УДК 004.056:378.147

ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА ДЛЯ ПРОВЕДЕНИЯ КИБЕРТРЕНИРОВОК

Несмашный Е.А., Румас С.С., Потапович И.А., Ананченко Р.А., студенты гр. 561401, Дубовский В.В., студент гр. 261402

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

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

Аннотация. Выполнен анализ платформ для кибертренировок, специализирующихся на эксплуатации Git-уязвимостей и LFI. Проведено сравнение по критериям типа доступа, наличия отработки указанных уязвимостей и сценария полного цикла атаки. Предложена виртуальная инфраструктура, включающая уязвимый веб-сервер и межсетевой экран pfSense в качестве целевого узла. Описаны инструменты и ожидаемый результат в ходе выполнения сценария тренировки, основанного на эксплуатации уязвимостей Git и LFI. Инфраструктура рекомендуется для подготовки специалистов по информационной безопасности.

Ключевые слова. Кибертренировка, Red Team, виртуальная инфраструктура, Git-уязвимости, LFI, pfSense, MITRE ATT&CK.

Введение. На сегодняшний день существует большое количество решений в сфере развития навыков эксплуатации уязвимостей информационных систем. В таблице 1 представлен сравнительный анализ платформ для кибертренировок, на основе которого был сделан вывод, что существующие CTF-платформы часто фрагментарны и не дают пояснения каждому этапу кибератаки и реализуемых тактик нарушителем, начиная от внешней разведки до доступа во внутреннюю сеть через межсетевой экран. Авторами работы предлагается к внедрению в учебный процесс виртуальной инфраструктуры для кибертренировок, которая содержит в себе сценарий полного цикла кибертаки с реализацией различных техник и тактик матрицы MITRE ATT&CK.

В данной статье рассматривается пример эксплуатации Git-уязвимости и уязвимости LFI на разработанной авторами виртуальной инфраструктуре для проведения кибертренировок. Выбор уязвимостей обусловлен популяризацией использования нейросетей в процессе разработки веб-приложений и веб-сайтов, что при неправильном использовании приводит к появлению уязвимостей такого рода. В матрице MITRE ATT&CK [1] описаны следующие техники для эксплуатации выбранных уязвимостей: T1213, T1190 и T1005. Таким образом, изучение Git и LFI уязвимостей, техник их эксплуатации в виде практической реализации в виртуальной инфраструктуре для проведения кибертренировок является актуальным для специалистов в области информационной безопасности.

Таблица 1 – Существующие решения в области кибертренировок вышеуказанных уязвимостей

Платформа	Тип	Доступ	Отработка Git и LFI уязвимостей	Сценарий полного цикла
BugCTF [2]	CTF	Бесплатно	Частично (флаг)	Нет
OverTheWire Bandit [3]	CTF	Бесплатно	Есть	Нет
TryHackMe [4]	CTF и курсы	Доступны только базовые сценарии	Есть	Частично
HackTheBox Labs [5]	Практические задания	Платно	Есть	Есть

Разработанная виртуальная инфраструктура для проведения кибертренировок представляет из себя практико-ориентированную модель. Обучающийся изначально получает IP-адрес в OpenVPN сети, в которой находится межсетевой экран pfSense, а также два IP-адреса сайтов с Git и LFI уязвимостями, для возможности реализации двух векторов кибератак, целью которых является получение учетных данных от панели администратора pfSense. Изначально сегмент внутренней сети (Internal) защищён межсетевым экраном и доступ к его конфигурации отсутствует. После получения учетных данных межсетевого экрана pfsense посредством изменения правил межсетевого экрана, доступ нарушителя во внутреннюю сеть становится доступен. Схематичное представление структуры разработанной виртуальной инфраструктуры приведено на рисунке 1.

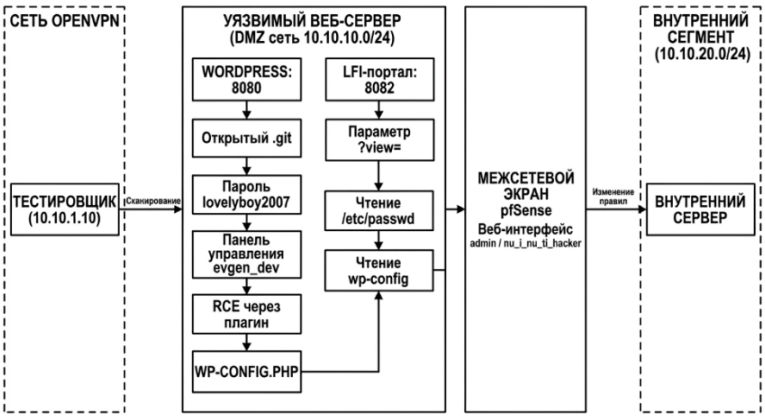

Рисунок 1 – Структура виртуальной инфраструктуры для проведения тренировок

Вектор кибератаки. В разработанной виртуальной инфраструктуре присутствуют два независимых вектора кибератаки: на первом веб-сайте необходимо эксплуатировать уязвимость репозитория кода (MITRE ATT&CK T1213.003 [1]); на втором веб-сайте – уязвимость локальной файловой системы (MITRE ATT&CK T1005 [1]). Вектора кибератаки представлены схематично на рисунке 2.

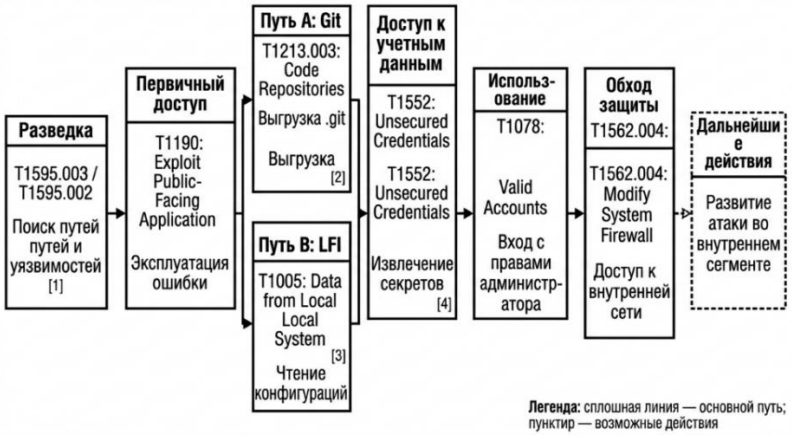

Рисунок 2 – Вектора кибератаки при использовании Git-уязвимости и LFI

Сценарий кибертренировки. Обучающийся начинает сценарий с разведки внешнего периметра. С помощью утилиты nmap он определяет доступные сетевые сервисы, а с помощью gobuster выполняет перебор директорий и файлов веб-приложения. Цель этого этапа заключается в выявлении признаков ошибочной публикации служебных ресурсов и параметров, потенциально подверженных чтению локальных файлов.

В ходе разведки обучающийся обнаруживает один из двух векторов первичного доступа: открытую директорию «.git» в корне веб-сайта либо уязвимость LFI/path traversal в одном из параметров приложения. Далее он переходит к эксплуатации интернет-доступного приложения. Веб-интерфейс платформы с Git-уязвимостью представлен на рисунке 3.

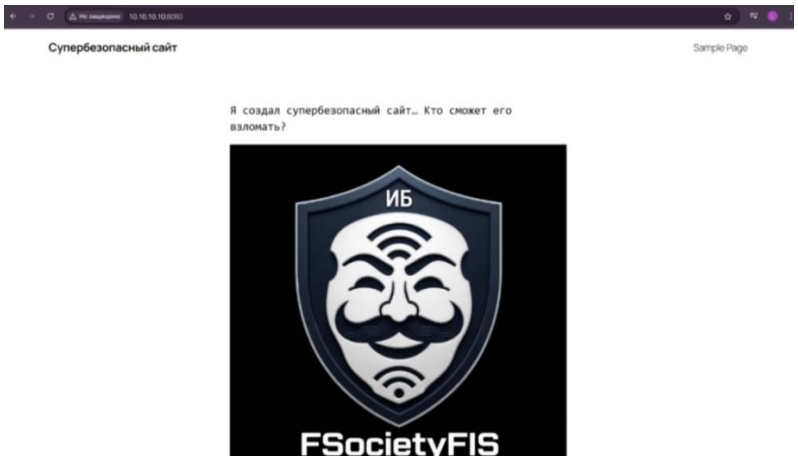

Рисунок 3 – Веб-интерфейс сервера с Git-уязвимостью

Если доступна директория «.git», обучающийся с помощью инструментов wget или GitTools выгружает и восстанавливает репозиторий, после чего анализирует исходные файлы и историю коммитов. Его задача заключается в определении учетных данных, оставленных в конфигурациях, исходном коде или удалённых из рабочей версии, но сохранившихся в истории. Если обнаруживаются логин и пароль администратора pfSense, это фиксируется как реализация техники. Вид папки .git уязвимого веб-сайта представлен на рисунке 4.

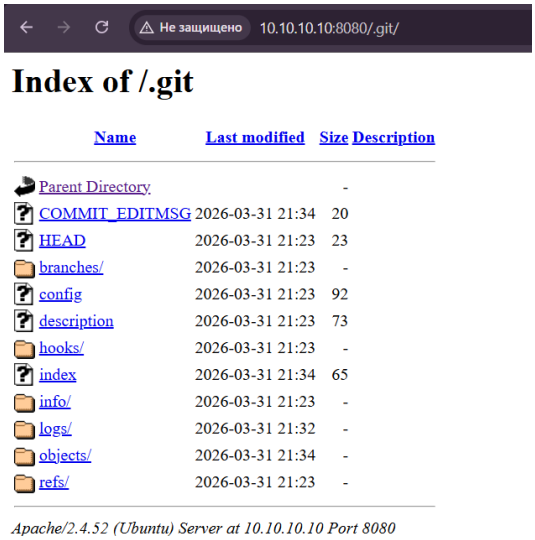

Рисунок 4 – Содержимое папки *.git* уязвимого веб-сайта

Если доступен LFI-вектор, обучающийся использует инструменты *curl* или *wget* для чтения локальных файлов веб-сервера. Он проверяет возможность доступа к конфигурационным файлам, служебным данным и другим артефактам, которые могут содержать учетные данные или сведения о сетевой инфраструктуре. Если в результате чтения файлов также удаётся получить учетные данные администратора pfSense, этот результат документируется как ключевой для дальнейшего развития кибератаки.

После получения учетных данных обучающийся выполняет вход в веб-интерфейс pfSense. В результате получения административных привилегий возможно изменение правил доступа на межсетевом экране, например, разрешение доступа к внутренним сегментам или изменение ограничений правил фильтрации. Эти действия рассматриваются как практическая реализация компрометации сетевого периметра и создания условий для дальнейшего продвижения. Панель администратора с правилами фильтрации трафика pfSense, после получения обучающимся учётных данных представлена на рисунке 5.

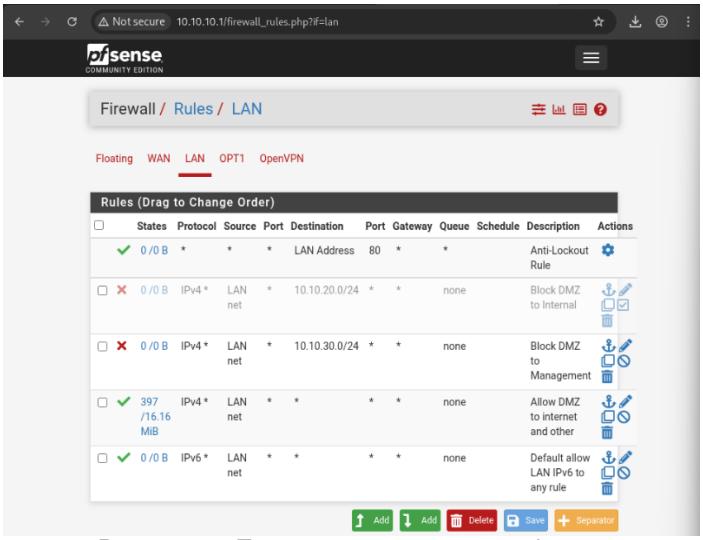

Рисунок 5 – Панель администратора *pfSense*

После изменения правил доступа обучающийся выполняет проникновение во внутреннюю сеть через разрешённые сервисы и маршруты. Для этого он использует доступные механизмы удалённого подключения и проверяет достижимость внутренних узлов. Основная идея сценария заключается в том, что компрометация веб-приложения через «.git» или LFI приводит не просто к утечке данных, а к

получению контроля над pfSense, после чего обучающийся может изменить правила сетевого доступа и получить возможность развивать кибератаку во внутреннем контуре.

При необходимости сценарий может завершаться демонстрацией закрепления на одном из достигнутых узлов. Для этого обучающийся может использовать инструмент metasploit и разместить серверный компонент на скомпрометированном хосте. Однако ключевой результат тренировки может быть отмечен получением учетных данных администратора pfSense, изменением правил фильтрации и последующим проникновением во внутреннюю сеть.

Заключение. Разработанная виртуальная инфраструктура рекомендуется для использования в учебном процессе при подготовке специалистов в области информационной безопасности для освоения навыков Red Team и Penetration testing. Она позволяет на практике отработать полный цикл кибератаки, включая техники внешней разведки, латерального перемещения через межсетевой экран и др. В отличие от существующих CTF-платформ, данная среда максимально приближена к реальной инфраструктуре предприятия. Разработанная виртуальная инфраструктура для кибертренировок может быть самостоятельно развернута в среде виртуализации VirtualBox или VMware и использована как в рамках учебного процесса, так и для самостоятельного обучения.

Список использованных источников:

1 MITRE ATT&CK®. – URL: https://attack.mitre.org (дата обращения: 05.04.2026).

2 BugCTF. – URL: https://ctf.bug-makers.ru (дата обращения: 05.04.2026).

3 OverTheWire: Bandit. – URL: https://overthewire.org/wargames/bandit/ (дата обращения: 05.04.2026).

4 TryHackMe. – URL: https://tryhackme.com (дата обращения: 05.04.2026).

5 HackTheBox. – URL: https://www.hackthebox.com (дата обращения: 05.04.2026).

UDC 004.056:378.147

VIRTUAL INFRASTRUCTURE FOR CYBERTRAINING

Nesmashny E.A., Rumas S.S., Potapovich I.A., Ananchenko R.A., student gr. 561401
Dubovsky V.V., student gr. 261402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD in Technical Sciences, Associate Professor

Annotation. An analysis was conducted of cyber training platforms specializing in the exploitation of Git vulnerabilities and LFI. A comparison was performed based on criteria such as access type, the availability of exercises for these vulnerabilities, and full-cycle attack scenarios. A virtual infrastructure is proposed, consisting of a vulnerable web server and a pfSense firewall as the target node. The tools and expected results during the execution of a training scenario based on the exploitation of Git and LFI vulnerabilities are described. The infrastructure is recommended for training information security specialists.

Keywords. Cyber training, Red Team, virtual infrastructure, Git vulnerabilities, LFI, pfSense, MITRE ATT&CK.