Лабораторная работа 3

Защита интеграционной платформы

Панченко Денис 1132229056

Савурская Полина 1132222827

Кочарян Никита 1132221541

Норсоян Шушаник 1132221545

Сухальская Ксения 1132229052

Умярова Камилла 1132229051

Содержание

# 1. Цель работы

Конкуренты решили нанести репутационный вред деятельности компании и для этого нашли исполнителя.Злоумышленник находит в Интернете сайт соответствующей организации и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Нужно защитить компанию от атаки.

# 2. Выполнение лабораторной работы

## 2.1 Уязвимость Bitrix vote RCE и последствие Bitrix deface

При входе на сайт компании, видим, что сайт взломан ([рис. 1](#fig-001)).

|  |
| --- |
| Рисунок 1: Взломанный сайт компании |

Подключаемся к серверу Bitrix через SSH ([рис. 2](#fig-002)).

|  |
| --- |
| Рисунок 2: Подключение к серверу Bitrix |

Закрываем локальное повышение привилегий, удалив файл apache\_restart ([рис. 3](#fig-003)).

|  |
| --- |
| Рисунок 3: Закрытие локального повышения привилегий |

|  |
| --- |
| Рисунок 4: Закрытие локального повышения привилегий |

Для закрытия уязвимости создаем файл .htaccess в директории, отклоняющий все запросы к директории vote ([рис. 5](#fig-005)).

|  |
| --- |
| Рисунок 5: Создание файла .htaccess |

Закрываем все вредоносные сессии ([рис. 6](#fig-006)).

|  |
| --- |
| Рисунок 6: закрытие вредоносных сессий |

Сбрасываем пароль администратора при помощи специального скрипта ([рис. 7](#fig-007)).

|  |
| --- |
| Рисунок 7: Скрипт |

|  |
| --- |
| Рисунок 8: Выполнение скрипта |

Восстанавливаем сайт из бэкапа ([рис. 9](#fig-009)).

|  |
| --- |
| Рисунок 9: Бэкап |

|  |
| --- |
| Рисунок 10: Восстановление сайта из бэкапа |

Сайт воостановлен ([рис. 11](#fig-011)).

|  |
| --- |
| Рисунок 11: Восстановленный сайт компании |

Уязвимость и последствие успешно устранены ([рис. 12](#fig-012)).

|  |
| --- |
| Рисунок 12: Устранение уязвимости и последствия |

## 2.2 Уязвимость GitLab RCE и последствие GitLab meterpreter

Подключаемся к серверу GitLab ([рис. 13](#fig-013)).

|  |
| --- |
| Рисунок 13: Подключение к серверу GitLab |

С локального ПК отправляем нужное обновление на сервер ([рис. 14](#fig-014)).

|  |
| --- |
| Рисунок 14: Отправка обновления |

Усстанавливаем обновление на сервер ([рис. 15](#fig-015)).

|  |
| --- |
| Рисунок 15: Установка обновления |

|  |
| --- |
| Рисунок 16: Обновление установлено |

Завершаем все активные вредоносные сессии ([рис. 17](#fig-017)).

|  |
| --- |
| Рисунок 17: Поиск вредоносных сессий |

|  |
| --- |
| Рисунок 18: Завершение вредоносных сессий |

Уязвимость и последствие успешно устранены ([рис. 19](#fig-019)).

|  |
| --- |
| Рисунок 19: Устранение уязвимости и последствия |

## 2.3 Уязвимость WSO2 API-Manager RCE и последствие WSO2 User web

Подключаемся к WSO2 API-Manager ([рис. 20](#fig-020)).

|  |
| --- |
| Рисунок 20: Подключение к серверу |

Для устранения уязвимости добавляем проверку уязвимого маршрута в конфигурационный файл deployment.toml ([рис. 20](#fig-020)).

|  |
| --- |
| Рисунок 21: Добавление проверки в конфигурационный файл |

Удаляем все эксплойты и полезные нагрузки с сервера ([рис. 22](#fig-022)).

|  |
| --- |
| Рисунок 22: Удаление вредоносных файлов |

Подключаемся к веб-интерфейсу ([рис. 22](#fig-022)).

|  |
| --- |
| Рисунок 23: Подключение к веб-интерфейсу |

Удаляем вредоносного пользователя веб-интерфейса ([рис. 24](#fig-024)).

|  |
| --- |
| Рисунок 24: Удаление вредоносного пользователя |

Уязвимость и последствие успешно устранены ([рис. 25](#fig-025)).

|  |
| --- |
| Рисунок 25: Устранение уязвимости и последствия |

# 3. Выводы

В результате выполнения работы мы успешно устранили все уязвимости и их последствия ([рис. 26](#fig-026)).

|  |
| --- |
| Рисунок 26: Успешное устранение всех уязвимостей и последствий |