1.Функциональные возможности Сканера

Сканер обеспечивает возможность проведения анализа защищенности внешнего периметра исследуемых информационных систем. Серверы Сканера предоставляют возможность обеспечивать проведение анализа не менее чем из 7 (семи) территориально распределенных IP-сетей.

Заказчику предоставляется интерфейс управления Сканером в виде веб-консоли, доступной из сети Интернет, для получения информации по выявленным уязвимостям, а также получения доступа к запуску выборочных проверок и формированию отчетов.

В ходе анализа защищенности внешнего периметра Сканером должно осуществляться:

– выявление всех открытых портов;

– инвентаризация доменных имен и связанных PTR записей;

– анализ всех уязвимостей, выявленных на объектах, и формирование рекомендаций по их устранению;

– проверка наличия в веб-приложениях следующих уязвимостей:

а) уязвимости, связанные с безопасностью компонентов сторонних производителей (Third-Party Components);
б) уязвимости инъекции внешних сущностей XML (XXE);
в) уязвимости конфигураций безопасности;
г) уязвимости аутентификации и управления сеансами;
д) уязвимости управления доступом;
е) внедрение SQL-кода (SQLi);
ж) межсайтовый скриптинг (XSS);
з) подделка HTTP-запросов (CSRF);
и) уязвимости WebSocket и REST API;
к) уязвимости конфигураций контейнеров и оркестрации (например, Kubernetes, Docker);
л) уязвимости, возникающие по причине некорректной конфигурации серверов и приложений (Misconfiguration Vulnerabilities);
м) уязвимости инъекции команд (Command Injection);
н) уязвимости обхода средств защиты информации (Bypass Vulnerabilities);
о) уязвимости, возникающие по причине недостаточной проверки ввода (Input Validation);
п) уязвимости подключения файлов (LFI, RFI);
р) уязвимости обхода бизнес-логики (Business Logic Vulnerabilities);
с) уязвимости, возникающие по причине неправильной обработки ошибок (Improper Error Handling);

– обнаружение и анализ скрытых путей и файлов в веб-приложениях;

– использование методов эмуляции браузера для проверки безопасности веб-приложений;

– проверка наличия и эффективности средств защиты от автоматических атак (например, использование автоматизированного теста Тьюринга);

– анализ безопасности криптографических протоколов и сертификатов SSL/TLS;

– проверка конфигураций веб-серверов и приложений;

– определение типов и имен сервисов (HTTP, FTP, SMTP, POP3, DNS, SSH и др.) на нестандартных портах с использованием эвристического метода;

– интерактивное обнаружение веб-уязвимостей в соответствии с классификатором OWASP TOP10 2021, включая XSS, SQLi, NoSQLi, CMDi, OBJi, DoR, Security Missconfiguration, Cryptographic Failures;

– обнаружение ошибок в конфигурации прикладного ПО веб-серверов, в частности, некорректную настройку прав доступа к файлам веб-приложений;

– проверка безопасности передачи данных между клиентом и сервером, включая проверку корректности настройки HTTPS, использования безопасных протоколов и сертификатов;

– обнаружение возможности реализации угроз типа CSRF (Cross-Site Request Forgery) и XXE (XML External Entity);

– проверка и анализ безопасности REST и SOAP API, включая тестирование на уязвимости в аутентификации, авторизации и обработке данных;

– обнаружение и анализ применения старых или неподдерживаемых версий ПО, которые могут содержать известные уязвимости;

– автоматическое сканирование новых или обновленных веб-страниц и приложений для выявления потенциальных угроз безопасности;

– генерация детализированных отчетов с описанием обнаруженных уязвимостей, рекомендациями по их устранению и оценкой риска для бизнеса;

– обнаружение и анализ уязвимостей, связанных с использованием сторонних библиотек и фреймворков в программных продуктах;

– верификация выполнения рекомендаций по безопасности и настройкам, предложенных стандартами (например, PCI-DSS, ISO 27001);

– обнаружение и анализ уязвимостей в IoT (Internet of Things) устройствах и системах;

– проверка реализации механизмов резервного копирования и восстановления данных, оценка их устойчивости к компьютерным атакам;

– обнаружение и анализ уязвимостей в приложениях, использующих микросервисную архитектуру и контейнеризацию (например, Docker, Kubernetes);

– анализ безопасности файлового хранилища и систем обмена файлами, включая проверку прав доступа и защищенности данных;

– активное сетевое сканирование без аутентификации (Black box);

– активное сетевое сканирование с аутентификацией в веб-приложениях (Gray box);

– возможность задания целей сканирования по IP-адресам, доменным именам, спискам активов;

2 Формирование отчетов по результатам работы Сканера

Формируемый Сканером отчет содержит:

– перечень просканированных узлов с указанием IP-адресов, открытых портов, сетевых служб;

– общую сводку по обнаруженным уязвимостям с указанием их уровней опасности;

– подробные сведения по каждой выявленной уязвимости, содержащие следующую информацию:

а) название уязвимости;

б) краткое и подробное описание уязвимости;

в) расширенная официальная информация об уязвимости, в том числе CVSS v2, CVSS v3, CVSS v4, ссылки на соответствующие базы знаний;
г) информация о наличии эксплойта;
д) описание способов устранения уязвимости (рекомендации по устранению).