





Сканер-ВС анализ защищенности

КРАТКОЕ РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

О КОМПАНИИ

АО «НПО «Эшелон» специализируется на комплексном обеспечении информационной безопасности.

Основными направлениями деятельности являются:

 проектирование, внедрение и сопровождение комплексных систем обеспечения информационной безопасности;

 сертификация средств защиты информации и систем в защищенном исполнении;

- аттестация объектов информатизации;

лицензирование деятельности в области создания средств защиты информации;

- проведение анализа защищенности компьютерных систем;

аудит информационной безопасности организаций;

 обучение сотрудников компаний по вопросам обеспечения информационной безопасности;

поставка оборудования и средств защиты информации;

разработка средств защиты информации, средств анализа
эффективности защиты информации и устройств в защищенном исполнении;

 испытания, экспертизы, исследования в области безопасности информации;

Более детальную информацию о компании вы сможете найти на сайте <u>npo-echelon.ru</u>.

О РУКОВОДСТВЕ

Это руководство разработано с целью ознакомить пользователя с некоторыми возможностями обновленного средства анализа защищенности «Сканер-ВС» (далее – «Сканер-ВС»). Данный документ содержит только основные инструкции для начала использования «Сканер-ВС» и не является заменой руководства оператора.

СОДЕРЖАНИЕ

1. НОВЫЙ ИНТЕРФЕЙС	5
2. ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ	8
2.1. Что такое проект. Создание проекта	8
2.2. Поиск целей	10
2.2.1. Краткое описание	10
2.2.2. Запуск	11
2.2.3. Поиск целей	12
2.2.4. Завершение работы	13
2.3. Поиск уязвимостей	15
2.3.1. Краткое описание	15
2.3.2. Начало работы	15
2.3.3. Поиск уязвимостей	16
2.3.4. Завершение работы	18
2.4. Эксплуатация	20
2.4.1. Краткое описание	20
2.4.2. Запуск	20
2.4.3. Поиск эксплойтов	21
2.4.4. Сетевой аудит паролей	23
2.4.5. Завершение работы	27
2.5. Отчеты	28
2.5.1. Краткое описание	28
2.5.2 Настройки отчета	28

1. НОВЫЙ ИНТЕРФЕЙС

В предыдущей версии средства анализа защищенности «Сканер-ВС» (далее – «Сканер-ВС») все инструменты располагались на панели управления в нижней части рабочего стола (Рисунок 1). В новой версии «Сканер-ВС» на смену панели управления пришел пользовательский веб-интерфейс (Рисунок 2).

Одинаковыми цифрами на рисунках 1 и 2 обозначены элементы интерфейса, запускающие одни и те же инструменты.

Веб-интерфейс новой версии «Сканер-ВС» существенно управления предыдущей Bce отличается OT панели версии. веб-интерфейса можно графические элементы разделить HC следующие группы:

справочная информация (на рисунке 2 выделена зеленой рамкой);

проекты (на рисунке 2 выделена фиолетовой рамкой);

- инструменты (на рисунке 2 выделена красной рамкой).

Пиктограмма настроек «Сканер-ВС» находится в верхней части веб-интерфейса. Для доступа к настройкам нужно нажать ее левой кнопкой мыши.

Пиктограммы запуска инструментальных программ, реализующих функции «Сканер-ВС», которые в прошлой версии продукта «Сканер-ВС» располагались на панели управления, теперь сгруппированы в двух областях веб-интерфейса:

– проекты;

- инструменты.

Функции «Сканер-ВС», включенные в разделы «Проекты» и «Инструменты», представлены в таблице 1.



Рисунок 1 – Панель управления «Сканер-ВС» предыдущей версии

сканер-ВС анализ защищенности				● × ◆ ⊡
Главная				
Проекты	Инструменты			
Всего проектов	Аудит OC Astra Linux	Локальный аудит паролей	Поиск от	таточной информации
	Аудит обновлений ОС Windows	Системный аудитор	ОО ОО ОО ОО ОО ОО ОО Серанти 12	рованное уничтожение информации
	Аудит беспроводных сетей	Сетевой анализатор	Контро	ольное суммирование
Состояние системы				
Лицензия	Сервисы	Сканер безопасности		
Организация: Echelon	Сканер сети	Семейств 59		
Продукт: Сканер-ВС для 32 ІР-адресов	Сканер безопасности	Плапинов 50140		
Номер лицензии: 00000001	Эксплуатация уязвимостей	Политик	Обновить	Справка
Лицензия истекает: 01.01.2018			Concerne	Chipablia

Рисунок 2 – Пользовательский веб-интерфейс «Сканер-ВС» новой версии

Таблица 1. Функции старой и новой версий программного комплекса «Сканер-ВС»

N⁰	Было	Стало
	Раздел «П	ооекты»
1	Сканер сети	Поиск целей
2	Сканер безопасности	Поиск уязвимостей
3	Сетевой аудит паролей	Сетевой аудит паролей
	Средство проведения	
4	тестирования на	Поиск эксплойтов
	проникновение	
	Раздел «Инс	грументы»
5		Аудит OC Astra Linux
6	Аудит обновлений OC Windows	Аудит обновлений OC Windows
7	Аудит беспроводных сетей	Аудит беспроводных сетей
8	Локальный аудит паролей	Локальный аудит паролей
9	Системный аудитор	Системный аудитор
10	Сетевой анализатор	Сетевой анализатор
11	Поиск остаточной	
	информации	поиск остаточной информации
10	Гарантированной уничтожение	Гарантированной уничтожение
ΙZ	информации	информации
13	ПИК Эшелон	Контрольное суммирование

2. ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ

2.1. Что такое проект. Создание проекта

B новой версии «Сканер-ВС» создана единая среда ДΛЯ проведения тестирования защищенности. Для каждого НОВОГО тестирования создается проект, представляющий собой совокупность всех данных, относящихся к текущему тестированию. Проект включает в себя исходные данные фаз тестирования (поиск целей, поиск уязвимостей, сетевой аудит паролей, поиск эксплойтов) и результаты тестирования в виде сгенерированного отчета. Для проведения тестирования пользователь может создать новый проект или, в случае сохраненного продолжения начатого ранее И тестирования, ИСПОЛЬЗОВАТЬ ЕГО.

Для создания проекта в левой части веб-интерфейса нажмите левой кнопкой мыши по разделу «Проекты» или нажмите на кнопку **Проекты** в верхнем правом углу веб-интерфейса (Рисунок 3).

сканер-ВС анализ защищенности					• ×	• 🖸
Главная						
Проекты	Инструменты					
Всего проектов	Аудит OC Astra Linux	Ê	Локальный аудит паролей	6	Поиск остаточной информации	SECRET TODOT
	Аудит обновлений ОС Windows		Системный аудитор		Гарантированное уничтожение информации	
	Аудит беспроводных сетей		й 📀 Сетевой анализатор		Контрольное суммирование	Σ
Состояние системы						
Лицензия Организация: Echelon Продукт: Сканер-ВС для 32 IP-адресов	Сервисы Сканер сети Сканер сети Сканер безопасности Эскоплодтация изанимостей		о безопасности тв во ов воно к в	S	; 6	
тожер лиценани, оконосот Лиценани истекает: 01.01.2018				Обновить	Спра	вка

Рисунок 3 – Раздел «Проекты» веб-интерфейса «Сканер-ВС»

В открывшемся окне нажмите на кнопку **Новый проект** или выберите уже существующий проект из перечисленных в рабочей области (Рисунок 4).

Сканер-ВС анализ защищенности	
Главная / Проекты	
Новый проект	
Новый проект	ø x
Хосты	85
Уязвимости	41
Подобранные пароли	3
Подобранные эксплойты	96

Рисунок 4- Создание проекта

При нажатии на кнопку Новый проект откроется окно (Рисунок 5):

сканер-ВС анализ защищенности		e v	✻	٥	0
Главная / Проекты / Новый проект					
Добавление нового проекта					
* RMN					
Описание *					
	/				
Сохранить Отмена					

Рисунок 5 – Добавление нового проекта

Поля «Илля» (в него вводят название проекта) и «Описание» (в данное поле вводят краткое описание проекта) обязательны для заполнения. После заполнения полей для сохранения введенной информации о новом проекте нажмите кнопку **Сохранить**, если же по каким-либо причинам проект создавать не требуется, нажмите кнопку **Отмена**. После нажатия кнопки **Сохранить** или после выбора ранее сохраненного проекта рабочее пространство примет вид, похожий на показанный на рисунке 6.

сканер-ВС анализ защищенности						۵	∗	٠	::
Главная / Проекты / 2									
Поиск целей			Поиск уязвимостей						
Количество хостов	0		Количество уязвимостей					C)
Операционные системы	Нет данных		Критичные					0	,
			Средней критичности					C)
			Низкой критичности					0	j.
			Заметки					0)
🖋 Эксплуатация			📑 Задачи						
Количество подобранных учетных записей		0	Задача	Всего	Активные	Завершенн	ые	Ошиб	ка
Количество подобранных эксплойтов		0	Поиск целей	0	0	0		0	
			Поиск уязвимостей	0	0	0		0	
			Онлайн подбор паролей	0	0	0		0	
			Эксплуатации	0	0	0		0	
🖻 Отчёт		_							
Название проекта	Тест								

Рисунок 6 – Вид рабочего пространства проекта

Рабочее пространство разделено на сектора, каждый из которых соответствует определенной фазе тестирования. В разделах 2.2. - 2.5. описаны действия пользователя при проведении каждой фазы тестирования.

2.2. Поиск целей

2.2.1. Краткое описание

В начале тестирования обязательным является *поиск целей* - обзор локальной сети, к которой подключен «Сканер-ВС», с целью выявления объектов тестирования для следующих фаз проверки. Поиск целей производится путем сканирования IP-адресов и портов (TCP-и UDP-портов) компьютеров, присоединенных к локальной сети. Без поиска целей невозможно использовать все возможности «Сканер-ВС», в частности, невозможно производить поиск эксплойтов (см. п. 2.4. «Эксплуатация»). Найденные в результате поиска целей действующие подключения с

IP-адресами и задействованными TCP- и UDP-портами далее будем называть *активами*. Данные о них располагаются в секторе «Поиск целей» на вкладках «Хосты» и «Порты» в виде таблиц. Дополнительно поиск целей может быть использован для определения сервисов (служб), запущенных на включенном в сеть компьютере, для идентификации ОС и приложений.

2.2.2. Запуск

Нажмите левой кнопкой мыши по сектору «Поиск целей» (Рисунок 7).

C C	канер- ализ защищен	- ВС нности			-	∗	۰	0
Главная / Пр	ооекты / 2 / П	Іоиск целей						
Хосты	Порты	Задачи						
					Поиск:			
ІР-адрес			11	Операционная система				
				В таблице нет данных				

Рисунок 7 – Сектор «Поиск целей»

Перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 8).

Сканер-ВС анализ защищенности			÷	╳	۰	53
Главная / Проекты / 2 / Поиск целей	i					
Хосты Порты Задачи	и					
Новое сканирование						
			Поиск:			
N≘ ↓≣	Имя		Статус			J1
		В таблице нет данных				

Рисунок 8 – Вкладка «Задачи»

2.2.3. Поиск целей

Настройки, необходимые для запуска сканирования сети, находятся на вкладке «Базовые» (Рисунок 9), где в поле «Цели» пользователь задает *цели сканирования:* конкретный IP-адрес, множество IP-адресов - сеть или подсеть.

Сканер-ВС анализ защищенности			✻	٠	0
Главная / Проекты / 2 / Поиск целей / Ново	ре сканирование				
Базовые	Цели *	Пример:			
Расширенные		127.0.0.1 192.168.1.0/24			
Задача			h		
Запустить Отмена					

Рисунок 9 – Основные настройки сканирования

Дополнительные настройки сканирования сети расположены на вкладке «Расширенные» и используются пользователем при необходимости (Рисунок 10).

Сканер-В	С		-	∗	٠	53
Главная / Проекты / 2 / Поис	к целей / Новое сканирование					
Базовые	Сканировать конкретные ТСР-порты					
Расширенные	Сканировать конкретные UDP-порты	_P				
Залача	Скорость сканирования	Normal	•			
o apparta	Таймаут сканирования					
	Дополнительные аргументы Nmap	Пример: -Рп				
	Игнорировать результаты Ping					
	Не пытаться определять версию сервисов					
Запустить Отмена						

Рисунок 10 – Дополнительные настройки сканирования

На вкладке «Задача» пользователь задает имя и описание текущего сканирования в соответствующие пустые поля (Рисунок 11). Если поля

оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования.

анализ защище	-BC			⋇	۰	13
Главная / Проекты / 2 / Г	Поиск целей / Новое сканирование					
Базовые	Сканировать конкретные ТСР-порты					
Расширенные	Сканировать конкретные UDP-порты	()P				
Залача	Скорость сканирования	Normal	Ŧ			
бидини	Таймаут сканирования					
	Дополнительные аргументы Nmap	Пример: -Pn				
	Игнорировать результаты Ping					
	Не пытаться определять версию сервисов	_				
Запустить Отмена						

Рисунок 11 – Имя и описание сканирования

Чтобы начать сканирование нажмите кнопку Запустить (Рисунок 11).

2.2.4. Завершение работы

После запуска сканирования на вкладке «Задачи» в таблице появится номер задачи, ее имя, текущий статус (цветной индикатор). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый - сканирование успешно завершено (Рисунок 12), красный - процесс сканирования завершен с ошибкой.

	Скан Інализ за	ер-ВС цищенности			÷	✻	۰	13
Главная / Г	Проекты /	2 / Поиск целей						
Хосты	Пор	ты Задачи						
Новое ск	анирован	ие						
		_		По	ИСК:			
Nº	47	Имя	1	Статус				
17		Сканирование 192.168.5.221		Завершена			C	

Рисунок 12 – Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 12), расположенную справа от индикатора статуса сканирования. Если сканирование завершено с ошибкой, для получения подробной информации об ошибке нажмите левой кнопкой мыши по индикатору статуса сканирования (в этом случае он красного цвета), после чего откроется новое окно с информацией о задаче, деталях запуска и ошибках во время запуска задачи.

После завершения сканирования во вкладке «Порты» появятся данные об IP-адресах, которые будут сгруппированы в таблицу (Рисунок 13).

Сканер-	вс			2	× * 🖸
Главная / Проекты / 2 / По	иск целей				
Хосты Порты	Задачи				
				Поиск:	I
Хост 💵	Протокол 🕂	Порт 👘	лими 11	Продукт ป†	Версия 🕂
192.168.5.1	tcp	80	http	-	-
192.168.5.1	tcp	23	telnet	-	-
192.168.5.112	tcp	912	apex-mesh	-	-
192.168.5.112	tcp	19780	unknown	-	-
192.168.5.112	tcp	2869	icslap	-	-
192.168.5.112	tcp	1110	nfsd-status	-	-
192.168.5.112	tcp	3389	ms-wbt-server	-	-
192.168.5.112	tcp	139	netbios-ssn	-	-
192.168.5.112	tcp	22	ssh	-	-
192.168.5.112	tcp	902	iss-realsecure	-	-
192.168.5.112	tcp	445	microsoft-ds	-	-
192.168.5.112	tcp	135	msrpc	-	-
192.168.5.114	tcp	22	ssh	-	-
192.168.5.114	tcp	80	http	-	-
192.168.5.114	tcp	10001	scp-config	-	-

Рисунок 13 – Вкладка «Порты»

Во вкладке «Хосты» в таблице показаны IP-адреса и операционные системы (далее – ОС), которые им соответствуют (Рисунок 14).

Сканализ з	іер-ВС зщищенности	-	⋇	٠	0
Главная / Проекты	/ 2 / Поиск целей				
Хосты По	рты Задачи				
		Поиск:			
ІР-адрес ↓	Операционная система				
192.168.5.1	D-Link DES-3010F or DES-3010G switch				
192.168.5.112	Microsoft Windows Server 2008 R2 SP1				
192.168.5.114	Linux 3.11 - 3.14				
192.168.5.115	Microsoft Windows Server 2008 R2 SP1				
192.168.5.118	Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8				
192.168.5.119	Linux 3.11 - 3.14				
192.168.5.121	Linux 3.11 - 3.14				
192.168.5.122					
192.168.5.125	Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7				
192.168.5.126	Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7				
192.168.5.127	Linux 3.11 - 3.14				
192.168.5.130	Linux 3.11 - 3.14				

Рисунок 14 – Вкладка «Хосты»

2.3. Поиск уязвимостей

2.3.1. Краткое описание

Под уязвимостью программного обеспечения (далее – ПО) подразумевается дефект ПО, который может стать причиной нарушения информационной безопасности. Поиск уязвимостей - действия по обнаружению таких дефектов.

Поиск уязвимостей можно производить разными способами:

 запуская специальные инструментальные программы, как на одном компьютере, так и в пределах компьютерной сети;

 воздействуя специальными программами на работающие в сети компьютеры с помощью одного из компьютеров.

В данном случае описан второй вариант поиска.

2.3.2. Начало работы

Чтобы начать поиск уязвимостей нажмите левой кнопкой мыши по сектору «Поиск уязвимостей», затем перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 15).

Сканер-ВС анализ защищенности			۵	×	٠	11
Главная / Проекты / 2 / Поиск уязвимост	ей					
Уязвимости Задачи						
Новое сканирование						
			Поиск:			
N≘ ↓₹	Имя	ţt.	Статус			
В таблице нет данных						

Рисунок 15- Сектор «Поиск уязвимостей»

2.3.3. Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся на вкладке «Базовые» (Рисунок 16), где пользователь задает *цели поиска уязвимостей* (IP-адреса проверяемых компьютеров, сетей или подсетей) и выбирает *политику сканирования* (набор правил сканирования): базовую (сканирование веб-сервисов, либо полное сканирование) или пользовательскую, настраиваемую пользователем. Цели поиска уязвимостей можно задавать несколькими способами: вводя вручную адреса в поле «Цели», импортируя цели из активов или загружая из файла.

Для загрузки из активов целей поиска уязвимостей в поле «Импорт целей из активов» нажатием левой кнопки мыши отметьте нужные IPадреса (если IP-адрес выбран, рядом с ним в пустом квадрате появится галочка) или нажмите кнопку **Выделить все** (все IP-адреса в поле будут отмечены автоматически). Затем нажмите кнопку **Выбрать** и отмеченные IP-адреса появятся в поле «Цели».

Для загрузки целей сканирования из файла подготовьте соответствующий список целей поиска уязвимостей в формате .TXT, где одна строка должна содержать только один IP-адрес компьютера, сети или подсети. Затем нажмите кнопку **Выберите файл** и в открывшемся окне отметьте имя файла с импортируемым списком, далее нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле «Цели».

сканер-ВС				-	*	٥	83
Главная / Проекты / 2 / Поиск уя	звимостей / Новое сканирование						
Базовые	Политика сканирования *	Полное сканирование					
Выявление хостов	Цели *	Пример: 192.168.1.1 192.168.1.0/24					
Сканирование портов		192.168.0.0-16	ĥ				
Расширенные	Импорт целей из активов	Выбрать 0 Выделить все					
Задача		192.168.5.221					
		B.B. forum thân					
	инторт из фанла	воссрятс фана					
Запустить Отмена							

Рисунок 16 - Основные настройки сканирования

Далее выберите политику сканирования. По умолчанию установлено **Полное сканирование**. Если необходимо сменить политику сканирования, нажмите на кнопку **Полное сканирование** и выберите одну из базовых политик или создайте свою (Рисунок 17).

Сканер-ВС анализ защищенности				∗	۰	13		
Главная / Проекты / 2 / Поиск уязвимостей / Вы	Бор политики сканирования							
Выбор политики								
Базовые политики								
	Ô	к ж к ж						
Веб-приложения	Пустой шаблон	Пол	ное ска	аниров	ание			
Сканирование веб-сервисов	Для создания собственной политики с нуля	Сканировани	ие всех и	звестны)	суязвимо	стей		
Пользовательские политики								
	Пользовательская политика							
	Политика, созданная пользователем.							

Дополнительные настройки сканирования расположены на вкладках «Выявление хостов», «Сканирование портов», «Расширенные» (Рисунок 16) и используются пользователем при необходимости.

На вкладке «Задача» (Рисунок 18) пользователь задает имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.

Сканер-ВС анализ защищенности		<u>.</u>	✻	٠	0
Главная / Проекты / 7 / Поиск уязвимостей /	Новое сканирование				
Базовые	Имя				
Выявление хостов	Введите имя				
Сканирование портов	Введите описание				
Расширенные					10
Задача					
Запустить Отмена					

Рисунок 18 – Имя и описание сканирования

Для начала процесса сканирования нажмите кнопку **Запустить** (Рисунок 18).

2.3.4. Завершение работы

После запуска сканирования в таблицу на вкладке «Задачи» будет добавлена строка, содержащая номер задачи, ее имя и индикатор статуса (Рисунок 19). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый - сканирование успешно завершено, красный - процесс сканирования завершен с ошибкой.

авная / Проекты / 7 / Поиск уязвимостей				
Уязвимости Задачи				
Новое сканирование				
	Поиск:			
№ ↓∓ Имя		Стату	с	
26 Поиск уязвимостей (Полное сканирование) для 192.168.5.181		В	процессе	

Рисунок 19 - Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 12), расположенную справа от индикатора статуса. Если сканирование завершено с ошибкой, для получения подробной информации об ошибке, нажмите левой кнопкой мыши по красному индикатору, после чего откроется новое окно с информацией о текущем сканировании, его основных параметрах, ошибках.

После завершения сканирования на вкладке «Уязвимости» появятся данные об обнаруженных уязвимостях, которые будут сгруппированы в таблицу (Рисунок 20).

СКС анализ	нер-	вс	<u>e</u>	* * C
Главная / Проек	пы / 2 / По	иск уязвимостей		
Уязвимости	Задач	ЧИ		
			Поиск:	
Хост 🕼	Порт 🕼	Описание	OID J†	Критичность 🕌
192.168.5.181	80	Tik/Wiki is prone to multiple unspecified vulnerabilities, including: - An unspecified SQL-injection vulnerability - An unspecified authentication- bypass vulnerability - An unspecified vulnerability Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible. Versions prior to TikiWiki 4.2 are vulnerable.	1.3.6.1.4.1.25623.1.0.100537	Высокая
192.168.5.181	80	Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.	1.3.6.1.4.1.25623.1.0.11229	Высокая
192.168.5.181	80	Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.	1.3.6.1.4.1.25623.1.0.10498	Высокая
192.168.5.181	80	phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability. These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible. Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.	1.3.6.1.4.1.25623.1.0.100078	Высокая
192.168.5.181	80	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.	1.3.6.1.4.1.25623.1.0.800320	Высокая
192.168.5.181	21	vsftpd is prone to a backdoor vulnerability.	1.3.6.1.4.1.25623.1.0.103185	Высокая
192.168.5.181	80	PHP is prone to an information-disclosure vulnerability.	1.3.6.1.4.1.25623.1.0.103482	Высокая
192.168.5.181	80	According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability. An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible. phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.	1.3.6.1.4.1.25623.1.0.100144	Высокая
192.168.5.181	6200	vsftpd is prone to a backdoor vulnerability.	1.3.6.1.4.1.25623.1.0.103185	Высокая
192.168.5.181	0	OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore	1.3.6.1.4.1.25623.1.0.103674	Высокая

Рисунок 20 – Результаты поиска

2.4. Эксплуатация

2.4.1. Краткое описание

Фаза «Эксплуатация» объединяет две задачи: сетевой аудит паролей и поиск эксплойтов - возможностей несанкционированного удаленного использования ресурсов компьютера (доступ к информации, эксплуатация вычислительных мощностей, возможность действовать от лица других пользователей) посредством специальных программ или без них. Часто эксплойтом называют программу, предоставляющую возможность использования ресурсов компьютера.

Задача сетевого аудита паролей - выявление возможности получения доступа к ресурсам компьютеров в проверяемой сети путем подбора имени и пароля пользователя. Задача поиска эксплойтов - тестирование компьютеров в проверяемой сети на возможность их использования описанными выше способами.

2.4.2. Запуск

Для запуска сетевого аудита паролей и поиска эксплойтов (Рисунок 21) нажмите левой кнопкой мыши по сектору «Эксплуатация».

сканер-В анализ защищеннос	С				-	⋇	٠	::
Главная / Проекты / 2 / Эксп.	луатация							
Поиск эксплойтов С	Сетевой аудит паролей	Задачи						
Автоматический поиск эксплойтов Ручной поиск экслойтов								
					Поиск:			
Адрес 👫 Путь	↓↑ Название экспл	ойта 🄱	Описание		Уровень скрытно	сти		
		В таблице нет	данных					

Рисунок 21 - Сектор «Эксплуатация»

2.4.3. Поиск эксплойтов

Для проведения тестирования возможности несанкционированного удаленного использования ресурсов компьютера выберите вкладку «Поиск эксплойтов». Если перед запуском поиска эксплойтов в проекте были проведены поиск целей и поиск уязвимостей, то нажмите кнопку Автоматический поиск эксплойтов, в ином случае нажмите кнопку Ручной поиск эксплойтов.

После нажатия кнопки **Автоматический поиск эксплойтов** откроется окно «Настройка автоматического поиска эксплойтов» (Рисунок 22).

Сканер-ВС анализ защищенности				✻	٠	0
Главная / Проекты / 2 / Эксплуатация / Автоматический поиск эксплойтов						
Настройка автоматического пои	ска эксплойтов					
Цель	-					•
Тип сервиса						
Продукт	•					
Версия						
Строгий поиск						
Залустить Отмена						

Рисунок 22 – Интерфейс настройки и запуска автоматического поиска

В поле «Цель» выберите IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. Далее указываются критерии поиска эксплойтов: «Тип сервиса», «Продукт», «Версия». Тумблер «Строгий поиск» добавляет условие, что по выбранным критериям будет проведен поиск эксплойтов, для которых все выбранные параметры поиска будут иметь заданные значения, если тумблер выключен, будет произведен поиск эксплойтов, для которых совпадает хотя бы один параметр поиска. После завершения настройки для запуска тестирования нажмите копку Запустить.

После нажатия кнопки **Ручной поиск эксплойтов** откроется окно «Настройка ручного поиска эксплойтов» (Рисунок 23).

••••• Сканер-ВС анализ защищенности			÷.	×	٥		
Главная / Проекты / 2 / Эксплуатация / Ручной поиск экслойтов							
Настройка ручного поиска эксплойтов							
Цель Ключевые слова *	-					•	
						11	
Запустить Отмена							

Рисунок 23 – Интерфейс настройки и запуска ручного поиска эксплойтов

В поле «Цель» введите IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. В многострочное поле «Ключевые слова» вводятся параметры поиска - фрагменты текста, которые должны обязательно присутствовать в названии, описании и других данных эксплойта из базы эксплойтов. Одна строка многострочного поля должна содержать только одно значение. Когда все параметры будут внесены, нажмите копку **Запустить**. Поиск будет производиться аналогично строгому поиску (см. п.2.4.3).

2.4.4. Сетевой аудит паролей

Перейдите на вкладку «Сетевой аудит паролей» и нажмите на кнопку **Новый подбор паролей** (Рисунок 24).

Ска	нер защищ	-ВС енности							e v	╳	۰	-83
лавная / Проекть	ol / 2 /	Эксплуатация										
Поиск эксплой	тов	Сетевой ау,	дит пар	олей	Задачи							
Новый подбор п	аролей											
								П	оиск:			
Хост	14	Порт		Сервис	;		Пользователь		Паро	ль		
					Вта	аблице н	ет данных					

Рисунок 24 – Интерфейс запуска подбора паролей

На вкладке «Базовые» расположены базовые параметры сетевого аудита паролей, которые требуется задать (Рисунок 25): тестируемый сервис (протокол), порт (если используется порт не по умолчанию) и цели тестирования: IP-адрес, сеть или подсеть. Цели можно задать вручную, импортировать из поиска целей или загрузить из файла.

Для загрузки целей поиска уязвимостей из активов в поле «Импорт хостов из активов» нажатием на левую кнопку мыши отметьте нужные IPадреса (если IP-адрес выбран, рядом с ним в пустом квадрате появится галочка) или нажмите кнопку **Выделить все** (все IP-адреса в поле будут отмечены автоматически). Затем нажмите кнопку **Выбрать** и отмеченные IP-адреса появятся в поле «Цели».

Для загрузки целей сканирования из файла подготовьте соответствующий список целей поиска уязвимостей в формате .TXT, где одна строка документа должна содержать только один IP-адрес, сети или подсети. Затем нажмите кнопку Выберите файл и в открывшемся окне отметьте имя импортируемого списка. Нажмите кнопку Открыть. Перечень целей сканирования появится в поле «Цели».

сканер-ВС анализ защищенности			✻	٥	:3
Главная / Проекты / 2 / Эксплуатация / Новый под	цбор паролей				
Базовые	Сервис *	ftp	Ŧ		
Пользователи	Указать порт	-			
Пароли	Цели *	Пример: 192.168.1.1 192.168.1.0/24			
Расширенные		192.168.0.0-16	h		
Задача	Импорт из файла	🖺 Выберите файл			
	Импорт хостов из активов	Выбрать 0 Выделить все			
		192.168.5.138	-		
		192.168.5.125	1		
		192.168.5.115			
		192.168.5.241			
		192.168.5.181	-		
Запустить Отмена					

Рисунок 25 – Основные настройки подбора паролей

Для того, чтобы указать сервис (протокол), нажмите левой кнопкой мыши на выпадающий список напротив надписи «Сервис» и выберите нужное значение.

На вкладке «Пользователи» пользователь задает идентификаторы (имена, login) пользователей проверяемых IP-адресов (Рисунок 26). Задать их можно вручную в поле «Пользователи», или импортировать из файла в формате .TXT, где одна строка документа должна содержать только одно имя. Дополнительные настройки («Списки по умолчанию», «Найденные ранее пользователи») используются пользователем при необходимости.

Сканер-ВС			-	ж	٠	13
Главная / Проекты / 2 / Эксплуатация / Новый под	цбор паролей					
Базовые	Пользователи	Пример:				
Пользователи		admin root				
Пароли	Импорт из файла	🖹 Выберите файл		li		
Расширенные	Списки по умолчанию					
Задача	Найденные ранее пользователи					
Запустить Отмена						

Рисунок 26 - Настройка подбора паролей, вкладка «Пользователи»

На вкладке «Пароли» в поле «Пароли» пользователь задает комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации (Рисунок 27). Каждая комбинация должна находиться на отдельной строке. Настройки программы поддерживают загрузку паролей из файла в формате .TXT, где одна строка документа должна содержать ТОЛЬКО ОДИН пароль. Дополнительные настройки («Пароли по умолчанию», «Найденные пароли» другие) ИСПОЛЬЗУЮТСЯ ранее И пользователем при необходимости.

Сканер-ВС			<u>.</u>	✻	۰	0
Главная / Проекты / 2 / Эксплу	атация / Новый подбор паролей					
Базовые Пользователи	Паропи Прим 12345 qwert	ер: ;6 у				
Пароли	Импорт из файла 📑 Вы	берите файл		h		
Расширенные	Пароли	Проверить				
Задача	ио умолчанию Найденные ранее пароли Проверить пустой пароль	совпадающий с логином Проверить пароль совпадающий с погином в обратном порядке (admin- nimda)		*		
Запустить Отмена	- нодиночить сноварь			Ŧ		

Рисунок 27 – Настройка подбора паролей

Для завершения подбора паролей при первой подобранной паре имя - пароль, перейдите на вкладку «Расширенные» и активируйте «Закончить подбор при первом положительном результате» (Рисунок 28).

Сканер-ВС			2	×	0	13
Главная / Проекты / 7 / Эксплуатац	ия / Новый подбор пароле	й				
Базовые	Закончить подбор пр	ри первом положите	льном р	езультате	2	
Пользователи						
Расширенные						
Задача						
Запустить Отмена						

Рисунок 28 – Расширенные настройки подбора паролей

На вкладке «Задача» пользователь задает название и описание для задачи поиска в соответствующие пустые. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек тестирования.

Нажмите кнопку Запустить (Рисунок 28).

2.4.5. Завершение работы

После нажатия кнопки **Запустить** на вкладке «Задачи» в таблице появится номер задачи, имя и индикатор статуса (Рисунок 29). Желтый цвет индикатора означает процесс сканирования, зеленый - завершение сканирования, красный - процесс сканирования выполнен с ошибкой.

Скан	ер-ВС цищенности	÷	× •	0
Главная / Проекты	2 / Эксплуатация			
Поиск эксплойт	в Сетевой аудит паролей Задачи			
		Поиск:		
Nº ↓7	Имя	↓† Статус		
29	Онлайн подбор для 192.168.5.181	В процессе		
27	Ручной поиск эксплойтов для 192.168.5.115	Завершена	C	
26	Автоматический поиск эксплойтов для 192.168.5.181	Завершена	C	

Рисунок 29 – Таблица задач поиска эксплойтов

После завершения сканирования в разделе «Онлайн подбор паролей» появятся данные о подобранных паролях (Рисунок 30), а в разделе «Эксплойты» таблица с найденными эксплойтами (Рисунок 31).

Скане анализ защии	р-В ценно	С					÷.	╳	٠	0
павная / Проекты / 1	Эксп	луатация								
Поиск эксплойтов	(Сетевой ауд	цит паро	олей	Задачи					
Новый подбор пароле	й									
							Поиск:			
Хост	14	Порт		Сервис		Пользователь		Пароль		
192.168.5.122		21		ftp		msfadmin		msfadmin		
192.168.5.122		21		ftp		ftp		000000		

Рисунок 30 – Информация о подобранных паролях

ско анализ	нер-ВС защищенности		• ·	× ¢	- 13
Главная / Проек	ты / 2 / Эксплуатация				
Поиск экспло	йтов Сетевой аудит п	аролей Зада	и		
Автоматически	й поиск эксплойтов Ручной	поиск экслойтов	Поиск		
Адрес 🏨	Путь ↓↑	Название эксплойта ↓↑	Описание	Уровені скрытно	, ости ↓†
192.168.5.181	unix/ftp/vsftpd_234_backdoor	VSFTPD v2.3.4 Backdoor Command Execution	This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.	Высокий	

Рисунок 31 – Информация о найденных эксплойтов

2.5. Отчеты

2.5.1. Краткое описание

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в «Сканер-ВС» используется сектор «Отчет» (Рисунок 6), с помощью которого можно построить отчет с результатами тестирований.

2.5.2 Настройки отчета

После того как был выбран сектор «Отчет», в нем отображается страница с предварительно построенным полным отчетом, который можно просмотреть и экспортировать в формате .PDF или напечатать с помощью кнопки **Печать**. Для настройки отчета можно воспользоваться конструктором отчета (Рисунок 32), который можно активировать с помощью кнопки **Настройки** (активирован по умолчанию).

Сканер-ВС анализ защищенности	-	✻	٠	-
Главная / Проекты / 2 / Отчёт				
	н	астройки		ечать
Настроики отчета				
Резюме				
Порты				
Уязвимости				
Пароли				
Эксплоиты		n	рименит	њ

Рисунок 32 – Конструктор отчетов

Полный отчет состоит из следующих разделов: «Резюме», «Порты», «Уязвимости», «Пароли» и «Эксплойты». Раздел «Резюме» - краткая информация по всем этапам тестирования в виде диаграмм и общей таблицы распределения уязвимостей по хостам (Рисунок 33).

Сканер-ВС Отчёт				
Имя проекта		Te	ест	
Описание		Пробный проект	по тестированию.	
Тип отчёта		Oõ	щий	
Дата формирования		11.05.201	7 17:05:35	
Общее количество хостов		7	78	
Резюме	вимостей по уровням риска Ра Низкая Заметка Высокая Средняя	аспределение паролей по уровням стойкс Очень сл	сти Распределение экспл іабый	койтов по уровням скрытности Высокий
з ^{нелов} ^{увит} в ^{ребие} себ ^{ро} в ^{ребие} ко ^{во} таблица распределения уязвимостей по хостам				
Хост / Критичность	Высокая	Средняя	Низкая	Всего
192.168.5.181	13	7	22	42

Рисунок 33 – Фрагмент отчета «Сканер-ВС»

Раздел «Порты» соответствует фазе «Поиск целей», раздел «Уязвимости» - фазе «Поиск уязвимостей», раздел «Пароли» и «Эксплойты» - фазе «Эксплуатация». При необходимости любой раздел отчета можно исключить из конечного отчета по тестированию, для этого необходимо с помощью левой кнопки мыши отключить тумблер напротив каждого исключаемого раздела отчета, затем нажать кнопку **Применить**. Отчет изменится согласно новым условиям.