Литература:

1. *Козирацкий Ю.Л.* Модели информационного конфликта средств поиска и обнаружения. Монография. – М.: Радиотехника, 2013. – 232 с.

2. *Леньшин А.В., Кравцов Е.В., Славнов К.В.* Методика оценки эффективности защиты информации на объектах комплексного технического контроля // Радиотехника. – 2021. – №1. – С. 20-27.

3. *Кравцов Е.В.* Методический подход к комплексной оперативной оценке возможностей выявления сведений об объектах защиты // Телекоммуникации. – 2020. – № 9. – С. 33-41.

DOI: 10.25728/iccss.2022.22.51.063

Еронин Д. А., Мелихов А.А.

Разработка автоматизированного средства, предназначенного для выявления потенциально опасных конфигураций ИС малого предприятия

Аннотация: В работе рассматривается проблематика использования средств обнаружения уязвимостей в конфигурации ИС малого предприятия и предложено решение позволяющие автоматически проводить регулярный аудит и выявлять уязвимости.

Ключевые слова: обнаружение уязвимостей, сканер безопасности, аудит безопасности, управление уязвимостями

Введение

Поддержание надёжного функционирования бизнес-процессов и обеспечение конфиденциальности данных сегодня актуально для любого типа предприятия - как большого, так и малого. Однако возможностей для построения системы обеспечения безопасности у малого предприятия значительно меньше. Это вызвано как бюджетными ограничениями, так и отсутствием финансовой возможности найма отдельных специалистов, занимающихся непосредственно обеспечением информационной безопасности. В итоге, задача обеспечения информационной безопасности предприятия ложится на системного администратора, для которого

она имеет гораздо меньший приоритет, чем обеспечение физической работоспособности вверенной системы, что в свою очередь непосредственно влияет на качество и оперативность принимаемых решений [1].

Отдельную проблему представляет собой инструментарий. Полномасштабные автоматизированные системы контроля защищённности дороги и сложны в эксплуатации, у малого предприятия просто не будет средств на их закупку. Альтернатива – применение бесплатных инструментов с открытым исходным кодом, однако их условная бесплатность на практике требует существенно больших временных затрат на адаптацию инструментов к условиям конкретной информационной среды предприятия. Такой подход позволяет покрыть базовые задачи, возникающие в рамках процесса управления уязвимостями, однако требует использования разнородных компонент фактически в ручном режиме, что существенно снижает общую производительность сотрудника, замедляя реакцию на возникающие угрозы. Помимо этого, обработка данных, полученных из различных источников, требует их детального анализа и консолидации с учётом особенностей режимов работы применяемых инструментов [2].

Таким образом, возникает задача объединения результатов работа различных сканеров в единый внутренне непротиворечивый отчёт, на основе которого квалифицированный системный администратор сможет оперативно и обоснованно принимать решения, направленные на повышение защищённости вверенной системы.

В рамках настоящей публикации предложено решение данной задачи, позволяющее автоматизировать процесс выявления опасных конфигураций информационных систем малого предприятия и отслеживать их устранение. Данное решение было представлено и защищено в качестве бакалаврской выпускной квалификационной работы на кафедре информатики и вычислительных сетей ИНБИКСТ МФТИ.

Требования к системе

Основная идея разрабатываемого решения – взять доступные утилиты, используемые для ручного анализа защищённости и объединить их в единую автоматизированную систему, требующую

от оператора только задания необходимого диапазона сканирования. В рамках процесса управления уязвимостями подразумевается определять подверженность сканируемой инфраструктуры к следующим видам атак: эксплуатации уязвимостей ПО, подбору учётных записей и атакам на незащищённые протоколы.

Разрабатываемая система должна быть реализована на основе модульной архитектуры, где каждый модуль отвечает за свой вид проверок, покрывающих обнаружение одной из указанных выше уязвимостей, или другие задачи, как например составление отчёта. Это позволяет использовать лишь необходимые проверки, а в случае необходимости, изменять имеющиеся или добавлять новые модули без изменения остальных.

Выбор интегрируемых компонентов должен быть обоснован функциональными возможностями. Поскольку разрабатываемое средство относится к классу средств защиты, необходимо контролировать прозрачность получения исходных кодов, определять и устранять найденные в них уязвимости, а также обеспечить независимое хранение на базе локального репозитория [3].

Техническая реализация

Для унификации данных о сканируемой системе используется единый JSON-объект, создаваемый при запуске сканирования и впоследствии пополняемый модулями проверок. Требуемые параметры сканирования хранятся в конфигурационном файле, где указываются IP-адреса сканируемых хостов, требуемые модули и их конфигурация.

Система включает в себя модули сетевого сканирования, проверки по базе данных известных уязвимостей, определения разрешённых/запрещённых сервисов, подбора учётных записей и составления отчёта.

В основе модуля сетевого сканирования лежит утилита Nmap – сетевой сканер с открытым исходным кодом, со скриптовым движком NSE, позволяющим значительно расширить функционал. Так, проверка на наличие известных уязвимостей ПО реализована в виде NSE-скрипта, где в качестве базы данных уязвимостей используется Vulners, которая представляет из себя агрегатор популярных баз уязвимостей, баг-репортов поставщиков ПО и

общедоступных эксплоитов. Это облегчает задачу, поскольку получаемы данные имеют единый вид, а за счёт большого количества источников, снижается вероятность не обнаружить имеющуюся уязвимость. Результаты сетевого сканирования и проверке по базе уязвимостей сохраняются в XML-формате, после чего преобразуются в JSON-объект.

Затем выполняется проверка обнаруженных сервисов, запущенных на сканируемом хосте, по спискам разрешённых/запрещённых, указанным в конфигурационном файле.

Подбор учётных записей производится утилитой Patator. Данная утилита способна работать с большим количеством протоколов и позволяет самостоятельно настраивать фильтрацию получаемых от серверов ответов, что позволяет исключить ложные срабатывания. В конфигурационном файле указывается, какие из возможных сервисов требуется сканировать. Учётные данные успешных подключений добавляются в CSV-файл, откуда парсятся и добавляются в список всех обнаруженных уязвимостей.

После всех проверок, создаётся HTML-отчёт. Выполняется сравнение, результаты текущего сканирования сравниваются с предыдущими, указываются новые хосты и порты. Для каждого хоста указывается его операционная система, время работы с последней перезагрузки, открытые порты, сервисы, запущенные на этих портах и их версии. Для каждого порта указываются названия модулей проверок и список обнаруженных ими уязвимостей. Если какие-либо уязвимости не были закрыты с предыдущего сканирования, это также указывается. Цветом обозначается уровень уязвимости соответствующего порта: зелёный – уязвимостей не обнаружено, жёлтый – низкий уровень опасности, оранжевый – средний, красный – высокий. Уровень опасности соответствует наибольшему CVSS среди обнаруженных для него уязвимостей. Полученный HTML-отчёт сохраняется. Помимо этого, в JSON-формате сохраняется вся информация о просканированной системе с названием, соответствующим текущей дате и времени на момент завершения сканирования.

Тестирование программного средства

Для подтверждения соответствия разработанного решения поставленной задаче, проводилось два вида тестирования: первый –

для подтверждения корректности обнаружения уязвимостей и полноты покрытия модели реализации внешних угроз, возникающих на этапе преодоления периметра; второй — с целью убедиться в корректности подтверждения закрытия ранее обнаруженных уязвимостей. В первом случае тестирование производилось на платформе Metasploitable2 – машине под управлением операционной системы Ubuntu, содержащей множество уязвимостей. Во втором случае – на машине с неактуальной версией ОС Ubuntu и с устаревшими версиями ssh-сервера OpenSHH и http-сервера Apache2, после чего было проведено обновление до актуальных версий. Таким образом, было подтверждено, что система способна определять, насколько уязвима сканируемая инфраструктура к таким техникам атак как: эксплуатация уязвимостей ПО, подбор учётных записей и атака на незащищённые протоколы, а также для мониторинга процесса устранения уязвимостей.

Заключение

В настоящей работе была рассмотрена проблема защиты информационных систем малого предприятия, а именно обнаружение уязвимостей в рамках процесса управления уязвимостями. Разработано программное средство, позволяющее проводить сканирование инфраструктуры предприятия на подверженность к распространённым техникам реализации угроз информационной безопасности со стороны внешнего нарушителя. Данное средство прошло апробацию и подтвердило свою эффективность.

Литература:

1. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Анализ фактора неопределённости в процессе подготовки управленческих решений / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 40-46.

2. *Козлов А.Д., Нога Н.Л.* Достоверность информации как элемент обеспечения информационной безопасности и оценка её уровня / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 195-200.

3. *Мелихов А.А.* Обеспечение непрерывной разработки программных продуктов, сертифицируемых по требованиям безопасности / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 189-195.

DOI: 10.25728/iccss.2022.65.81.064

Ковач Е.В., Ткаченко В.А.

Анализ как инструмент улучшения системы управления промышленной безопасностью и охраной труда

Аннотация: Рассмотрены и прокомментированы требования к процедуре проведения анализа функционирования системы управления промышленной безопасностью и охраной труда, предъявляемые со стороны международного стандарта ISO 45001:2018. Приведены рекомендации по проведению такого анализа в части рассмотрения необходимых сведений, формированию полученных результатов. Сделан вывод о том, что досконально проведённый анализ – инструмент улучшения системы управления.

Ключевые слова: анализ, управление, промышленная безопасность и охрана труда

Вопросы обеспечения безопасности производства не теряют своей актуальности. Череда событий с крайне негативными, резонансными последствиями, которая произошла в конце 2021 года, к сожалению, в очередной раз подтвердила остроту этой проблемы. Безусловно, максимум озабоченности был достигнут в результате аварии на шахте «Листвяжная». Ситуация вынудила обратить самое пристальное внимание на решение этой проблемы всю вертикаль управления в Российской Федерации, включая её самые верхние уровни. Стоит отметить тот факт, что работа по повышению результативности существующих мер управления рисками в области промышленной безопасности, охраны труда и других смежных областей, может протекать на самых разных уровнях управления, начиная уровнем соответствующих федеральных органов