Отчёт по лабораторной работе 1-D

Кибербезопасность предприятия. 1-D

Лобанова Полина Иннокентьевна, Лушин Артём Андреевич

Содержание

# 1 Цель работы

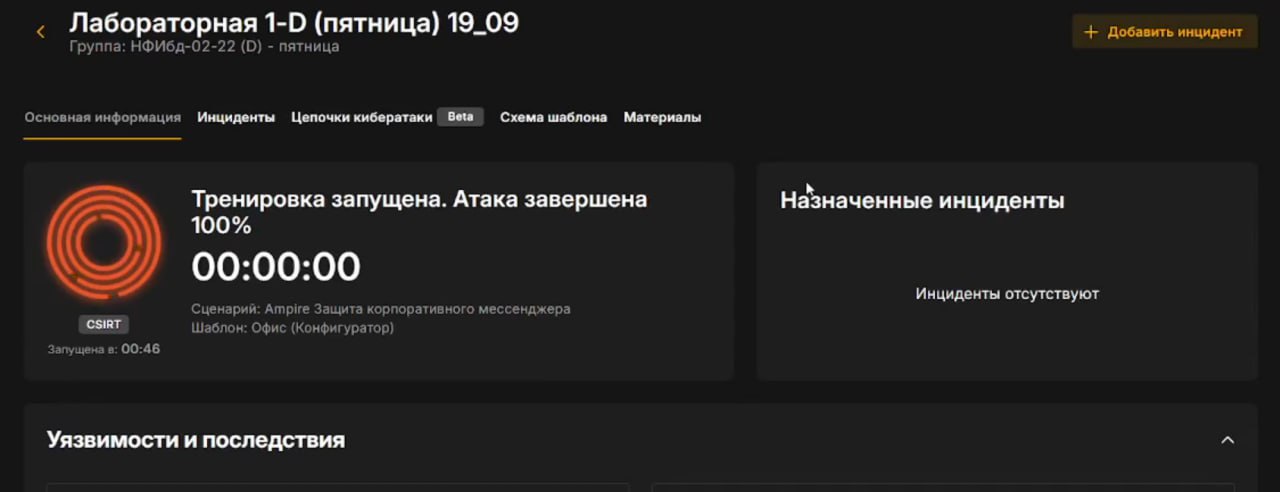
Обеспечить защиту корпоративного мессенджера.

# 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.

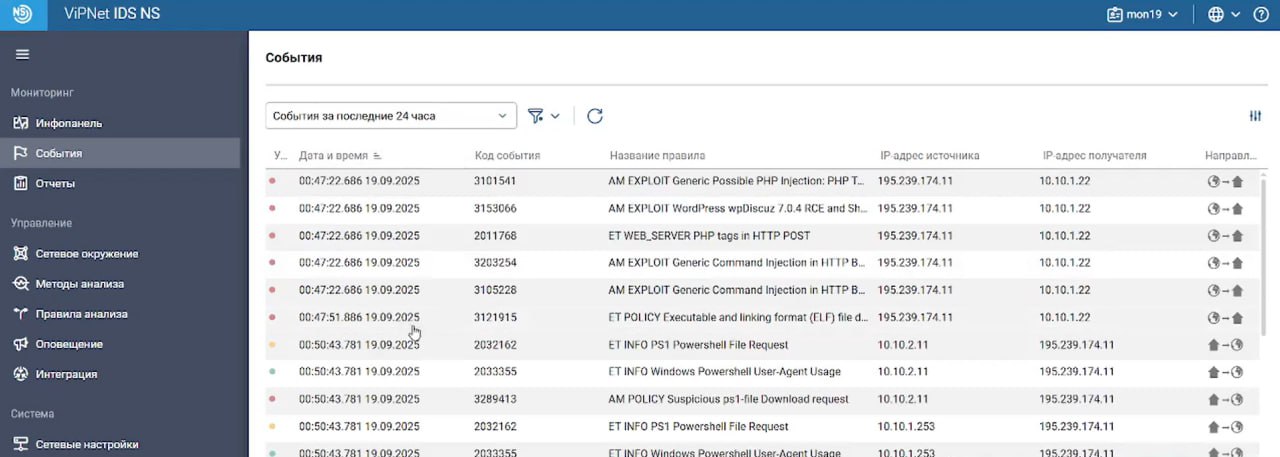
# 3 Выполнение лабораторной работы

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



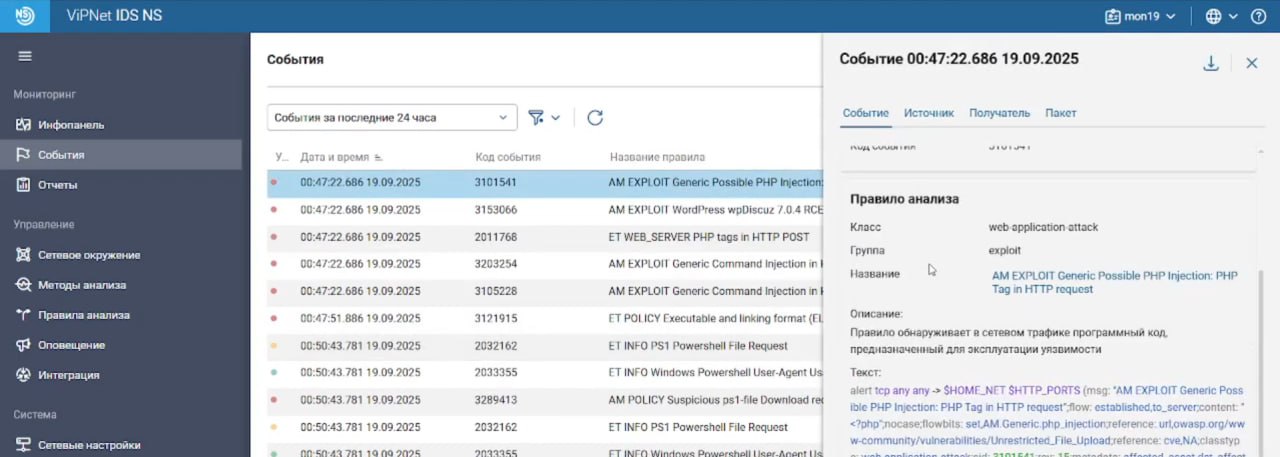
Начало атаки

1. Посмотрели журнал событий с интервалом 15 минут.



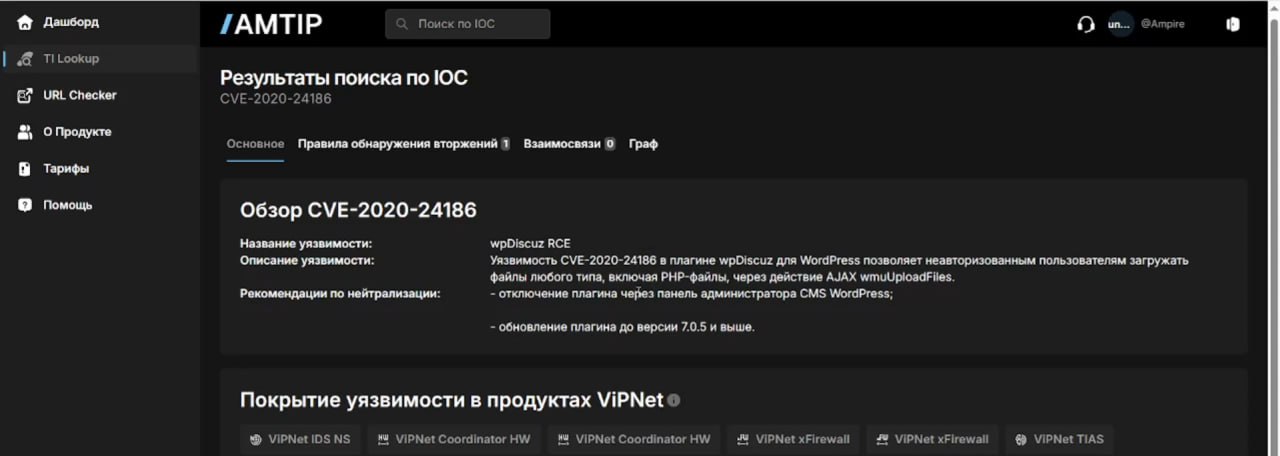
Просмотр журнала

1. Увидели подозрительное событие. Согласно нему правило обнаружило в сетевом трафике программный код, который нужен был для эксплуатации уязвимости.



Подозрительное событие

1. Проверил проверку события по СVE.



Проерка по CVE

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

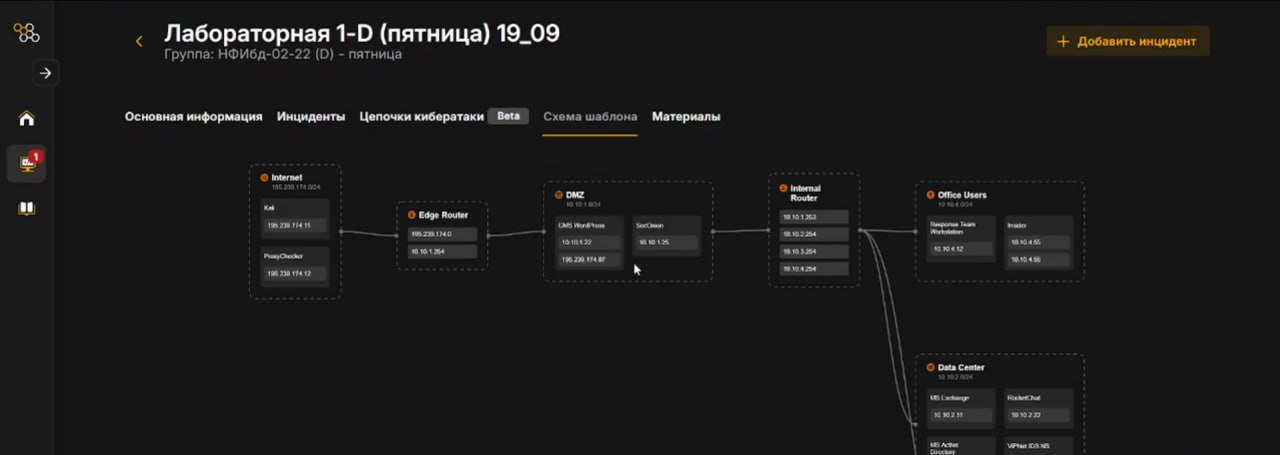
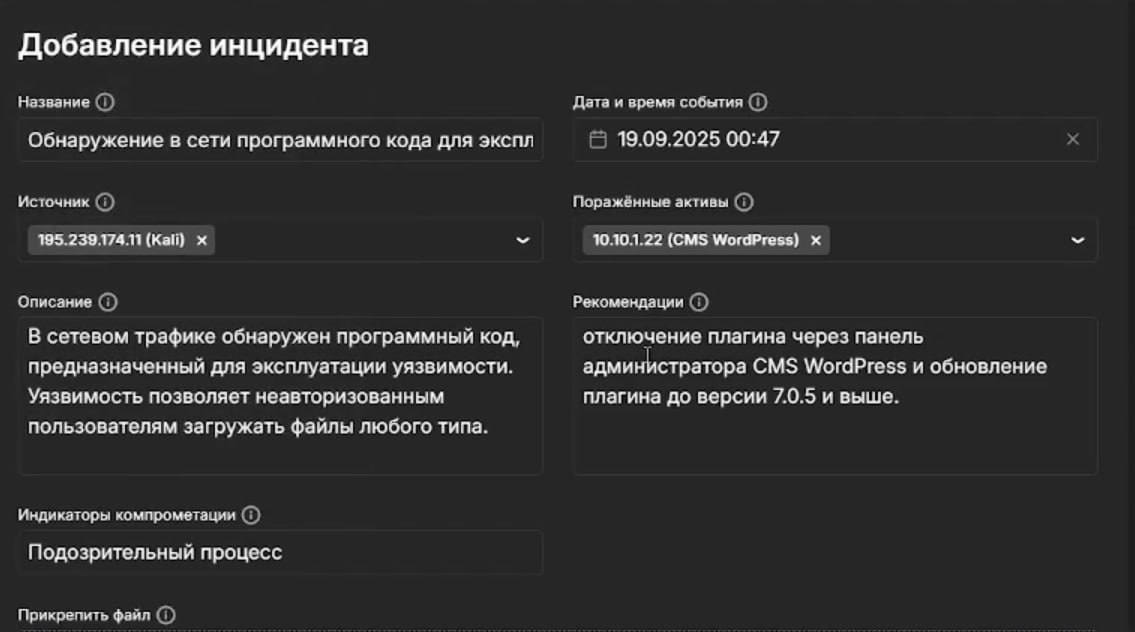


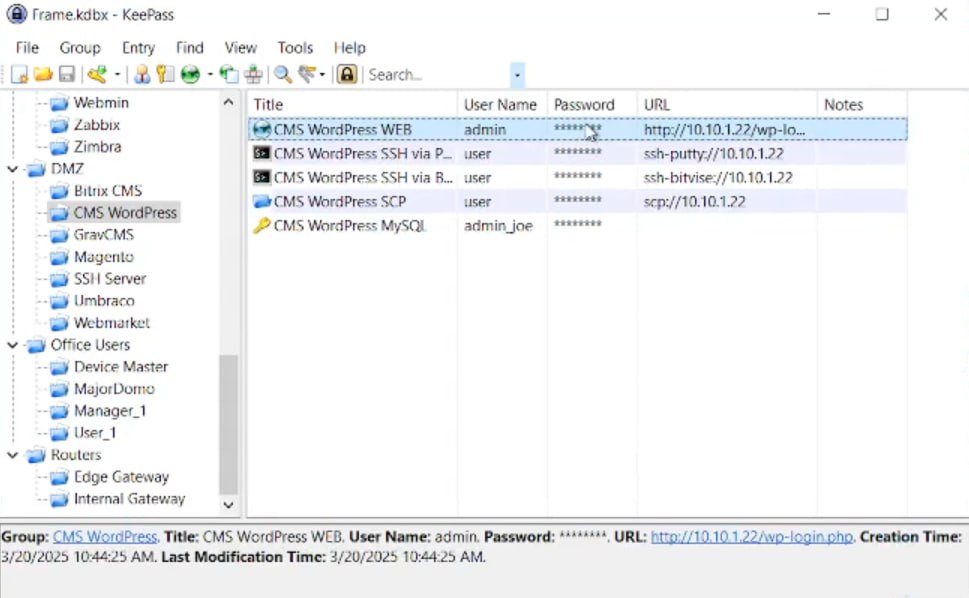
Схема атаки

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



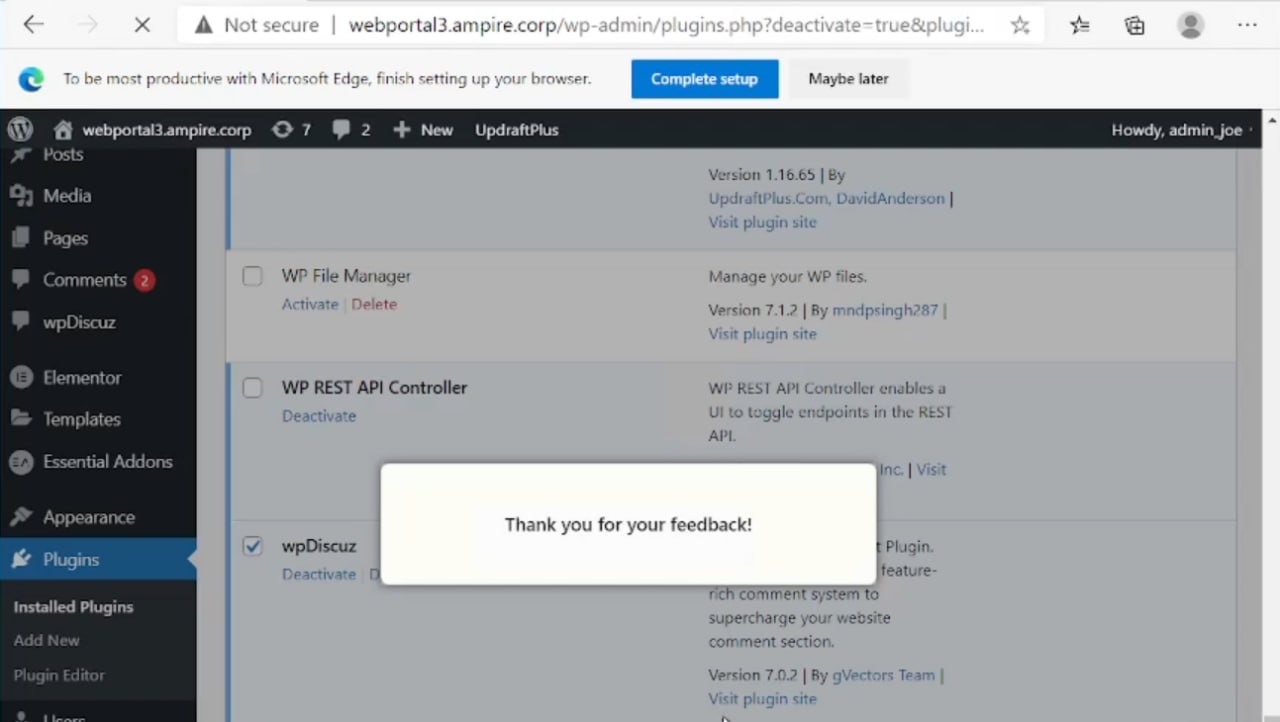
Создание первого инцидента

1. 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.



Подключение к устройству

1. 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.



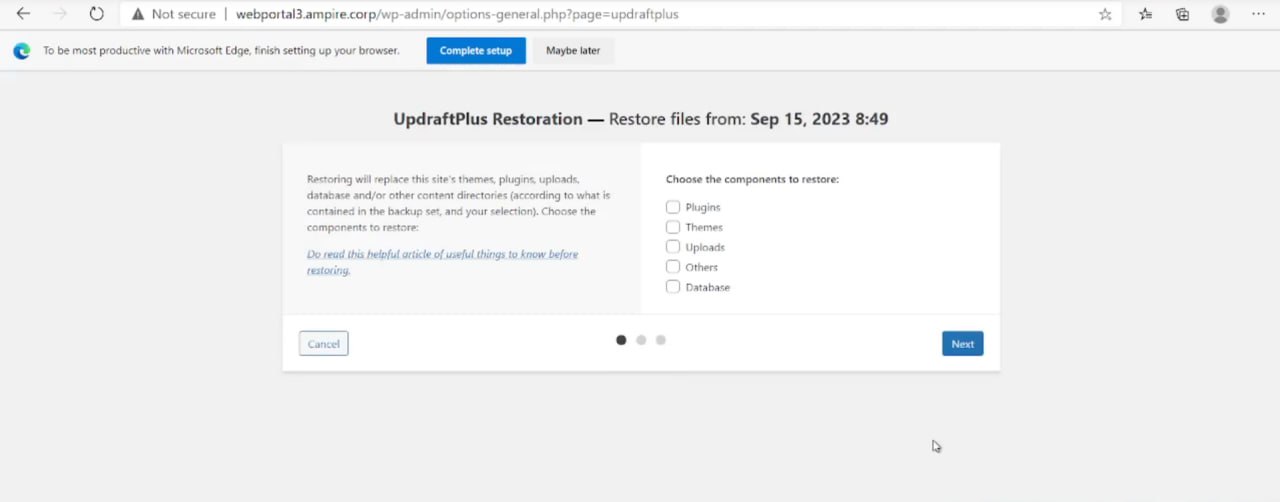
Отключение плагина

1. На странице сайта компании увидели изменения в виде другой фотографии.

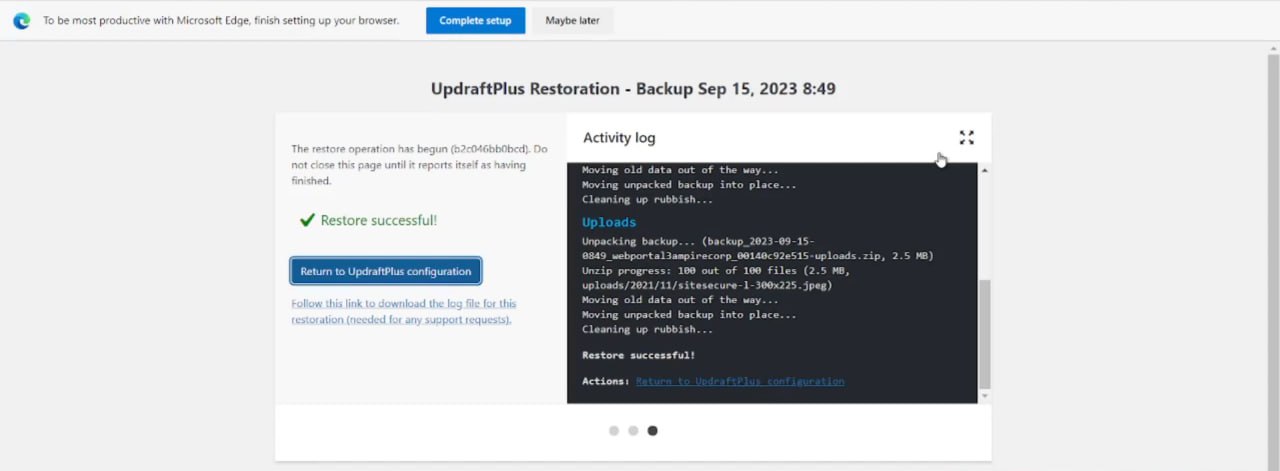


Изменения на сайте компании

1. 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.

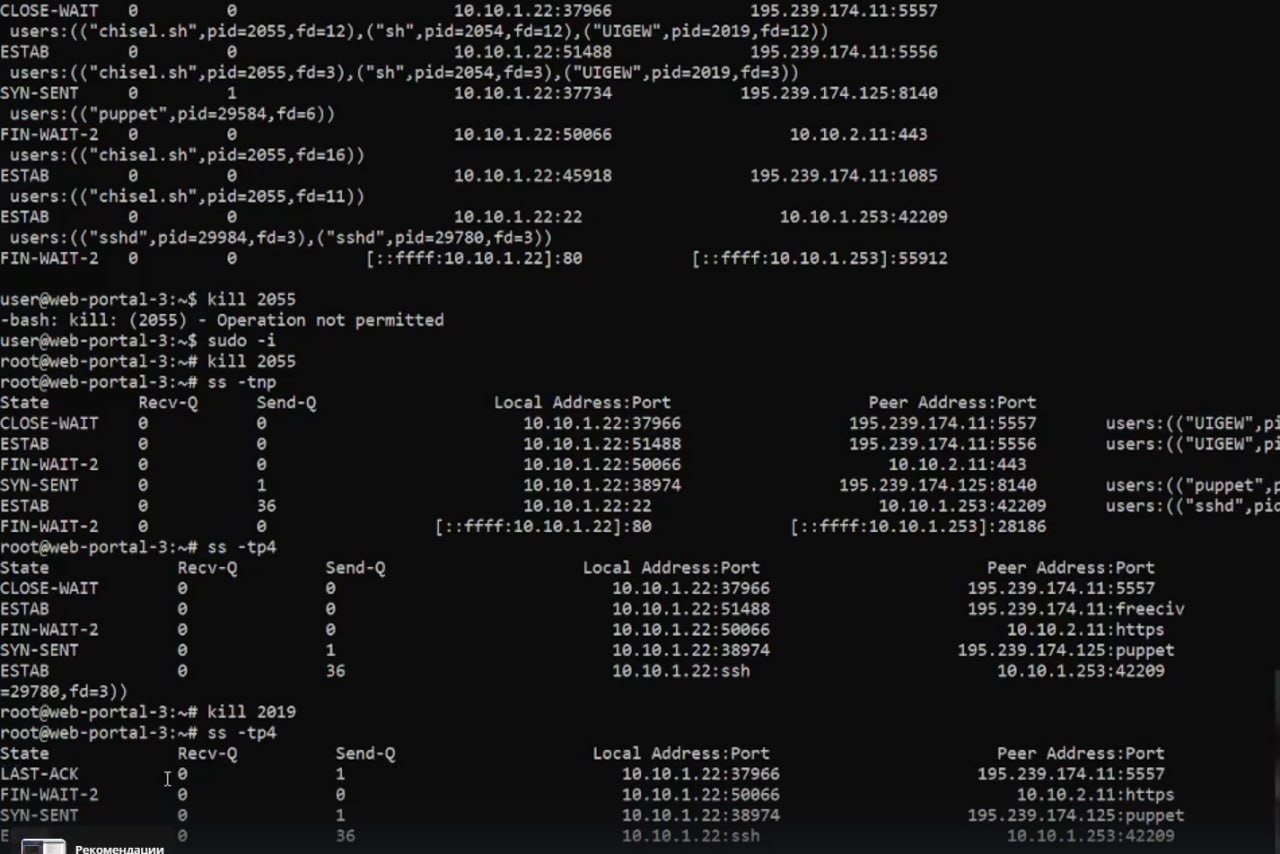


Выбор компонентов



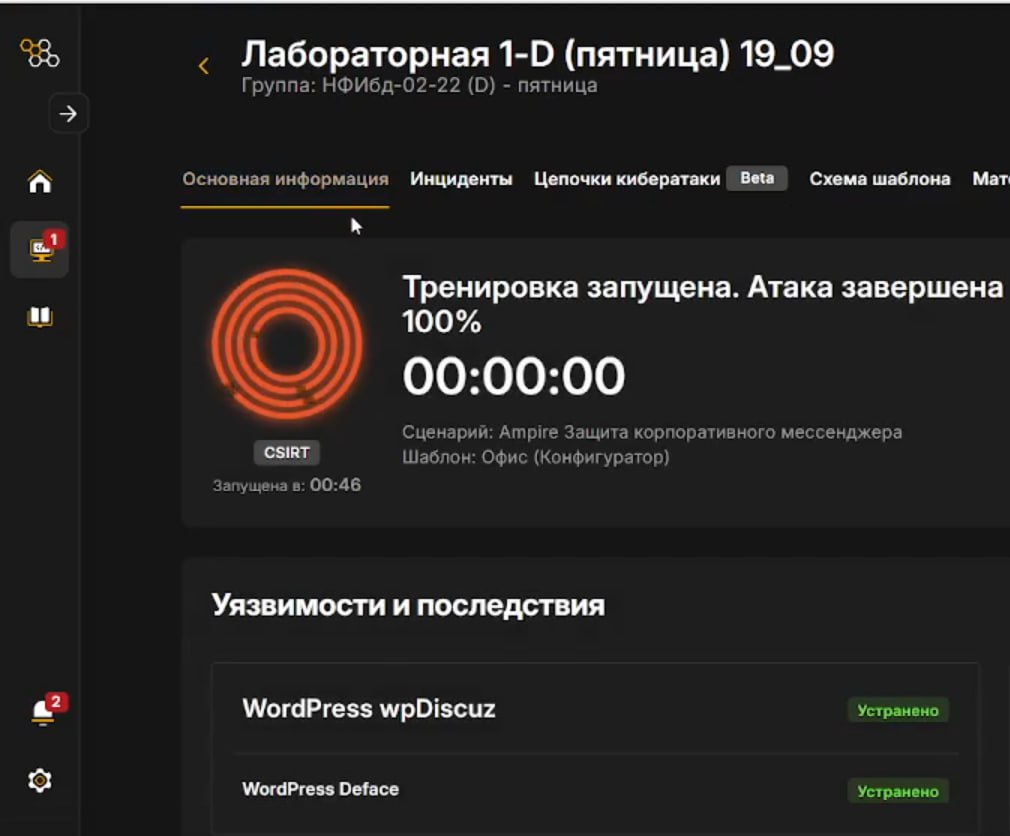
Успешное выполнение установления

1. 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.



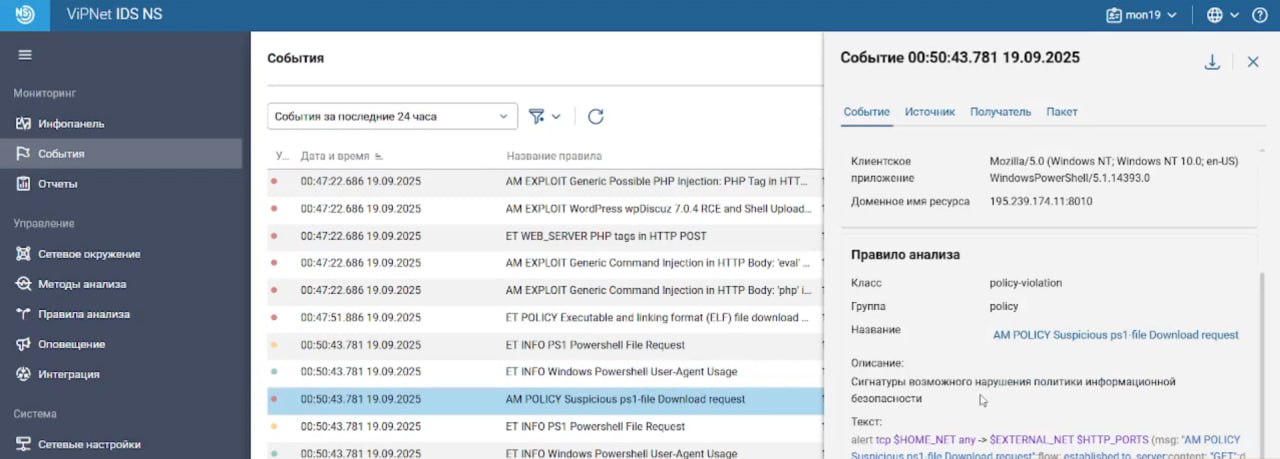
Процесс закрытия соединения

1. Проверили, что уязвимость и последствие WordPress устранены.



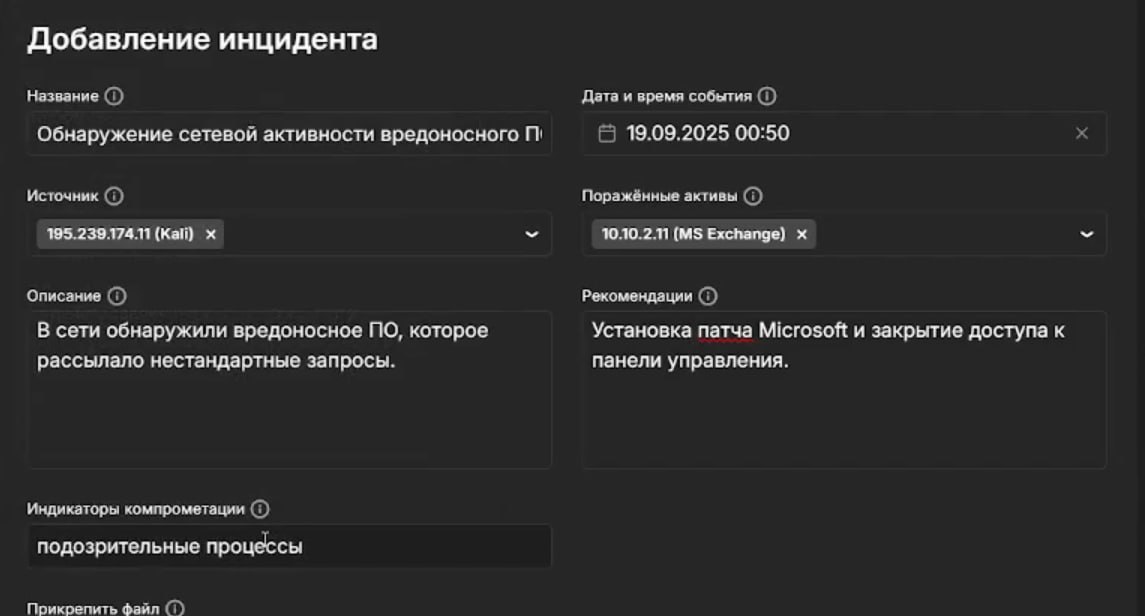
Проверка первого события

1. Перешли вновь к журналу событий. Увидели вторую подозрительную активность.



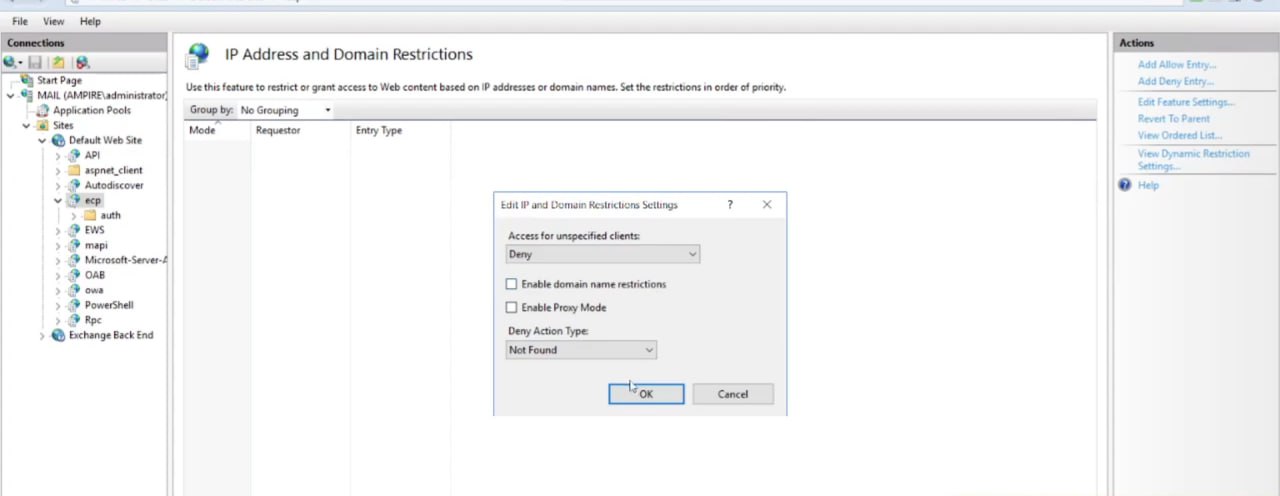
Второе событие

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



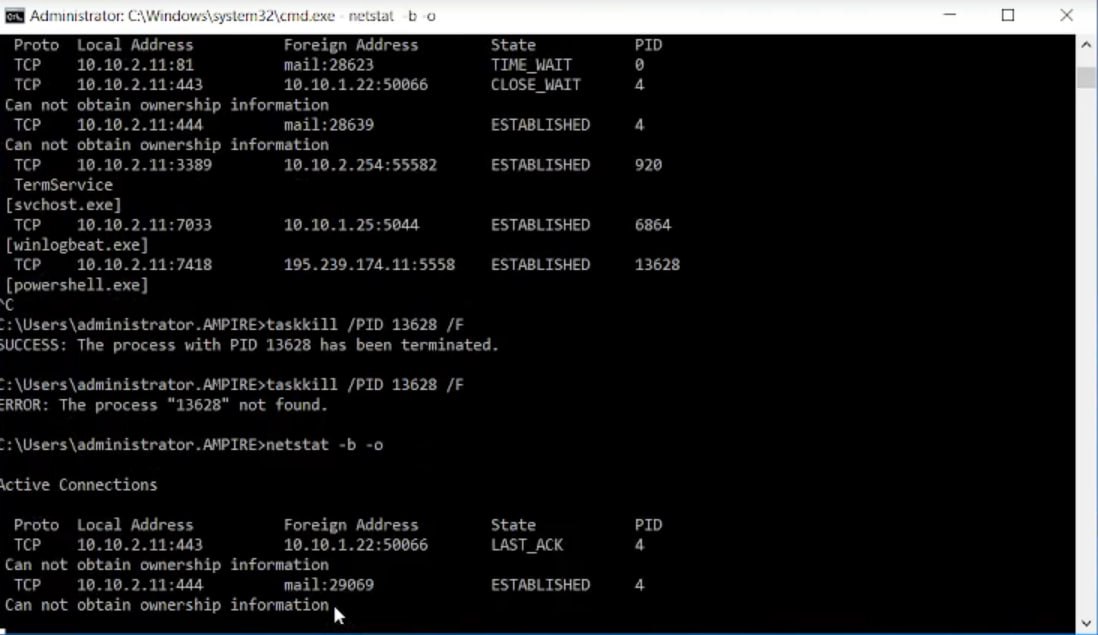
Второй инцидент

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



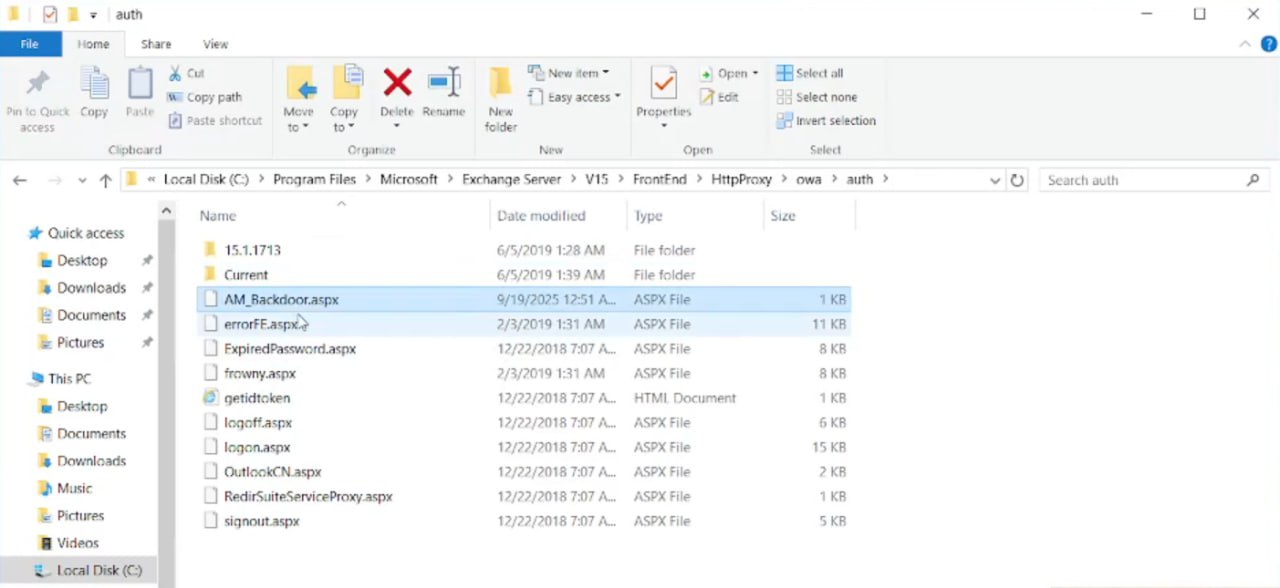
Ограничение к директории

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



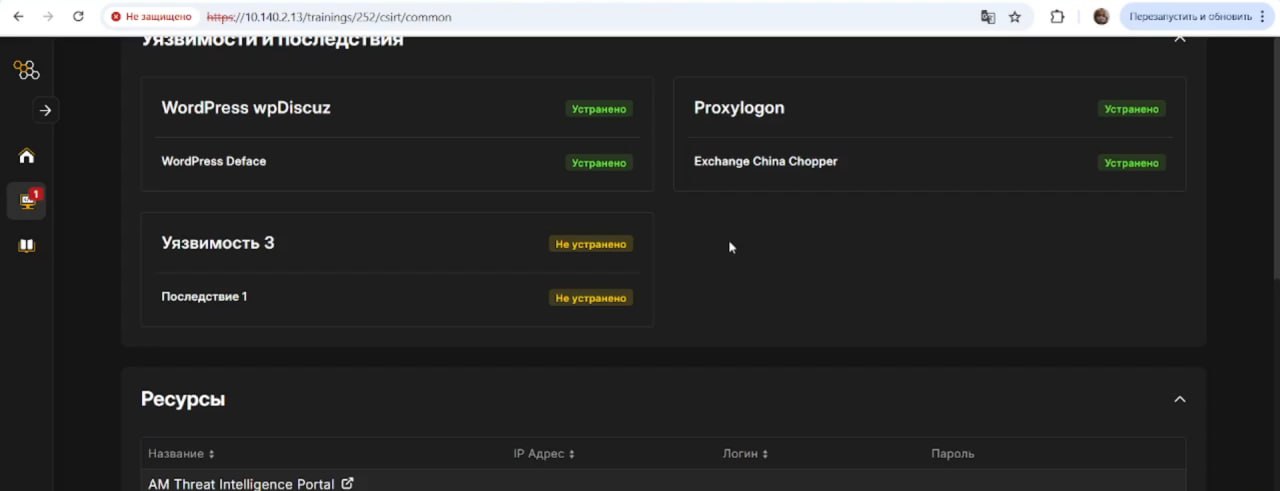
Закрытие соединения

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



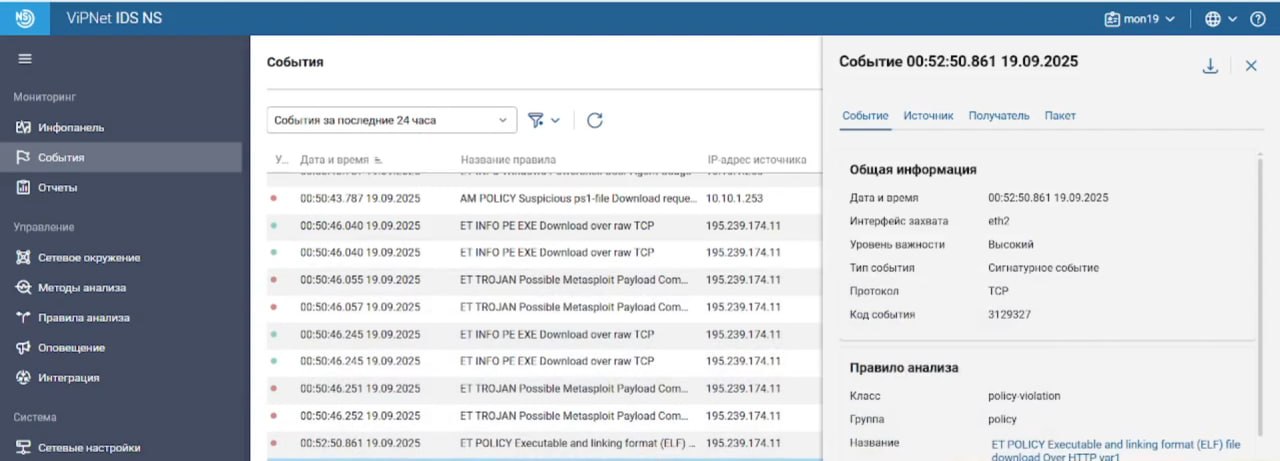
Удаление файла

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



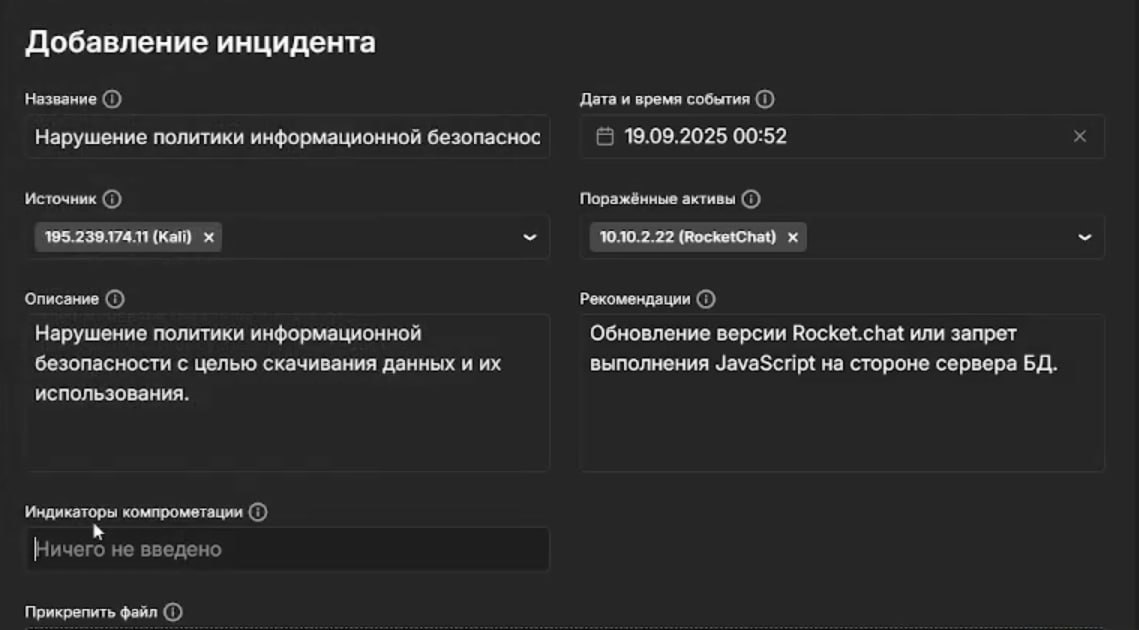
Устранение Proxylogon

1. Снова проверили журнал событий. Нашли ещё одно подозрительное событие.



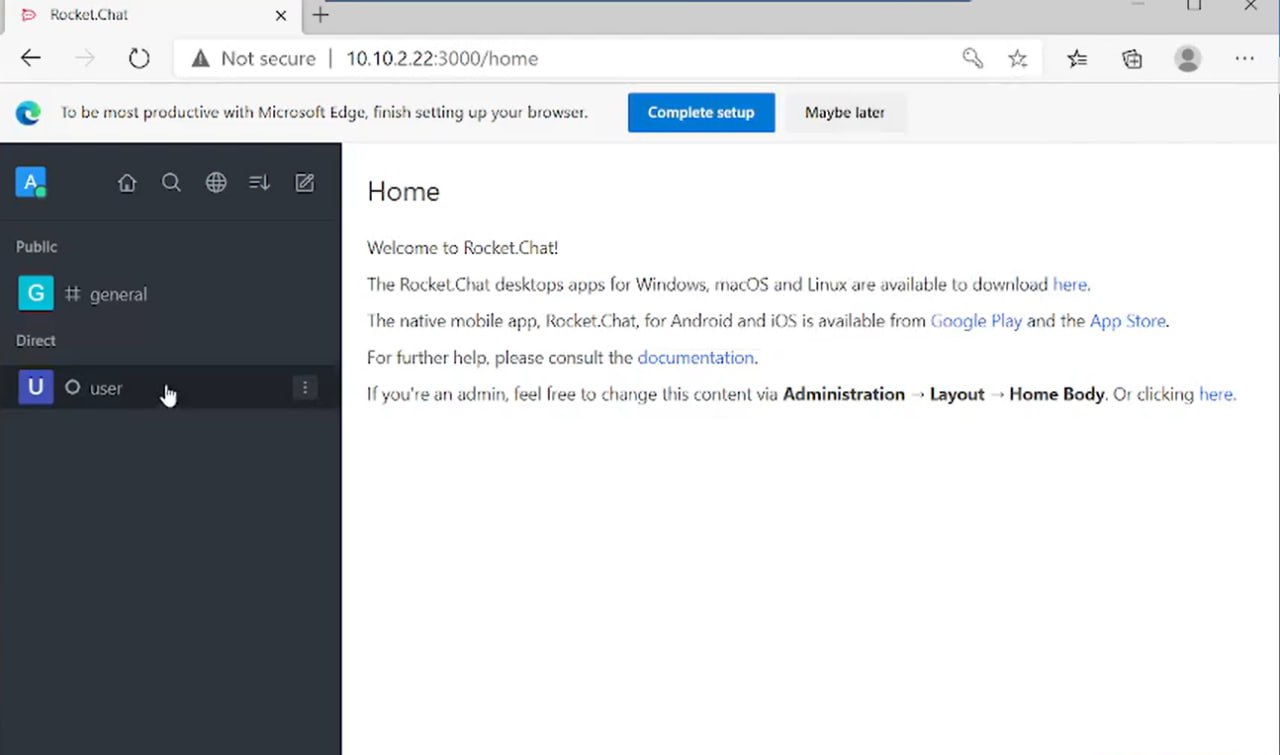
Проверка журнала

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



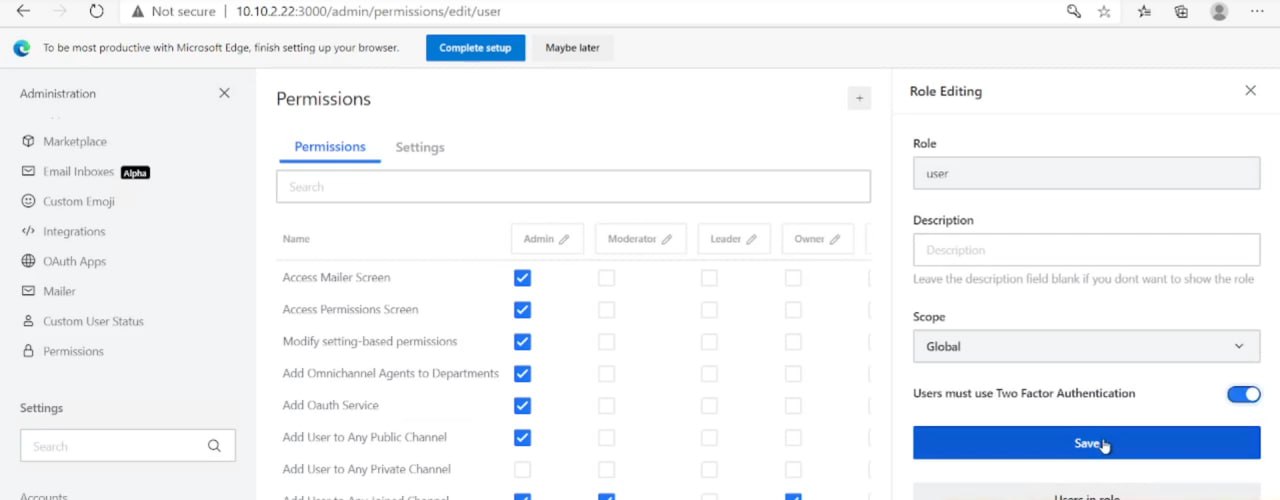
Третий инцидент

1. 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.



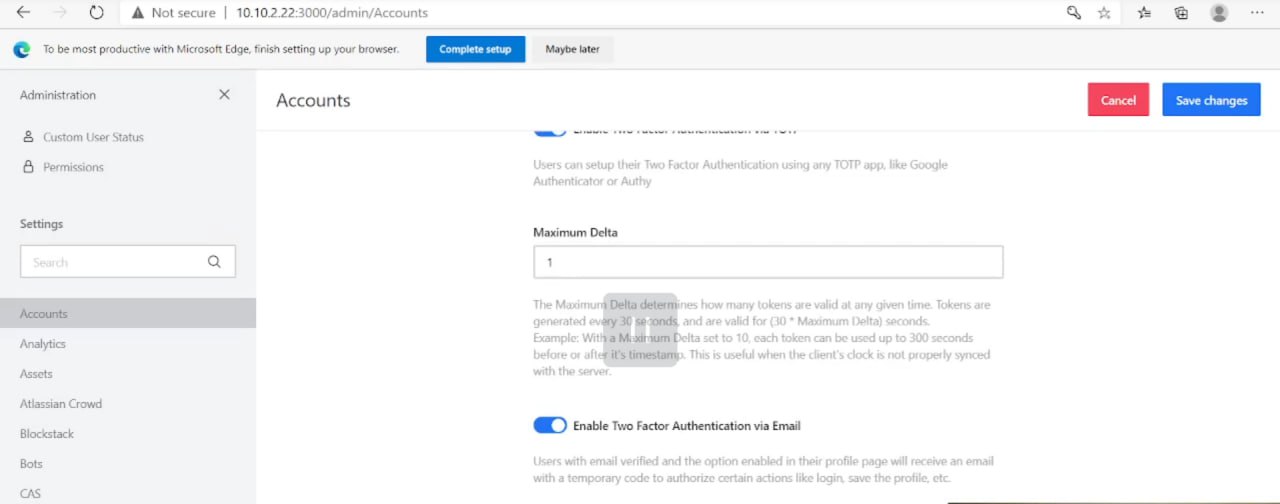
Вход на сайт через администратора

1. Включили обязательную двухфакторную аутентификацию для простых уже зарегистрированных пользователей.



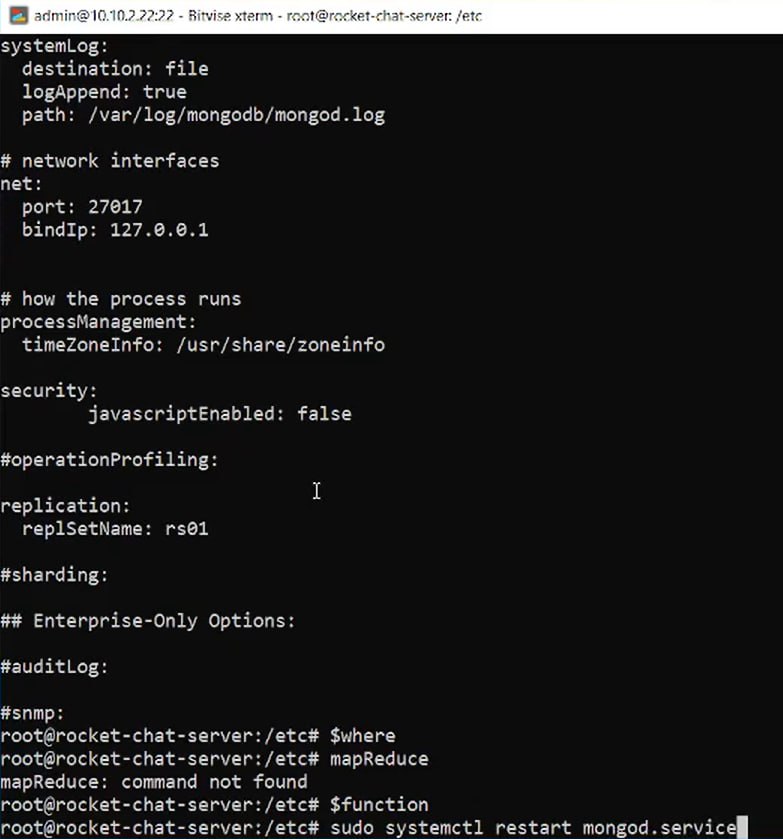
Двухфакторная аутентификация

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



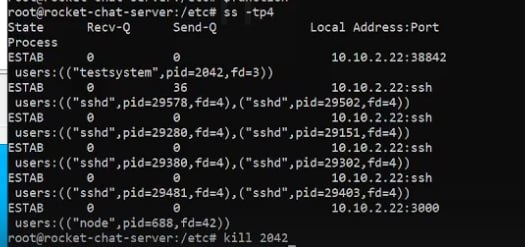
Настройки регистрации новых пользователей

1. Отключили параметр javascriptEnabled и перезапустили службу.



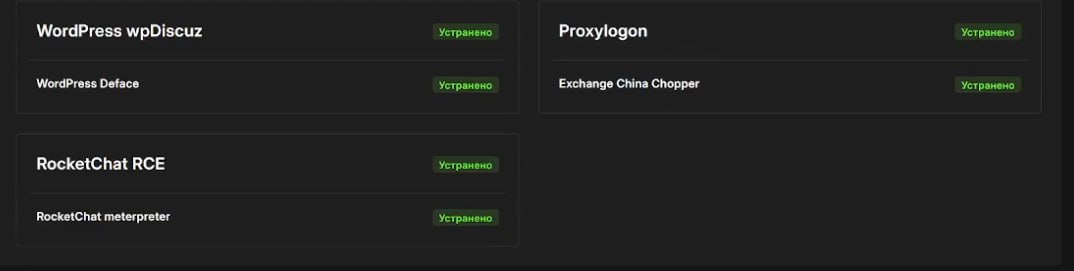
Отключение javascriptEnabled

1. Для устранения последствия необходимо было отключить атакующего от нашего пользователя. Завершили все сессии с устройства Kali на наш компьютер.



Завершение всех сессий атакующего

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



Устранение всех последствий

# 4 Вывод

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