СЦЕНАРИИ РЕАГИРОВАНИЯ НА КИБЕРАТАКИ В ОБРАЗОВАТЕЛЬНОМ КИБЕРПОЛИГОНЕ CYBERLAB

Белоусова Е. С., Вербило Н. А., Филиппов А. Н.
Кафедра защиты информации,
Белорусский государственный университет информатики и радиоэлектроники
Национальный детский технопарк
Минск, Республика Беларусь
E-mail: belousova@bsuir.by, nickolay3132@gmail.com, filipov_andrew@mail.ru

В данной статье представлено описание разрабатываемого авторами образовательного киберполигона CyberLab для профориентации учащихся средний учебных заведений и развитие навыков реагирования на кибератаки у студентов в области информационной безопасности. Киберполигон CyberLab является полностью автономным и может быть самостоятельно установлен и настроен пользователем. Для удобства пользователей авторами разрабатываются сценарии, а также реализована онлайн платформа для проверки правильности их прохождения и получения актуальной информации о появлении обновлений.

Введение

Киберполигон – это инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них [1].

На сегодняшний день существует множество киберполигонов различных по масштабу (локальные и национальные), архитектуре (виртуальные и гибридные) и реализации (индивидуальные и командные). Кроме того для прохождения киберполигона используются разные виды сценариев (CTF, Red Team, Blue Team, Purple Team).

Авторами статьи ведется разработка и популяризация образовательного киберполигона CyberLab, предназначенного для изучения учащимися средних и высших учебных заведений распространенных кибератак и способов их блокировки.

I. Назначение CyberLab

CyberLab – образовательный киберполигон с сегментированной сетевой архитектурой, включающей как одноуровневую, так и двухуровневую демилитаризованные зоны (DMZ), что позволяет моделировать различные сценарии кибератак и защиты в условиях, приближенных к реальным. Для образовательного киберполигона CyberLab авторами разрабатываются и внедряют сценарии по моделям Red Team и Blue Team.

Для популяризации и получение актуальной информации о версиях образовательного киберполигона CyberLab был разработан веб-ресурс [2], на котором подробно описаны архитектура, функциональность административного инструментария CyberLab Management Tool, системные требования для развертывания образовательного киберполигона и др. На рис. 1 представлен фрагмент страницы сценариев веб-ресурса CyberLab, предназначенной для отображения и запуска интерактивных обучающих сценариев, связанных с различными типами кибератак в области информационной безопасности.

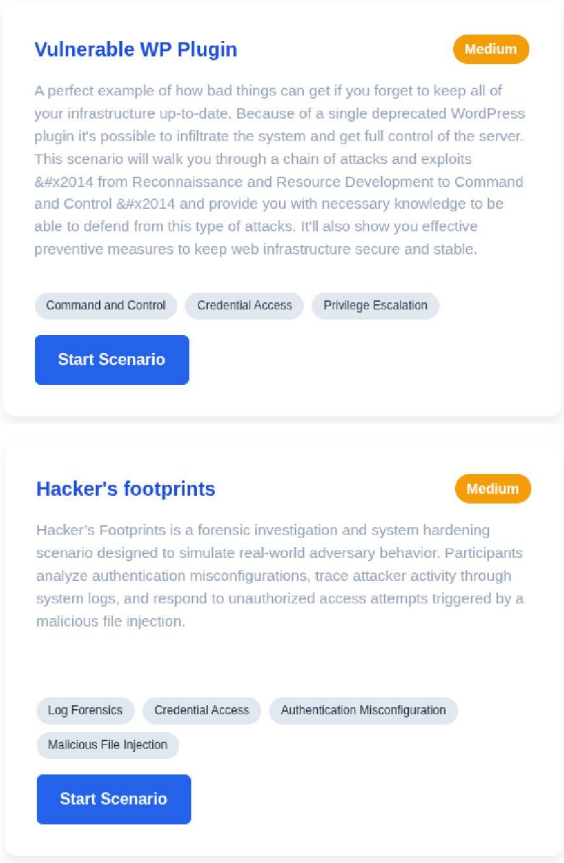

Рис. 1 – Внешний вид веб-ресурса для ознакомления с содержанием сценариев образовательного киберполигона CyberLab

Интерфейс для ознакомления с этапами прохождения сценариев и проверки правильности их выполнения реализован в виде набора фильтров и карточек, каждая из которых представляет отдельный сценарий с названием,

меткой сложности, кратким описанием, списком категорий кибератак. Как видно из рис. 1 на текущий момент реализовано два сценария: Vulnerable WP Plugin, имитирующий действия RedTeam; Hacker's footprints, имитирующий действия BlueTeam.

Для автоматизации локальной установки и управлением образовательным киберполигоном CyberLab была разработана программа CyberLab Management Tool [3], которая предоставляет быстрое взаимодействие со всеми виртуальными машинами в составе образовательного киберполигона.

II. Сценарий Vulnerable WP Plugin

В качестве примера в данной статье приведено описание сценария Vulnerable WP Plugin, основной целью которого является получение доступа к веб-серверу, расположенному в демилитаризованной зоне образовательного киберполигона CyberLab, посредством эксплуатации уязвимости CVE-2015-10144.

Сценарий Vulnerable WP Plugin демонстрирует вектор кибератаки нарушителя, в ходе которого осуществляет сканирование сервера утилитой wpscan с целью получение информации о CMS WordPress и его плагинах, BruteForce атака для получения имени пользователя и пароля к CMS WordPress, получение несанкционированного доступа к серверу посредством инструмента Metasploit для внедрения вредоносного кода, повышение привилегий и настройка удалённого доступа к серверу посредством backdoor. Таким образом, при прохождении сценария учащийся проходит все этапы, которые могут быть реализованы нарушителем. Формирование у учащегося знаний и навыков проведения кибератак позволит развить его понимание способов отслеживания действий нарушителя и их блокировку. Сценарий Vulnerable WP Plugin разделен на следующие этапы:

1. Знакомство с операционной системой Kali Linux;
2. Разведка;
3. Получение данных администратора;
4. Несанкционированный доступ к веб-серверу;
5. Повышение привилегий.

III. Пример прохождения сценария

В процессе прохождения сценария учащийся должен вводить флаги и таким образом проверять правильность выполнения заданий в сценарии. На рисунке 2 представлен пример прохождения одного из этапов сценария Vulnerable WP Plugin и результат нахождения флагов. На рисунке 3 продемонстрирован процесс проверки флага в результате выполнения одного из задания сценария.

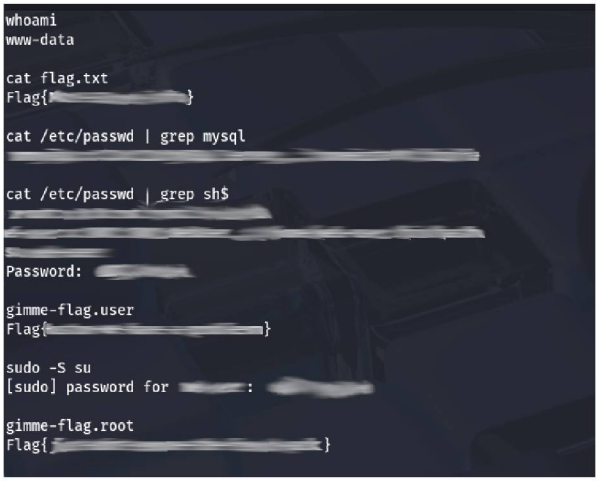

Рис. 2 – Пример процесса прохождения задания сценария Vulnerable WP Plugin

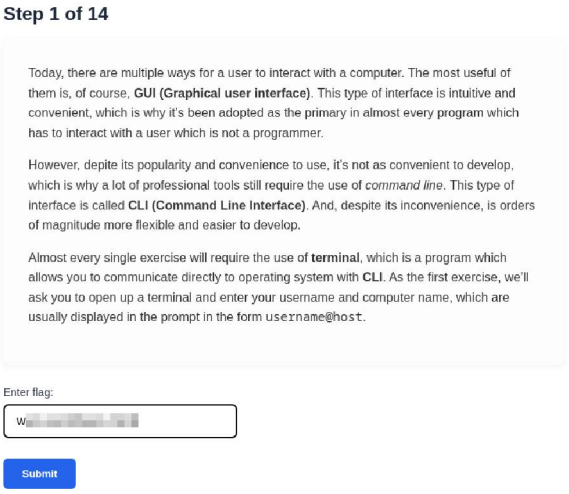

Рис. 3 – Проверка правильности выполнения сценария Vulnerable WP Plugin

На момент написания статьи авторами продолжается работа по разработке и внедрению новых сценариев в образовательный киберполигон CyberLab, который рекомендуется для внедрения в учреждениях среднего и высшего образования для профориентации учащихся в сфере информационной безопасности.

1. Об утверждении методик расчета показателей федеральных проектов национальной программы [Электронный ресурс] / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – Москва, 2025. – Режим доступа: https://digital.gov.ru/documents/prikaz-minczifry-vhc-143. – Дата доступа: 26.09.2025.
2. CyberLab Releases [Электронный ресурс] / CyberLab. – Минск, 2025. – Режим доступа: https://techno-cyber-lab.store. – Дата доступа: 06.09.2025.
3. Программа для автоматизации образовательного киберполигона CyberLab Management Tool [Электронный ресурс] / Нац. центр интеллект. собств. – Минск, 2025. –Режим доступа: https://search.ncip.by/depon/index.php?page=3&target=2315. – Дата доступа: 26.09.2025.