С. А. Макиенко, Д. С. Преподобный, А. Е. Козлов
Тюменский государственный университет, г. Тюмень
УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ REDCHECK И MAXPATROL 8

Аннотация. В статье представлен сравнительный анализ двух сканеров уязвимостей RedCheck и MaxPatrol 8. Рассмотрены режимы работы сканеров. Был сделан вывод о том, какой организации и сегменту сети функционал сканера соответствует наилучшим образом.

Ключевые слова: сканер безопасности, уязвимость, тестирование на проникновение, аудит.

Введение. С каждым годом количество кибератак на различные информационные системы только растет. Согласно отчету компании Positive Technologies [1], количество успешных инцидентов за 2022 г. увеличилось почти на 21%. Для предотвращения несанкционированного доступа необходимо выявлять уязвимости в системе до момента их эксплуатации злоумышленниками. С этим могут помочь сканеры уязвимостей [2]. Были определены уязвимости системы безопасности сети и рабочих станций, разработан сканер уязвимостей [3]. Статьи [4-5] легли в основу нашей статьи, были заимствованы процессы сравнения и анализа сканеров. В статье [6] авторы проводят сравнительный анализ зарубежных сканеров уязвимостей, нами были дополнены некоторые важные критерии сравнения.

Проблема исследования. В нынешних реалиях приобрести зарубежное ПО не является возможным, качественные и проверенные временем сканеры уязвимостей ушли с рынка продаж, следовательно повышается спрос и актуальность отечественных сканеров. В нашей статье мы проведем сравнительных анализ двух отечественных сканеров уязвимостей — RedCheck и MaxPatrol 8.

Материалы и методы. Для начала, необходимо понять, что такое сканер уязвимостей. Сканер уязвимостей — это сложное программное/аппаратное решение для сканирования информационной системы. Главной задачей сканера является оценка безопасности и поиск уязвимостей.

Функционал у двух приложений одинаковый — модули pentest и audit.

Pentest — с его помощью можно сканировать порты и хосты, а также контролировать защиту периметра от возможных сетевых угроз.

Модуль Audit может решать проблемы контроля программного обеспечения на рабочих станциях с двух сторон: по отслеживанию разрешенного установления (инвентаризации) и обнаружению уязвимостей в ПО. Он также отвечает за оперативные обновления.

Основываясь на критериях сравнения сканеров из статьи [6], нами были выбраны следующие критерии сравнения — поддерживаемые системы, стоимость, качество работы модулей Pentest и Audit, удобство эксплуатации модулей Pentest и Audit, техническая поддержка, наличие бесплатной версии.

Pentest (Качество работы модуля)

Оба сканера уязвимостей справляются с поиском и категоризацией уязвимостей хорошо. RedCheck создан на основе Nmap сканера и имеет большое количество скриптов. MaxPatrol 8 создан на основе XSpider, имеет большое количество скриптов, а также “умный алгоритм” применения данных скриптов.

Pentest (Удобство эксплуатации модуля)

В удобстве эксплуатации лучше себя проявил сканер MaxPatrol 8, так как сканирование осуществляется с использованием «умного алгоритма». Сначала сканер строит список сетевых активов, затем применяет скрипты, относящиеся именно к идентифицированным сервисам, а не все подряд к каждому, как у RedCheck. Данный подход в разы ускоряет процесс сканирования.

Audit (Качество работы модуля)

Лучше находит уязвимости — RedCheck. Сканер смог обнаружить больше уязвимостей в том числе и критических. Режим Audit в RedCheck — сильная сторона данного продукта. Сканер решит вопрос с постоянным мониторингом уязвимостей ПО и его автоматическим обновлением.

Audit (Удобство эксплуатации модуля)

В этом режиме минусом RedCheck является ограничение в одну учетную запись на одну задачу. Таким образом, удобнее в эксплуатации оказался MaxPatrol 8. В нем не нужно создавать несколько

задач под разные операционные системы и профили сканирования — это удобно, ведь в больших компаниях рабочие машины появляются часто, меняются IP адреса. С RedCheck придется постоянно отслеживать эти изменения и создавать новые задачи. MaxPatrol 8 делает это самостоятельно. MaxPatrol 8 подойдет постоянно развивающемуся сегменту, а RedCheck более статичному.

Результаты. По результатам сравнения сканеров (табл. 1), сложно определить какой продукт лучше, так как каждый имеет свои преимущества и недостатки:

- MaxPatrol 8 проявил себя лучше в режиме Pentest, а также его конфигурационные настройки в этом режиме удобнее, но он имеет посредственный режим Audit. Больше подходит развивающемуся сегменту сети.
- RedCheck находит больше уязвимостей в режиме Audit, но не так удобен в эксплуатации, как MaxPatrol 8. Больше подходит статичному сегменту сети.

Таблица 1

Сравнение сканеров уязвимостей

Сканер	*RedCheck*	*MaxPatrol 8*
1	*2*	*3*
Поддерживаемые системы	Microsoft Windows, RedHat, Debian, Ubuntu, SUSE, Oracle Linux, CISCO IOS, Huawei VRP и др.	Microsoft Windows
Стоимость	Общедоступные прайс-листы. 10 IP-адресов, 1 год = 62 800 руб.	По согласованию с производителем ПО. ≈ 7 000 000 руб.
Pentest	Сканер Nmap, скрипты. Долгое сканирование	Сканер XSpider, скрипты. Собственный «умный алгоритм», ускоряющий сканирование
Audit	Найдено больше уязвимостей. Постоянный мониторинг ПО и автоматическое обновление. Ограничение — одна учетная запись на одну задачу	Найдено меньше уязвимостей. Меньший функционал. Отсутствует ограничение — одна учетная запись на одну задачу

Окончание табл. 1

1	*2*	*3*
Техническая поддержка	Присутствует, но продается отдельно	Присутствует при приобретении
Бесплатная версия	Есть 30-дневный бесплатный период с полным функционалом	Демонстрация работы продукта, в том числе и на устройстве заказчика

Заключение. Таким образом, если вам нужен сканер с упором на сетевое сканирование уязвимостей, то лучше окажется MaxPatrol 8, если упор идет на внутреннее сканирование (Audit), то, соответственно, — RedCheck. Также немаловажным фактором при выборе сканера будет цена, так как она значительно отличается, то разумнее выбрать сканер RedCheck.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: итоги 2022 года. — Текст: электронный // Positive technologies: официальный сайт. — 2023. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 01.05.2023).
2. Крутофал Г. Е. О необходимости применения сканеров уязвимостей для обеспечения информационной безопасности / Г. Е. Крутофал — Текст: электронный // Евразийский научный журнал. — 2022. — №. 4. — URL: https://cyberleninka.ru/article/n/o-neobhodimosti-primeneniya-skanerov-uyazvimostey-dlya-obespecheniya-informatsionnoy-bezopasnosti/viewer (дата обращения: 01.05.2023).
3. Долгин А. А. Разработка сканера уязвимостей компьютерных систем на основе защищенных версий ОС Windows / А. А. Долгин, П. Б. Хорев // Труды международной научно-технической конференции «Информационные средства и технологии. — 2005. — URL: https://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=7&pa=14&ar=6 (дата обращения: 01.05.2023).
4. Габитов А. Э. Сравнительный анализ сетевых сканеров безопасности / А. Э. Габитов — Текст : электронный // Мавлютовские чтения. — 2021. — URL: https://www.elibrary.ru/item.asp?id=47305109 (дата обращения: 01.05.2023).

5. Ильин Е. В. Обзор сканеров уязвимостей веб-приложений / Е. В. Ильин, К. Е. Сергеев — Текст : электронный // Информатика и вычислительная техника. — 2021. — URL: https://www.elibrary.ru/item.asp?id=46643284 (дата обращения: 01.05.2023).
6. Рожкова Е. О. Обзор и сравнение сканеров уязвимостей / Е. О. Рожкова, И. В. Ильин, С. Я. Галушин. — Текст : электронный // Научное сообщество студентов XXI столетия. Технические науки. — 2015. — URL: https://sibac.info/sites/default/files/archive/technic/3(29).pdf#page=78 (дата обращения: 01.05.2023).
7. АЛТЭКС-СОФТ : IT компания : [сайт]. — URL: https://www.altx-soft.ru (дата обращения 01.05.2023). — Текст : электронный.
8. Positive Technologies : IT компания : [сайт]. — URL: https://www.ptsecurity.com/ru-ru/ (дата обращения 01.05.2023). — Текст : электронный.
9. Марков А. С. Опыт тестирования сетевых сканеров уязвимостей / А. С. Марков, С. В. Миронов, В. Л. Цирлов. — Текст: электронный // Информационное противодействие угрозам терроризма. — 2005. — №. 5. — URL: https://elibrary.ru/item.asp?id=9572216 (дата обращения 01.05.2023).
10. Грин Д. Сравнение сканеров уязвимостей: AppDetectivePro 5.4. 6 и AuditPro Enterprise 4.0 / Д. Грин. — Текст : электронный // Windows IT Pro/RE. — 2012. — №. 6. — URL: https://elibrary.ru/item.asp?id=18378787 (дата обращения 01.05.2023).