Отчёт по лабораторной работе 1-D

Кибербезопасность предприятия. 1-D

Лобанова Полина Иннокентьевна, Лушин Артём Андреевич

Содержание

Список иллюстраций

1 Цель работы

Обеспечить защиту корпоративного мессенджера.

2 Легенда

Конкуренты решили скомпрометировать деятельность Компании и нашли для этого исполнителя. Злоумышленник находит в Интернете сайт соответствующего предприятия и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель стремится захватить управление другими ресурсами защищаемой сети, в том числе, пытается закрепиться на почтовом сервере и продолжить атаку. Главная задача злоумышленника - получение доступа к переписке сотрудников компании, раскрытие учётных данных пользователей, зарегистрированных в приложении корпоративного мессенджера, с целью использования их для нанесения ущерба репутации конкурирующей Компании. Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

3 Выполнение лабораторной работы

1) Атака на мессенджер на началась в 00:46. Наша задача устранить 3 уязвимости и 3 последствия.

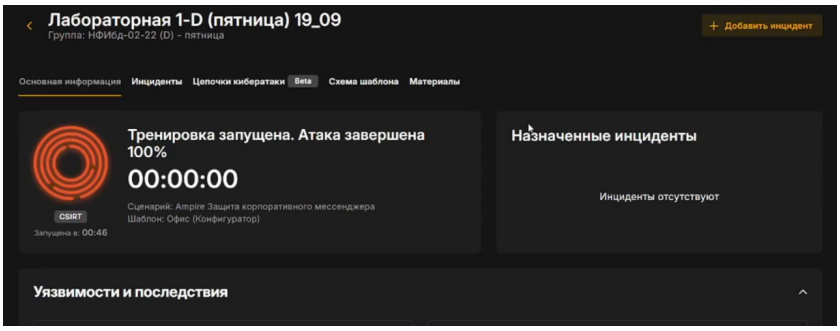

Рис. 3.1: Начало атаки

2) Посмотрели журнал событий с интервалом 15 минут.

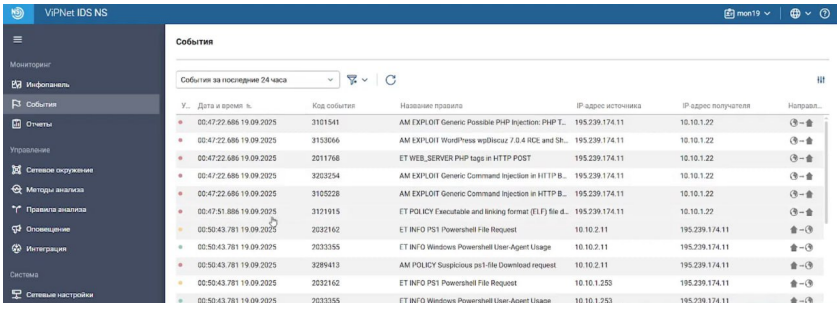

Рис. 3.2: Просмотр журнала

3) Увидели подозрительное событие. Согласно нему правило обнаружило в

сетевом трафике программный код, который нужен был для эксплуатации уязвимости.

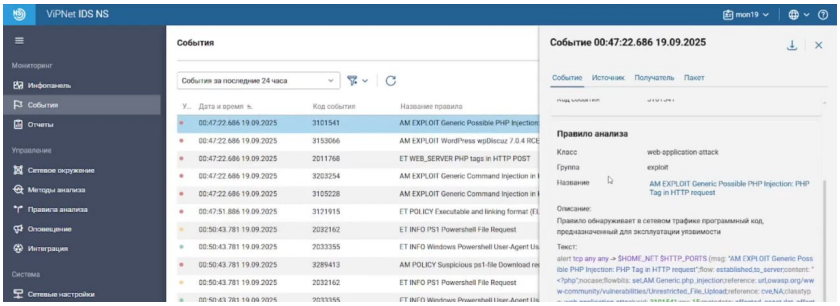

Рис. 3.3: Подозрительное событие

4) Проверил проверку события по CVE.

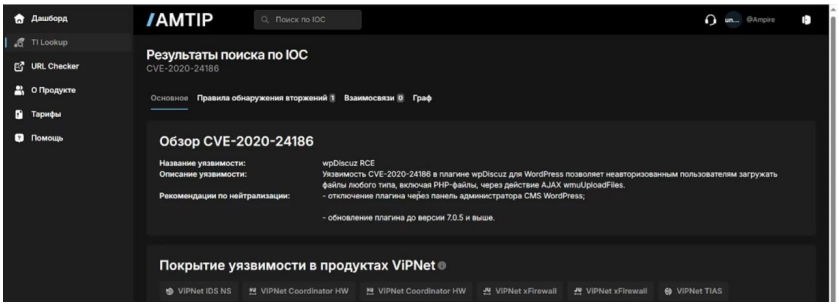

Рис. 3.4: Проерка по CVE

5) Посмотрели схему работы компании. Увидели, что атака шла с Kali на один из серверов DMZ.

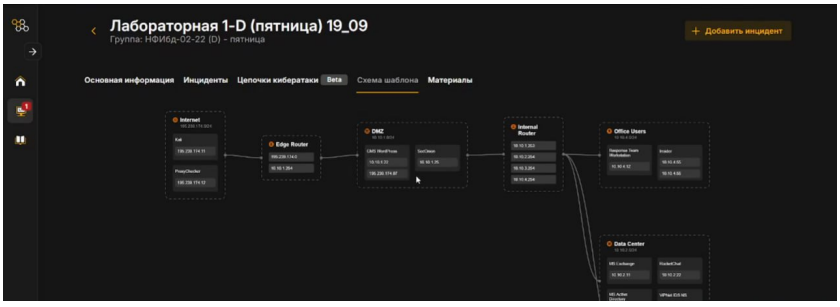

Рис. 3.5: Схема атаки

6) Создали инцидент согласно событию. Описали сам инцидент, написали откуда шла атака и на какой сервер. Указали точное время события, индикаторы компрометации и прописали рекомендации.

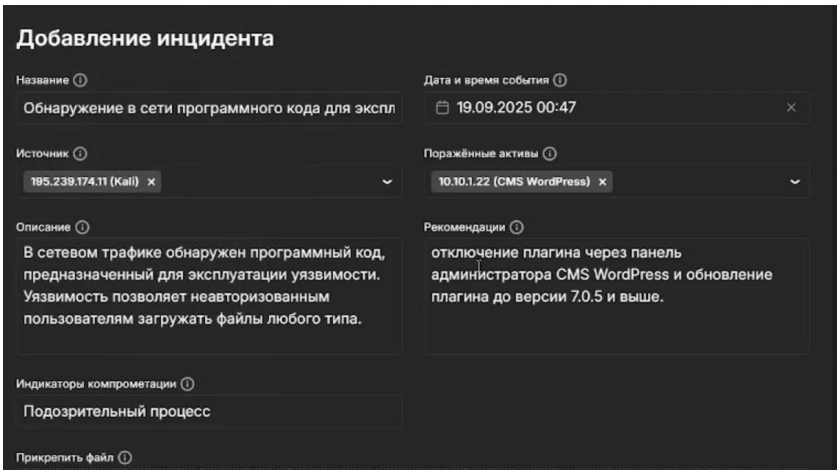

Рис. 3.6: Создание первого инцидента

7) Для устранения уязвимости мы перешли на удалённый рабочий стол и подключились к админу, который может подключиться к любому компьютеру сети. Затем подключились к устройству на который происходит атака.

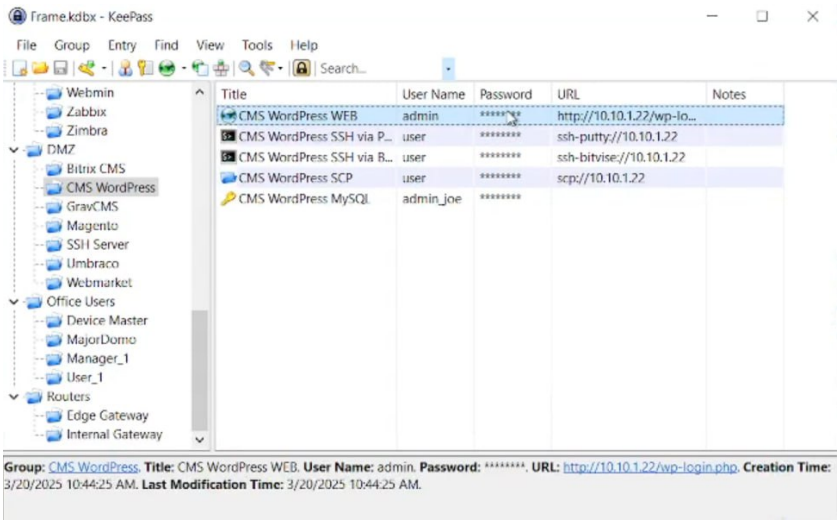

Рис. 3.7: Подключение к устройству

8) Для устранения уязвимости, необходимо было или отключить плагин WpDiscuz, или обновить WpDiscuz до новой версии 7.0.5 и выше. Так как у нас отсутствовало подключение к интернету, отключили плагин.

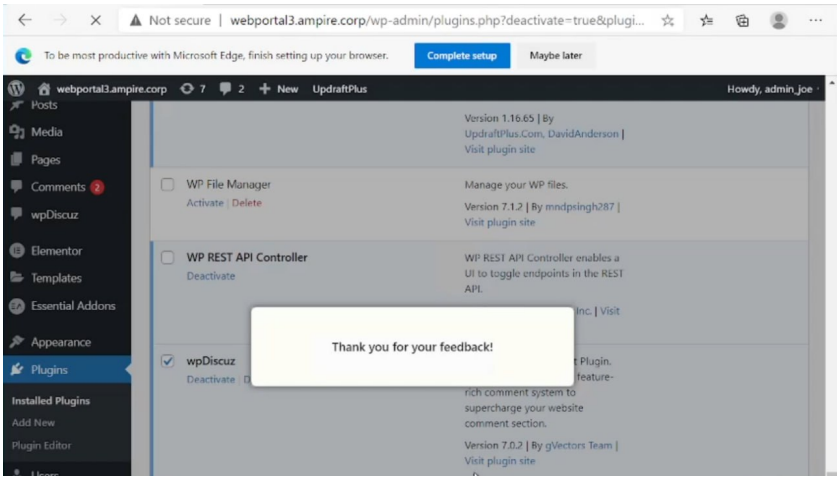

Рис. 3.8: Отключение плагина

9) На странице сайта компании увидели изменения в виде другой фотографии.

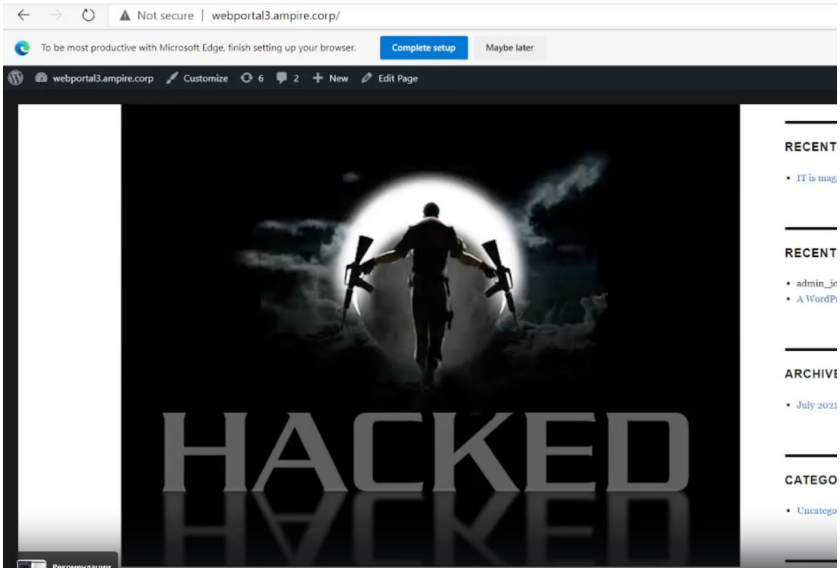

Рис. 3.9: Изменения на сайте компании

10) Для нейтрализации данной полезной нагрузки необходимо было сформировать резервную копию с помощью плагина Updraft Backup/Restore. Мы активировали версию от 15 сентября и попытались восстановить данные. В качестве компонентов для переустановки мы указали Themes и Uploads. У нас возникла ошибка восстановления и мы нажали кнопку Delete Old Directories. Затем восстановили резервную копию.

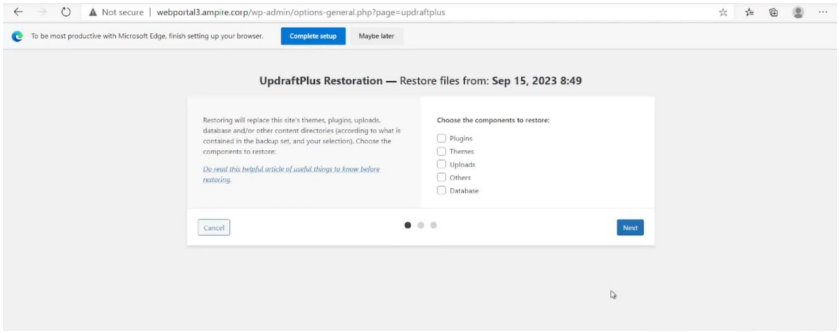

Рис. 3.10: Выбор компонентов

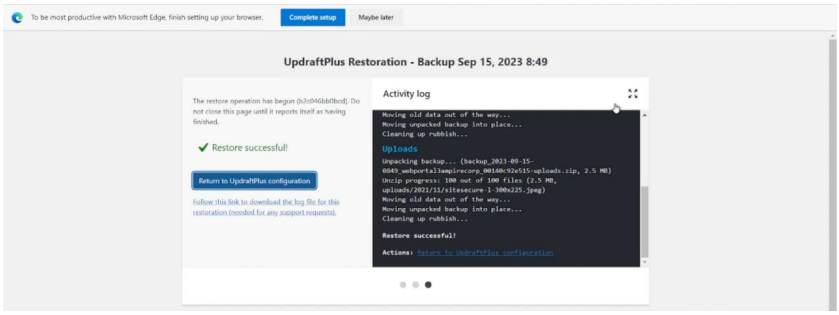

Рис. 3.11: Успешное выполнение установления

11) Чтобы удалить последствия события, мы подключились к консоли атакуемого устройства. Посмотрели сокеты и увидели соединение с Kali. Разорвали соединение и проверили, чтоб лишних соединений нет.

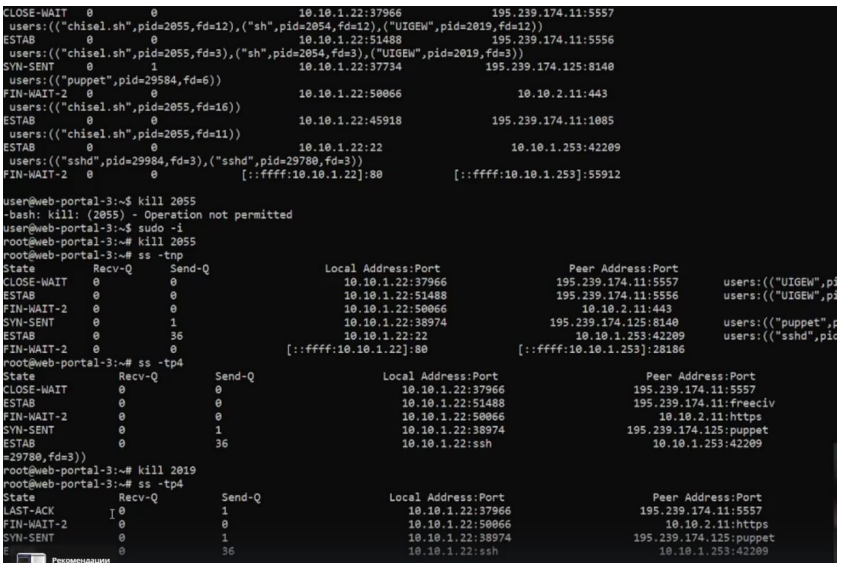

Рис. 3.12: Процесс закрытия соединения

12) Проверили, что уязвимость и последствие WordPress устранены.

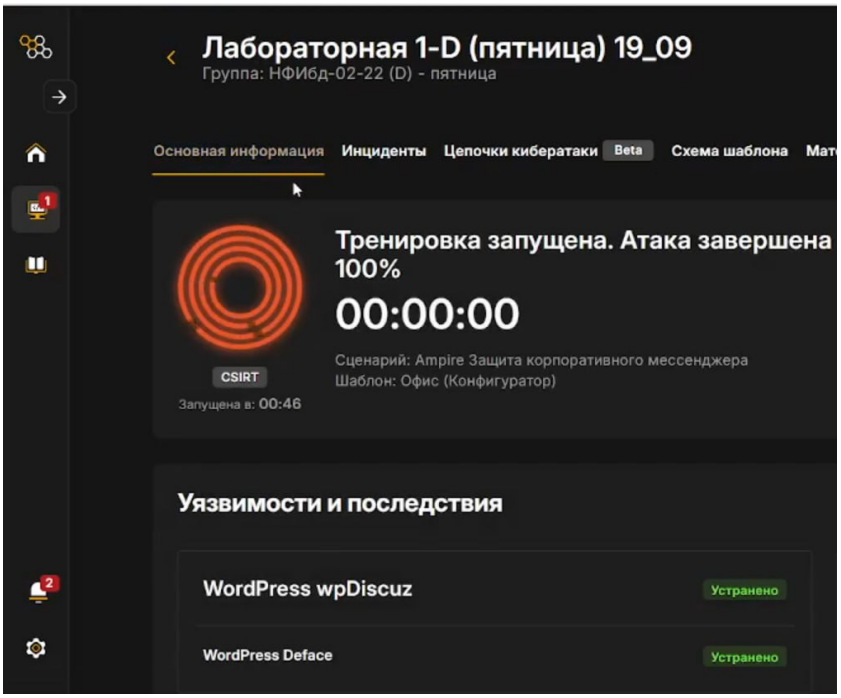

Рис. 3.13: Проверка первого события

13) Перешли вновь к журналу событий. Увидели вторую подозрительную ак-

тивность.

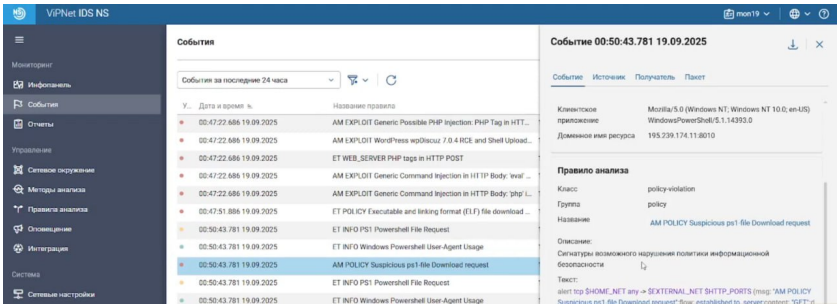

Рис. 3.14: Второе событие

14) Создали новый инцидент. Указали описание и название. Указали источник атаки и поражённые активы. Указали точное время атаки и индикатор компрометации. Написали рекомендации по решению.

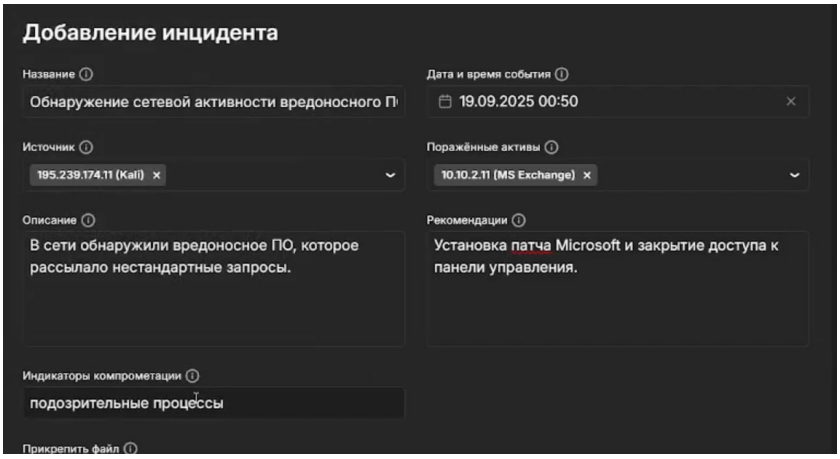

Рис. 3.15: Второй инцидент

15) Чтобы устранить уязвимость, с помощью удалённого компа подключились к атакуемому устройству. Ограничили доступ к указанной директории для запрета эксплуатации уязвимости.

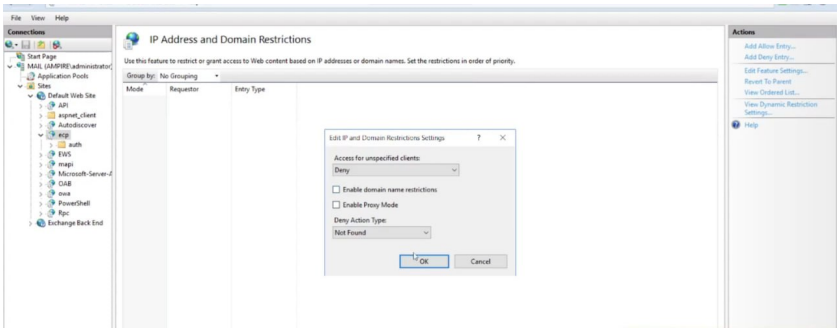

Рис. 3.16: Ограничение к директории

16) Чтобы убрать последствия события, в консоли мы закрыли meterpretter-сессию для завершения соединения.

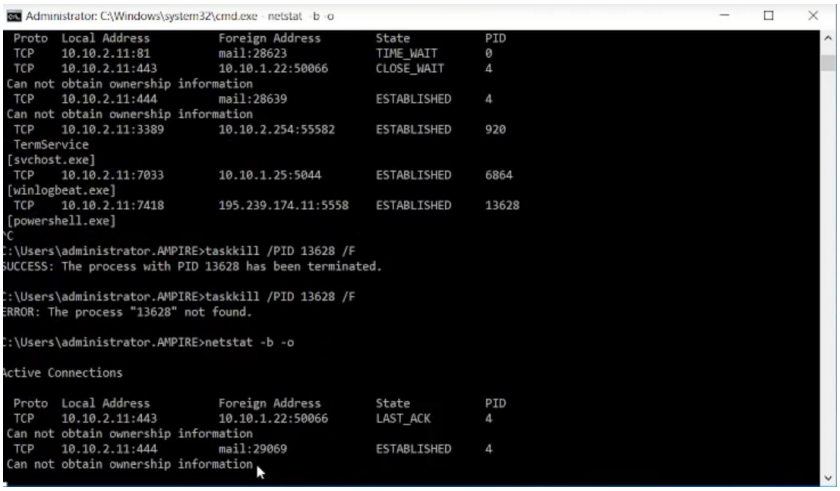

Рис. 3.17: Закрытие соединения

17) И в конце мы удалили файл, чтобы последствие полностью стереть.

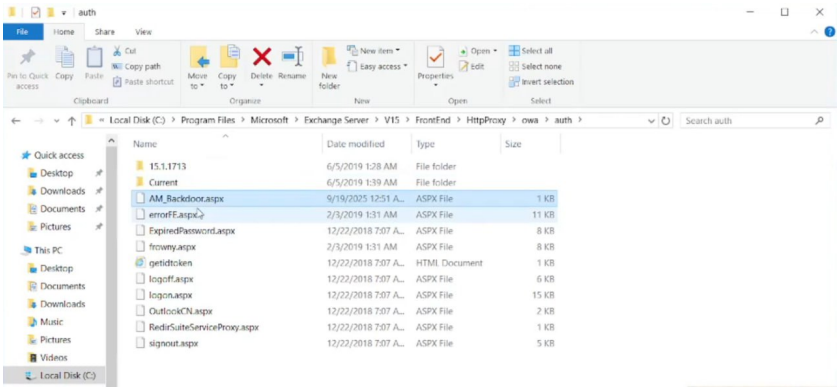

Рис. 3.18: Удаление файла

18) Проверили, что уязвимость Proxylogon полностью устранена. Последствия атаки также устранены.

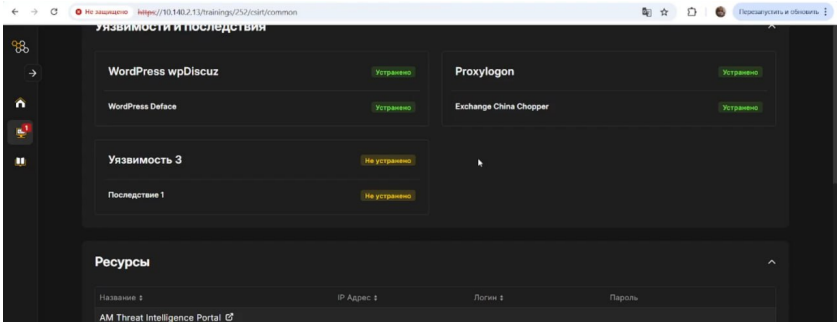

Рис. 3.19: Устранение Proxylogon

19) Снова проверили журнал событий. Нашли ещё одно подозрительное событие.

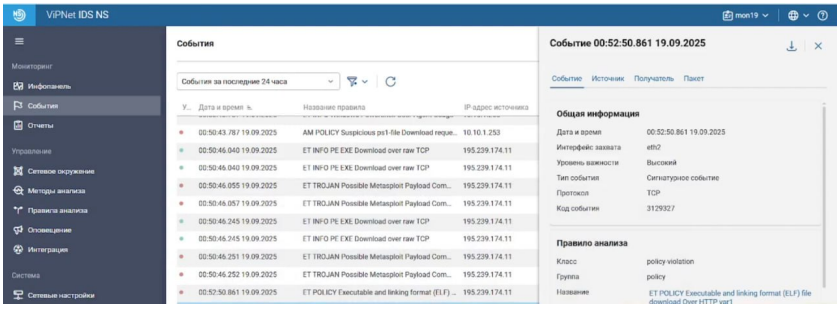

Рис. 3.20: Проверка журнала

20) Создали инцидент по последнему событию. Написали название, описание события. Указал источник и атакуемое устройство. Указали точное время начала атаки и индикатор компрометации. Написали рекомендации.

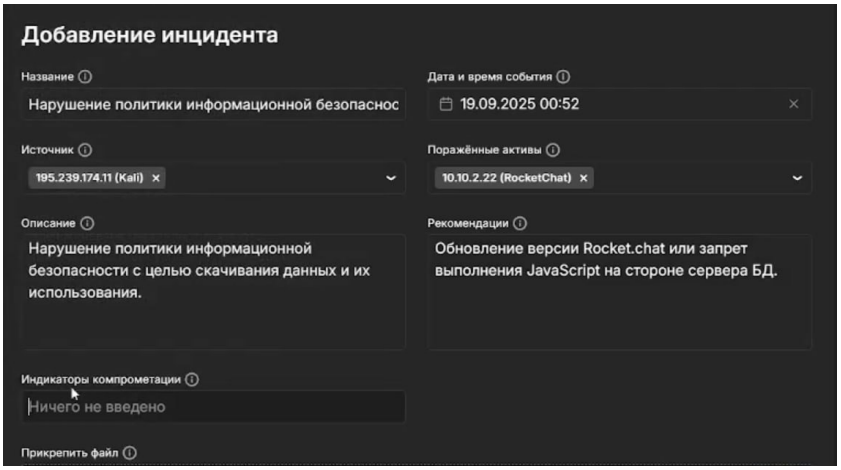

Рис. 3.21: Третий инцидент

21) Для устранения уязвимости, нам нужно было изменить настройки сайта. Для того, чтобы зайти на сайт, нужен аккаунт администратора. Для восстановления доступа к аккаунту администратора необходимо было сменить пароль. Письмо с ссылкой для сброса отправлялось на почту. С помощью утилиты mail мы проверили почту. Указали новый пароль и необходим был одноразовый код. В качестве одноразового кода мы использовали коды восстановления. После успешного сброса пароля, мы зашли на сайт под аккаунтом администратора.

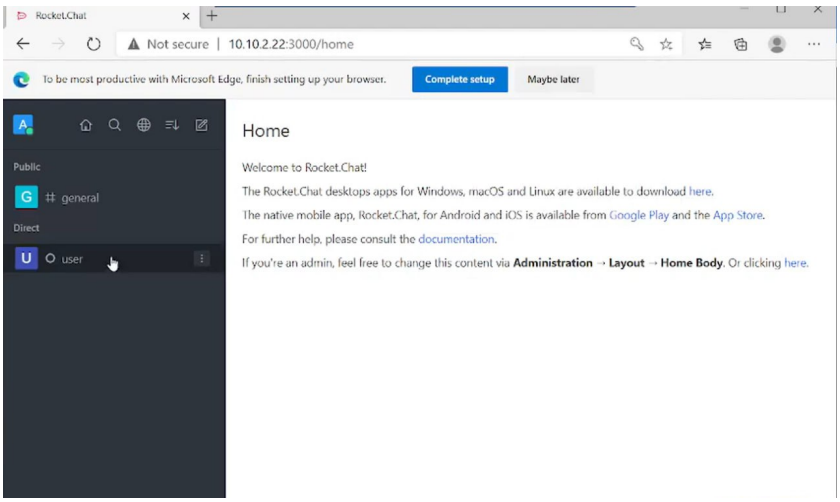

Рис. 3.22: Вход на сайт через администратора

22) Включили обязательную двухфакторную аутентификацию для простых уже зарегистрированных пользователей.

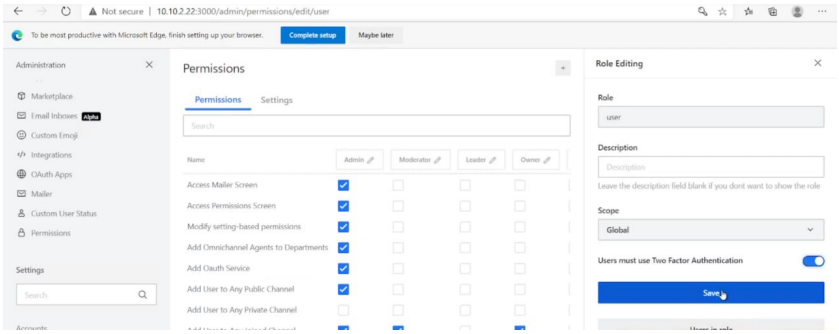

Рис. 3.23: Двухфакторная аутентификация

23) Включили обязательную двухуровневую аутентификацию для новых пользователей. А также сделали подключение новых пользователей вручную.

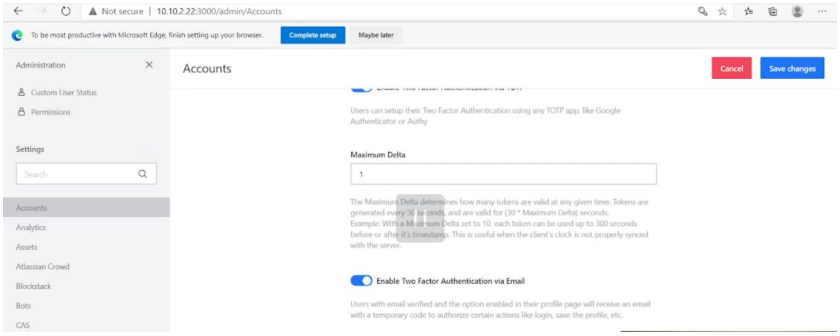

Рис. 3.24: Настройки регистрации новых пользователей

24) Отключили параметр javascriptEnabled и перезапустили службу.

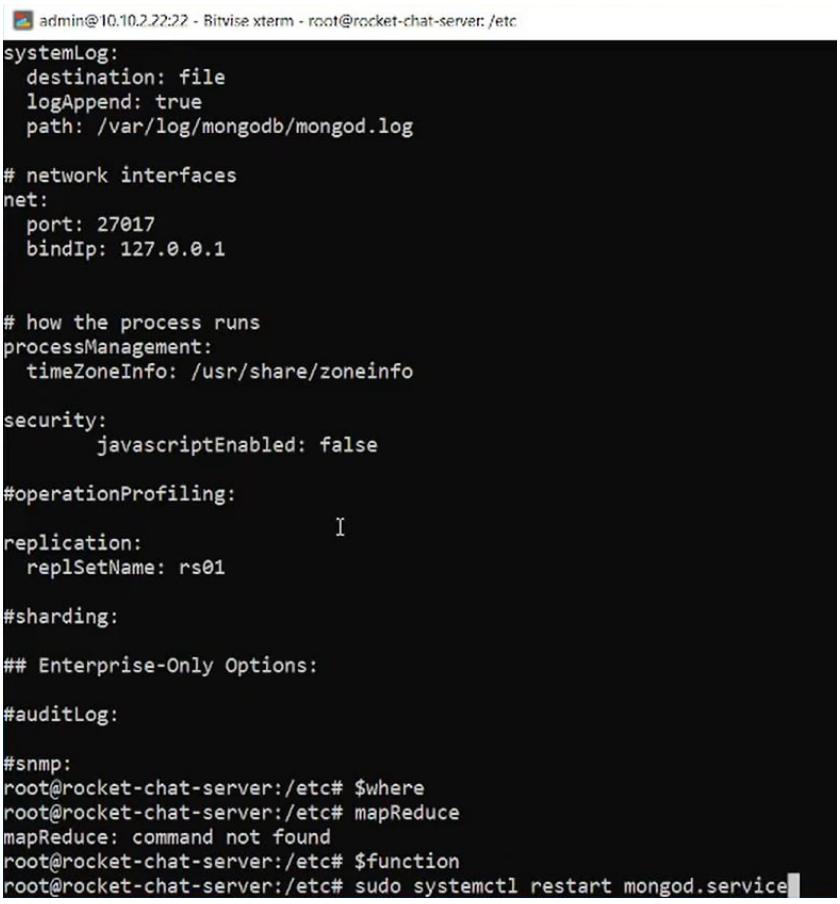

Рис. 3.25: Отключение javascriptEnabled

25) Для устранения последствия необходимо было отключить атакующего от

нашего пользователя. Завершили все сессии с устройства Kali на наш компьютер.

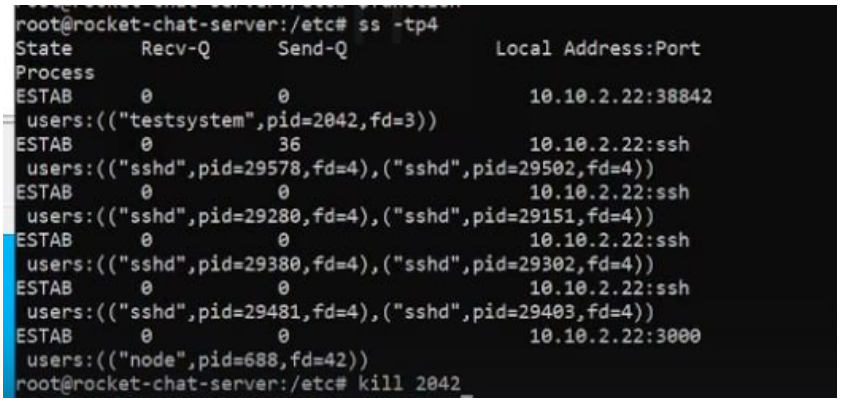

Рис. 3.26: Завершение всех сессий атакующего

26) Проверили, что последний инцидент устранён. Все 3 уязвимости и 3 последствия устранены.

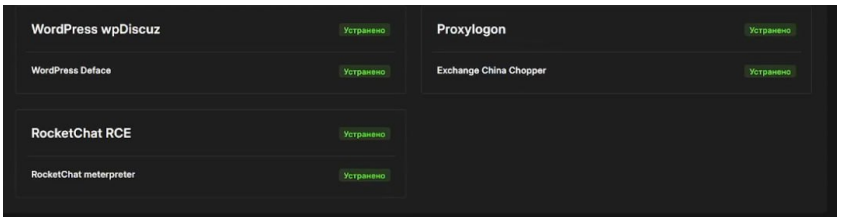

Рис. 3.27: Устранение всех последствий

4 Вывод

Мы устранили все последствия и уязвимости после атаки на мессенджер, тем самым обеспечили защиту корпоративного мессенджера.