

# 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 средних 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 фраг-

мент страницы сценариев веб-ресурса CyberLab, предназначенной для отображения и запуска интерактивных обучающих сценариев, связанных с различными типами кибератак в области информационной безопасности.

### Vulnerable WP Plugin

Medium

A perfect example of how bad things can get if you forget to keep all of your infrastructure up-to-date. Because of a single deprecated WordPress plugin it's possible to infiltrate the system and get full control of the server. This scenario will walk you through a chain of attacks and exploits &#x2014; from Reconnaissance and Resource Development to Command and Control &#x2014; and provide you with necessary knowledge to be able to defend from this type of attacks. It'll also show you effective preventive measures to keep web infrastructure secure and stable.

Command and Control    Credential Access    Privilege Escalation

Start Scenario

### Hacker's footprints

Medium

Hacker's Footprints is a forensic investigation and system hardening scenario designed to simulate real-world adversary behavior. Participants analyze authentication misconfigurations, trace attacker activity through system logs, and respond to unauthorized access attempts triggered by a malicious file injection.

Log Forensics    Credential Access    Authentication Misconfiguration

Malicious File Injection

Start Scenario

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 осуществляется сканирование сервера утилитой wpScan с целью получения 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.

```
whoami
www-data
cat flag.txt
Flag{[REDACTED]}
cat /etc/passwd | grep mysql
[REDACTED]
cat /etc/passwd | grep sh$
[REDACTED]

Password:
gimme-flag.user
Flag{[REDACTED]}
sudo -S su
[sudo] password for [REDACTED]:
gimme-flag.root
Flag{[REDACTED]}
```

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

### Step 1 of 14

Today, there are multiple ways for a user to interact with a computer. The most useful of them is, of course, GUI (Graphical user interface). This type of interface is intuitive and convenient, which is why it's been adopted as the primary in almost every program which has to interact with a user which is not a programmer.

However, despite its popularity and convenience to use, it's not as convenient to develop, which is why a lot of professional tools still require the use of command line. This type of interface is called CLI (Command Line Interface). And, despite its inconvenience, is orders of magnitude more flexible and easier to develop.

Almost every single exercise will require the use of terminal, which is a program which allows you to communicate directly to operating system with CLI. As the first exercise, we'll ask you to open up a terminal and enter your username and computer name, which are usually displayed in the prompt in the form `username@host`.

Enter flag:  
w...

Submit

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-mincifry-vbif-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.