ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ЭКЗЕМПЛЯРА ПО

1. Наименование и назначение Системы

Наименование Системы — ПО «METASCAN» в русской транскрипции «МЕТАСКАН».

Назначение Системы:

Облачный сканер «МЕТАСКАН» представляет собой ПО-оркестратор набора специализированных программных средств (микросервисов), позволяющее пользователям автоматизировать работы по контролю доступных из сети Интернет информационных активов (сервера, сервисы и веб-ресурсы). Для достижения максимальной экономии трудозатрат «МЕТАСКАН» автоматический формируются отчеты содержащие исчерпывающую информацию об обнаруженных активах.

2. Система представляет собой:

ПО «METASCAN» представляет собой оркестратор набора специализированных программных средств (микросервисов) и предназначено для контроля доступных из сети Интернет информационных активов (сервера, сервисы и веб-ресурсы), а именно:

- обнаружение и идентификация;
- инвентаризация и регулярный контроль изменений;
- обнаружение ошибок конифгураций и уязвимостей;
- техническая, статистическая и аналитическая отчетность;
- интеграция с любой смежной системой (IRP, SGRC, SIEM и др.).

3. Технические характеристики устройства для установки Системы:

Для использования ПО «METASCAN» необходимо:

- персональный компьютер или планшет, с подключением к сети Интернет
- рекомендуется использовать устройства с разрешением экрана не менее чем 1920x1080
- браузер с поддержкой технологии React 1.2.

4. Функциональные возможности Системы:

Функциональные возможности ПО «METASCAN» позволяют проводить проверку неограниченного количества ресурсов в течении не более одних суток (24 часа) с проведением проверок на сетевых уровнях от L3 до L7, идентифицировать доступные сетевые порты в диапазоне 0-65535 работающих по протоколам TCP или UDP, обнаруживать уязвимости и ошибки конфигурации системных и веб-сервисов, автоматический генерировать скрипт для ручной проверки выявленных уязвимостей.

ПО «METASCAN» позволяет:

1. проводить поиск ресурсов доступных из сети Интернет;
2. регулярно проверять доступность каждого порта внешнего сетевого периметра и контролировать их соответствие на соответствие списку разрешенных портов на внешнем сетевом периметре;
3. для всего программного и программно-аппратного обеспечения доступного из сети Интернет определять отсутствующие обновления безопасности;
4. ранжировать уязвимости ПО по критичности;
5. подбирать пароли для ssh, ftp, ftps, ms-sql, mysql, postgresql, vnc. Подбираются пароли для сетевого оборудования - snmp, cisco-telnet, winbox;
6. выявлять ошибки администраторов и разработчиков в настройке прав на файлы и папки на веб-серверах приводящие к утечке критичных данных;
7. обнаруживать уязвимости в веб-приложениях позволяющие захватить контроль над приложением или сервером, атаковать посетителей сайтов (используется классификация по OWASP-TOP-10. Обнаружение XSS, SQLi, NoSQLi, RCE, XXE и других).
8. выявлять уязвимости в используемых компонентах веб-фреймворков и CMS. Поддерживается Magento, Wordpress, Bitrix. Находим уязвимости в js-библиотеках используемых веб-приложением.
9. генерировать скрипт для ручной проверки эксплуатации уязвимости.

4.1. Категории пользователей Системы:

4.2. Возможность использования определенных функциональных возможностей Системы для определенного категории пользователей:

В данном разделе представлены функциональные возможности для каждой группы пользователей:

Посетитель – неавторизованный пользователь, обладает правами:

- Просмотр всех справочных материалов, размещенных в открытом доступе на сайте;
- Поиск по размещенным на сайте справочным материалам;
- Регистрация и аутентификация;

- Запросы на предоставление дополнительной информации по размещаемым на платформе материалам через отправку запроса в формах заявок, формах обратной связи.

Авторизованный Пользователь — Пользователь, идентифицированный Сайтом и/или Платформой. Авторизованный пользователь обладает правами:

- Посетителя;
- использования функционала ПО «METASCAN»:
  - добавление и редактирование данных о узлах в сети Интернет.
  - запуск сканирования ресрусов по адресу, доменному имени или подсети.
  - получение отчетов по результатам проведенного сканирования, в виде веб-формы или в формате CSV
  - получение статистической информации о работе ПО «METASCAN».

4.3. Состав программных средств

Система состоит из следующих логических модулей:

Общее назначение	Назначение	Модуль
Разведка	Пассивая сетевая разведка	Subfinder
	Активная сетевая разведка	Amass, dnsrecon
	Поиск доменов уязвимых к Hijack	Subjack
Обнаружение открытых портов	Обнаружение открытых портов со скоростью до 1млн. syn в секунду	Masscan
	Обнаружение версий используемоего ПО	Nmap + custom probes
Поиск системных уязвимостей	Запуск эксплойтов для сетевых сервисов	NSE, NASL
	Обращение к базам NIST и CVEdetails	NIST Module, CVEdetails module
	Подбор паролей для системных сервисов	hydra, patator
Поиск веб-уязвимостей	Съемка скриншотов для всех веб-сервисов отвечающих по http	screenshooter
	Обнаруженеи используемых WAF	Wafw00f
	Поиск уязвимостей в CMS	magescan

	Построение карты веб-приложения	katana
	Поиск ошибок в настройке прав на файлы и папки	dirsearch
	Поиск недостатков в настройке заголовков веб-приложений отвечающих за ИБ	securityheaders
	Поиск Generic OWASP-TOP-10 веб-уязвимостей	ZAP
	Поиск уязвимостей конкретных веб-приложений	Nuclei

Система поддерживает следующие современные браузеры: Mozilla Firefox, Safari, Google Chrome, Yandex.Browser.

4.4. Для функционирования Системы требуются:

- ПК или планшет с подключением к сети Интернет
- рекомендованное разрешение экрана 1980x1080
- Веб-браузер должен иметь ворможность выполнять JavaScript коди и быть совместим с React 18. Поддерживается последними версиями браузеров:
  - Edge 15 или новее,
  - Firefox 59 или новее,
  - Opera 12.10 или новее,
  - Google Chrome 66 или новее;

  Для корректной работы системы рекомендуется регулярно обновлять браузер.
  - Неподдерживаемые веб-браузеры: Internet Explorer, Opera версий до версии 12.02, прочие браузеры.
- Пакет офисного ПО (например, LibreOffice или Microsoft Office) для удобства работы с техническими отчетами выгружаемыми из интерфейса в формате CSV.

4.5. Язык программирования

Языками программирования для Системы являются Python и JavaScript.