РАЗВЕРТЫВАНИЕ И КОНФИГУРИРОВАНИЕ GOBYSEC НА БЕЗЕ ОС АЛЬТ. ТЕСТИРОВАНИЕ СЕТИ

Садовников Алексей Александрович

студент, ТЭК Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, РФ, г. Москва

Введение

GobySec представляет собой перспективный инструмент для автоматизированного поиска уязвимостей. В ходе тестирования бета-версии этого продукта были отмечены как сильные, так и слабые стороны. Главным достоинством GobySec можно считать его понятный интерфейс, который упрощает работу для специалистов разного уровня подготовки. Это особенно ценно в сфере информационной безопасности, где многие аналогичные решения отличаются излишней сложностью. Важной особенностью инструмента является встроенная функция генерации отчетов, значительно упрощающая анализ результатов. Благодаря модульной структуре GobySec можно адаптировать под конкретные задачи, что расширяет область его применения.

При тестировании в среде Alt Linux инструмент успешно определил все открытые порты, что подтверждает его работоспособность в данной операционной системе. Основным недостатком текущей версии оказалось продолжительное время сканирования, что может ограничивать применение в условиях, требующих оперативного реагирования. Однако учитывая статус бета-версии, можно ожидать оптимизации этого параметра в будущих релизах.

Обзор GobySec

GobySec - современное решение для автоматизированной проверки сетевой безопасности. Кроссплатформенность позволяет использовать его в различных операционных средах. Отличительной чертой инструмента является удачное сочетание мощного функционала и удобного интерфейса.

Основные возможности включают:

- Автоматическое обнаружение активных узлов в заданном IP-диапазоне
- Идентификацию сетевых сервисов и версий ПО
- Поиск известных уязвимостей с использованием актуальных баз данных
- Генерацию отчетов в различных форматах (HTML, PDF, JSON)
- Поддержку модульного расширения функционала

Отчеты содержат не только перечень найденных уязвимостей, но и практические рекомендации по их устранению. Возможность интеграции с другими системами через API делает GobySec удобным компонентом комплексных решений безопасности.

Ключевые преимущества перед аналогами:

1. Меньший расход ресурсов по сравнению с Nessus
2. Более простая кривая обучения, чем у OpenVAS
3. Оптимален для сканирования сетей среднего размера

Операционная система Альт

Садовников А.А. РАЗВЕРТЫВАНИЕ И КОНФИГУРИРОВАНИЕ GOBYSEC НА БЕЗЕ ОС АЛЬТ. ТЕСТИРОВАНИЕ СЕТИ // Студенческий форум: электрон. научн. журн. 2025. № 17(326). URL: https://nauchforum.ru/journal/stud/326/172731 (дата обращения: 07.09.2025).

Alt Linux - отечественная ОС, разрабатываемая компанией "Базальт". Дистрибутив представлен в двух основных вариантах: "Альт Рабочая Станция" для пользовательских ПК и "Альт Сервер" для серверных решений. Это разделение помогает пользователям выбирать ту версию, которая наиболее всего подходит их потребностям и задачам, которые они перед собой ставят.

Система соответствует требованиям российских стандартов безопасности, включая поддержку ГОСТ-шифрования и СКЗИ. Имеет сертификаты ФСТЭК, что позволяет использовать ее в госучреждениях.

Технические особенности:

- Пакетная база более 30 000 приложений
- Поддержка RPM-пакетов
- Долгосрочная поддержка (до 10 лет)
- Совместимость с отечественными процессорами (Эльбрус, Байкал)
- Соответствие требованиям 152-ФЗ и 187-ФЗ

Методология тестирования сетей

1. Пассивное сканирование:

Метод, при котором цифровой трафик подвергается анализу с целью сбора информации без активного вмешательства в сеть. В качестве основных методов используются анализ ARP-таблиц и DNS-запросов.

Преимущества: высокая скрытность, повышенная безопасность.

Недостаток: возможная неполнота данных.

2. Активное сканирование:

Метод, при котором подразумевается отправка специальных запросов к целевым системам для получения информацию. В качестве основных методов используются TCP/UDP сканирование и ping-проверка. Разновидностями активного сканирования являются: полная проверка всех портов; привилегированное сканирование, требующее авторизации для доступа к системе; веб-ориентированная проверка (HTTP/HTTPS)

Преимущество: получение полной информации о системе.

Недостаток: возможное нарушение работы систем.

GobySec эффективно сочетает оба метода, обеспечивая комплексную оценку безопасности.

Таблица 2.1.

Классификация уязвимостей

По уровню опасности:	**По типу:**	**По происхождению:**
Критические (CVSS 9.0-10.0)	Сетевые (открытые порты, неправильные настройки)	Программные (ошибки в коде
Высокие (CVSS 7.0-8.9)	Веб-уязвимости (SQL-инъекции, XSS)	Аппаратные (уязвимости микропрограмм)
Средние (CVSS 4.0-6.9)	Аутентификации (слабые пароли, перебор)	Человеческий фактор (ошибк администрирования)
Низкие (CVSS 0.1-3.9)	Конфигурационные (дефолтные учетки)	

Практическая часть

Подготовка среды

Требования к оборудованию и ПО:

- Минимальные системные требования:
  - Процессор: x86_64, 2 ядра
  - ОЗУ: 4 ГБ (рекомендуется 8 ГБ для больших сетей)
  - Диск: 50 ГБ свободного места
  - Сетевой интерфейс: 1 Гбит/с
- Поддерживаемые ОС:
  - Альт Рабочая Станция 10+
  - Альт Сервер 8.2+
- Дополнительное ПО:
  - Python 3.9.6
  - Git 2.42.2
  - pip 22.2.2

Установка GobySec

Установка:

Рисунок 1. Скриншот 3.1. команда для скачивания zip архива с goby для линукс

Рисунок 2. Скриншот 3.2 - команда для разархивирования zip архива с goby для линукс

Запуск и проверка:

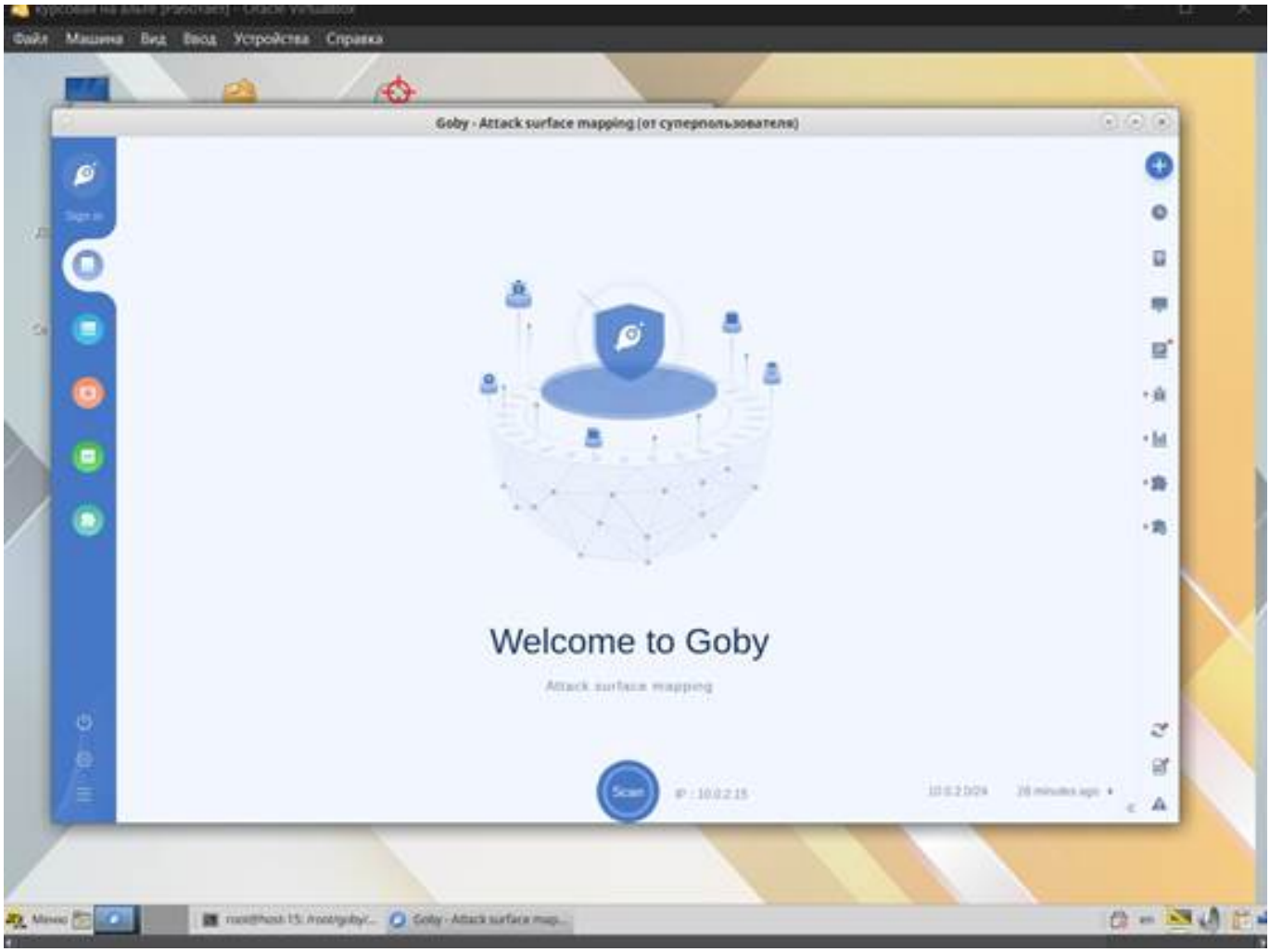

Рисунок 3. Скриншот 3.3 - итог развертывния Goby

Результаты сканирования:

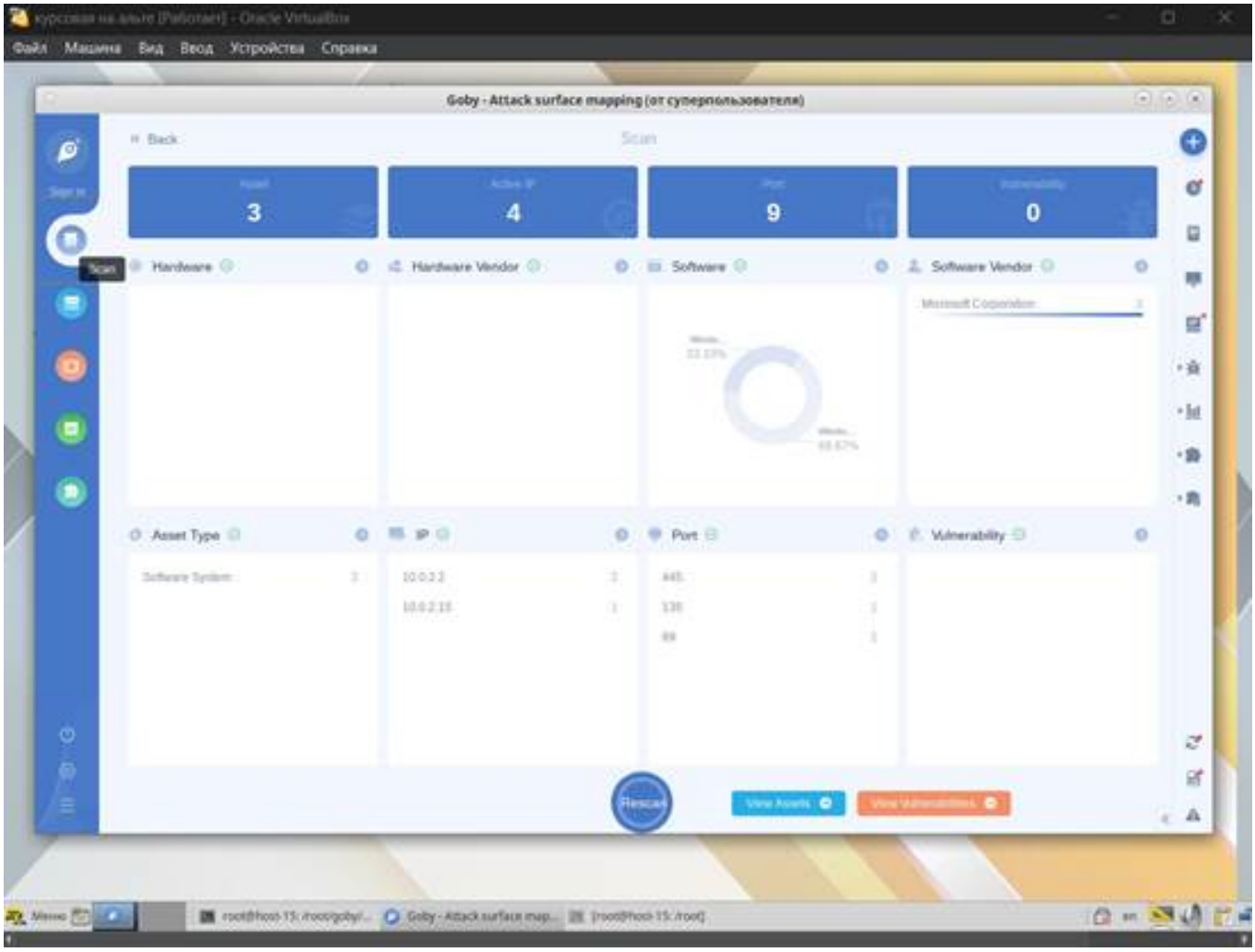

Рисунок 4. Скриншот 3.4 - проверка ip адреса 10.0.2.15

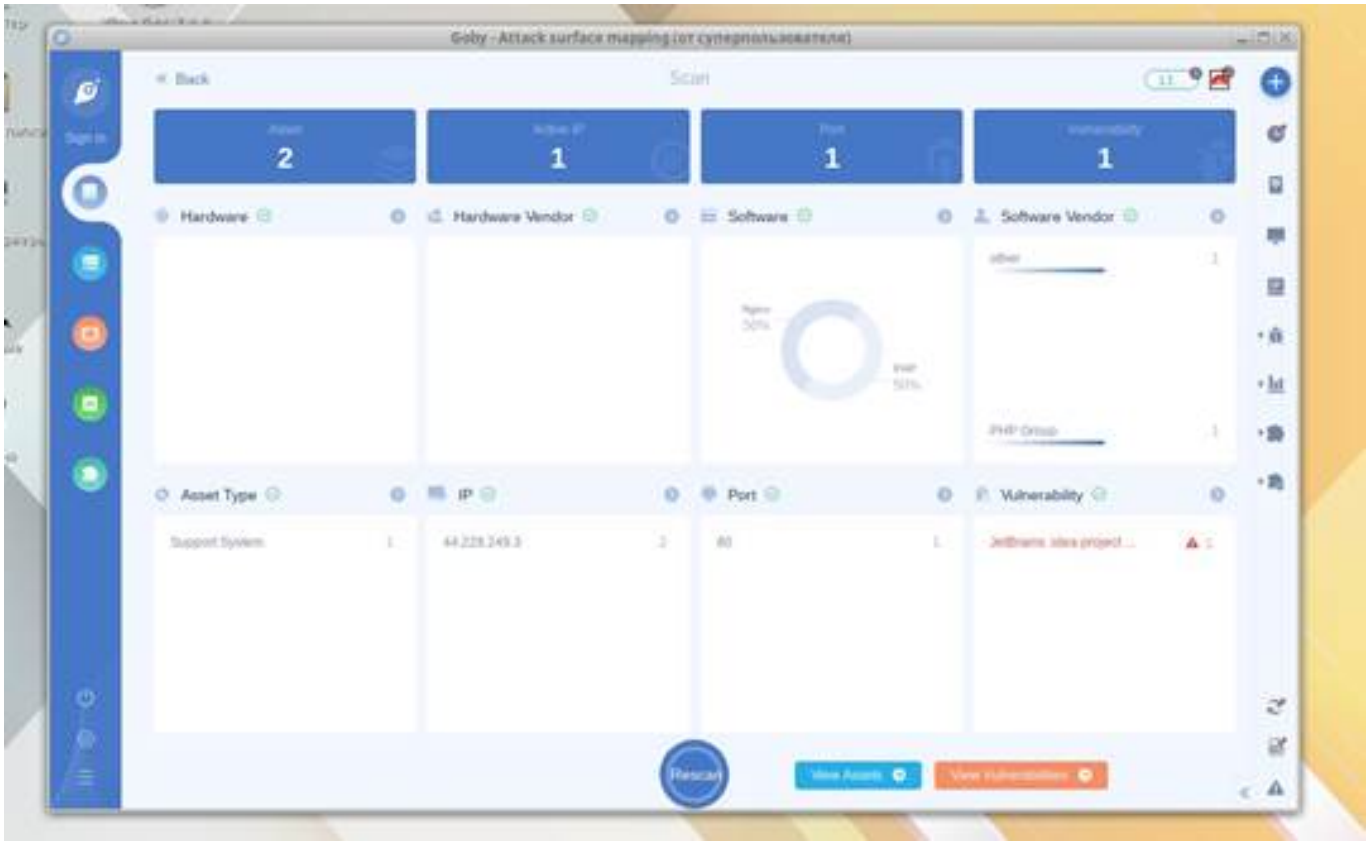

Рисунок 5. Скриншот 3.5 - проверка домена testphp.vulnweb.com

Конфигурирование

В ходе исследования функциональности GobySec и практического тестирования было обнаружено, что файл конфигурации config.json имеет ограниченную область применения. Как показал анализ, этот файл не затрагивает параметры сетевого сканирования, что важно учитывать при настройке программы.

Фактически, config.json отвечает только за настройки интерфейса. В частности, в нем задаются:

- цветовые схемы программы
- параметры шрифтов
- расположение элементов интерфейса

Все основные параметры сканирования (диапазоны IP-адресов, перечень проверяемых портов, используемые плагины) настраиваются через графический интерфейс программы. Это подтвердилось в ходе тестирования - изменения в config.json не влияли на процесс сканирования, затрагивая лишь внешний вид приложения.

Поэтому при работе с GobySec важно понимать, что настройка сканирования осуществляется не через конфигурационный файл, а с помощью соответствующих элементов интерфейса программы. Файл config.json служит исключительно для изменения визуального представления данных.

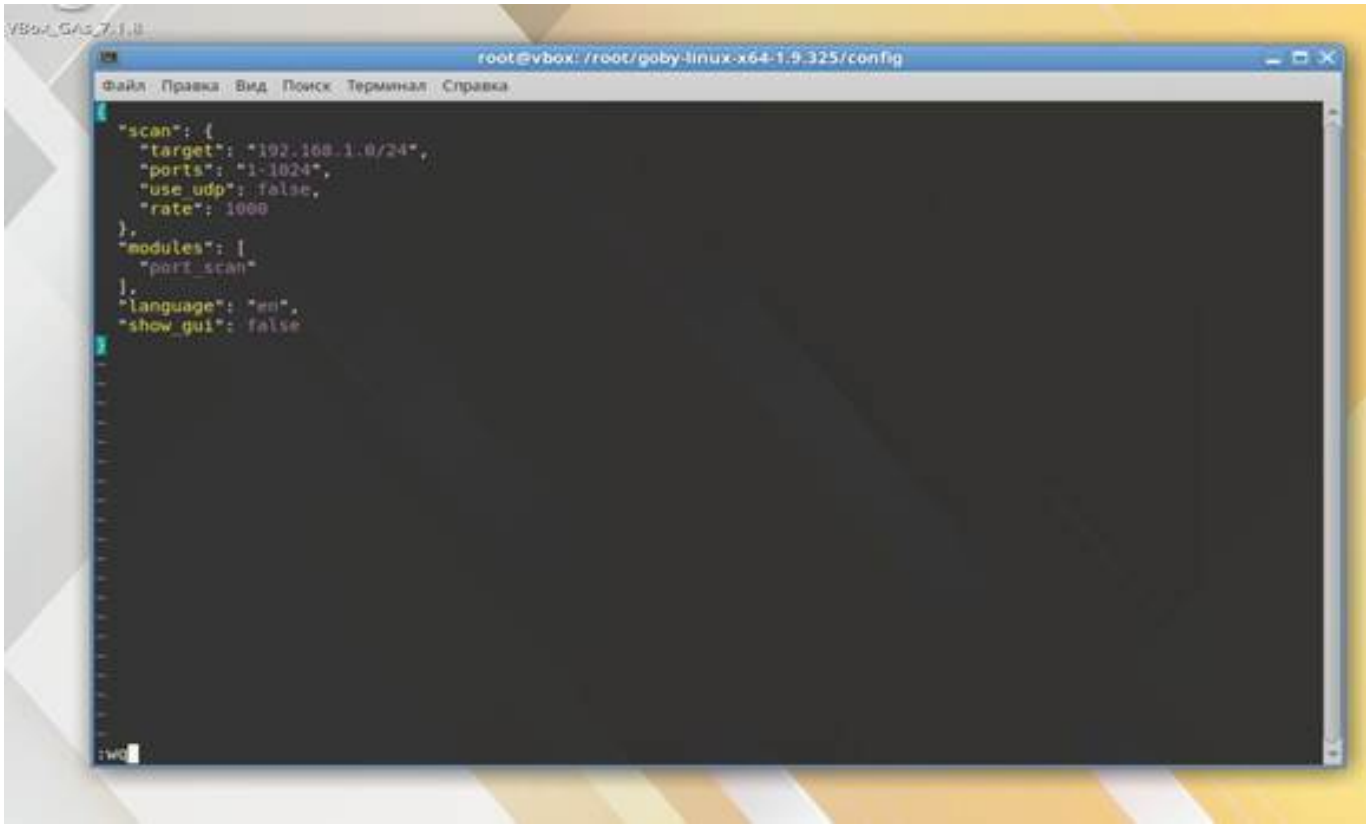

Рисунок 6. Скриншот 3.6 - изменение конфигурационного файла config.json

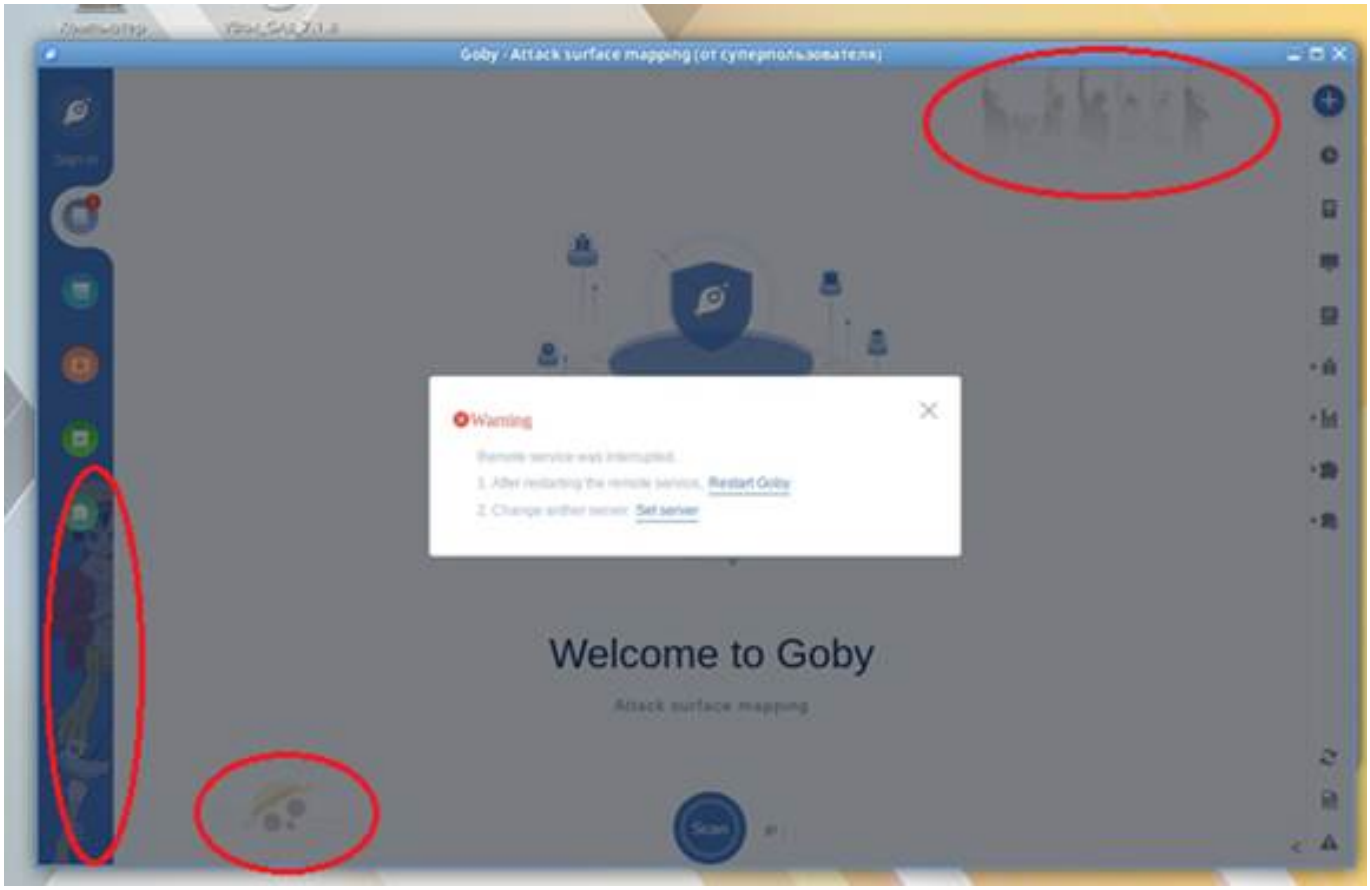

Рисунок 7. Скриншот 3.7 - результат изменения конфигурационного файла config.json

Рисунок 8. Скриншот 3.8 - конфигурации/настройки сканирования

Основные параметры сканирования:

IP/Domain - Целевой адрес для сканирования (домен или IP).

- Пример: demo.testfire.net — тестовый сайт для проверки уязвимостей.

Black IP - Исключение определенных IP-адресов из сканирования.

- Enterprise - предустановленный шаблон для корпоративных сетей (исключает критичные инфраструктурные узлы).

Port - Список портов для проверки. Формат:

- 21,22,80 — TCP-порты
- U:53,U:69 — UDP-порты (префикс U:)

Дополнительные опции:

Don't scan network printers - Исключает сетевые принтеры из сканирования для избежания их перегрузки.

Advanced - Включает расширенные настройки (продемонстрированы ниже).

Vulnerability - Тип проверяемых уязвимостей.

• Пример: General PoC — базовые проверки с доказательством концепции (Proof of Concept).

Order - Приоритет сканирования.

• Пример: Assets First — сначала проверяет ключевые ресурсы (веб-серверы, БД).

Расширения

GobySec поддерживает использование дополнительных плагинов для расширения возможностей сканирования. Однако практическое применение этих модулей сопряжено с объективными сложностями. Основная проблема заключается в языковом барьере – большинство доступных плагинов, включая специализированные проверки для уникальных уязвимостей, имеют интерфейс и документацию только на китайском языке. Трудности возникают на всех этапах работы. Без перевода невозможно точно определить функциональные возможности модуля и выбрать подходящий плагин. Параметры конфигурации также представлены только на китайском языке, что усложняет настройку продукта. Отчеты и диагностические сообщения не понятны без перевода – это мешает интуитивному анализу результатов.

Особенные проблемы вызывает работа с узкоспециализированными проверками, например, для китайских CMS. В таких случаях даже технические термины в отчетах используют китайскую лексику, что делает интерпретацию результатов практически невозможной для иностранных пользователей.

Из-за имеющегося языкового барьера использование продукта имеет некоторые негативные стороны. Объективно снижается эффективность использования инструмента, возникает риск неправильной интерпретации данных сканирования и возникают потенциальные ошибки в оценке уровня безопасности. На мой взгляд, для решения проблемы необходимы локализация плагинов со стороны разработчиков или создание сообщество переводов документации. Также важна разработка англоязычных/русскоязычных аналогов специализированных проверок.

Текущая ситуация существенно ограничивает применение GobySec в международной среде, несмотря на его технические возможности.

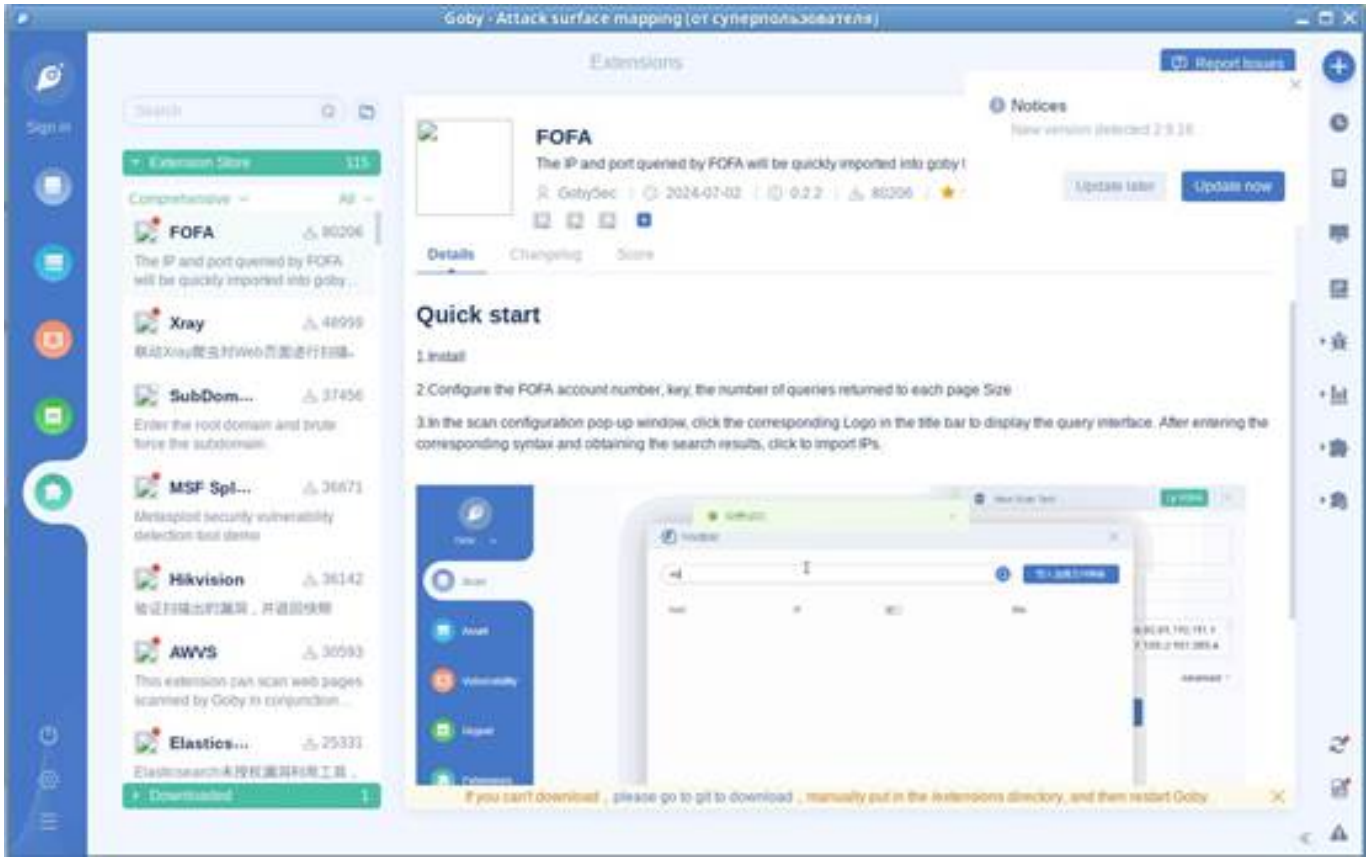

Рисунок 9. Скриншот 3.9 – демонстрация расширений и их локализации

Заключение

При выполнении данной курсовой работы был выполнен полный анализ инструмента GobySec, который создан для тестирования сетевой безопасности. GobySec функционирует на базе операционной системы Alt-Linux. В числе целей данного исследования значились:

1. Настройка GobySec.
2. Осуществление сканирования тестовой сети.
3. Выявление существующих уязвимостей.
4. Разработка рекомендаций по их устранению.

В ходе исследования удалось успешно достичь всех поставленных целей.

Выводы, сделанные в результате проведенной работы, подтверждают, что GobySec представляет из себя эффективный инструмент для автоматизированного сканирования уязвимостей. GobySec сочетает в себе обширный функционал и простоту использования. Эти особенности делают его очевидным выбором для специалистов, работающих в области кибербезопасности. Но необходимо отметить, что основным минусом продукта для русскоязычных пользователей является языковой барьер - большинство плагинов представлены исключительно на китайском языке.

Но даже при наличии данного недостатка, GobySec все равно остаётся наиболее перспективным инструментом в контексте его использования для интеграции с системами SIEM (Security Information and Event Management), а также для разработки собственных модулей, которые могут пригодиться для расширения возможностей продукта.

Операционная система Alt-Linux зарекомендовала себя как стабильная и надёжная платформа для развертывания GobySec. Она полностью соответствует всем российским стандартам информационной безопасности что делает её особенно подходящей для использования в отечественных организациях.

В результате проведенного анализа были выработаны следующие рекомендации:

1. Регулярно использовать GobySec для мониторинга корпоративных сетей — это позволит своевременно выявлять и устранять уязвимости.
2. Для расширения функциональности инструмента важно разрабатывать локализованные плагины. Это позволит сделать его более доступным для пользователей, говорящих на русском языке.
3. Учитывать юридические аспекты тестирования, чтобы избежать возможных правонарушений.

Перспективы дальнейшего исследования включают в себя углублённое изучение API GobySec и сравнение эффективности GobySec с другими известными инструментами, такими как Nessus и OpenVAS. Более доскональное исследование API для автоматизации процесса сканирования позволит значительно повысить эффективность работы с инструментом, а сравнение инструментов поможет лучше понять сильные и слабые стороны каждого из продуктов и выбрать наиболее подходящий для каждой конкретной задачи.

Таким образом GobySec - ценный инструмент для специалистов по кибербезопасности, который значительно повысит уровень защиты данных в организациях, а его интеграция в отечественные инфраструктуры будет способствовать улучшению общей безопасности информационных систем в России. Дальнейшее развитие проекта и активное участие сообщества помогут устранить существующие ограничения и расширить сферу применения GobySec.

Список литературы:

1. GobySec Official Documentation – GitHub Repository Официальная документация по установке, настройке и использованию GobySec.

2. ALT Linux Documentation – Базальт СПО Руководство по установке и администрированию ОС Альт.

3. Nessus vs. OpenVAS: Comparison Guide – Tenable, 2023. Сравнительный анализ инструментов для тестирования уязвимостей.

4. Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры" – 2023. Требования к защите сетевой инфраструктуры.

5. СТБ 34.101.77-2023 "Методы тестирования защищенности ИС" Стандарты проведения аудита безопасности.

6. GDPR (General Data Protection Regulation) – Европейский регламент, 2018. Правовые аспекты тестирования систем, работающих с персональными данными.

7. Уймин, А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65. – EDN VSLWIA.