Эшелон
комплексная безопасность

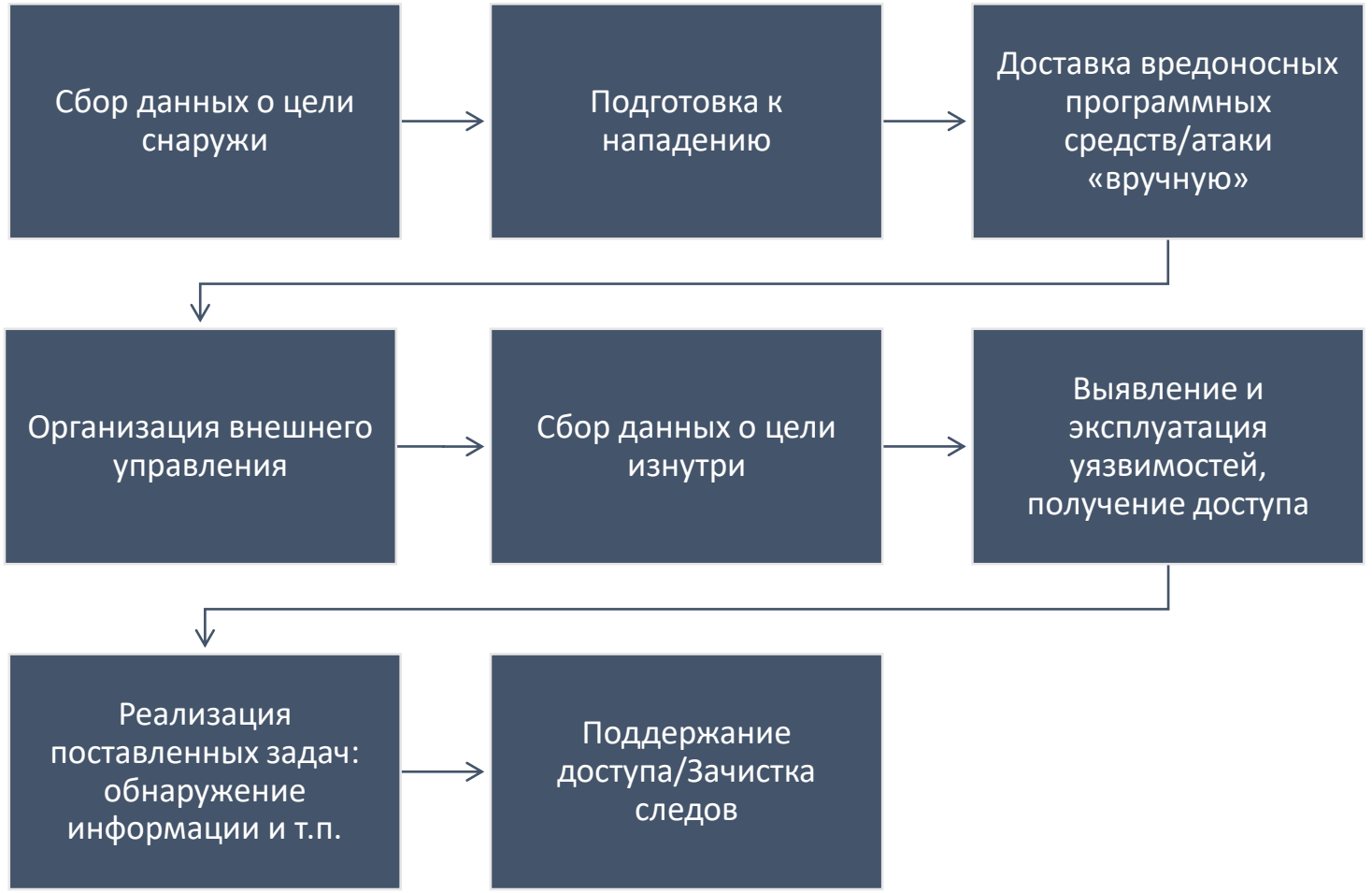
Подходы к тестированию защищенности. Обзор возможностей Сканер-ВС 6

Дорофеев Александр, CISSP, CISA, CISM

План

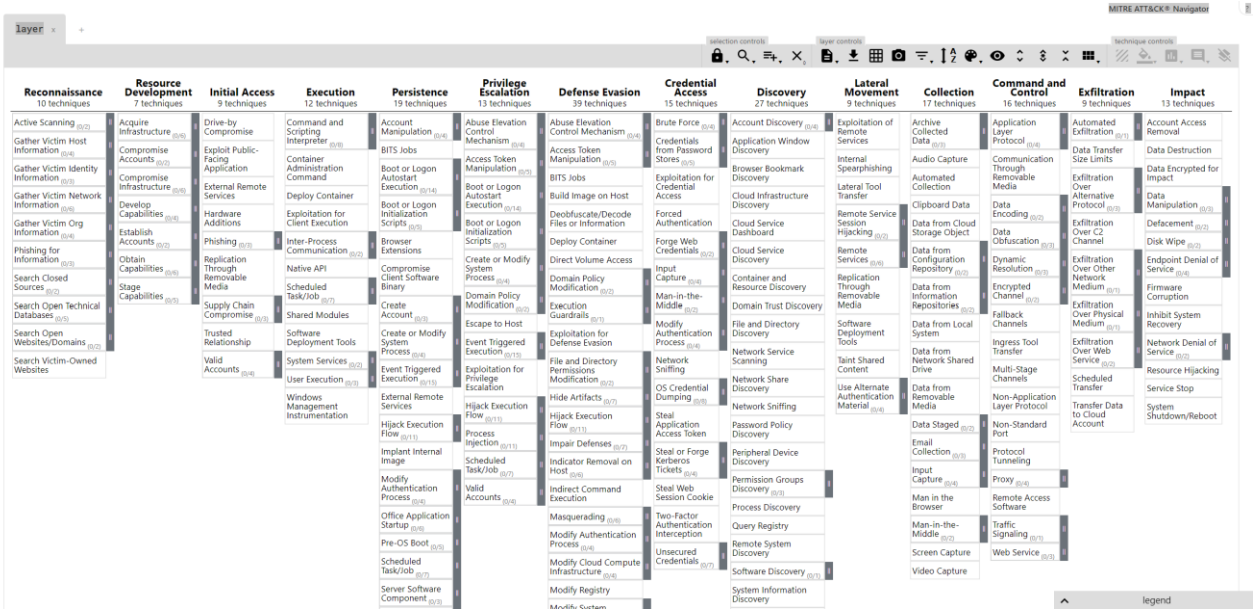
1. Современная кибератака
2. Подходы к тестированию защищенности
3. Сканеры уязвимостей: принципы работы и ограничения
4. Обзор возможностей Сканер-ВС 6

Современная таргетированная атака (APT) = спецоперация



MITRE ATT@CK (1)

1. Reconnaissance – сбор информации о цели снаружи
2. Resource Development – подготовка ресурсов для нападения
3. Initial Access – первоначальный доступ
4. Execution – попытка запуска вредоносного ПО
5. Persistence – организация постоянного доступа к целевой инфраструктуре
6. Privilege Escalation – повышение уровня доступа
7. Defense Evasion – обход средств защиты информации

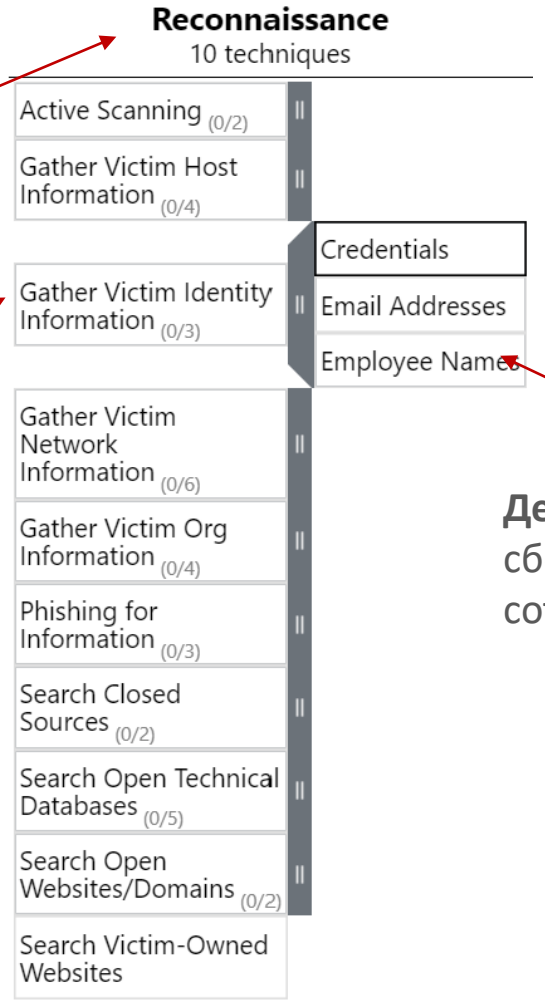


MITRE ATT@CK (2)

8. Credential Access – получение доступа с помощью действующих учетных записей
9. Discovery – сбор информации о цели изнутри
10. Lateral Movement – перемещение внутри целевой ИТ-инфраструктуры
11. Collection – сбор интересующих данных
12. Command and Control – организация внешнего управления
13. Exfiltration – передача интересующих данных вовне
14. Impact – разрушающее воздействие на ИТ-инфраструктуру

Задача: разведка

Набор действий: сбор данных, идентифицирующих цель



Действие: сбор имен сотрудников

Приложение 11 к Методике оценки угроз ФСТЭК России

Приложение 11
к Методике оценки угроз
безопасности информации

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

Таблица 11.1

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора. Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера
		Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей. Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства
		Т1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)
		Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		Т1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		Т1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках

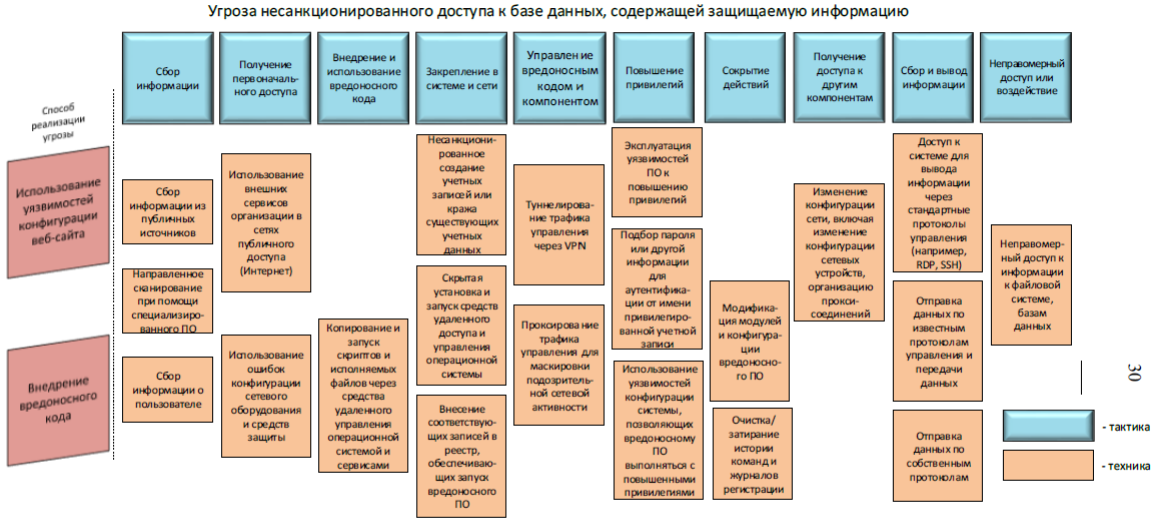


Рисунок 7. Пример сценария реализации угрозы безопасности информации

Что можно позаимствовать у хакеров для комплексной методики анализа защищенности?

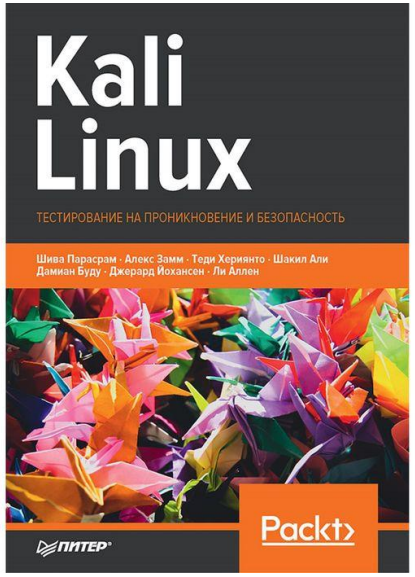
- Цели
- Приемы взлома
- Инструменты

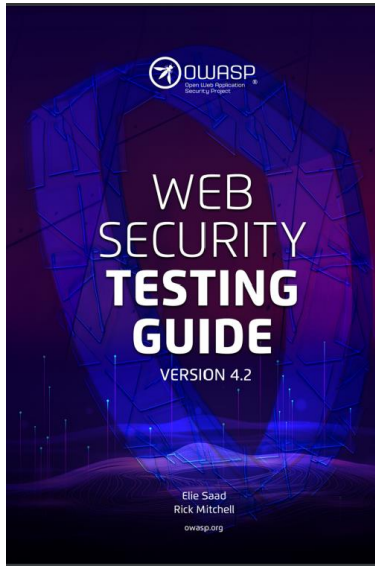
Цели

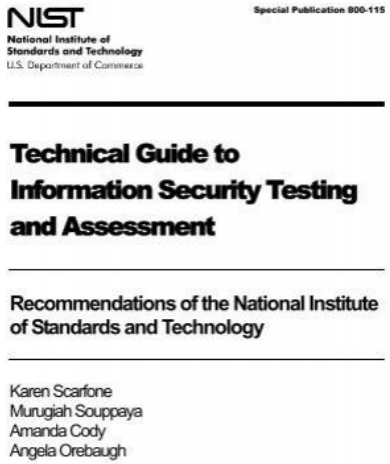
Административный доступ

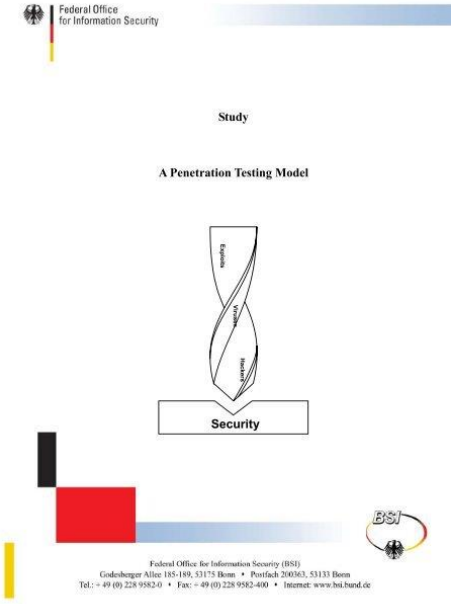
Конкретные данные для демонстрации их незащищенности руководству

Приемы взлома/тестирования









Книги

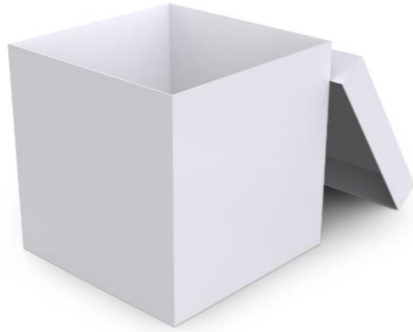
Методики от профессиональных сообществ

Методики от организаций, спонсируемых государствами

Существующие подходы к оценке защищенности

Классический тест
на проникновение

Сканирование на
наличие уязвимостей



Анализ конфигурации

Классический тест на проникновение

- Имитация действий реального злоумышленника – поиск первой уязвимости, позволяющей получить доступ к системе
- Больше искусство, чем аудит. Качество сильно зависит от уровня специалиста
- Обычный результат: несколько опасных уязвимостей
- Высокий риск нарушения доступности систем

Сканирование

- Использование исключительно сканеров для поиска уязвимостей
- Качество сильно зависит от используемого сканера.
- Результат: множество уязвимостей различного уровня опасности
- Средний риск нарушения работоспособности систем

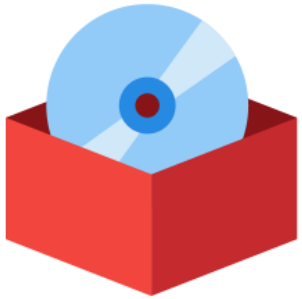
Анализ конфигурации системы

- Проверка настроек систем в соответствии с рекомендуемыми вендорами или сообществами профессионалов по ИБ (NIST, Center Internet Security).
- Результат: множество уязвимостей различного уровня опасности
- Низкий риск нарушения работоспособности систем

Комплексный подход: комбинация всех подходов и приемов злоумышленников

Инструментарий хакеров: этичных и не очень

Специалисты по тестированию защищенности



Зловреды/ кибероружие

Хакерские утилиты с открытым исходным кодом

Утилиты операционн ой системы

Сканеры уязвимостей

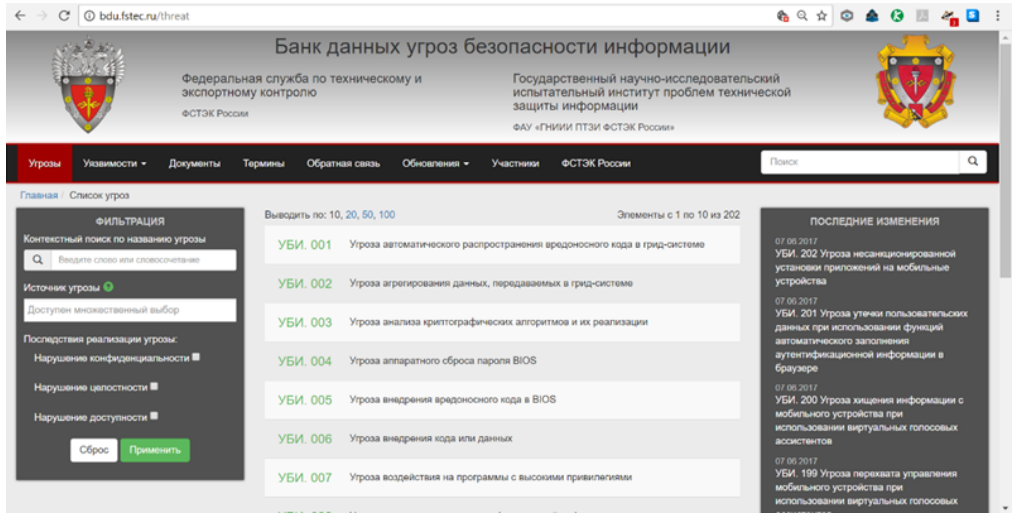
Злоумышленники

Немного об уязвимостях (ГОСТ Р 56546-2015)

- Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации
- Уязвимость может быть внесена в процессе проектирования (уязвимость архитектуры), разработки (уязвимость кода) и в процессе задания конфигурации (уязвимость конфигурации).

Уязвимости:

известные



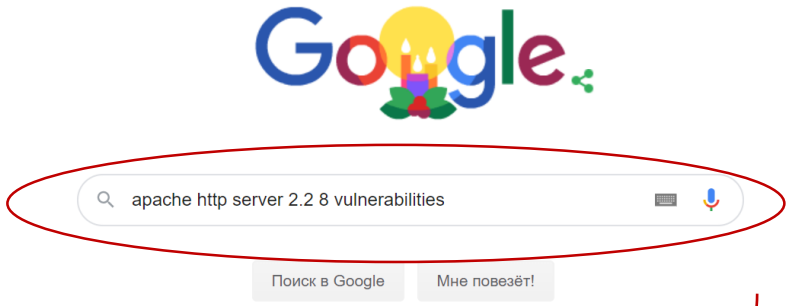
Запись об уязвимости внесена в базу данных уязвимостей и ей присвоен идентификатор (CVE, BDU)

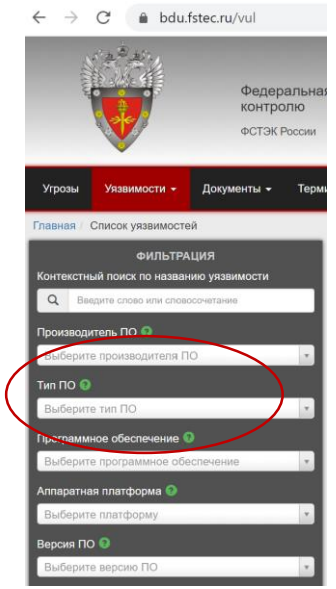
нулевого дня

Об уязвимости знает только ограниченный круг лиц, вендор ПО не знает, либо пока не успел выпустить обновление безопасности.

Технология поиска известных уязвимостей

Apache HTTP Server 2.2.8





Apache » Http Server » 2.2.8 : Security Vulnerabilities (Execute Code)

Cpe Name:*cpe:/a:apache:http_server:2.2.8*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-1862	310		Exec Code	2013-06-10	2017-09-18	5.1	None	Remote	High	Not required	Partial	Partial	Partial

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

2	CVE-2010-0425			Exec Code	2010-03-05	2018-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

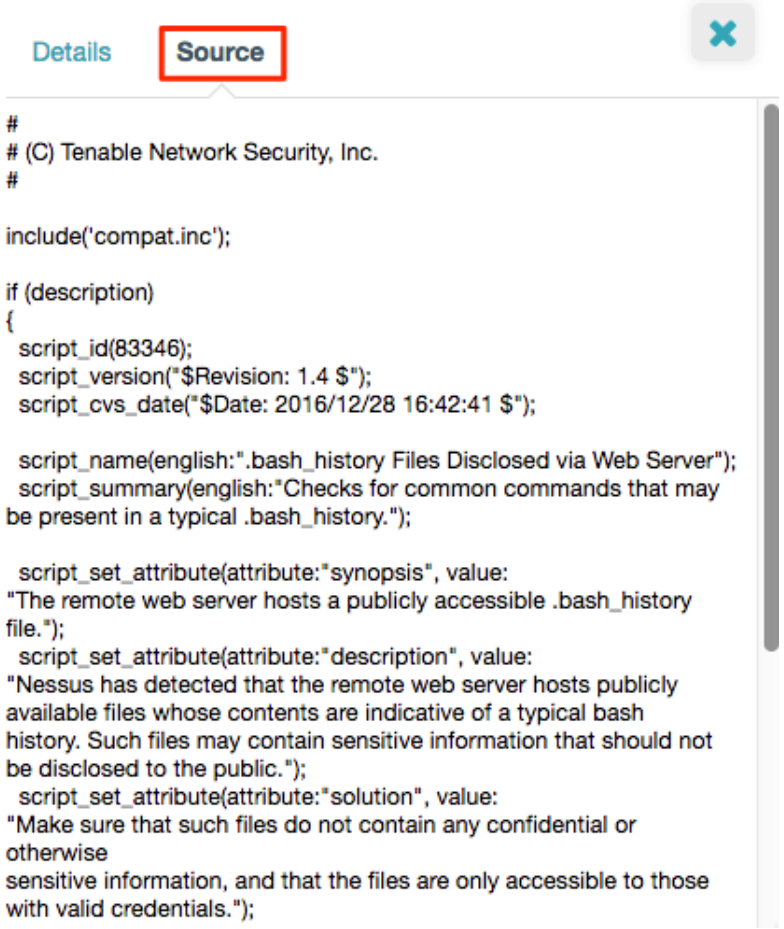
modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Total number of vulnerabilities : 2 Page : 1 (This Page)

Автоматизация поиска: создания скрипта на каждую уязвимость

Nessus Attack Scripting Language

Nmap Scripting Engine



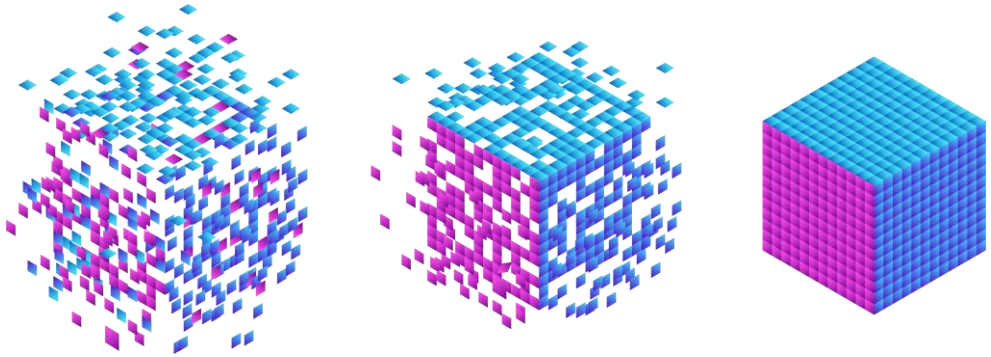
Результат: в ходе сканирования одного узла запускаются тысячи скриптов

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	586	0.30
1-2	1143	0.70
2-3	7769	4.60
3-4	8399	5.00
4-5	40132	23.70
5-6	32372	19.10
6-7	25056	14.80
7-8	34010	20.10
8-9	826	0.50
9-10	19222	11.30
Total	169515	

Современный подход: использование агрегированной базы данных уязвимостей

- БДУ ФСТЭК России
- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- …

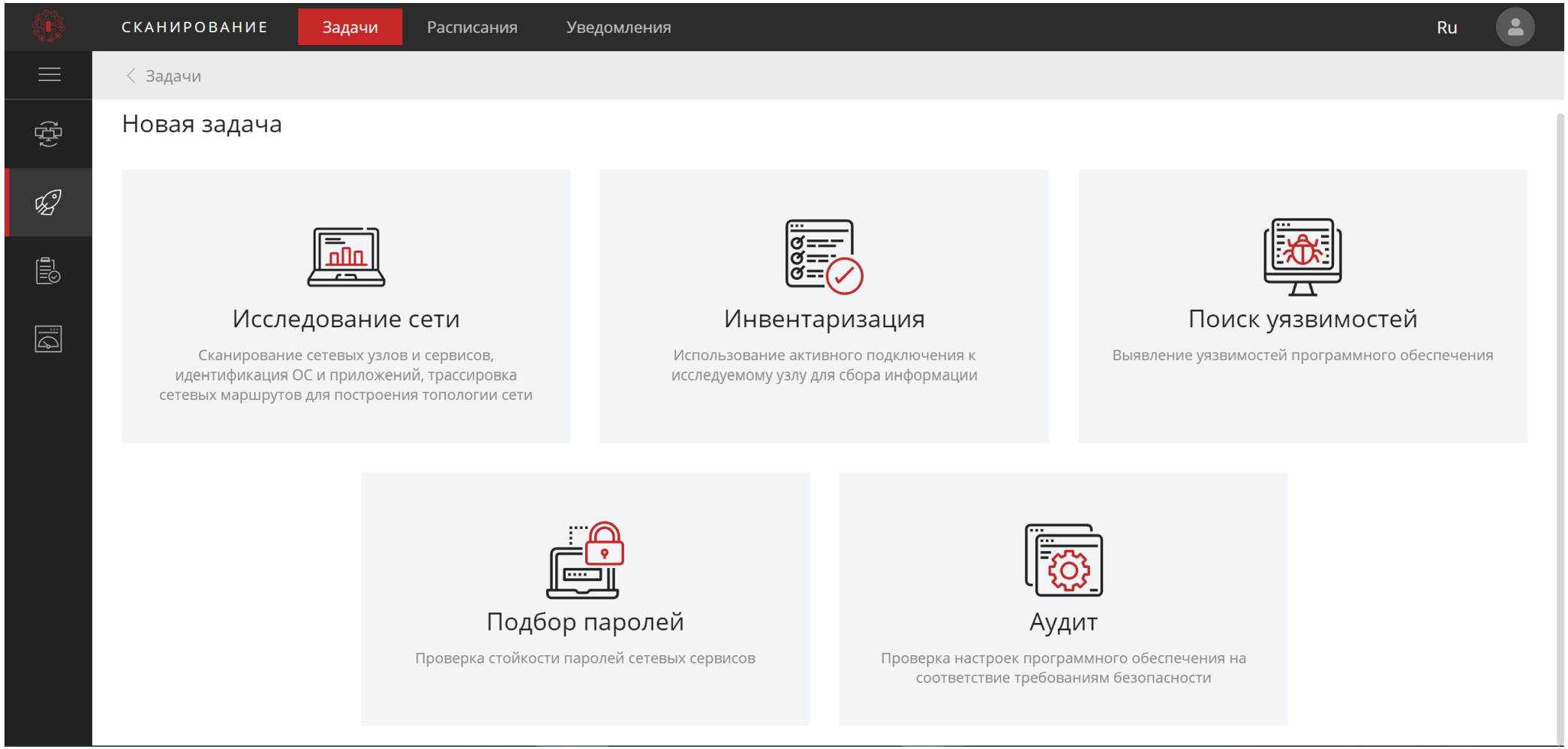


Клиент-серверная архитектура

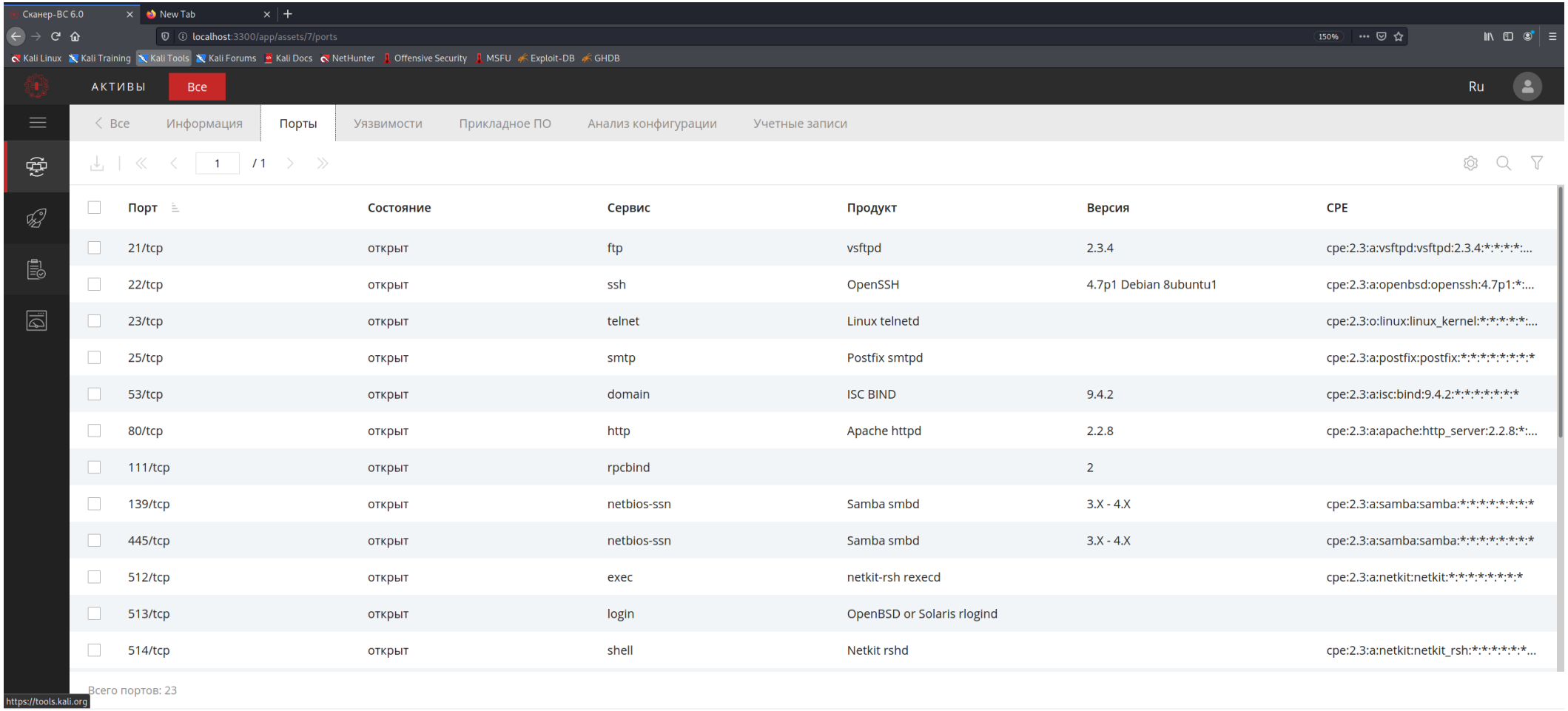
Web-браузер
ОС: Windows\Linux

Сканер-ВС 6.0
ОС: Debian-based Linux

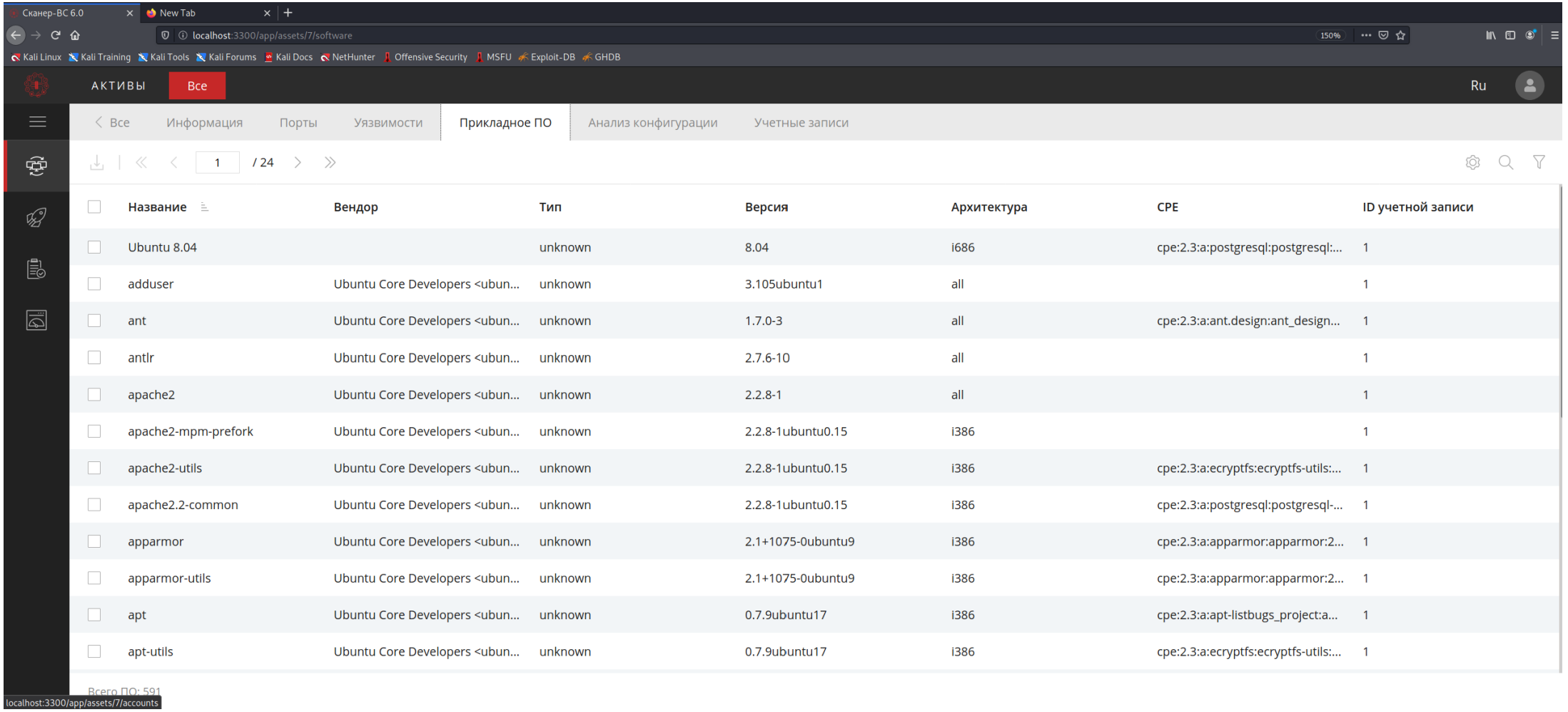
Ключевой функционал



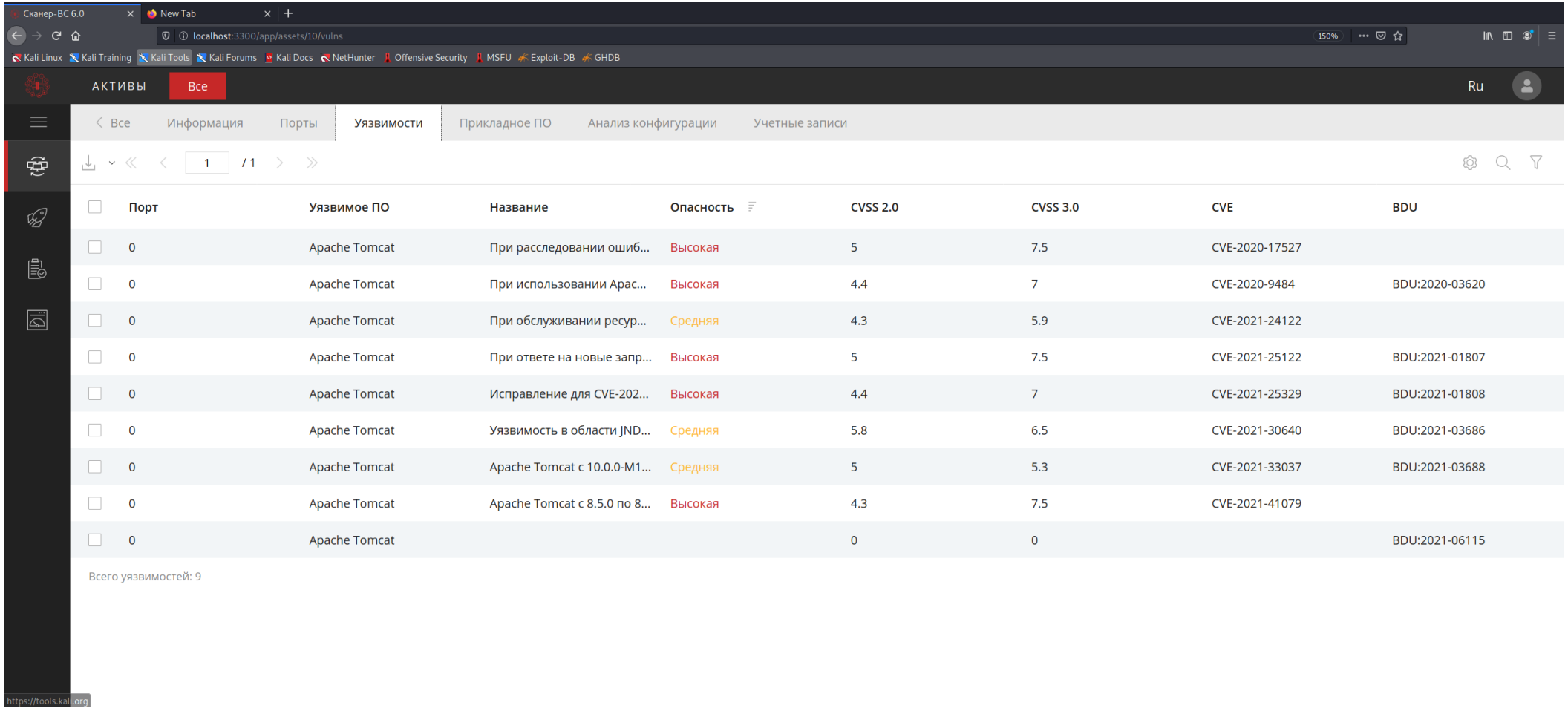
Открытые сетевые порты



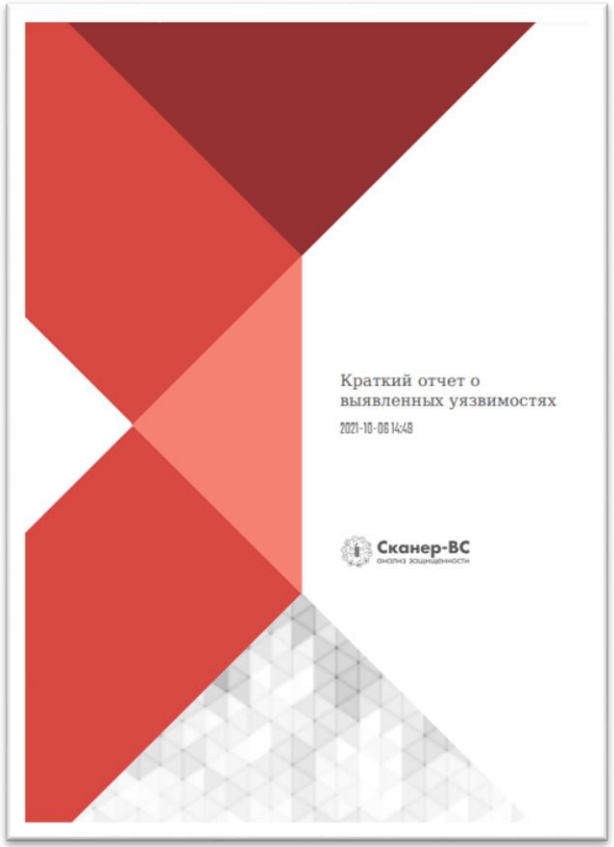
Установленное ПО

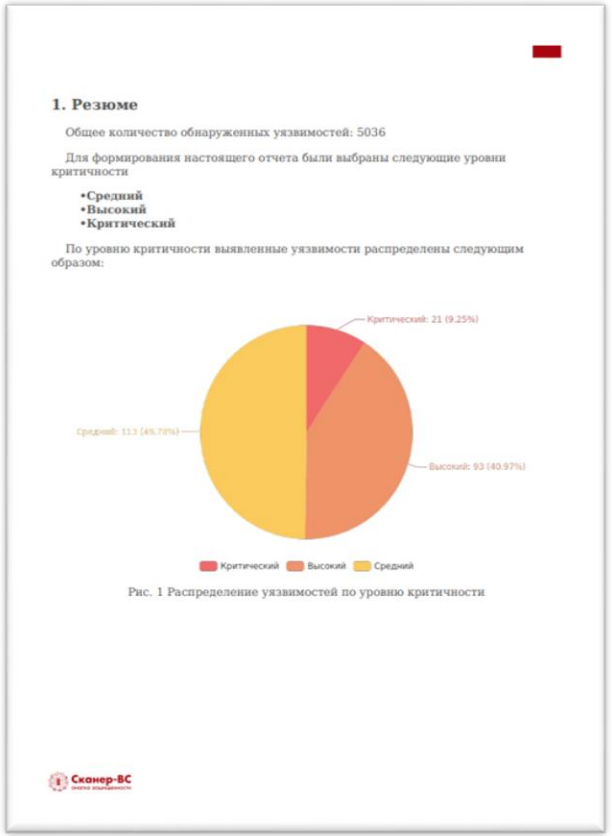


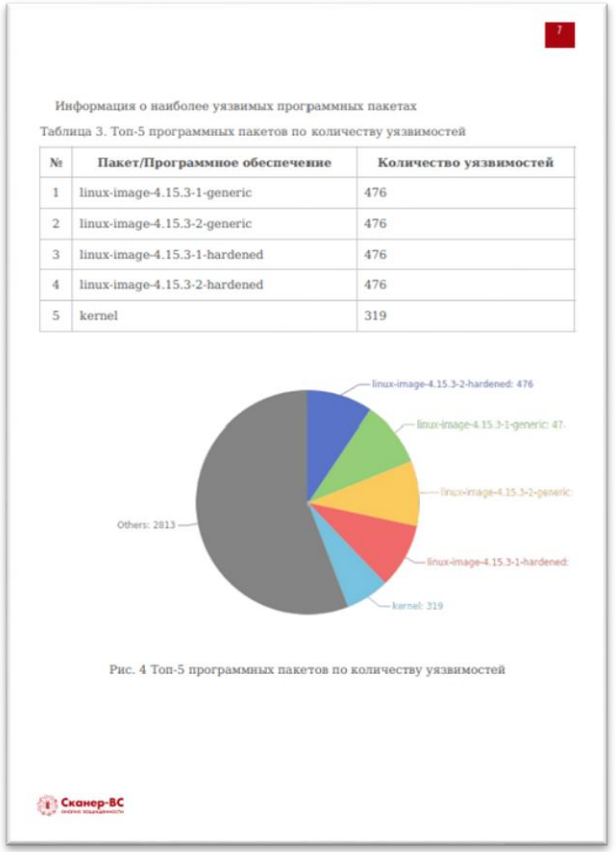
Список обнаруженных уязвимостей



Отчеты с результатами сканирования

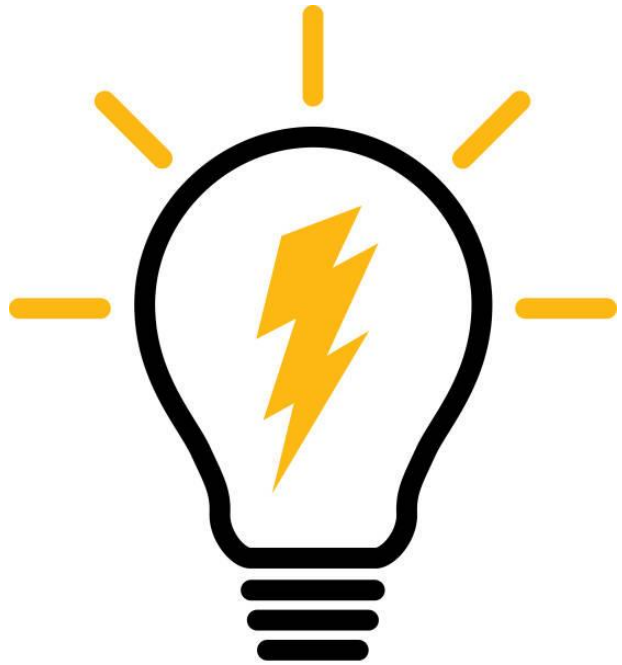






Отличительные особенности:

- База уязвимостей, включающая все известные уязвимости (~170 тыс)
- Поддержка актуальных версий ОС: Windows, Linux
- Высокая скорость поиска уязвимостей
- Дистрибутив под Astra Linux SE
- Подбор паролей по распространенным протоколам (ftp, ssh, smtp, postgres и т.д.)



Как получить превью-версию Сканер-ВС 6?

- getscanner@npo-echelon.ru – email для получения превью-версии Сканер-ВС 6
- https://t.me/scanervs чат пользователей продукта
- https://www.youtube.com/channel/UCIwZEG8EcL7tnZN4Qzjt13w

канал учебного центра «Эшелон» с обучающими видео

СПАСИБО ЗА ВНИМАНИЕ!

Марков Алексей Сергеевич
д.т.н., CISSP, CEH
a.markov@npo-echelon.ru


Эшелон
комплексная безопасность