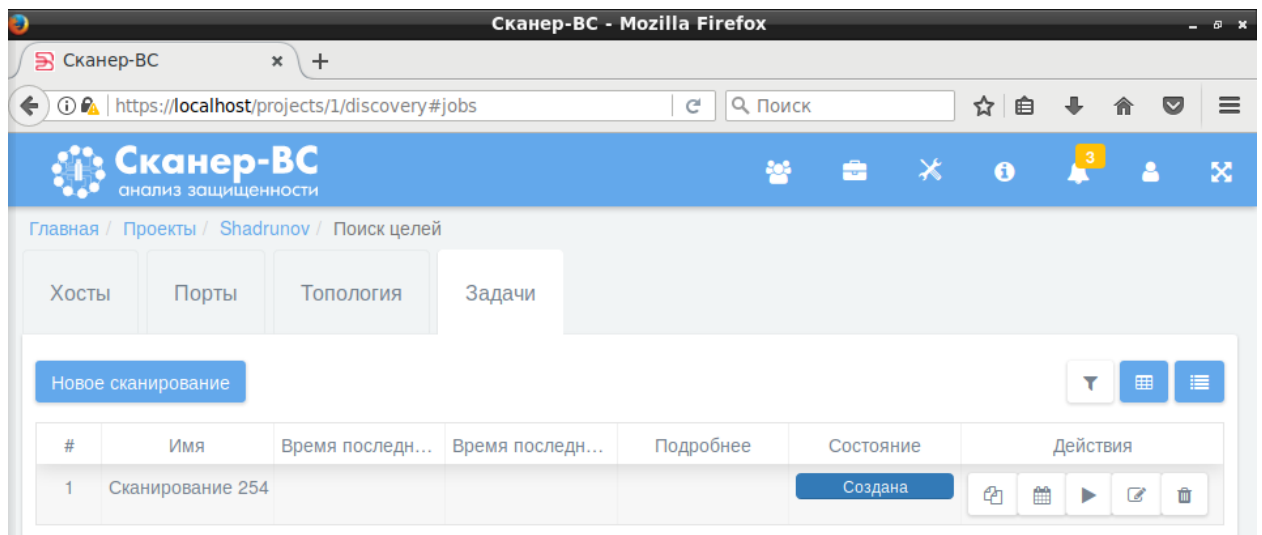


Рисунок 4 – Новая задача

Запустим задачу (Рисунок 5). В результате на вкладке Порты увидим открытые порты метаспллойта (Рисунок 6). На вкладке Хосты отображаются найденные устройства (Рисунок 7).

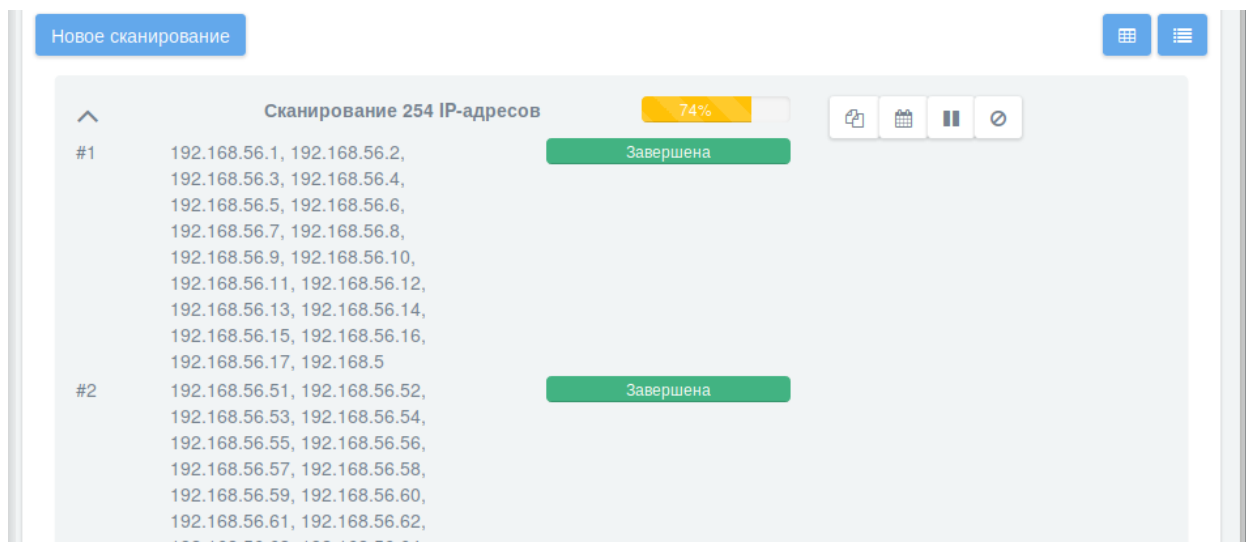


Рисунок 5 – Выполнение задачи



<div> <div>  <div> <div>Сканер-ВС</div> <div>анализ защищенности</div> </div> </div> <div> <div> <div>👤</div> <div>📁</div> <div>✂️</div> <div>ℹ️</div> <div>🔔12</div> <div>👤</div> <div>✕</div> </div> </div> </div>								
<div> <div>Главная</div> / <div>Проекты</div> / <div>Shadrinov</div> / <div>Поиск целей</div> </div>								
<div> <div>Хосты</div> <div>Порты</div> <div>Топология</div> <div>Задачи</div> </div>								
<div> <div> <div>📄</div> <div>🔍</div> <div>📊</div> <div>🗃️</div> </div> </div>								
#	Адрес	Протокол	Порт	Состояние	Обновлено	Сервис	Продукт	Версия
1	192.168.56.102	tcp	21	открыт	21.06.2023 17:46	ftp	-	-
2	192.168.56.102	tcp	22	открыт	21.06.2023 17:46	ssh	-	-
3	192.168.56.102	tcp	23	открыт	21.06.2023 17:46	telnet	-	-
4	192.168.56.102	tcp	25	открыт	21.06.2023 17:46	smtp	-	-
5	192.168.56.102	tcp	53	открыт	21.06.2023 17:46	domain	-	-
6	192.168.56.102	tcp	80	открыт	21.06.2023 17:46	http	-	-
7	192.168.56.102	tcp	111	открыт	21.06.2023 17:46	rpcbind	-	-
8	192.168.56.102	tcp	139	открыт	21.06.2023 17:46	netbios-ssn	-	-
9	192.168.56.102	tcp	445	открыт	21.06.2023 17:46	microsoft-ds	-	-
10	192.168.56.102	tcp	512	открыт	21.06.2023 17:46	exec	-	-
11	192.168.56.102	tcp	513	открыт	21.06.2023 17:46	login	-	-
12	192.168.56.102	tcp	514	открыт	21.06.2023 17:46	shell	-	-
13	192.168.56.102	tcp	1099	открыт	21.06.2023 17:46	rmiregistry	-	-
14	192.168.56.102	tcp	1524	открыт	21.06.2023 17:46	ingreslock	-	-
15	192.168.56.102	tcp	2049	открыт	21.06.2023 17:46	nfs	-	-
16	192.168.56.102	tcp	2121	открыт	21.06.2023 17:46	ccproxy-ftp	-	-
17	192.168.56.102	tcp	3306	открыт	21.06.2023 17:46	mysql	-	-
18	192.168.56.102	tcp	5432	открыт	21.06.2023 17:46	postgresql	-	-
19	192.168.56.102	tcp	5900	открыт	21.06.2023 17:46	vnc	-	-
20	192.168.56.102	tcp	6000	открыт	21.06.2023 17:46	X11	-	-

Рисунок 6 – Открытые порты

<div> <div> <div>  <div> <div>Сканер-ВС</div> <div>анализ защищенности</div> </div> </div> <div> <div> <div>👤</div> <div>📁</div> <div>✂️</div> <div>ℹ️</div> <div>🔔12</div> <div>👤</div> <div>✕</div> </div> </div> </div> </div>						
<div> <div>Главная</div> / <div>Проекты</div> / <div>Shadrinov</div> / <div>Поиск целей</div> </div>						
<div> <div>Хосты</div> <div>Порты</div> <div>Топология</div> <div>Задачи</div> </div>						
<div> <div> <div>📄</div> <div>🔍</div> <div>📊</div> <div>🗃️</div> </div> </div>						
#	Адрес	Обновлено	Имя хоста	MAC-адрес	Операционная си...	Тип устройства
1	192.168.56.1	21.06.2023 17:46:25		0A:00:27:00:00:00		-
2	192.168.56.100	21.06.2023 17:46:31		08:00:27:84:7E:6D		-
3	192.168.56.102	21.06.2023 17:46:36		08:00:27:CF:44:E5	Linux 2.6.9 - 2.6.33	устройство общего на
4	192.168.56.103	21.06.2023 17:46:36			Linux 3.8 - 4.14	устройство общего на

25

👁️

1 из 1

«

<

1

>

»

Рисунок 7 – Хосты в сети

Добавим новую задачу и в расширенных настройках выберем определять версию сервисов (Рисунок 8). В результате на вкладке Порты увидим версии сервисов, работающих на этих портах, например, httpd 2.2.8 на порту 80 (Рисунок 9).

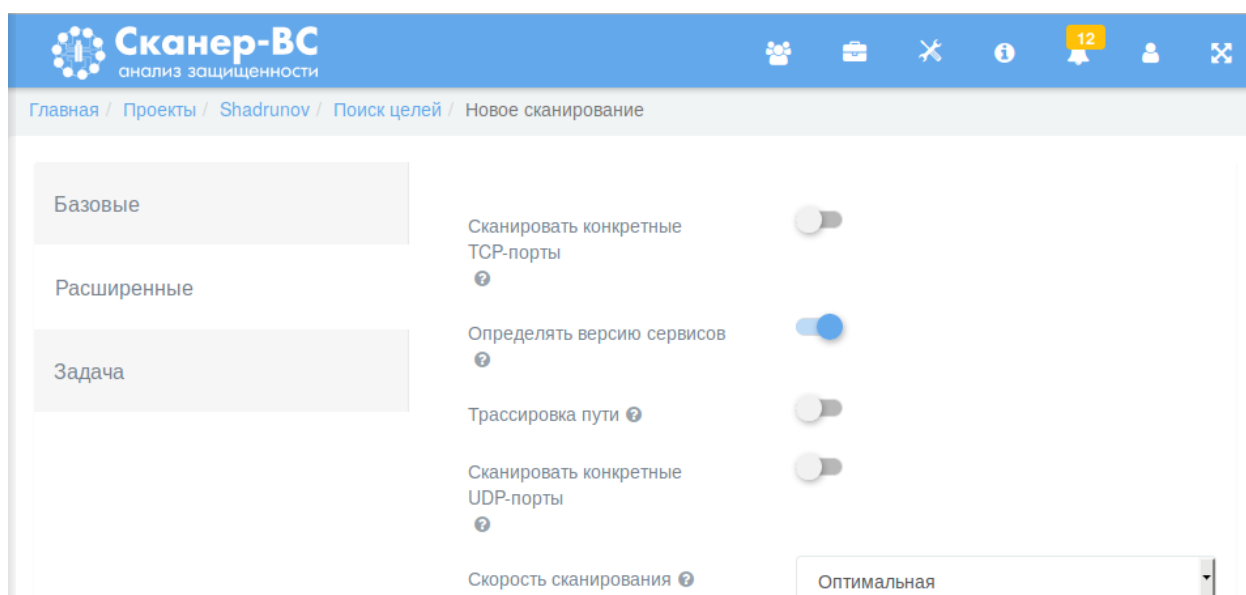


Рисунок 8 – Определять версию сервисов


<div> <div>  <div> <div>Сканер-ВС</div> <div>анализ защищенности</div> </div> </div> <div> <div> <div>👤</div> <div>📁</div> <div>✂</div> <div>ℹ</div> <div>🔔15</div> <div>👤</div> <div>✕</div> </div> </div> </div>								
<div> <div>Главная</div> / <div>Проекты</div> / <div>Shadrinov</div> / <div>Поиск целей</div> </div>								
<div> <div>Хосты</div> <div>Порты</div> <div>Топология</div> <div>Задачи</div> </div>								
<div> <div> <div>📄</div> <div>🔍</div> <div>📊</div> <div>🗖</div> </div> </div>								
#	Адрес	Протокол	Порт	Состояние	Обновлено	Сервис	Продукт	Версия
1	192.168.56.102	tcp	21	открыт	21.06.2023 17:48	ftp	vsftpd	2.3.4
2	192.168.56.102	tcp	22	открыт	21.06.2023 17:48	ssh	OpenSSH	4.7p1 Debian 8ub
3	192.168.56.102	tcp	23	открыт	21.06.2023 17:48	telnet	Linux telnetd	-
4	192.168.56.102	tcp	25	открыт	21.06.2023 17:48	smtp	Postfix smtpd	-
5	192.168.56.102	tcp	53	открыт	21.06.2023 17:48	domain	ISC BIND	9.4.2
6	192.168.56.102	tcp	80	открыт	21.06.2023 17:48	http	Apache httpd	2.2.8
7	192.168.56.102	tcp	111	открыт	21.06.2023 17:48	rpcbind	-	2
8	192.168.56.102	tcp	139	открыт	21.06.2023 17:48	netbios-ssn	Samba smbd	3.X - 4.X
9	192.168.56.102	tcp	445	открыт	21.06.2023 17:48	netbios-ssn	Samba smbd	3.X - 4.X
10	192.168.56.102	tcp	512	открыт	21.06.2023 17:48	exec	netkit-rsh rexecd	-
11	192.168.56.102	tcp	513	открыт	21.06.2023 17:48	login	OpenBSD or Sola	-
12	192.168.56.102	tcp	514	открыт	21.06.2023 17:48	shell	Netkit rshd	-
13	192.168.56.102	tcp	1099	открыт	21.06.2023 17:48	rmiregistry	GNU Classpath g	-
14	192.168.56.102	tcp	1524	открыт	21.06.2023 17:48	bindshell	Metasploitable ro	-
15	192.168.56.102	tcp	2049	открыт	21.06.2023 17:48	nfs	-	2-4
16	192.168.56.102	tcp	2121	открыт	21.06.2023 17:48	ftp	ProFTPD	1.3.1
17	192.168.56.102	tcp	3306	открыт	21.06.2023 17:48	mysql	MySQL	5.0.51a-3ubuntu5
18	192.168.56.102	tcp	5432	открыт	21.06.2023 17:48	postgresql	PostgreSQL DB	8.3.0 - 8.3.7
19	192.168.56.102	tcp	5900	открыт	21.06.2023 17:48	vnc	VNC	-

Рисунок 9 – Версии сервисов

Также добавим задачу на определение топологии сети. Для этого в расширенных настройках выберем трассировка пути (Рисунок 10). В результате на вкладке Топология появится топология нашей сети (Рисунок 11). В центре находится сканер, к нему подключен узел 192.168.56.102 (метасплойт), ещё устройства помечены пунктирной линией. Это DHCP-сервер гипервизора VirtualBox и хостовой адаптер.

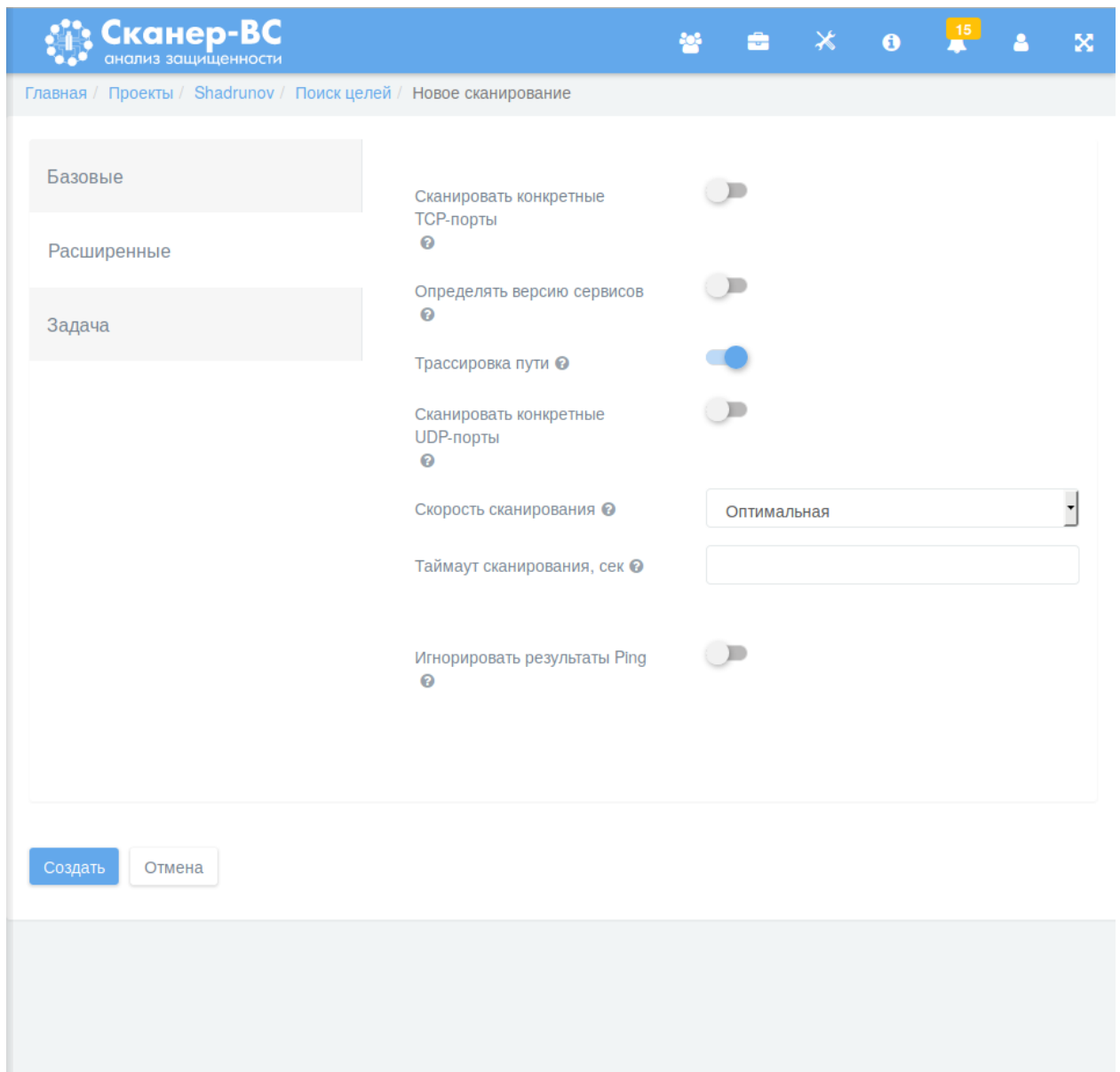


Рисунок 10 – Трассировка пути

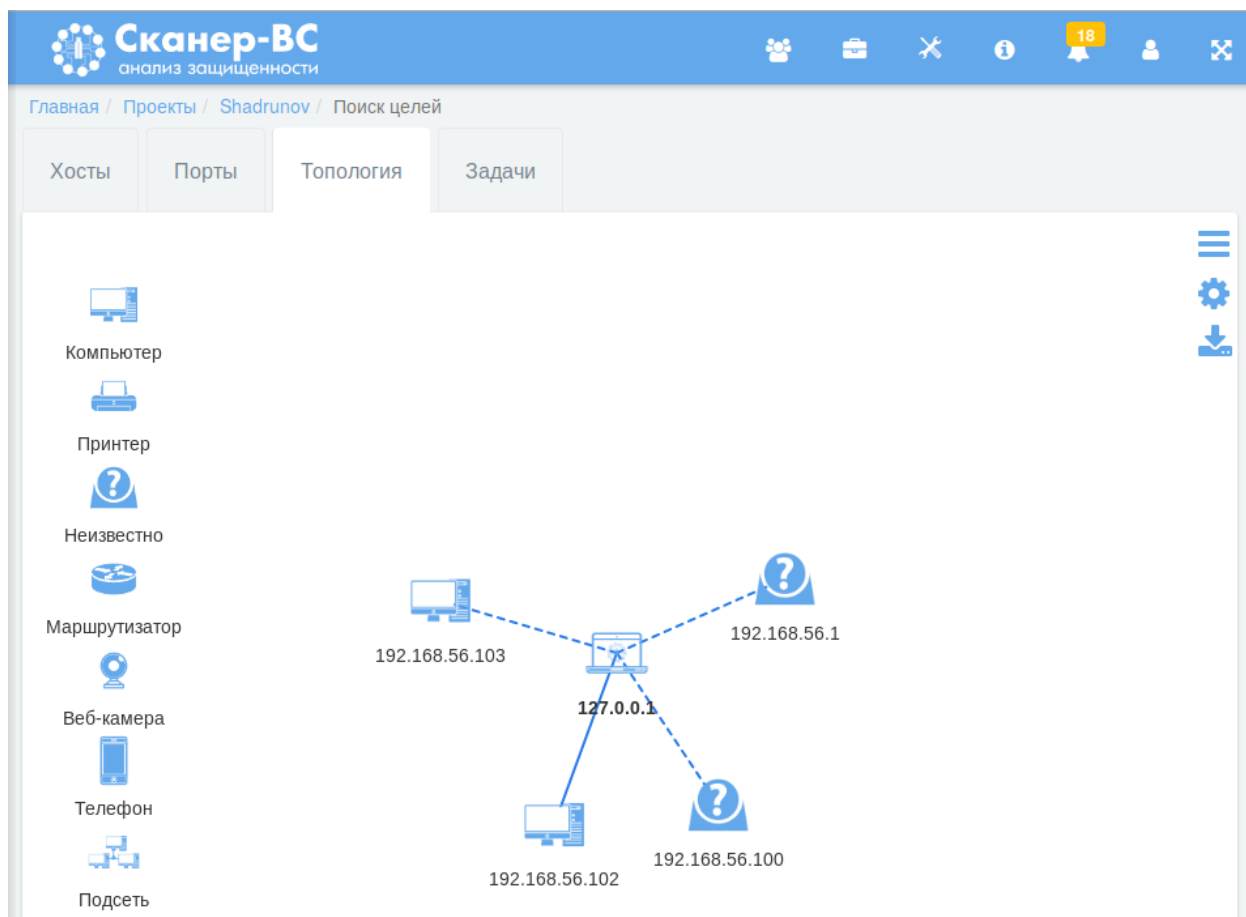


Рисунок 11 – Топология сети

2.3 Лабораторная работа 2. Поиск уязвимостей

В этой работе изучим принцип работы сканеров безопасности. Для этого перейдём на панель Поиск уязвимостей (Рисунок 12). Создадим новую задачу и выберем цель из активов, оставшихся от предыдущего сканирования (Рисунок 13).

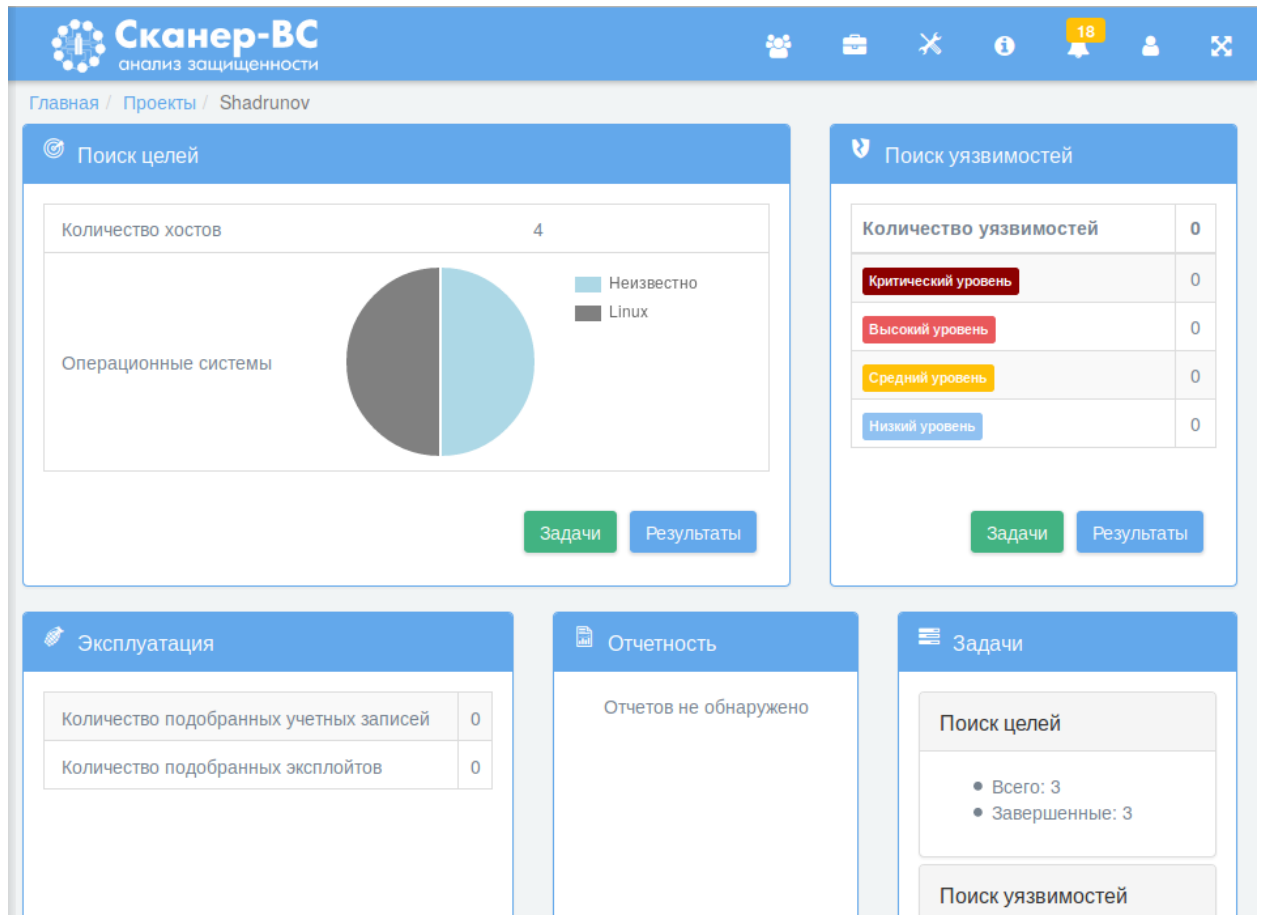


Рисунок 12 – Поиск уязвимостей

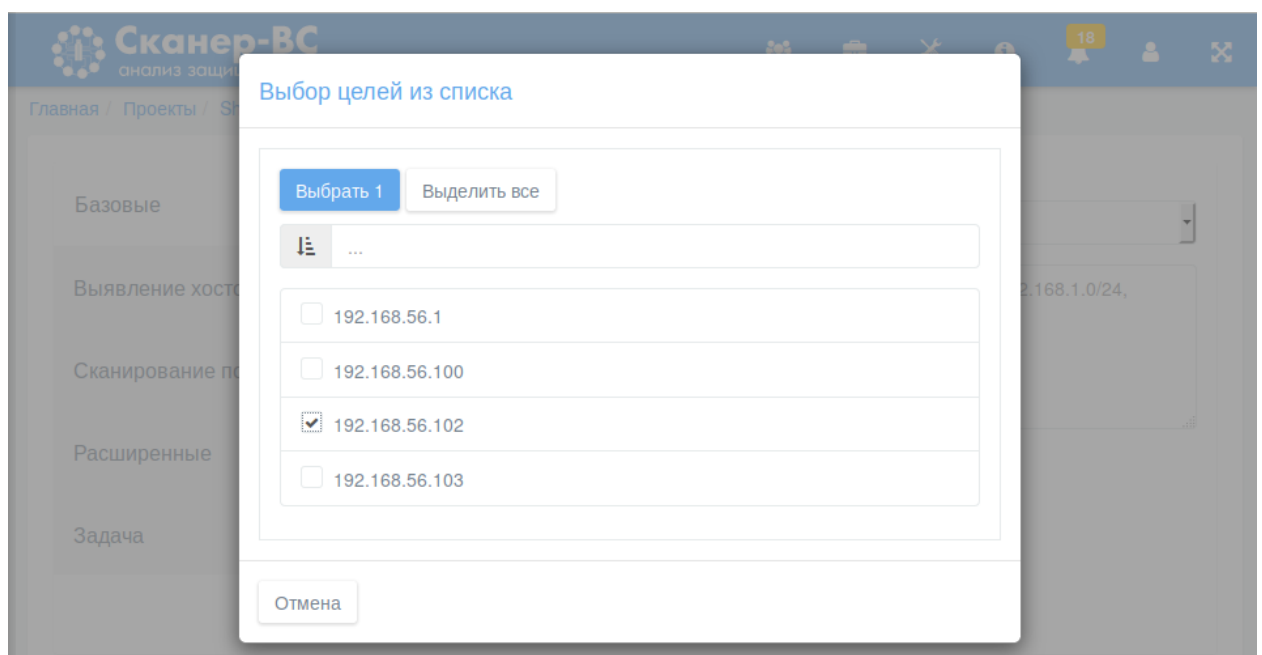
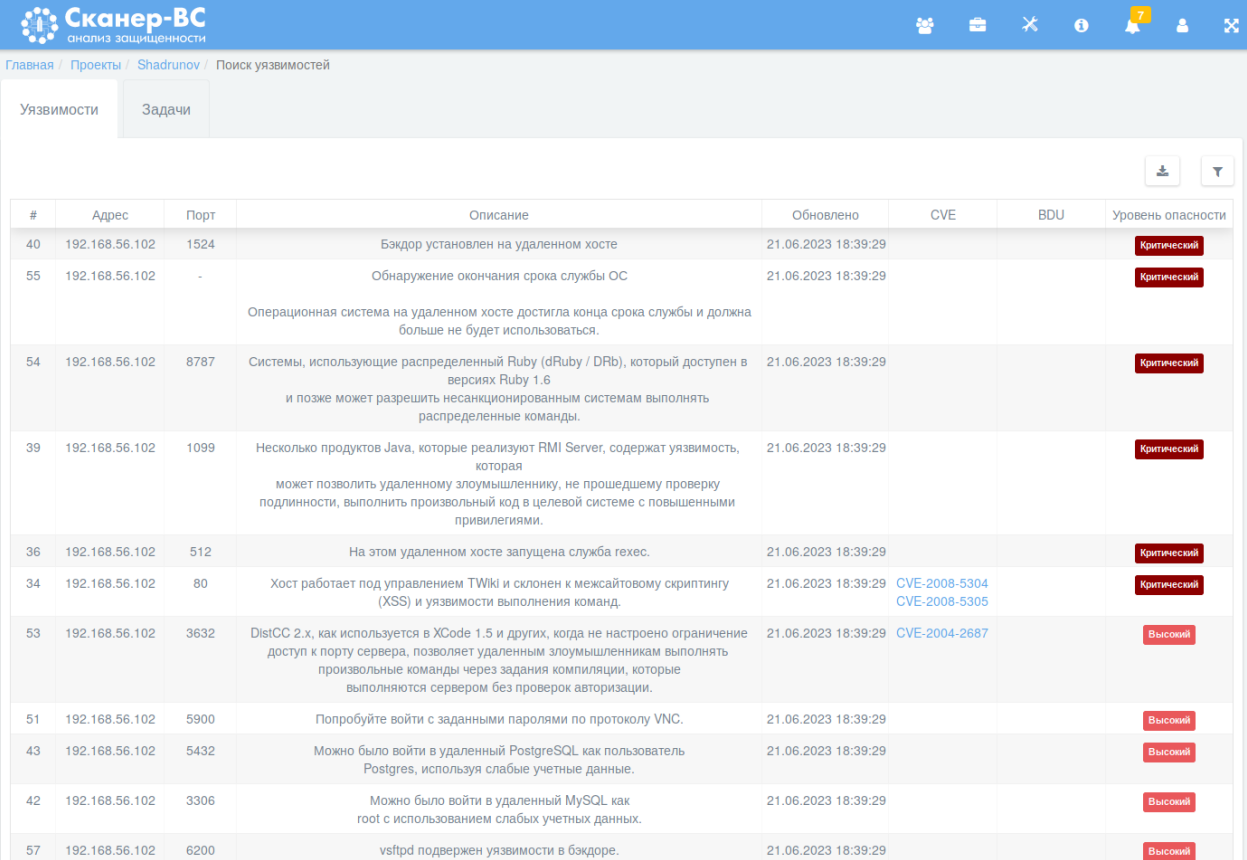


Рисунок 13 – Выбор целей из активов

Запустим задачу и подождём некоторое время, пока сканирование завершится. После этого на вкладке Уязвимости появится список найденных на сервере уязвимостей с указанием их критичности (Рисунок 14).



#	Адрес	Порт	Описание	Обновлено	CVE	BDU	Уровень опасности
40	192.168.56.102	1524	Бэkdор установлен на удаленном хосте	21.06.2023 18:39:29			Критический
55	192.168.56.102	-	Обнаружение окончания срока службы ОС Операционная система на удаленном хосте достигла конца срока службы и должна больше не будет использоваться.	21.06.2023 18:39:29			Критический
54	192.168.56.102	8787	Системы, использующие распределенный Ruby (dRuby / DRb), который доступен в версиях Ruby 1.6 и позже может разрешить несанкционированным системам выполнять распределенные команды.	21.06.2023 18:39:29			Критический
39	192.168.56.102	1099	Несколько продуктов Java, которые реализуют RMI Server, содержат уязвимость, которая может позволить удаленному злоумышленнику, не прошедшему проверку подлинности, выполнить произвольный код в целевой системе с повышенными привилегиями.	21.06.2023 18:39:29			Критический
36	192.168.56.102	512	На этом удаленном хосте запущена служба gexes.	21.06.2023 18:39:29			Критический
34	192.168.56.102	80	Хост работает под управлением TWiki и склонен к межсайтовому скриптингу (XSS) и уязвимости выполнения команд.	21.06.2023 18:39:29	CVE-2008-5304 CVE-2008-5305		Критический
53	192.168.56.102	3632	DistCC 2.x, как используется в XCode 1.5 и других, когда не настроено ограничение доступ к порту сервера, позволяет удаленным злоумышленникам выполнять произвольные команды через задания компиляции, которые выполняются сервером без проверок авторизации.	21.06.2023 18:39:29	CVE-2004-2687		Высокий
51	192.168.56.102	5900	Попробуйте войти с заданными паролями по протоколу VNC.	21.06.2023 18:39:29			Высокий
43	192.168.56.102	5432	Можно было войти в удаленный PostgreSQL как пользователь Postgres, используя слабые учетные данные.	21.06.2023 18:39:29			Высокий
42	192.168.56.102	3306	Можно было войти в удаленный MySQL как root с использованием слабых учетных данных.	21.06.2023 18:39:29			Высокий
57	192.168.56.102	6200	vsftpd подвержен уязвимости в бэkdоре.	21.06.2023 18:39:29			Высокий

Рисунок 14 – Уязвимости

2.4 Лабораторная работа 3. Сетевой аудит паролей

В этой работе проведём сетевой аудит паролей Metasploitable 2. Для этого перейдём на панель Эксплуатация (Рисунок 15). Создадим новую задачу и выберем цель из активов, оставшихся от предыдущего сканирования. Выберем сервис, который будет сканироваться, — ftp (Рисунок 16).

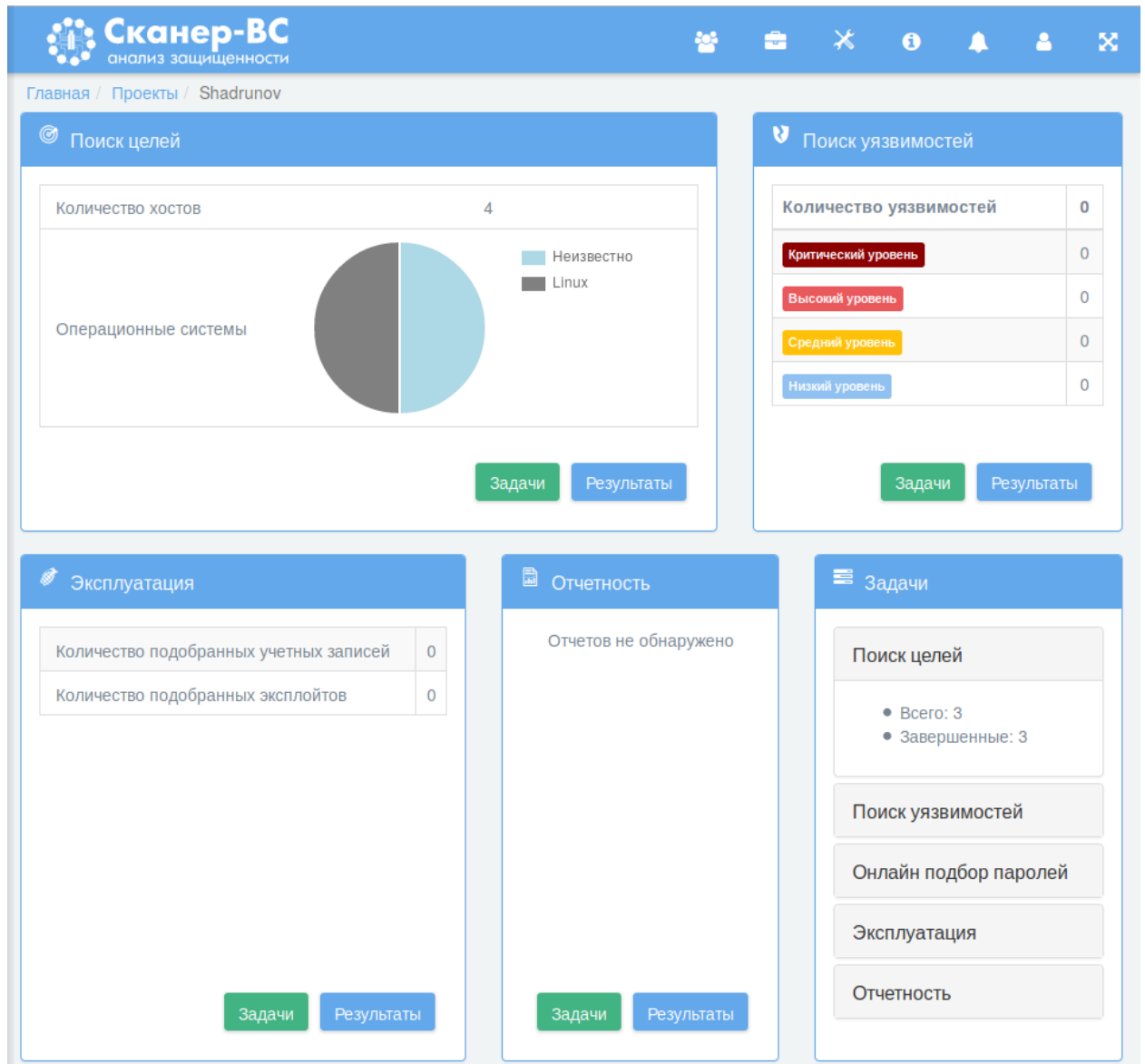


Рисунок 15 – Эксплуатация

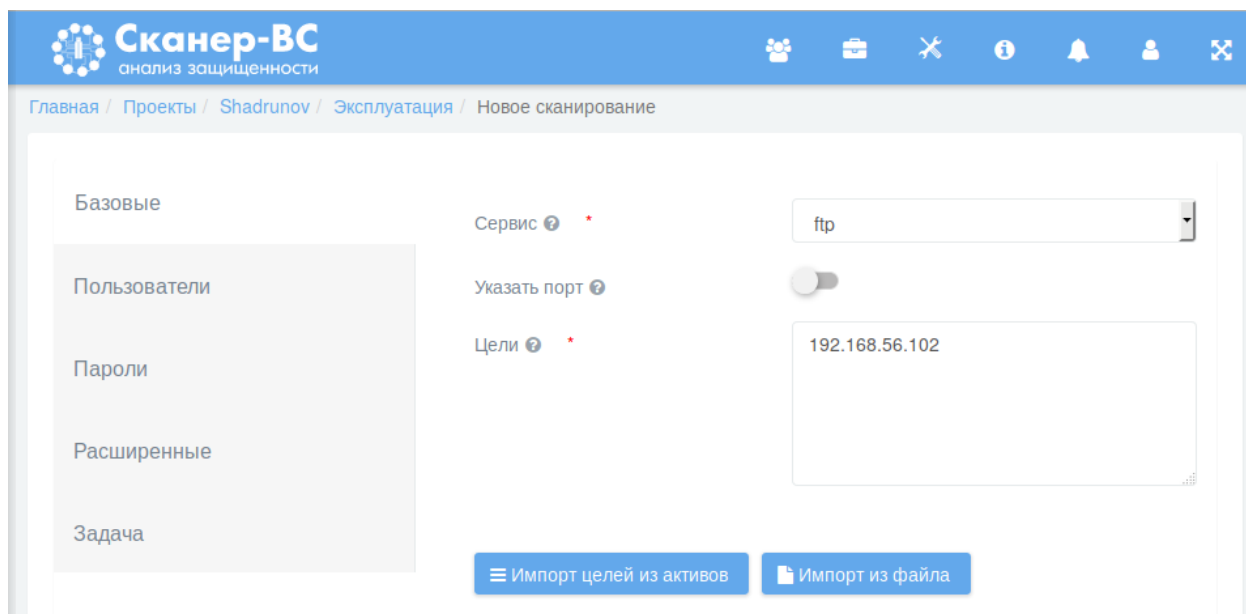


Рисунок 16 – Выбор сервиса ftp

Добавим юзернеймы и пароли в соответствующих вкладках (Рисунки 17-18).

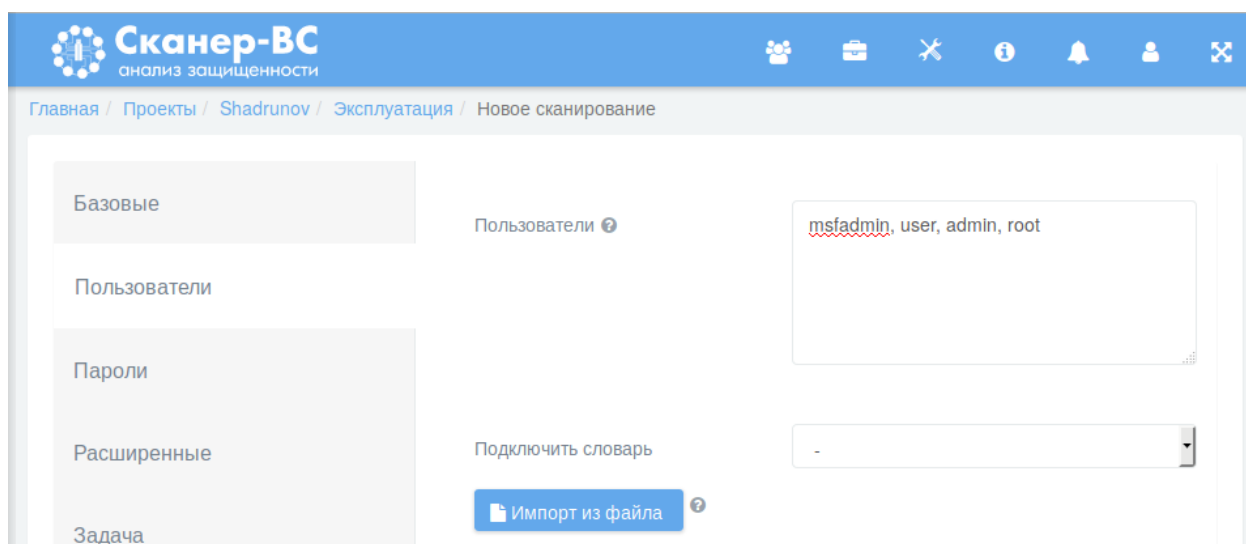


Рисунок 17 – Добавляем пользователей

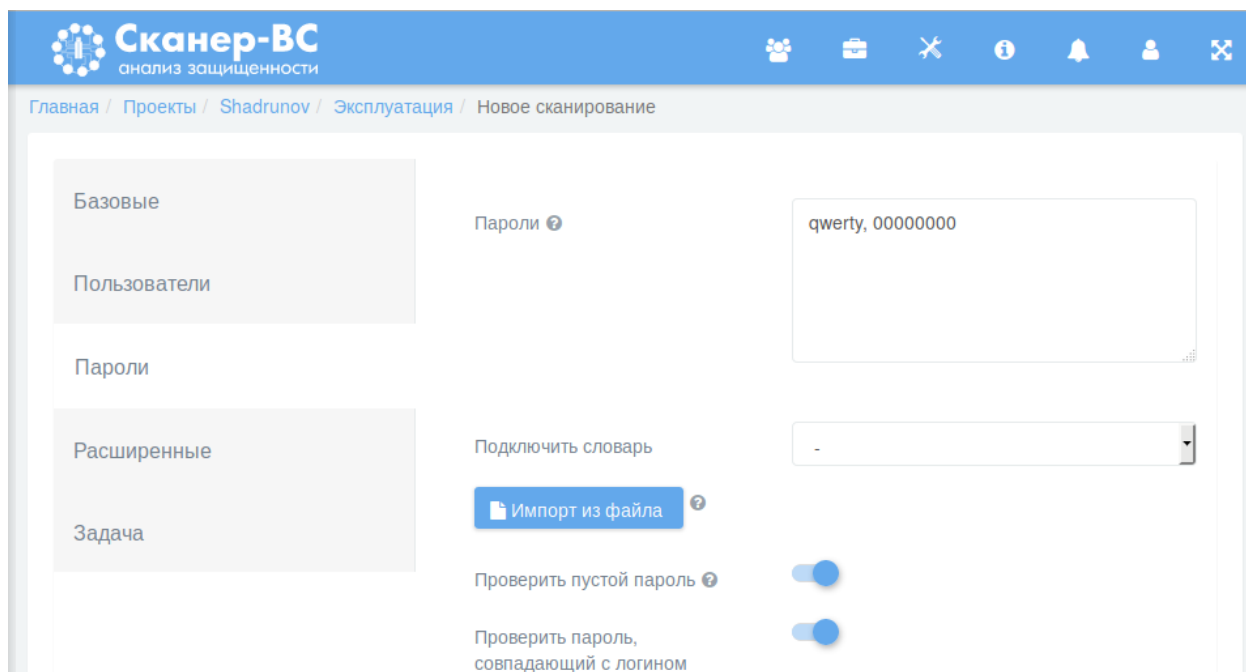


Рисунок 18 – Добавляем пароли

По завершению задачи (Рисунок 19) перейдём на вкладку Сетевой аудит паролей (Рисунок 20). Видим, что система подобрала пароли для сервиса ftp, этот сервис является уязвимостью для метаспллойта.

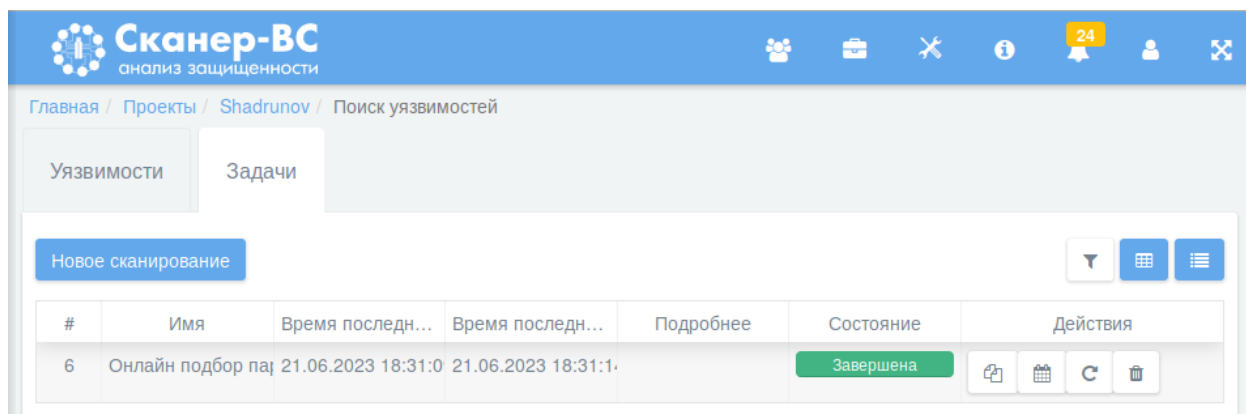


Рисунок 19 – Задача завершена

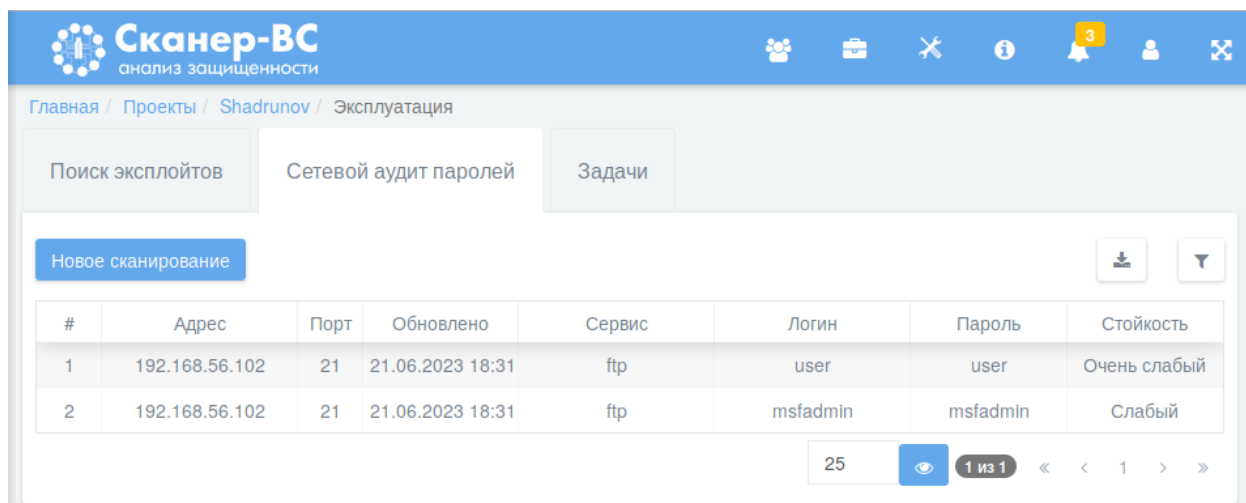


Рисунок 20 – Сетевой аудит паролей

Аналогично просканируем сервис smb (Рисунок 21). Сканирование отработало, однако новые пароли не отобразились на вкладке Сетевой аудит паролей. Это значит, что подобрать пароли к сервису smb не получилось.

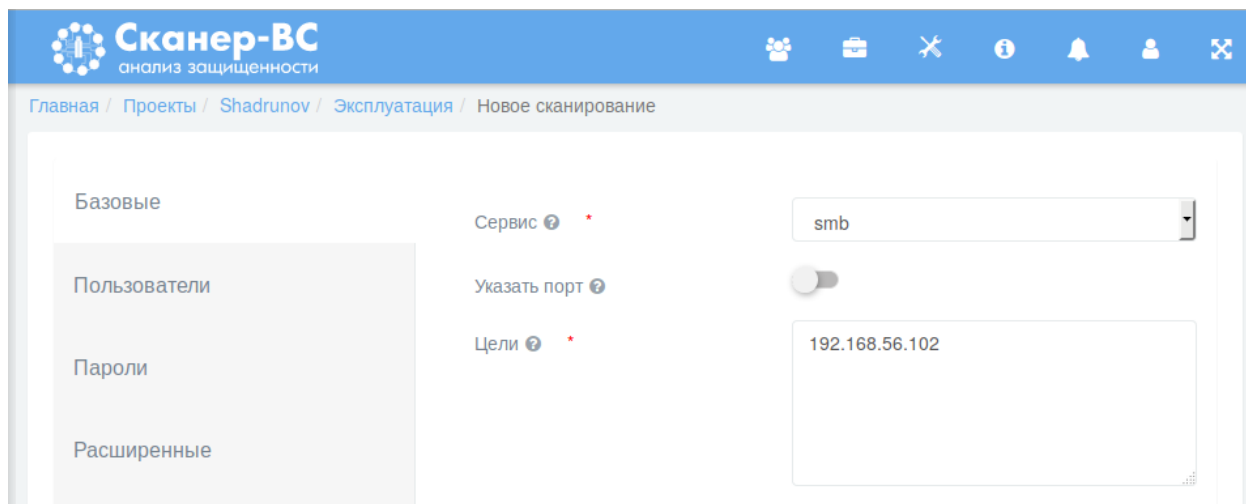


Рисунок 21 – Задача завершена

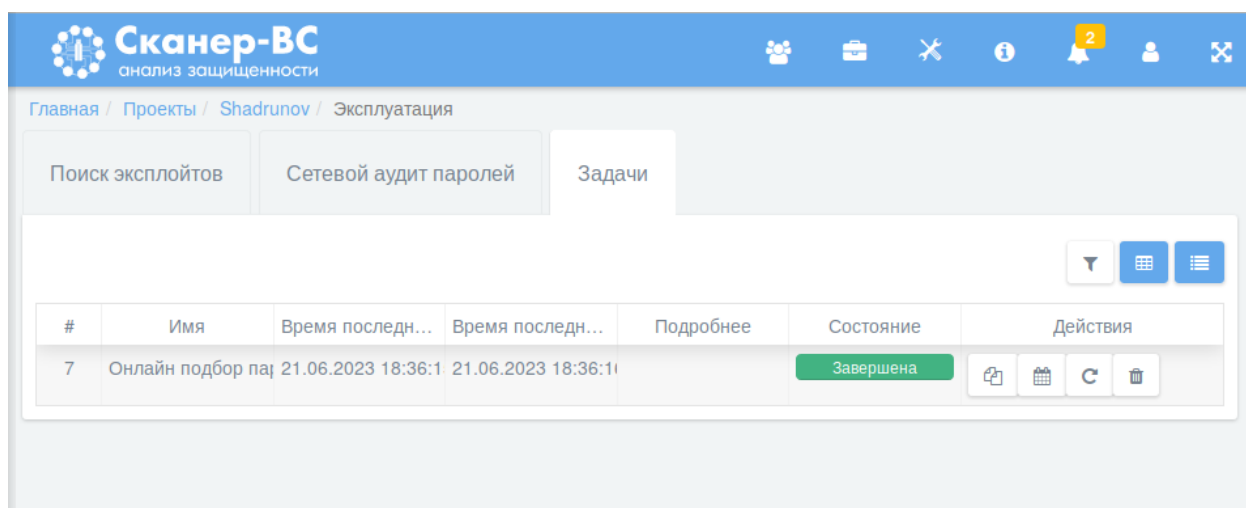


Рисунок 22 – Сетевой аудит паролей - smb

2.5 Лабораторная работа 4. Поиск подходящих эксплойтов

В этой работе научимся использовать веб-интерфейс Сканер-ВС для поиска эксплойтов. Для этого перейдем на панель Эксплуатация (Рисунок 23). Создадим новое сканирование на вкладке Поиск эксплойтов (Рисунок 24). Выберем тип сканирования (Рисунок 25). Результат отобразится на вкладке Поиск эксплойтов (Рисунок 26)

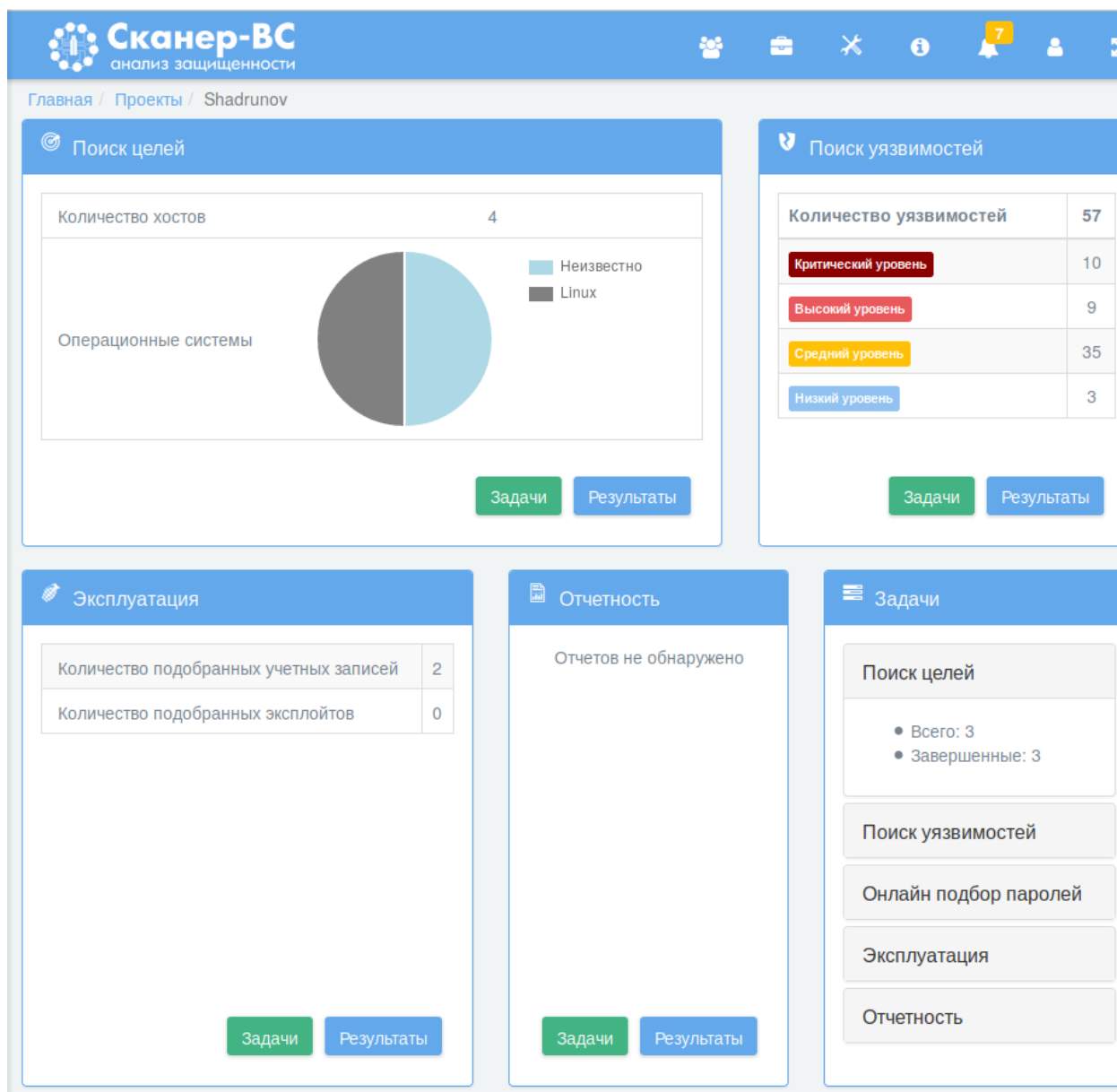


Рисунок 23 – Эксплуатация

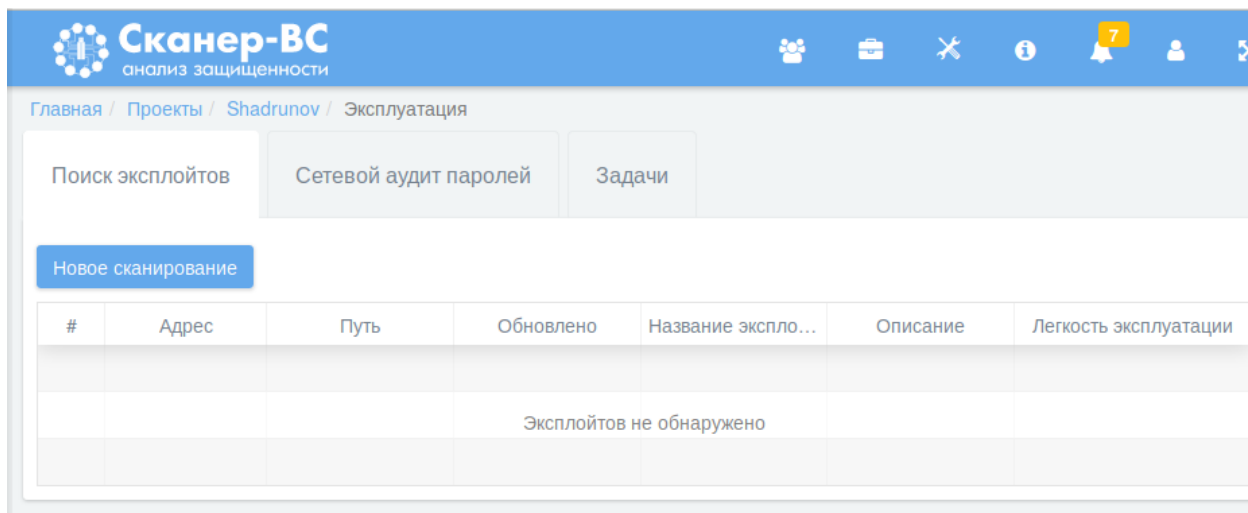


Рисунок 24 – Поиск эксплойтов

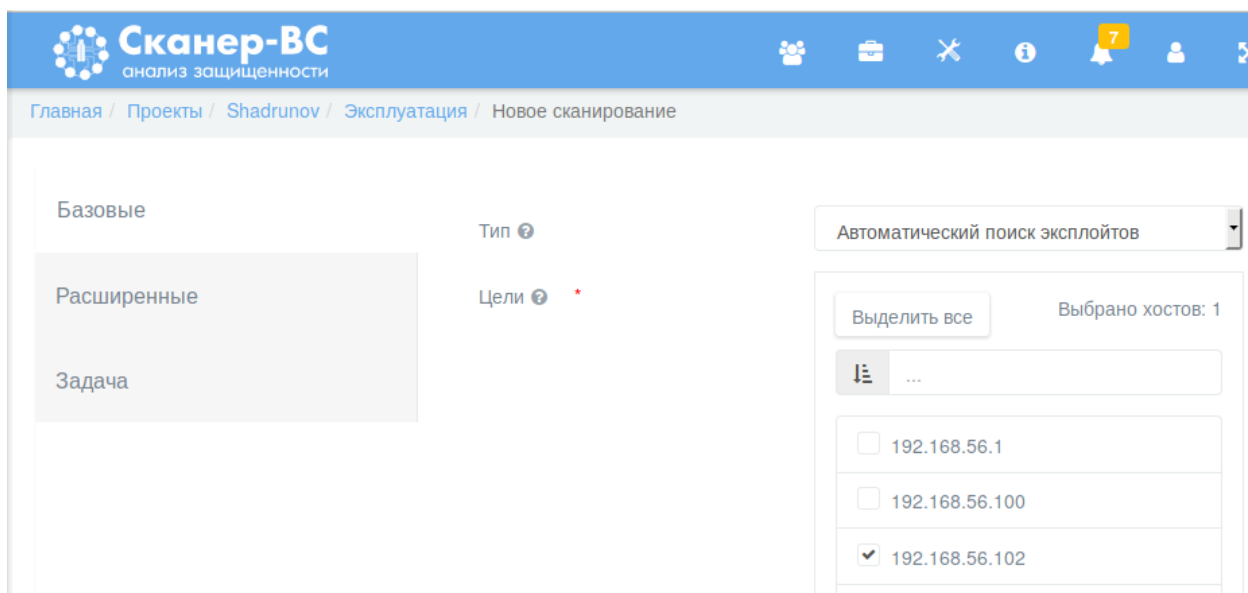


Рисунок 25 – Выбираем цель

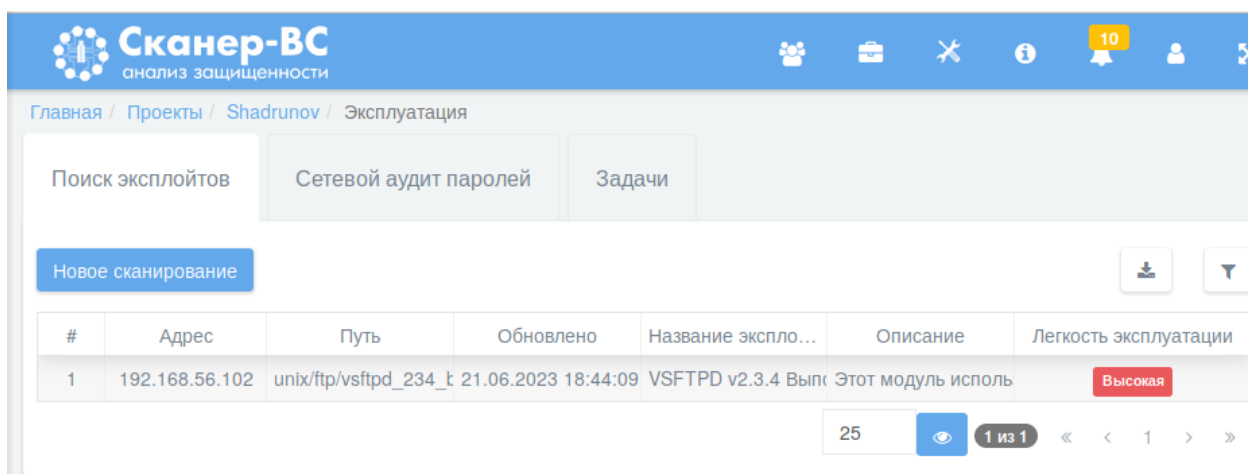


Рисунок 26 – Результаты

Создадим отчёт. Для этого откроем вкладку Отчёты и создадим задачу. Выберем полный отчёт и скачаем его в формате PDF (Рисунки 27-29). Некоторые страницы

отчёта приведены в приложении А.

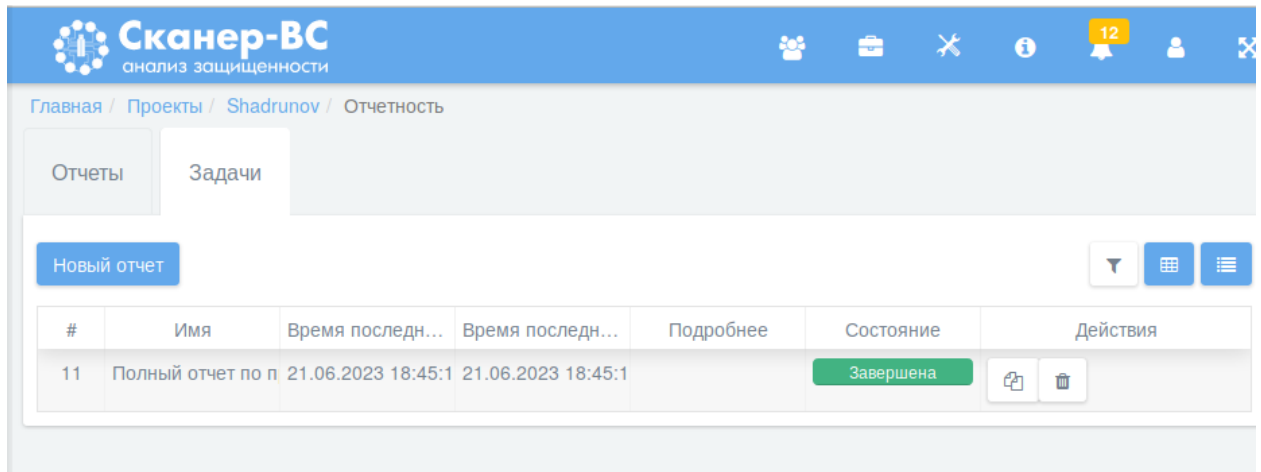


Рисунок 27 – Создаём отчёт

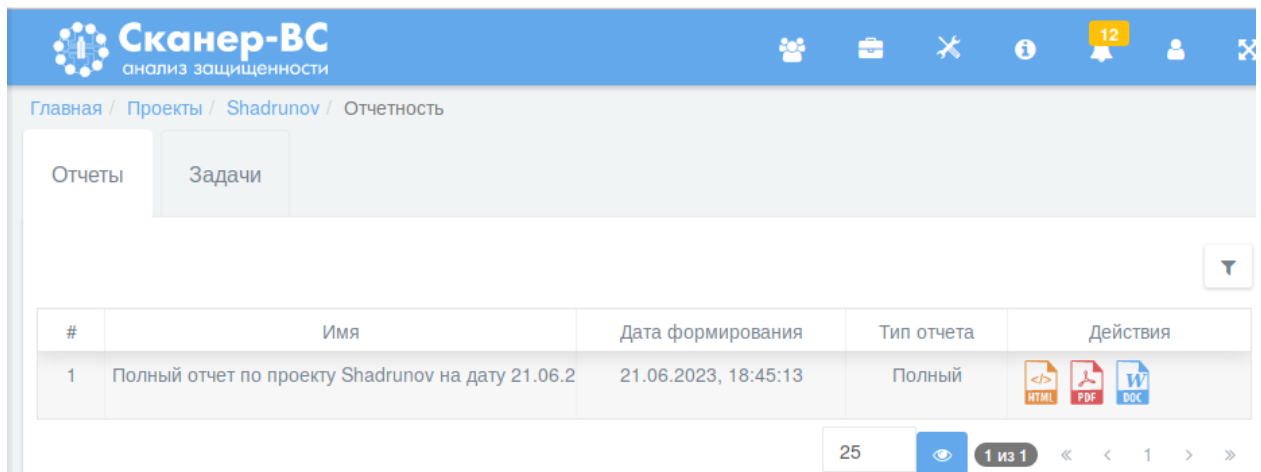


Рисунок 28 – Отчёт можно скачать в разных форматах

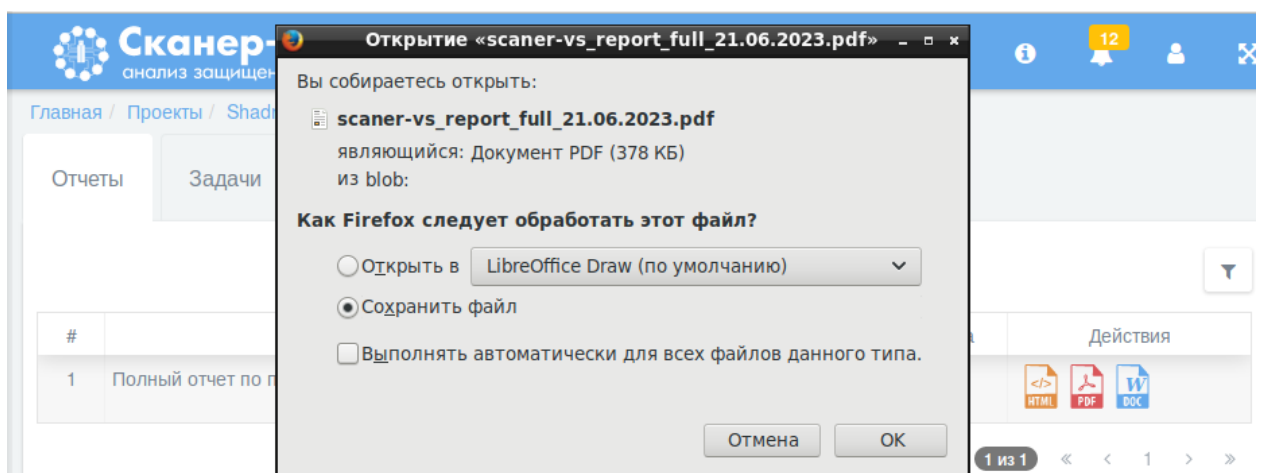


Рисунок 29 – Скачиваем отчёт

3 Выводы о проделанной работе

Я освоил основы работу со сканером уязвимостей Сканер-ВС, изучил уязвимости в системе метасплloit с использованием активных и пассивных методов.



Полный отчет по проекту "Shadrunov"
на
21.06.2023 18:45:40.



Сканер-ВС
анализ защищенности

Владелец лицензии: Для вузов (Не для коммерческого использования)
Продукт: Сканер-ВС v.5-1.0.7
Лицензия №500000001 истекает 09.01.2022
Программное обеспечение: © 2018 АО "НПО "Эшелон" <http://npo-echelon.ru>
Контакты службы технической поддержки: support.sca@cnpo.ru

Оглавление

1. Резюме для руководителя	4
2. Границы проекта	5
3. Хост 192.168.56.1	5
4. Хост 192.168.56.100	6
5. Хост 192.168.56.102	6
5.1. Порты и сервисы	6
5.2. Уязвимости	7
5.2.1. Анонимная отчетность по FTP	7
5.2.2. FTP незашифрованный открытый текст	7
5.2.3. Скомпрометированные исходные пакеты vsftpd Уязвимость бэкдора	7
5.2.4. SSH Brute Force Logins с отчетами по умолчанию для учетных данных	8
5.2.5. Поддерживаются слабые алгоритмы шифрования SSH	8
5.2.6. Поддерживаются слабые алгоритмы MAC SSH	8
5.2.7. Telnet незашифрованный открытый текст	8
5.2.8. Проверьте, отвечает ли почтовый сервер на запросы VRFY и EXPN	8
5.2.9. Многочисленные поставщики Реализация STARTTLS, связанная с незащищенным вводом произвольных команд	9
5.2.10. SSL / TLS: уязвимость DHE_EXPORT, связанная с обходом среднего уровня безопасности (LogJam)	9
5.2.11. SSL / TLS: срок действия сертификата истек	10
5.2.12. SSL / TLS: сертификат подписан с использованием алгоритма слабой подписи	10
5.2.13. SSL / TLS: устарело обнаружение протоколов SSLv2 и SSLv3	10
5.2.14. SSL / TLS: обмен ключами Диффи-Хеллмана недостаточная уязвимость группы DH	11
5.2.15. SSL / TLS: проблема понижения RSA_EXPORT при обработке временного ключа RSA (FREAK)	11
5.2.16. SSL / TLS: Уязвимость CBC Cipher Suite, распространяемая по протоколу SSLv3 (POODLE)	11
5.2.17. / doc каталог с возможностью просмотра	12
5.2.18. Уязвимость HTTP-сервера Apache 'httpOnly', приводящая к раскрытию информации о файлах cookie	12
5.2.19. Многочисленные локальные файлы awiki включают уязвимости	12
5.2.20. Открытый текст Передача конфиденциальной информации через HTTP	13
5.2.21. Методы отладки HTTP (TRACE / TRACK) включены	13
5.2.22. Уязвимость в PHP-CGI-настройках при разборе параметров строки запроса из файлов php.	13
5.2.23. Отчет о выводе phpinfo ()	14
5.2.24. phpMyAdmin 'error.php' Уязвимость межсайтового скриптинга	14
5.2.25. Проверка HTTP опасных методов	14
5.2.26. Уязвимость Tiki Wiki CMS Groupware 'fixedURLData', связанная с локальным включением файлов	14
5.2.27. Tiki Wiki CMS Groupware <17.2 Уязвимость SQL-инъекций	15
5.2.28. Tiki Wiki CMS Groupware <4.2 Многочисленные неучтенные уязвимости	15
5.2.29. Уязвимость Tiki Wiki CMS, связанная с вводом данных из-за недостатка санитарии	15
5.2.30. Уязвимость Tiki Wiki CMS Groupware XSS	16
5.2.31. Уязвимость TWiki <6.1.0 XSS	16
5.2.32. Уязвимость TWiki, связанная с подделкой запросов	16
5.2.33. Уязвимость межсайтового запроса TWiki - 10 сентября	16
5.2.34. Уязвимости TWiki XSS и выполнения команд	17
5.2.35. Уязвимость удаленной командной оболочки Samba MS-RPC, связанная с выполнением команд (активная проверка)	17
5.2.36. hexec без пароля / незашифрованный открытый текст	17
5.2.37. rlogin Пароль без пароля / незашифрованный открытый текст	18
5.2.38. rsh незашифрованный открытый текст	18
5.2.39. Небезопасная конфигурация Java RMI Server Уязвимость удаленного выполнения кода	18
5.2.40. Возможный Бэкдор: Ingreslock	18
5.2.41. FTP незашифрованный открытый текст	18
5.2.42. Слабый пароль MySQL / MariaDB	19
5.2.43. Слабый пароль PostgreSQL	19
5.2.44. SSL / TLS: срок действия сертификата истек	19
5.2.45. SSL / TLS: сертификат подписан с использованием алгоритма слабой подписи	19
5.2.46. SSL / TLS: устарело обнаружение протоколов SSLv2 и SSLv3	19

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканиер-BC

5.2.47. SSL / TLS: обмен ключами Диффи-Хеллмана недостаточная уязвимость группы DH	20
5.2.48. SSL / TLS: уязвимость OpenSSL CCS Man in Middle Security Bypass	20
5.2.49. SSL / TLS: сообщить о слабых комплектах шифров	21
5.2.50. SSL / TLS: Уязвимость CBC Cipher Suite, распространяемая по протоколу SSLv3 (POODLE)	21
5.2.51. VNC Brute Force Войти	22
5.2.52. VNC-сервер незашифрованная передача данных	22
5.2.53. Уязвимость DistCC, делающая возможным удаленное выполнение кода	22
5.2.54. Многочисленные уязвимости в распределенном Ruby (dRuby / DRb), делающие возможным удаленное выполнение кода	22
5.2.55. Обнаружение окончания срока службы ОС	23
5.2.56. Временные метки TCP	23
5.2.57. Скомпрометированные исходные пакеты vsftpd Уязвимость бэкдора	23
5.3. Скомпрометированные учетные данные	24
5.4. Эксплойты	24
6. Хост 192.168.56.103	24
6.1. Порты и сервисы	24

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканиер-BC

Операционная система: -
 MAC-адрес: 0A:00:27:00:00:00
 Тип устройства: -
 Уязвимостей не обнаружено

4. Хост 192.168.56.100

Операционная система: -
 MAC-адрес: 08:00:27:84:7E:6D
 Тип устройства: -
 Уязвимостей не обнаружено

5. Хост 192.168.56.102

Операционная система: Linux 2.6.9 - 2.6.33
 MAC-адрес: 08:00:27:CF:44:E5
 Тип устройства: устройство общего назначения

5.1. Порты и сервисы

№ п/п	Порт	Состояние	Сервис	Продукт	Версия
1	21/tcp	open	ftp	vsftpd	2.3.4
2	22/tcp	open	ssh	OpenSSH	4.7p1 Debian 8ubuntu1
3	23/tcp	open	telnet	Linux telnetd	
4	25/tcp	open	smtp	Postfix smtpd	
5	53/tcp	open	domain	ISC BIND	9.4.2
6	80/tcp	open	http	Apache httpd	2.2.8
7	111/tcp	open	rpcbind		
8	139/tcp	open	netbios-ssn	Samba smbd	3.X - 4.X
9	445/tcp	open	microsoft-ds		
10	512/tcp	open	exec	netkit-rsh rexecd	
11	513/tcp	open	login	OpenBSD or Solaris rlogind	
12	514/tcp	open	shell	Netkit rshd	
13	1099/tcp	open	rmiregistry	GNU Classpath grmiregistry	
14	1524/tcp	open	ingreslock		
15	2049/tcp	open	nfs		
16	2121/tcp	open	ccproxy-ftp		

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканер-ВС

№ п/п	Порт	Состояние	Сервис	Продукт	Версия
17	3306/tcp	open	mysql	MySQL	5.0.51a-3ubuntu5
18	5432/tcp	open	postgresql	PostgreSQL DB	8.3.0 - 8.3.7
19	5900/tcp	open	vnc	VNC	
20	6000/tcp	open	X11		
21	6667/tcp	open	irc	UnrealIRCd	
22	8009/tcp	open	ajp13	Apache Jserv	
23	8180/tcp	open	unknown		
24	3632/tcp	open	-		
25	8787/tcp	open	-		
26	6200/tcp	open	-		

5.2. Уязвимости

Анонимная отчетность по FTP

Уровень опасности: Средний

CVSS 2.0: 6.4

Порт: 21/tcp

Описание: Сообщает, разрешает ли удаленный FTP-сервер анонимный вход.

Вектор CVSS 2.0: AV:N/AC:L/Au:N/C:P/I:P/A:N

Рекомендации: Если вы не хотите делиться файлами, вы должны отключить анонимный вход.

Подробнее:

- <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

FTP незашифрованный открытый текст

Уровень опасности: Средний

CVSS 2.0: 4.8

Порт: 21/tcp

Описание: На удаленном хосте запущена служба FTP, которая позволяет входить в систему открытым текстом через незашифрованные соединения.

Вектор CVSS 2.0: AV:A/AC:L/Au:N/C:P/I:P/A:N

Рекомендации: Включите FTPS или установите соединение с помощью команды «AUTH TLS». Посмотри пожалуйста Руководство службы FTP для получения дополнительной информации.

Скомпрометированные исходные пакеты vsftpd Уязвимость бэкдора

Уровень опасности: Высокий

CVSS 2.0: 7.5

Порт: 21/tcp

Описание: vsftpd подвержен уязвимости в бэкдоре.

Вектор CVSS 2.0: AV:N/AC:L/Au:N/C:P/I:P/A:P

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканиер-BC

Рекомендации: Отремонтированный пакет можно скачать с [Ссылочная ссылка](#). Пожалуйста, подтвердите пакет с его подписью.

Подробнее:

- <http://www.securityfocus.com/bid/48539>
- <http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>
- <https://security.appspot.com/vsftpd.html>

SSH Brute Force Logins с отчетами по умолчанию для учетных данных

Уровень опасности: Высокий

CVSS 2.0: 7.5

Порт: 22/tcp

Описание: Можно было войти на удаленный SSH-сервер, используя учетные данные по умолчанию. Поскольку NVT «SSH Brute Force Logins с учетными данными по умолчанию» (OID: 1.3.6.1.4.1.25623.1.0.108013) может столкнуться с тайм-аут фактическое сообщение об этой уязвимости происходит в этом NVT вместо этого. Настройка сценария «Время ожидания отчета» позволяет настроить, если сообщается о таком тайм-ауте.

Вектор CVSS 2.0: AV:N/AC:L/Au:N/C:P/I:P/A:P

Рекомендации: Измените пароль как можно скорее.

Поддерживаются слабые алгоритмы шифрования SSH

Уровень опасности: Средний

CVSS 2.0: 4.3

Порт: 22/tcp

Описание: Удаленный сервер SSH настроен на использование слабых алгоритмов шифрования.

Вектор CVSS 2.0: AV:N/AC:M/Au:N/C:P/I:N/A:N

Рекомендации: Отключите слабые алгоритмы шифрования.

Подробнее:

- <https://tools.ietf.org/html/rfc4253#section-6.3>
- <https://www.kb.cert.org/vuls/id/958563>

Поддерживаются слабые алгоритмы MAC SSH

Уровень опасности: Низкий

CVSS 2.0: 2.6

Порт: 22/tcp

Описание: Удаленный SSH-сервер настроен на использование слабых алгоритмов MD5 и / или 96-битных MAC.

Вектор CVSS 2.0: AV:N/AC:H/Au:N/C:P/I:N/A:N

Рекомендации: Отключите слабые алгоритмы MAC.

Telnet незашифрованный открытый текст

Уровень опасности: Средний

CVSS 2.0: 4.8

Порт: 23/tcp

Описание: На удаленном хосте запущена служба Telnet, которая позволяет входить в систему открытым текстом через незашифрованные соединения.

Вектор CVSS 2.0: AV:A/AC:L/Au:N/C:P/I:P/A:N

Рекомендации: Замените Telnet протоколом, подобным SSH, который поддерживает зашифрованные соединения.

Проверьте, отвечает ли почтовый сервер на запросы VRFY и EXPN

Уровень опасности: Средний

CVSS 2.0: 5

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.08.2023

Автор:

Администратор Сканиер-ВС

Порт: 25/tcp

Описание: Почтовый сервер на этом хосте отвечает на запросы VRFY и / или EXPN.

Вектор CVSS 2.0: AV:N/AC:L/Au:N/C:N/I:N/A:P

Рекомендации: Отключите VRFY и / или EXPN на своем почтовом сервере. Для postfix добавьте «disable_vrfy_command = yes» в «main.cf». Для Sendmail добавьте опцию «O PrivacyOptions = goaway». Предполагается, что, если вы действительно хотите публиковать информацию такого типа, вы используете механизм о которых действительно знают законные пользователи, такие как Finger или HTTP.

Подробнее:

- <http://cr.yp.to/smtp/vrfy.html>

Многочисленные поставщики Реализация STARTTLS, связанная с незащищенным вводом произвольных команд

Уровень опасности: Средний

CVSS 2.0: 6.8

Порт: 25/tcp

Описание: Реализации STARTTLS от нескольких поставщиков подвержены уязвимости, позволяющая злоумышленникам вводить произвольные команды.

CVE: [CVE-2011-0411](#), [CVE-2011-1430](#), [CVE-2011-1431](#), [CVE-2011-1432](#), [CVE-2011-1506](#), [CVE-2011-1575](#), [CVE-2011-1926](#), [CVE-2011-2165](#),

Вектор CVSS 2.0: AV:N/AC:M/Au:N/C:P/I:P/A:P

Рекомендации: Обновления доступны. Пожалуйста, смотрите ссылки для получения дополнительной информации.

Подробнее:

- <http://www.securityfocus.com/bid/46767>
- <http://kolab.org/pipermail/kolab-announce/2011/000101.html>
- http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
- http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
- <http://www.kb.cert.org/vuls/id/MAPG-8D9M4P>
- <http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt>
- <http://www.postfix.org/CVE-2011-0411.html>
- <http://www.pureftpd.org/project/pure-ftpd/news>
- http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
- <http://www.spamdyke.org/documentation/Changelog.txt>
- http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1
- <http://www.securityfocus.com/archive/1/516901>
- <http://support.avaya.com/css/P8/documents/100134676>
- <http://support.avaya.com/css/P8/documents/100141041>
- <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>
- <http://inoa.net/qmail-tls/vu555316.patch>
- <http://www.kb.cert.org/vuls/id/555316>

SSL / TLS: уязвимость DHE_EXPORT, связанная с обходом среднего уровня безопасности (LogJam)

Уровень опасности: Низкий

CVSS 2.0: 4.3

CVSS 3.0: 3.7

Порт: 25/tcp

Описание: Этот хост принимает наборы шифров DHE_EXPORT и склонен к человеку в середине атаки.

CVE: [CVE-2015-4000](#),

BDU: [BDU:2015-11042](#),

Вектор CVSS 2.0: AV:N/AC:M/Au:N/C:N/I:P/A:N

Вектор CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканиер-BC

Рекомендации: - Удалить поддержку для шифра DHE_EXPORT люксы из сервиса - Если запущено обновление OpenSSL до версии 1.0.2b или 1.0.1n или новее.

Подробнее:

- <https://weakdh.org>
- <https://weakdh.org/imperfect-forward-secrecy.pdf>
- <http://openwall.com/lists/oss-security/2015/05/20/8>
- <https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained>
- <https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes>
- <http://www.bdu.fstec.ru/vul/2015-11042>

SSL / TLS: срок действия сертификата истек

Уровень опасности: Средний

CVSS 2.0: 5

Порт: 25/tcp

Описание: Сертификат SSL / TLS удаленного сервера уже истек.

Вектор CVSS 2.0: AV:N/AC:L/Au:N/C:N/I:P/A:N

Рекомендации: Замените сертификат SSL / TLS новым.

SSL / TLS: сертификат подписан с использованием алгоритма слабой подписи

Уровень опасности: Средний

CVSS 2.0: 4

Порт: 25/tcp

Описание: Удаленная служба использует сертификат SSL / TLS в цепочке сертификатов, которая была подписана с использованием криптографически слабый алгоритм хеширования.

Вектор CVSS 2.0: AV:N/AC:H/Au:N/C:P/I:P/A:N

Рекомендации: Серверы, использующие сертификаты SSL / TLS, подписанные с использованием слабого алгоритма хеширования SHA-1, MD5, MD4 или MD2, должны будут получить новый SHA-2 подписан сертификаты SSL / TLS, чтобы избежать предупреждений о сертификатах SSL / TLS веб-браузера.

Подробнее:

- <https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>

SSL / TLS: устарело обнаружение протоколов SSLv2 и SSLv3

Уровень опасности: Средний

CVSS 2.0: 4.3

CVSS 3.0: 6.8

Порт: 25/tcp

Описание: Было возможно обнаружить использование в этой системе устарел протокол SSLv2 и / или SSLv3.

CVE: [CVE-2016-0800](#), [CVE-2014-3566](#),

BDU: [BDU:2016-00661](#), [BDU:2015-00642](#),

Вектор CVSS 2.0: AV:N/AC:M/Au:N/C:P/I:N/A:N

Вектор CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N

Рекомендации: Рекомендуется отключить устаревший Протоколы SSLv2 и / или SSLv3 в пользу протоколов TLSv1 +.

Пожалуйста, смотрите ссылки для получения дополнительной информации.

Подробнее:

- <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>
- <https://bettercrypto.org/>
- <https://mozilla.github.io/server-side-tls/ssl-config-generator/>
- <https://drownattack.com/>
- <https://www.imperialviolet.org/2014/10/14/poodle.html>
- <http://www.bdu.fstec.ru/vul/2016-00661>

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.08.2023

Автор:

Администратор Сканиер-BC

5.3. Скомпрометированные учетные данные

№ п/п	Порт	Сервис	Логин	Пароль	Стойкость
1	21/tcp	ftp	user	user	Очень слабый
2	21/tcp	ftp	msfadmin	msfadmin	Слабый

Рекомендации:

1. Сменить пароли для указанных скомпрометированных учетных записей.
2. Разработать и внедрить парольную политику, определяющую, как минимум, следующие требования:
 - длина пароля: не менее 8 символов;
 - наличие специальных символов, таких как #, & и т.п.;
 - сочетание символов в верхнем и нижнем регистре;
 - наличие цифр;
 - смена пароля не реже, чем один раз в 3 месяца.

5.4. Эксплойты

Всего подобрано эксплойтов: 1.

№ п/п	Имя	Описание	Простота использования
1	VSFTPD v2.3.4 Выполнение выполнения Backdoor	Этот модуль использует вредоносный бэкдор, который был добавлен в архив загрузки VSFTPD. Этот бэкдор был введен в архив vsftpd-2.3.4.tar.gz между 30 июня 2011 года и 1 июля 2011 года в соответствии с самой последней доступной информацией. Этот бэкдор был удален 3 июля 2011 года.	Высокая

Рекомендуем устранить данные уязвимости в приоритетном порядке, так как наличие общедоступных эксплойтов увеличивает вероятность их эксплуатации злоумышленниками, обладающими даже невысокой квалификацией.

6. Хост 192.168.56.103

Операционная система: Linux 3.8 - 4.14

MAC-адрес: -

Тип устройства: устройство общего назначения

6.1. Порты и сервисы

№ п/п	Порт	Состояние	Сервис	Продукт	Версия
1	443/tcp	open	https		
2	5004/tcp	open	avt-profile-1		

Уязвимостей не обнаружено

Внимание! Тестирование проведено с устаревшей базой уязвимостей.

Дата формирования:

21.06.2023

Автор:

Администратор Сканиер-ВС