СЦЕНАРИЙ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В СЕРВИС ОНЛАЙН-РАЗАРХИВАТОРА

Максимович Р.А., Боровиков К.А., студенты гр. 461401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье рассматривается пример реализации сценария киберинцидента, демонстрирующий процесс тестирования на проникновение в сервис онлайн-разархиватора. Процесс создания сценария киберинцидента основывался на составленном векторе кибератаки. Для прохождения сценария описаны рекомендации и подобран инструментарий, который позволит обучающимся сформировать навыки для реализации тестирования на проникновения. Таким образом, реализованный сценарий рекомендуется к изучению для обучения молодых специалистов в областях SOC-аналитики, расследования киберинцидентов и т.п.

Ключевые слова. Информационная безопасность, форензика, киберинциденты, практическая подготовка, реагирование на инциденты, тестирование на проникновение, база знаний MITRE ATT&CK, сервис онлайн-разархиватора.

Современная цифровая среда характеризуется стремительным ростом числа и сложности кибератак. В этих условиях подготовка специалистов в области информационной безопасности требует не только теоретических знаний, но и развитых практических навыков. Одним из наиболее эффективных подходов является использование сценариев киберинцидентов – моделируемых ситуаций, имитирующих реальные киберинциденты и предоставляющие возможность их расследования. Практико-ориентированное обучение позволяет студентам погружаться в реальные условия работы специалистов по безопасности, формируя у них навыки анализа, принятия решений и работы с инструментами. Наибольший интерес сегодня вызывают задачи из компьютерной криминалистики (форензики), реверс-инжиниринга и тестирования инфраструктуры на проникновение (пентест). Именно эти навыки являются ключевыми для наиболее востребованных позиций в информационной безопасности [1].

Сценарий киберинцидента представляет собой структурированную учебную задачу, в которой обучающийся выступает в роли специалиста по информационной безопасности. Сценарии должны включать: описание инцидента, набор артефактов или целевую систему, цели, критерии оценки. Использование данных составляющих сценария позволяет максимально приблизить создаваемую ситуацию к реальной жизни.

Форензика – это процесс извлечения, анализа и предоставления электронных доказательств для раскрытия киберпреступлений [2]. Специалисты по компьютерной криминалистике занимаются сбором и анализом данных с устройств и систем, которые могут быть связаны с преступными действиями. После извлечения данных проводится анализ для выявления цифровых следов и понимания, какие действия были совершены и кем.

Обратное проектирование программного обеспечения – это процесс восстановления дизайна, спецификаций требований и функций продукта на основе анализа его кода. В ходе этого процесса создается база данных программ и генерируется информация на её основе [3]. Главной целью данного процесса, который также называется реверс-инжинирингом, является исследование некоторого уже собранного продукта с целью понять его принцип работы.

Пентест (Pentest или тестирование на проникновение) – процесс тестирования системы путем попыток ее взлома для выявления уязвимостей. Специалист по безопасности после согласования сторон пытается взломать или обойти защитные меры информационной системы, чтобы найти слабые места. Существует несколько видов тестирования на проникновение: пентест внешнего и внутреннего периметра, веб-приложений, мобильных устройств и физический пентест. В ходе тестирования на проникновение специалисты используют методы, которые могут применять нарушители, чтобы проникнуть в систему. Например, анализ сетевых уязвимостей, брутфорс-атаки, эксплуатация устаревших программных компонентов и другие тактики [4]. Главной задачей пентеста является выявление уязвимостей и оценка эффективности защиты инфраструктуры.

В ходе выполнения работы была поставлена цель: разработать комплексный сценарий киберинцидента, включающий преодоление внешнего периметра и последующую внутреннюю компрометацию инфраструктуры. Объектом кибератаки выступает веб-приложение, представляющее собой сервис онлайн-разархиватора (рисунок 1).

Система была разработана на PHP и Apache с использованием Docker для контейнеризации приложений, что позволило гарантировать изоляцию сервисов от основной системы и гибкость управления окружением. Для дополнительного уровня безопасности задействована виртуальная машина с операционной системой Linux.

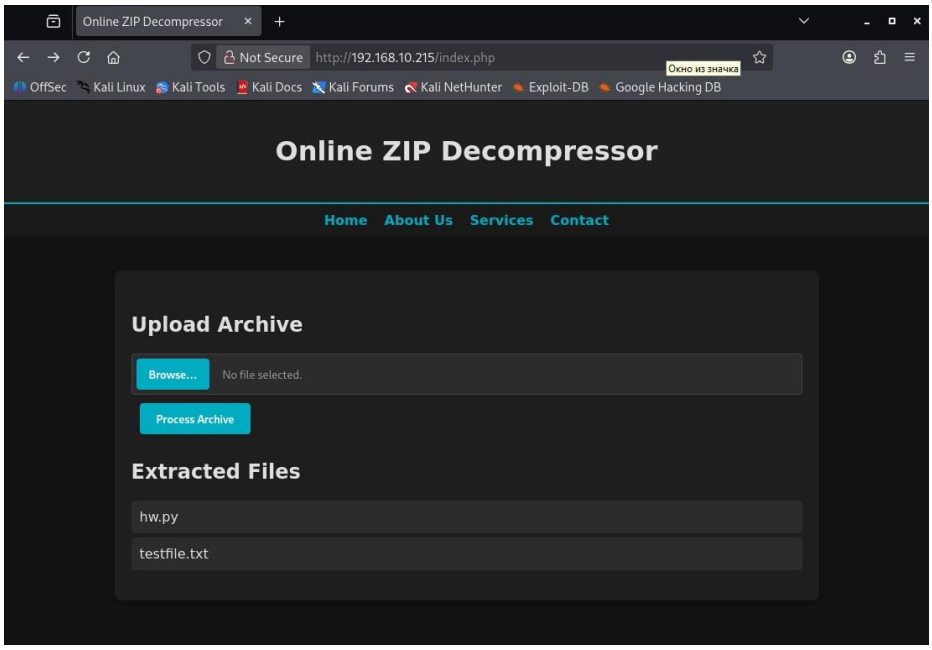

Рисунок 1 – Главная страница онлайн-разархиватора

В соответствии с общедоступной базой знаний MITRE ATT&CK был составлен вектор атаки, имитирующий последовательность действий нарушителя по компрометации целевой системы (рисунок 2) [5].

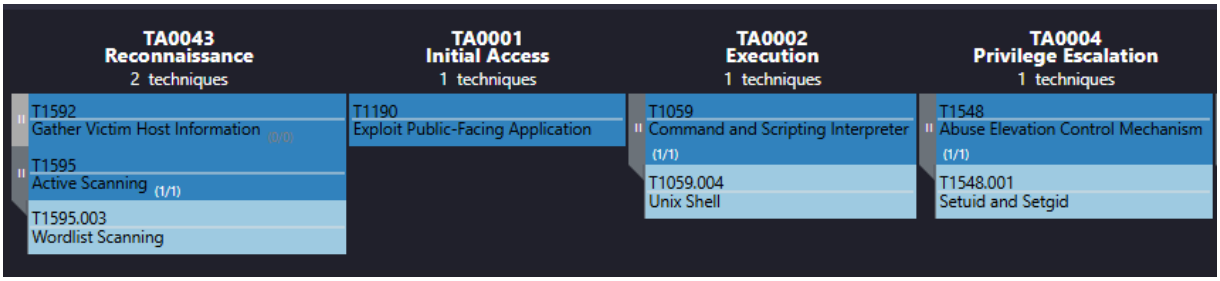

Рисунок 2 – Вектор атаки

На этапе разведки (Reconnaissance TA0043) применяется активное сканирование, в частности сканирование по словарю (Wordlist Scanning T1595.003), для обнаружения эндпоинтов веб-приложения и поиск открытых портов и информации об атакуемом узле (Active Scanning T1595, Gather Victim Host Information T1592). Первоначальный доступ (Initial Access TA0001) реализуется через эксплуатацию уязвимости целевого сервиса (Exploit Public-Facing Application T1190), который подвержен атаке типа Zip Slip (CWE-23: Relative Path Traversal). Данная уязвимость позволяет нарушителю осуществить запись файлов вне выделенной директории путем манипуляции именами файлов, содержащихся в архиве. Это приводит к этапу выполнения (Execution TA0002) путем загрузки вредоносного скрипта и использования командного интерпретатора (Unix Shell T1059.004) для получения удаленного доступа. Финальным этапом компрометации выступает повышение привилегий (Privilege Escalation TA0004) за счет злоупотребления механизмами контроля доступа, а именно – эксплуатации некорректно настроенных бинарных файлов с установленными флагами Setuid и Setgid (T1548.001).

Для успешной реализации данного сценария начинающему специалисту потребуется ряд специализированных инструментов. Для определения списка открытых портов, версий запущенных сервисов и другую информацию о хосте рекомендуется использовать инструмент nmap. Для выполнения техники Wordlist Scanning целесообразно использовать утилиты для перебора директорий, такие как ffuf или gobuster, которые позволяют быстро составить карту веб-приложения. Для генерации вредоносного архива, эксплуатирующего уязвимость Zip Slip, может применяться пользовательский скрипт на языке программирования Python. Для создания кода reverse shell удобно воспользоваться популярным инструментом для тестирования на проникновение Metasploit или онлайн-ресурсом revshells.com, на котором собрано множество вариантов для получения обратной оболочки, в зависимости от целевой системы [6]. Для отправки веб-запросов может использоваться инструмент curl, а взаимодействие с полученным веб-шеллом можно осуществить с помощью утилиты Netcat, обеспечивающей прием сетевого соединения. Для поиска векторов повышения

привилегий внутри инфраструктуры могут применяться скрипты перечисления, например, LinPEAS, а также онлайн-ресурс GTFOBins.org для поиска легитимных функций бинарных файлов в ОС Linux [7].

Успешное завершение сценария подтверждается получением прав суперпользователя и чтением специального текстового файла (рисунок 3).

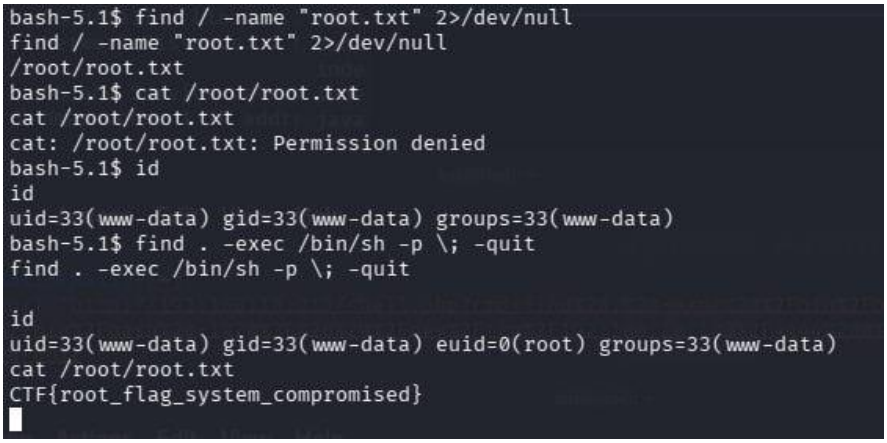

Рисунок 3 – Финальный этап задания

В результате проделанной работы был успешно спроектирован и реализован комплексный практико-ориентированный сценарий киберинцидента, направленный на формирование и закрепление прикладных навыков молодых специалистов в области информационной безопасности, в частности, в сфере тестирования на проникновения. Подобный подход позволяет обучающимся на практике освоить востребованный специализированный инструментарий и погрузиться в условия, максимально приближенные к реальным кибератакам. Навыки, полученные в ходе выполнения заданий по тестированию на проникновение, также могут быть полезны для таких позиций в информационной безопасности, как SOC-аналитик, аналитик по киберугрозам (Threat Intelligence), инженер по реагированию на инциденты (Incident Responder) и специалист по защите ПО (AppSec). Глубокое понимание техник и тактик нарушителей, сформированное в ходе пентестов, позволяет специалистам по защите качественнее настраивать системы мониторинга и выявлять аномальную активность на ранних стадиях, а тестировщикам на проникновение оттачивать приобретенные навыки.

Список использованных источников:

1. Топ-3 профессий в кибербезопасности: карьерный план на 2026 год [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Top-3-Cybersecurity-Jobs-AMLive-2025. – Дата доступа: 21.03.2026.

2. Форензика: искусство расследования инцидентов ИБ [Электронный ресурс]. – Режим доступа: https://securitymedia.org/info/forenzika-iskusstvo-rassledovaniya-intsidentov-ib.html. – Дата доступа: 21.03.2026.

3. Reverse Engineering - Software Engineering [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/software-engineering/software-engineering-reverse-engineering. – Дата доступа: 21.03.2026.

4. Пентест: что такое тестирование на проникновение [Электронный ресурс]. – Режим доступа: https://ddos-guard.ru/blog/chto-takoe-pentest. – Дата доступа: 21.03.2026.

5. MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/. – Дата доступа: 21.03.2026.

6. Reverse Shell Generator [Электронный ресурс]. – Режим доступа: https://www.revshells.com/. – Дата доступа: 21.03.2026

7. GTFOBins [Электронный ресурс]. – Режим доступа: https://gtfobins.org/. – Дата доступа: 21.03.2026.