Использование EVE-NG в исследовательской деятельности обеспечения безопасности информации

А.И. Бочарова, С.А. Будников, E-mail: ai.bocharova@yandex.ru,

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Аннотация. *Рассмотрена возможность использования среды моделирования EVE-NG для проведения исследований по защищенности инфраструктуры. Продемонстрирована модель компьютерной атаки, эксплуатирующей уязвимость ZeroLogon.*

Ключевые слова: *компьютерная атака, среда моделирования, топология, уязвимость.*

Введение

В настоящее время стали актуальными исследовательские стенды для полунатурного моделирования объектов, а также процессов, характеризующих условия функционирования этих объектов. Высокая точность соответствия разработанных исследовательских стендов [1] реальным объектам позволяет исследовать дорогостоящие инфраструктуры и не оказывать влияния на основные процессы объекта изменять конфигурацию и параметры системы. Такие стенды дают возможность без значительных финансовых затрат исследовать работу объекта в различных вариантах реализации [2], а также сокращают сроки и снижают стоимость проектирования.

Инфраструктура такого исследовательского стенда может быть реализована с использованием технологии аппаратной виртуализации [3], виртуализации сетей, дискретно-событийного моделирования [4] и специального программного обеспечения, моделирующего процессы обмена информации и передачи команд управления, циркулирующих в реальных системах управления технологическими процессами или объектами.

Одним из направлений использования исследовательских стендов является повышение информационной безопасности инфраструктуры организаций за счет: исследования защищенности, обучения персонала и проведения киберучений. Исследование защищенности – это процесс проверки безопасности информационных систем на наличие возможных уязвимостей программных и программно-аппаратных средств, средств защиты информации и сетевых служб, вызванных ошибками конфигурации, программного обеспечения и исходного кода

приложений [5]. Обучение персонала проводится для повышения квалификации, получения новых знаний и развития профессиональных компетенций. Киберучения – это процесс практической подготовки, освоения и проверки навыков у учащихся, специалистов, экспертов и руководителей по обеспечению информационной безопасности путем моделирования компьютерных атак и отработки реакций на них.

Одним из множества решений, наиболее подходящих для создания исследовательских стендов, является разработка моделей инфраструктур в программной среде моделирования EVE-NG [6].

Цель работы: оценка возможностей EVE-NG для проведения исследований по выявлению уязвимостей кода, уязвимостей архитектуры, уязвимостей конфигурации, организационные уязвимости и многофакторные уязвимости.

Среда моделирования Emulated Virtual Environment – Next Generation (EVE-NG) – это набор инструментов для работы с виртуальными устройствами, построением сетей, коммутацией с реальным оборудованием. Возможности данного продукта позволяют легко использовать, управлять, коммутировать моделируемое сетевое оборудование.

У EVE-NG удобный и понятный интерфейс управления: главное окно содержит кнопки управления, вкладки управления и папки и файлы лаборатории. Вдобавок можно осуществить настройки узлов: количество центральных процессоров, выделенных узлу, IDLE PC для узлов Dynamips, NVRAM в Кб, RAM в Мб, количество Ethernet портов, количество последовательных портов.

Таким образом EVE-NG позволяет моделировать испытательную инфокоммуникационную систему с различным уровнем архитектурной интеграции. Особенностью данного комплекса является реализация поддержки вложенного многопоточного режима виртуализации — multi-hypervisor. Использование этого подхода позволяет EVE-NG отойти от концепции использования автономных виртуальных машин для эмуляции соответствующих сетевых устройств. С помощью multi-hypervisor можно создавать виртуальные топологии на основе программных эмуляторов IOU/IOL, Dynamips и узлов QEMU, объединяя все необходимые программные модули и сценарии в виде одного файла в рамках одной платформы или информационной модели.

Ключевыми возможностями EVE-NG является использование [7]:

• QEMU/KVM. В данной связке QEMU выступает в роли эмулятора железа, он достаточно гибок и может запускать код, написанный для одной архитектуры процессора, на другой (ARM на x86 или PPC на ARM). KVM же, в свою очередь, позволяет достигать высокой

производительности благодаря виртуализации с аппаратной поддержкой, такой как Intel VT-x и AMD-V;

• IOU/IOL и Dynamips. Поддержка стареньких, но вполне рабочих коммутаторов и маршрутизаторов Cisco;

• Оптимизация памяти UKSM в ядре. При одновременном использовании однообразных ВМ позволяет дедуплицировать память и тем самым существенно снизить расход RAM;

• Полноценный веб интерфейс на HTML5;

• Многопользовательский режим для одновременной работы различных виртуальных лабораторий;

• Взаимодействие с «настоящей» сетью.

Особенность работы EVE-NG с QEMU-образами заключается в том, что сначала создается некий базовый образ, а при запуске и работе виртуальной машины все изменения пишутся в отдельный файл. Такой механизм очень удобен при групповом обучении, когда несколько пользователей делают параллельно одну исследовательскую работу: изменение настроек в образе у одного пользователя никак не влияет на остальных. Если образ стал неработоспособным вследствие неправильных настроек и на поиск проблемы нет времени, можно нажать кнопку Wipe (Wipe all nodes), и образ в лаборатории у конкретного пользователя вернется к состоянию базового.

Реализованная виртуализация по технологии QEMU в программной среде моделирования сетевых топологий EVE-NG позволяет моделировать типовые объекты как отдельные информационные модели. Созданные в среде QEMU образы основных (базовых) виртуальных устройств и средств позволяют развертывать достаточно сложные информационные модели объектов и формировать виртуальные топологии.

Далее рассмотрим пример моделирования в EVE-NG в интересах исследования защищенности систем в виде модели атаки ZeroLogon.

Компьютерная атака ZeroLogon основана на эксплуатации уязвимости BDU:2020-04016 (CVE-2020-1472). Уязвимость основана на криптографическом дефекте, где один из 256 случайно сгенерированных ключей шифрования состоит из всех нулевых байтов и, соответственно, приводит к шифрованию также всех нулевых байтов. Эта уязвимость позволяет, не прошедшему проверку подлинности, злоумышленнику с сетевым доступом к контроллеру домена аутентифицироваться и получить доступ к командной консоли на другом или этом же контроллере домена и впоследствии полностью контролировать всю критическую информационную инфраструктуру.

Сценарий атаки «Внутренний нарушитель – ZeroLogon» предполагает эксплуатацию уязвимости BDU:2020-04016 CVE-2020-1472 ZeroLogon на контроллере домена под управлением Windows Server 2012 для эскалации привилегий и внедрение полезной нагрузки (скрипта) (смотри рис. 1).

Порядок реализации сценария в среде моделирования EXE-NG.

1. Эксплуатация уязвимости BDU:2020-04016 Zerologon (CVE-2020-1472) на контроллере домена и добавление в группу «Администраторы домена» учетной записи нарушителя.

2. Использование доступа к командной консоли на АРМ оператора SCADA, формирование скрипта для выполнения команд на поиск технологической информации.

3. Эксплуатация уязвимости слабой системы парольной защиты интерфейсов управления и удаленного доступа (SSH) Сервера резервного копирования.

4. Получение доступа к архиву данных SCADA.

5. Поиск файлов, содержащих проекты управления, на АРМ оператора технологической установки, и удаление их.

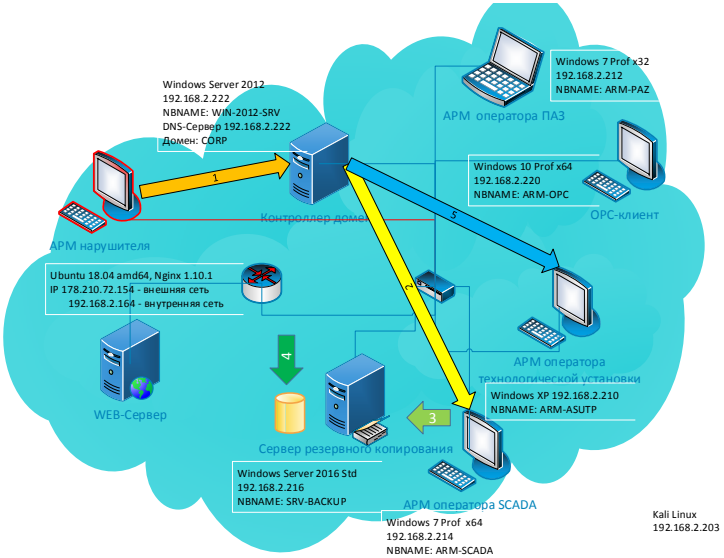

Рис. 1. Реализация сценария «Внутренний нарушитель – ZeroLogon»

Фрагменты реализации атаки ZeroLogon с использованием дистрибутива KaliLinux приведены на рис. 2 и рис. 3.

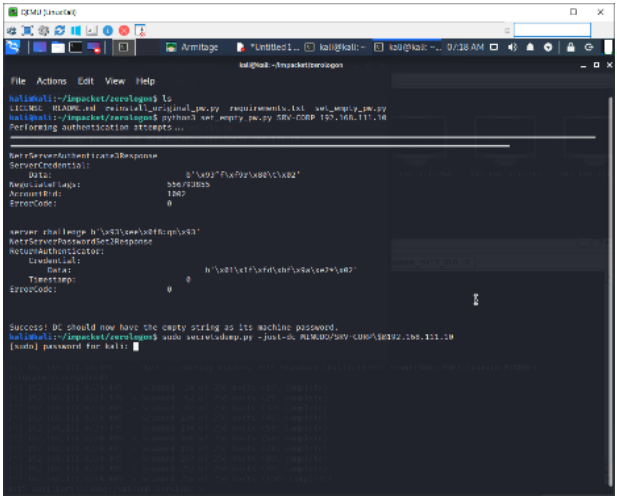

Рис. 2. Фрагменты реализации сценария «Внутренний нарушитель – ZeroLogon»

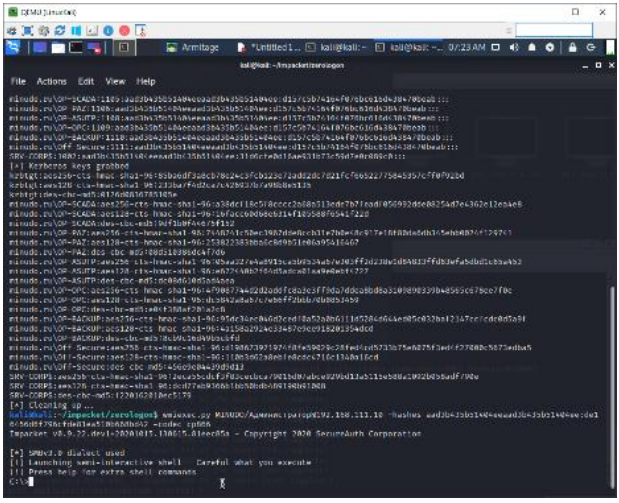

Рис. 3. Фрагменты реализации сценария «Внутренний нарушитель – ZeroLogon»

С использованием разработанной модели были обоснованы рекомендации по защите от компьютерной атаки ZeroLogon. Эти рекомендации сводятся к повышению оперативности реагирования на различных этапах проведения компьютерных атак соответствующих средств защиты.

Так снижение среднего времени срабатывания меры защиты от сниффинга с 15 до 8 минут, снижение среднего времени защиты от получения хэш-значений паролей из памяти с 15 до 10 мину, за счет использования системы более оперативного сигнатурного анализа сетевого трафика, исполнения правил для сетевых соединений, ведения черных и белых списков приложений позволит повысить время гарантированной защиты инфраструктуры организации с 10 часов до нескольких суток [9].

Заключение

Таким образом, можно сделать вывод. Программная среда моделирования EVE-NG предоставляет возможность для проведения широкого спектра исследований по выявлению уязвимостей. Она может быть использована для проведения учебно-тренировочных мероприятий, обучения персонала изучению, развертыванию, интеграции и тестированию разных продуктов.

Литература

1. Архангельский О.Д. Практические подходы к созданию инфраструктуры индустриального киберполигона/ О.Д. Архангельский, Д.В. Сютов, А.В. Кузнецов // Автоматизация в промышленности. – 2020. – №11. – С. 52 – 57.

2. Демьянов, А. Тестирование кибербезопасности встроенных систем с помощью их цифрового двойника/ А. Демьянов// Электроника: наука, технология, безопасность. – 2021. – №7 (208). –. 126 – 129.

3. Гультяев А.К. Виртуальные машины: несколько компьютеров в одном (+CD). – СПб.: Питер, 2006.– 224 сю: ил.

4. Карпов Ю. Имитационное моделирование систем. Введение в моделирование с AnyLogic5. – СПб.: БХВ – Петербург. 2005. – 400 с. ил.

5. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Текст]. – Введ. 2016-04-01. М. : Стандартинформ, 2015. – 12 с.

6. Программная среда на базе виртуализации для моделирования самых различных сетевых топологий в мультивендорной среде с эмулированием реального оборудования: [Электронный ресурс]. – Загл. с экрана. Яз. рус. – Режим доступа: http://eve-ng.ru/

7. Строим киберполигон. Используем EVE–NG, чтобы развернуть сеть для хакерских испытаний. Кирилл Мурзин. [Электронный ресурс]. – Загл. с экрана. Яз. рус. – Режим доступа: http://xakep.ru/2021/08/09/eve-ng/

8. Будников С.А. Моделирование APT-атак, эксплуатирующих уязвимость ZeroLogon/ С.А. Будников, Е.Е. Бутрик, С.В. Соловьев// Вопросы кибербезопансости. – 2021. – №6 (46). – с. 47-61.