# Цель работы

Показать этапы реализации атак и контрмер в сценарии компрометации научно-технической

информации предприятия, определить уязвимости, продемонстрировать доказательства успешной эксплуатации и предложить практические способы устранения.

# Теоретическое введение

Легенда: защита корпоративного мессенджера 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. Уязвимости и последствия:

1. WordPress-wpDiscuz (CVE-2020-24186) (критическая уязвимость в плагине wpDiscuz (версии 7.0 — 7.0.4), позволяющая неаутентифицированному пользователю загружать любые файлы через

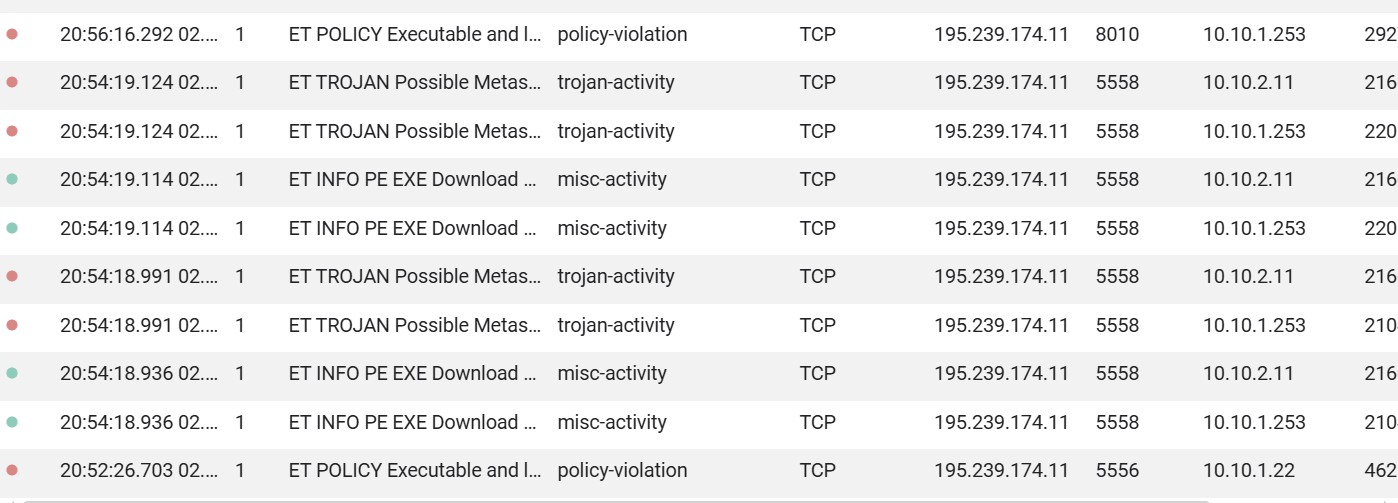
уязвимый AJAX-эндпоинт (включая PHP).) → Deface

1. Proxylogon (CVE 2021-27065) (при наличии аутентификации (или после обхода через другие уязвимости) злоумышленник мог записать произвольный файл на сервер Exchange и добиться RCE.) → Exchange China Chopper
2. Rocket.Chat (CVE-2021-22911, CVE-2022-0847) (уязвимость в Rocket.Chat — недостаточная санация входа, приводящая к NoSQL-инъекции в неаутентифицированном API, что могло позволить

похищение токенов сброса пароля и захват админского аккаунта) → Meterpreter

# Выполнение лабораторной работы

Обнаружение атак (рис. 1 - 2)



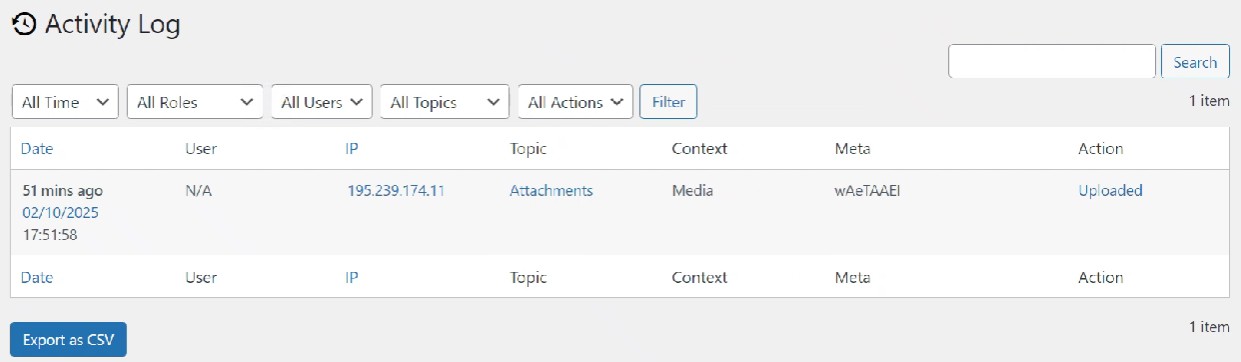
(рис. 1)



(рис. 2)

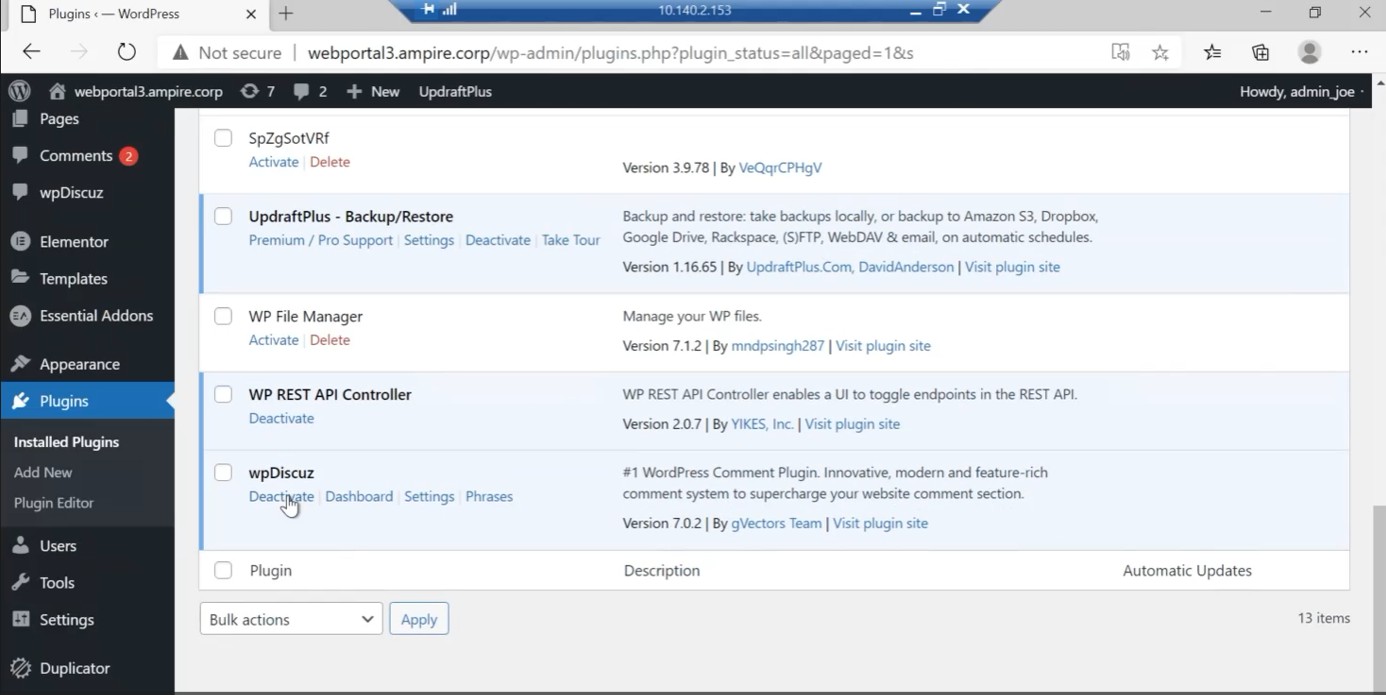
Уязвимость 1. WordPress-wpDiscuz (CVE-2020-24186) (рис. 2)

С помощью WP Activity Log можно проверить журнал и обнаружить время, дату, роль и IP-адрес пользователя, который внес изменения. По информации из журналов на сервере можно отыскать причину взлома и устранить возникшие уязвимости.



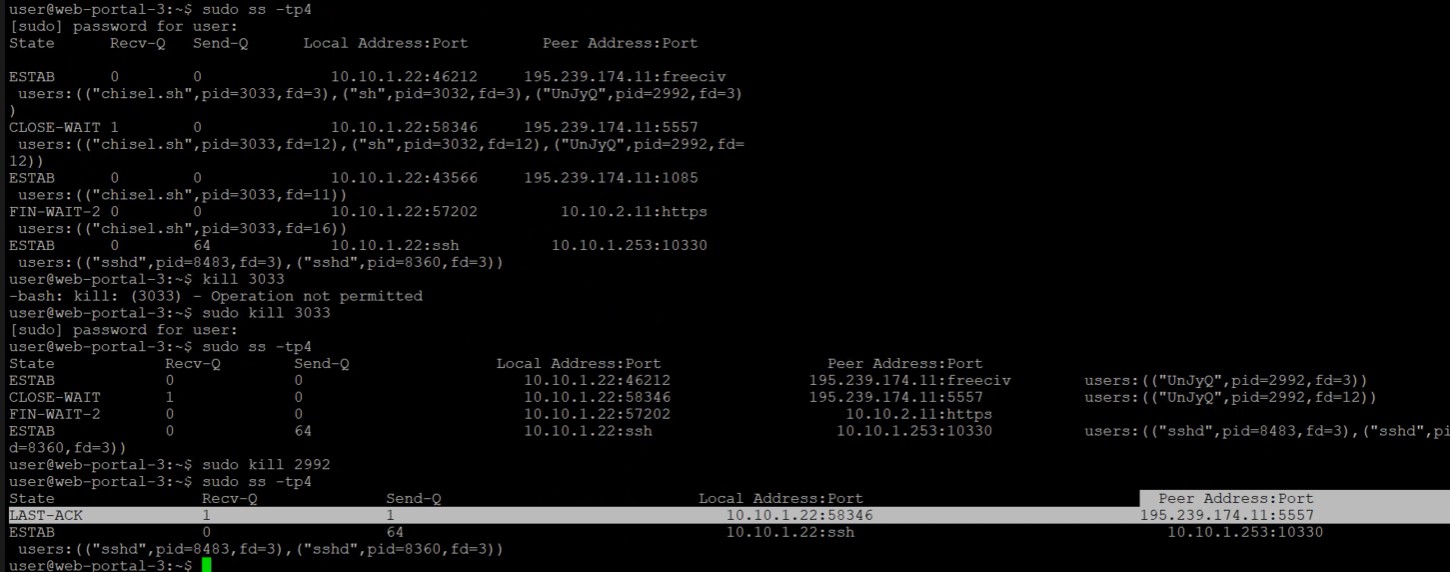
(рис. 3)

Для устранения уязвимости мы деактивировали WordPress.



(рис. 4)

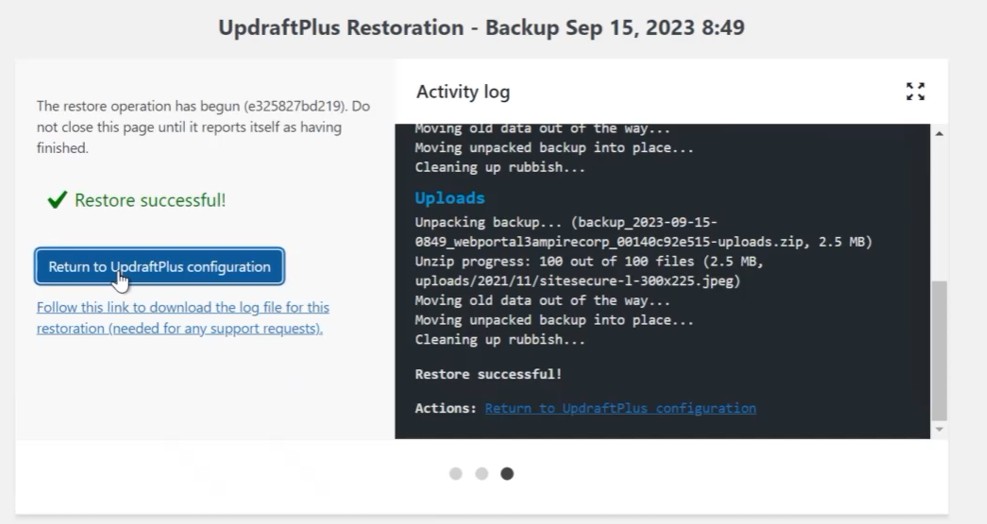
Также для устранения этой уязвимости необходимо удалить meterpreter сессию.



(рис. 5)

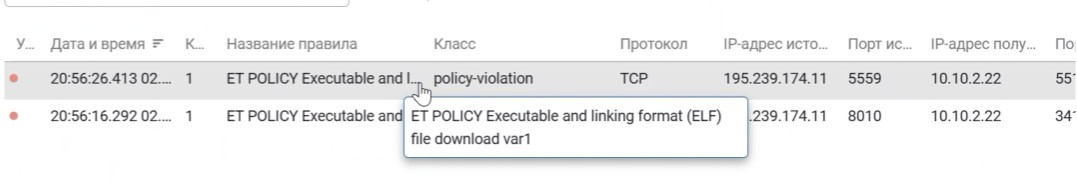
Последствие 1. Deface (рис. 6)

Для нейтрализации данной полезной нагрузки необходимо сформировать резервную копию с помощью плагина Updraft Backup/Restore.



(рис. 6)

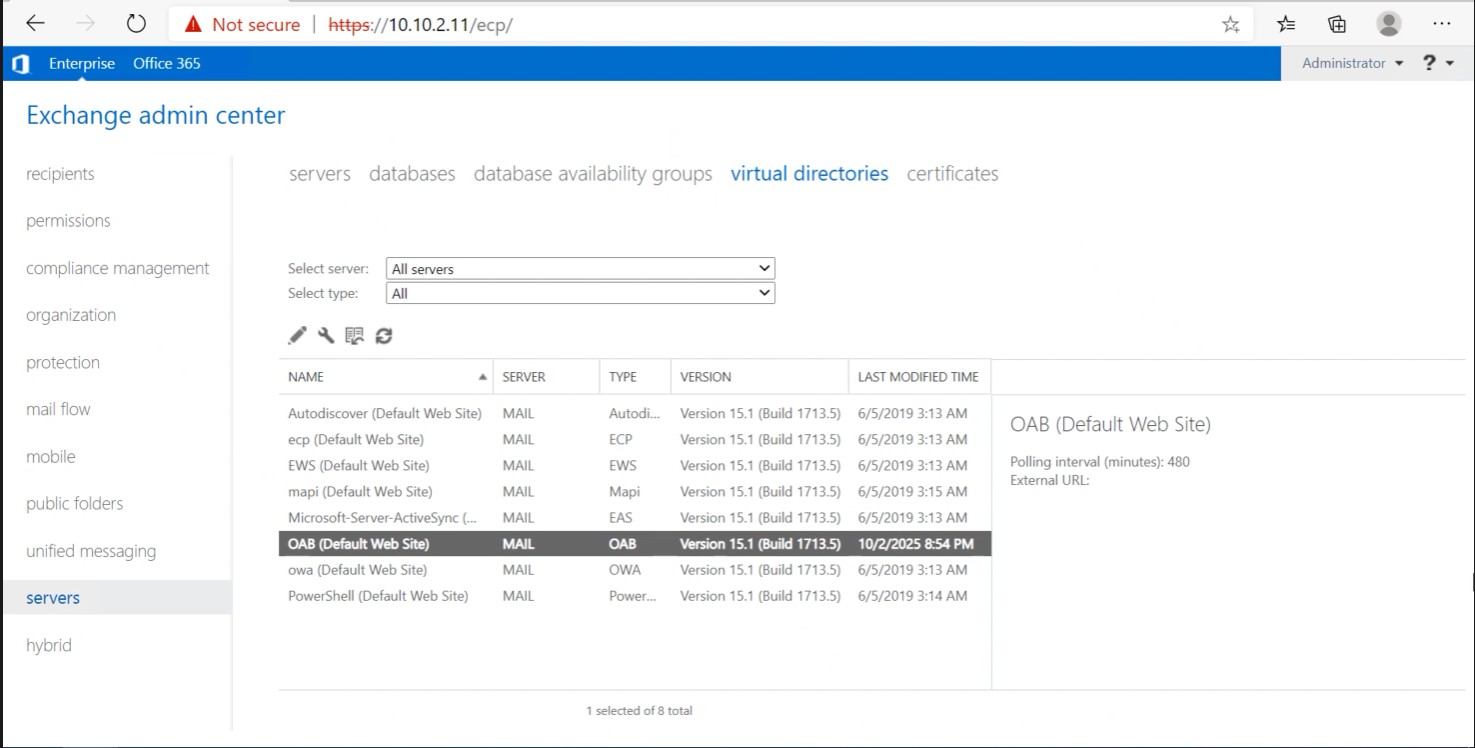
Уязвимость 2. Proxylogon (CVE 2021-27065) (рис. 7 - 011)



(рис. 7)

Данная уязвимость является следствием неэффективного ограничения выбора расположения backup виртуальной директории автономных адресных книг. Одним из шагов для эксплуатации данной

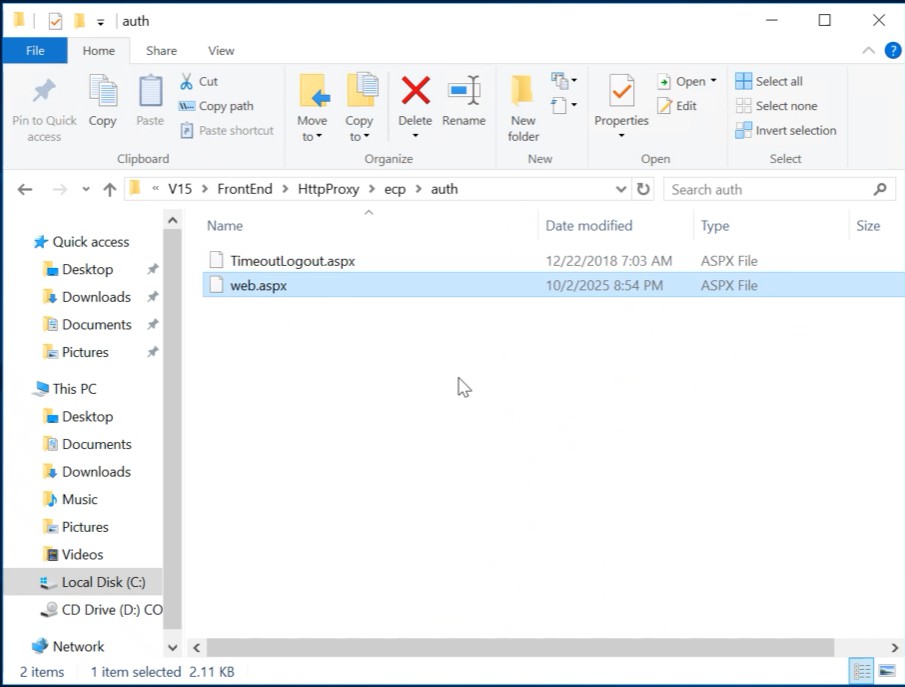
уязвимости является изменение параметров OAB. После успешной авторизации нарушитель открыл веб-интерфейс настройки «Exchange – ecp» (Exchange Control Panel), в «Servers – Virtual directories» (Рисунок 12) и изменил параметры виртуальной директории.



(рис. 8)

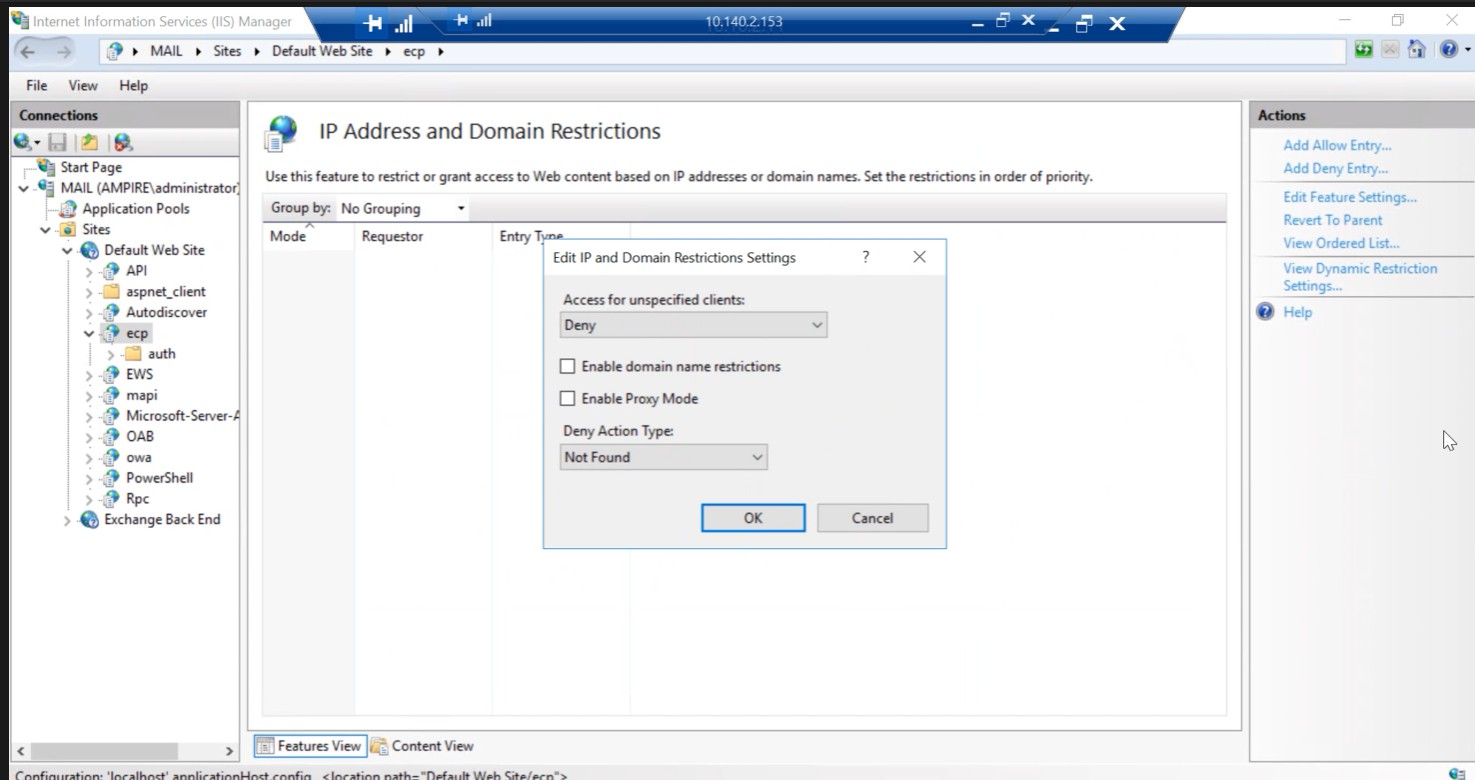
В нашей реализации файлом backdoor является web.aspx (Рисунок 19). Для доступа к системе

нарушителем выбрана директория /ecp, в данной директории находится вредоносный файл backdoor, представляющий из себя aspx web-shell.



(рис. 9)

Для устранение уязвимости мы ограничили доступ к указанной директории для запрета эксплуатации уязвимости:



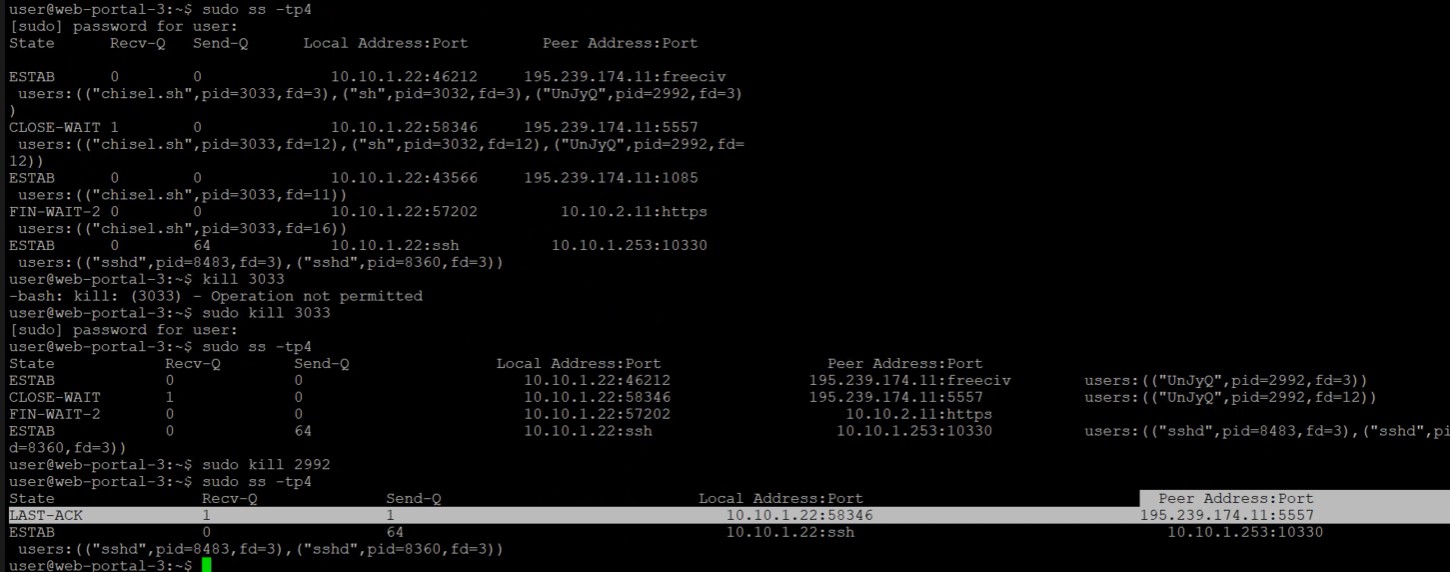
(рис. 10)

Индикатор устранения не изменился, для выполнения этого пункта также необходимо решить последствие 2.

Последствие 2. Exchange China Chopper (рис. 11)

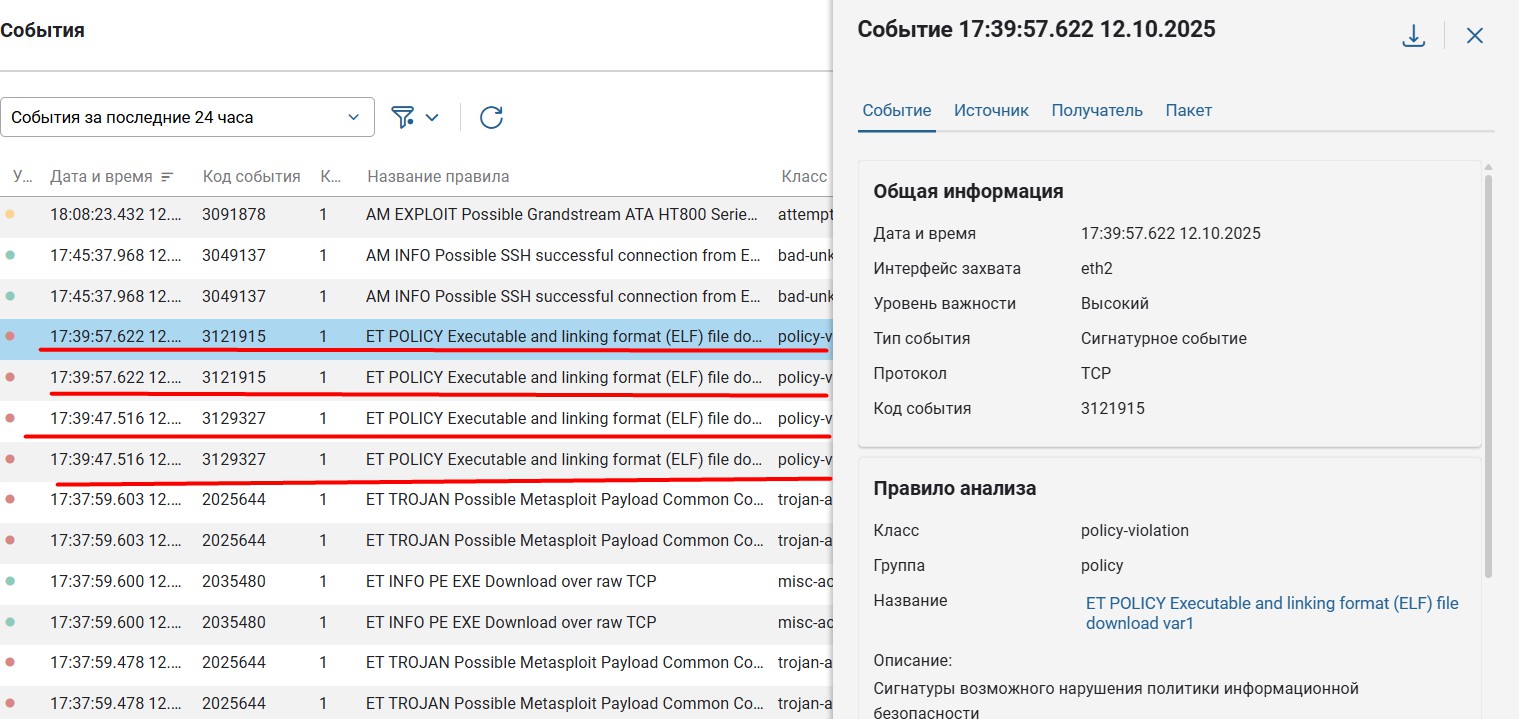
Для устранения полезной нагрузки мы удалили файл веб-оболочки по пути С:\Program

Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy..\auth; завершили все соединения между уязвимой машиной и нарушителем.



(рис. 11)

Уязвимость 3. Rocket.Chat (CVE-2021-22911, CVE-2022-0847) (рис. 12 - 19) Обнаружение уязвимости:

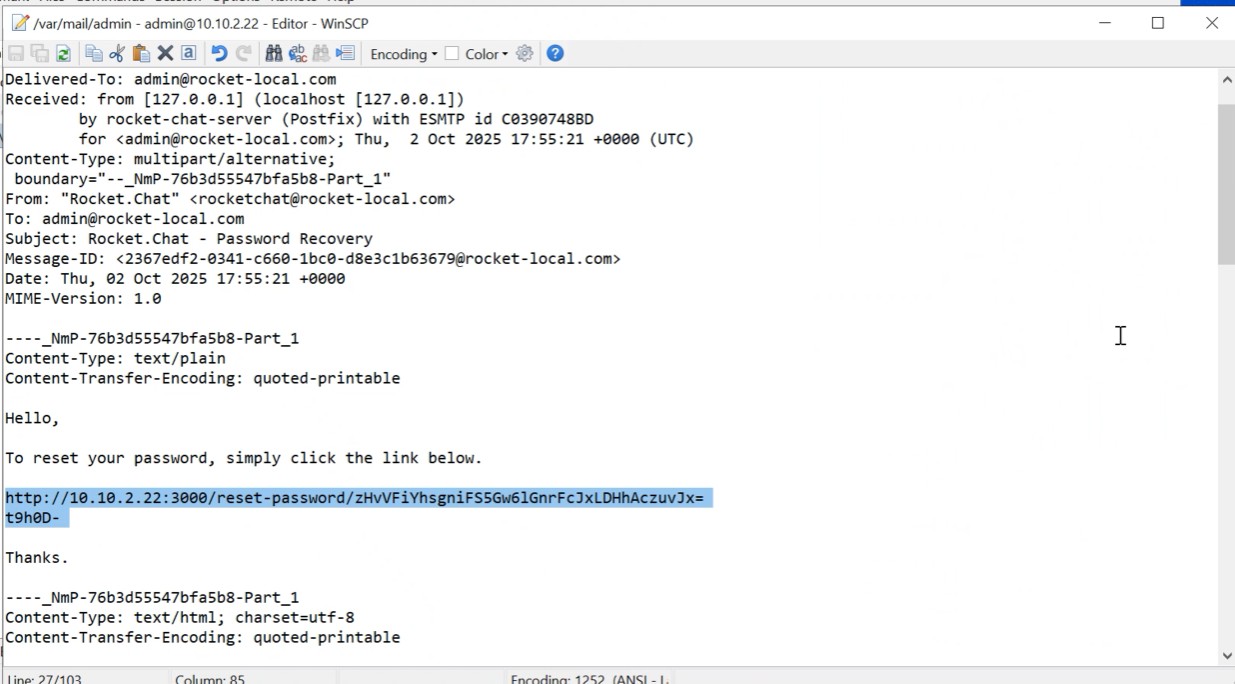


(рис. 12)

Для закрытия уязвимости мы выполнили следующие шаги (рис. 13 - 18):

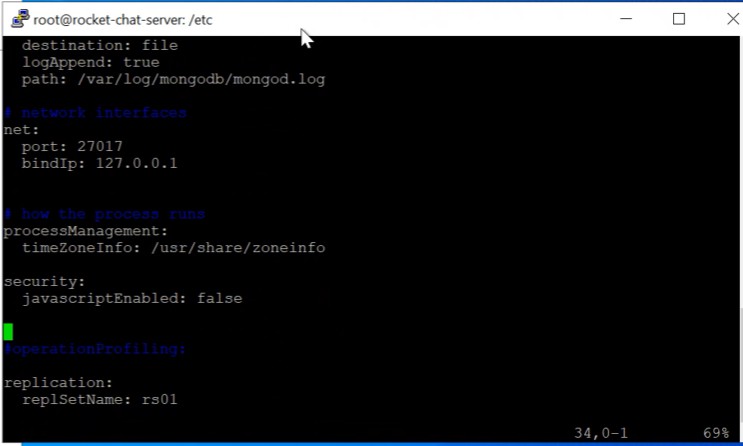
Для восстановления доступа к аккаунту администратора необходимо сбросить пароль. Письмо с инструкциями для сброса пароля мы открыли при помощи текстового редактора, прочитав файл

/var/mail/admin (рис. 1)

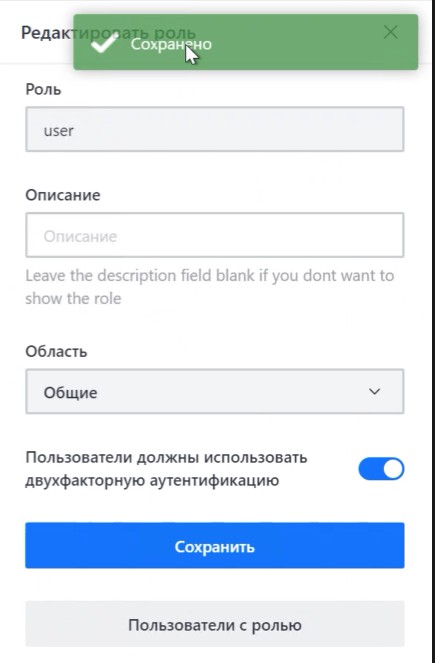


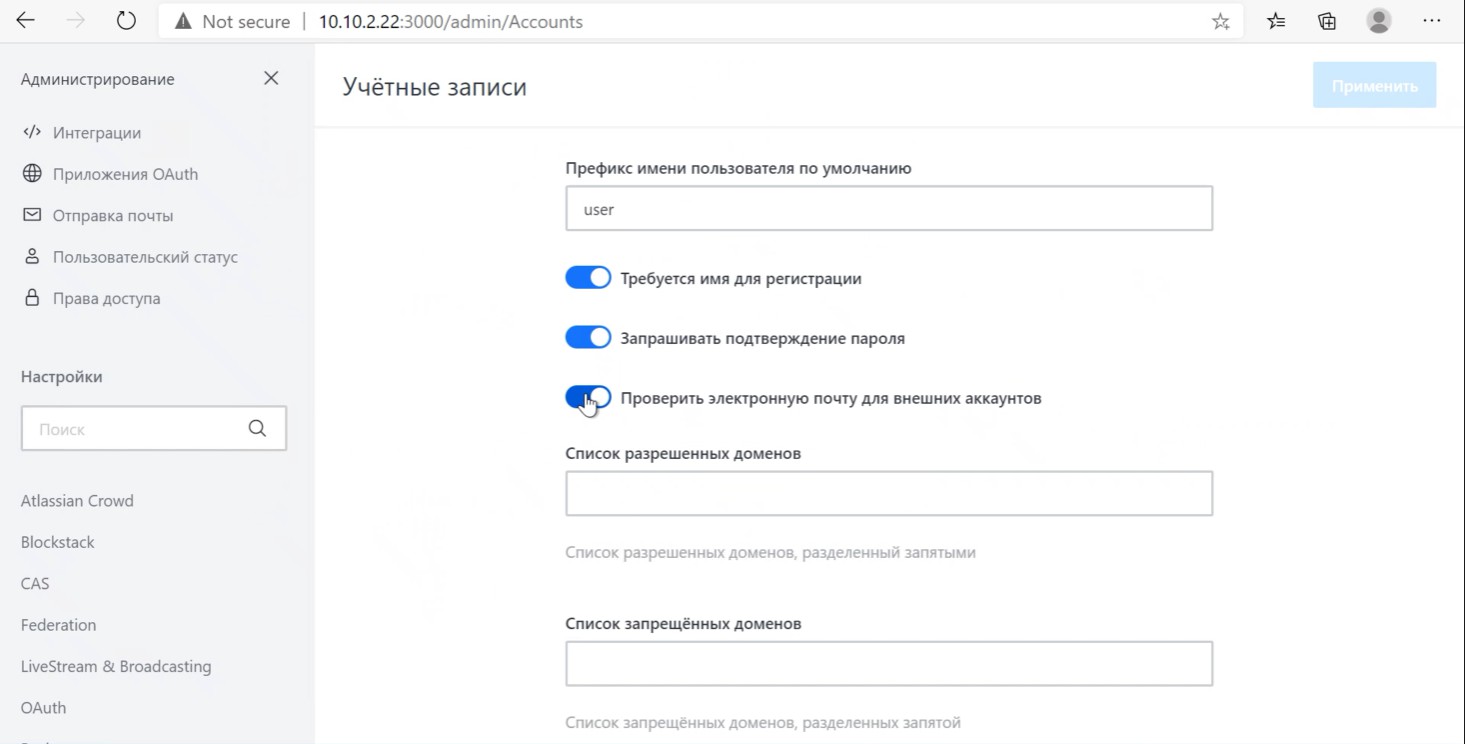
(рис. 13)

Изменив пароль, мы отредактировали файл конфигурации БД /etc/mongod.conf:

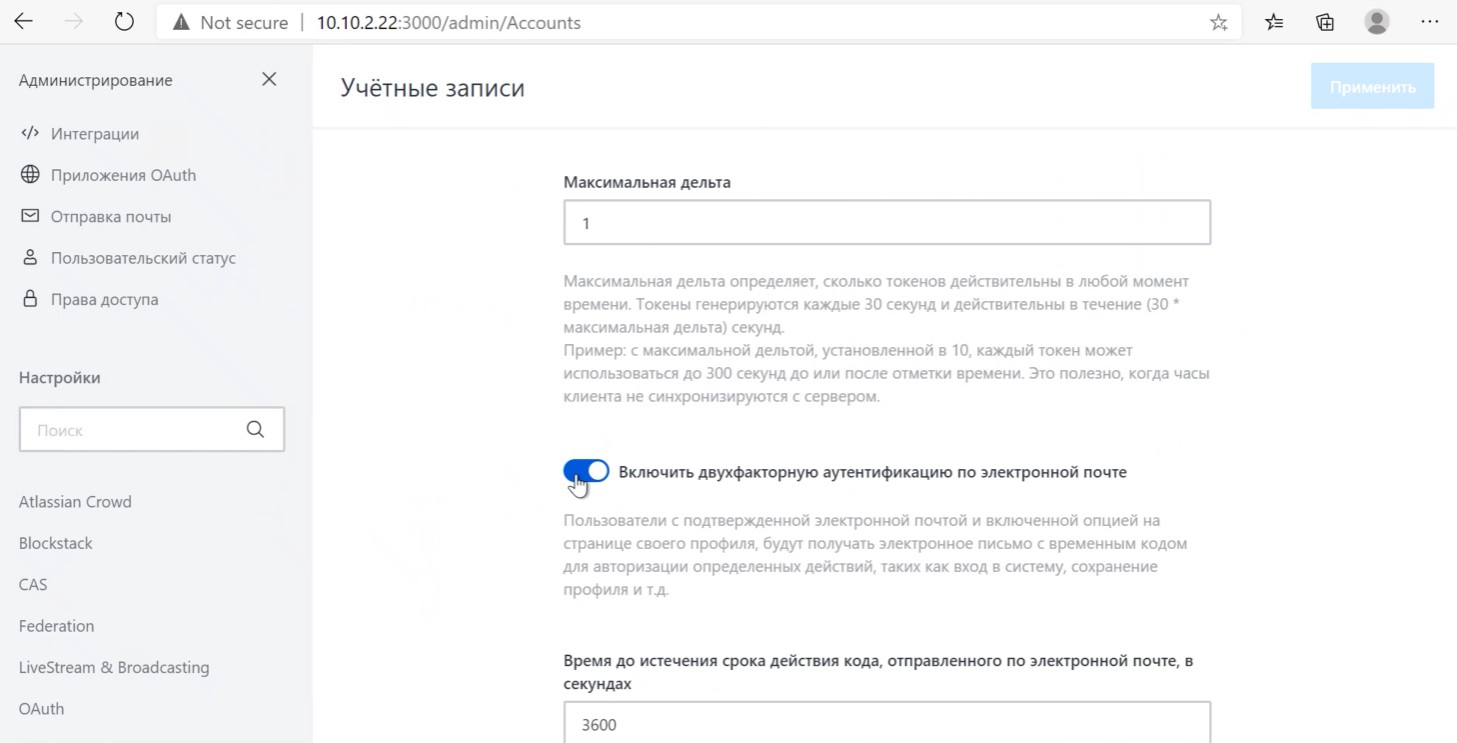


(рис. 14)

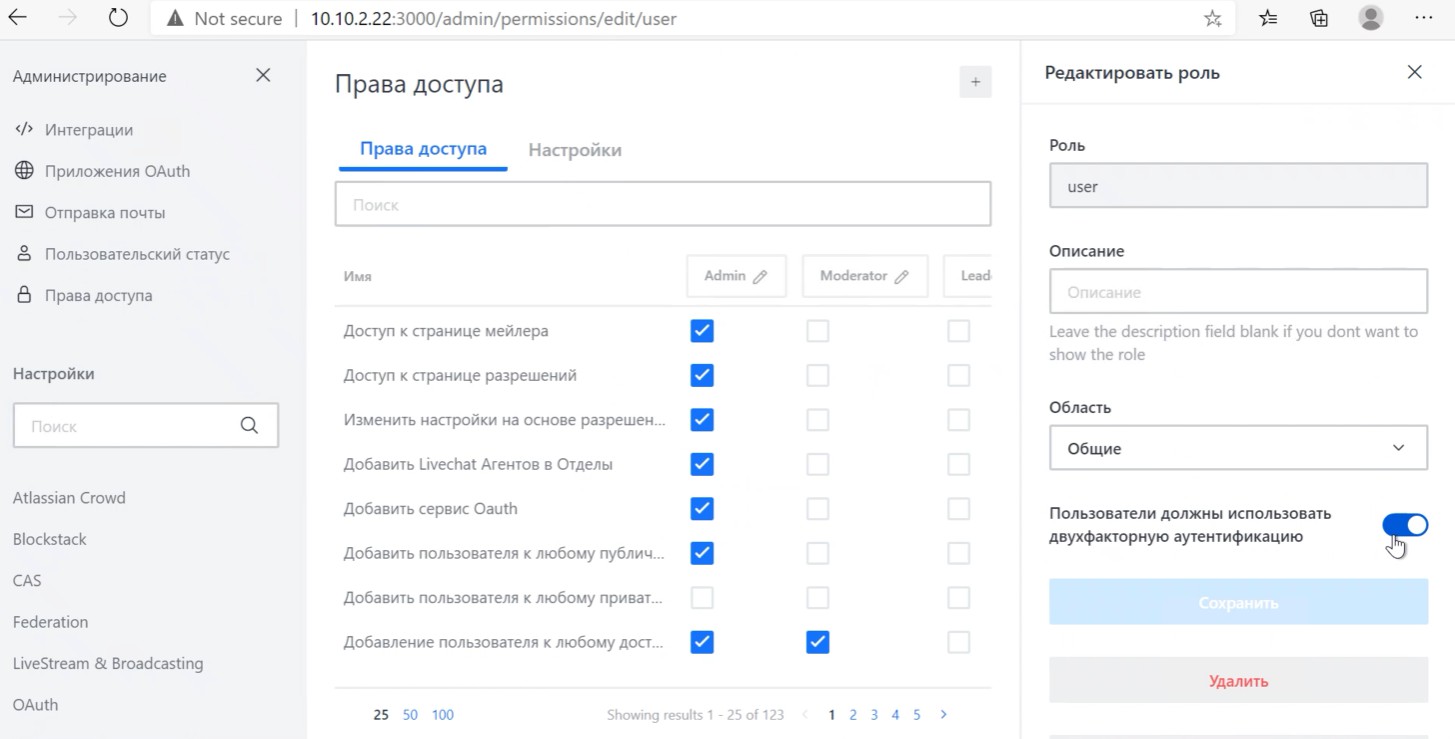
(рис. 15)



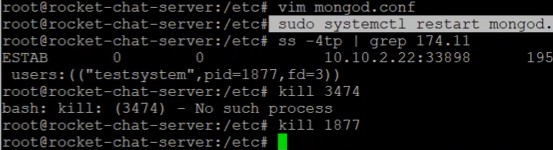
(рис. 16)



(рис. 17)

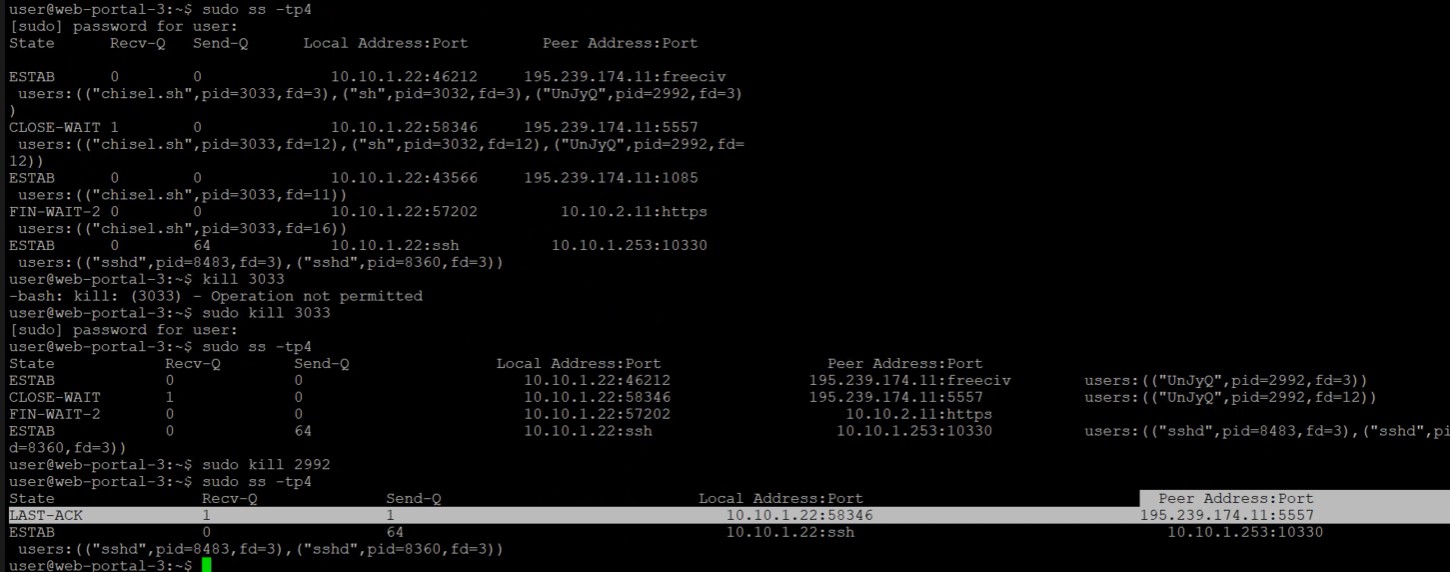


(рис. 18)

(рис. 19)

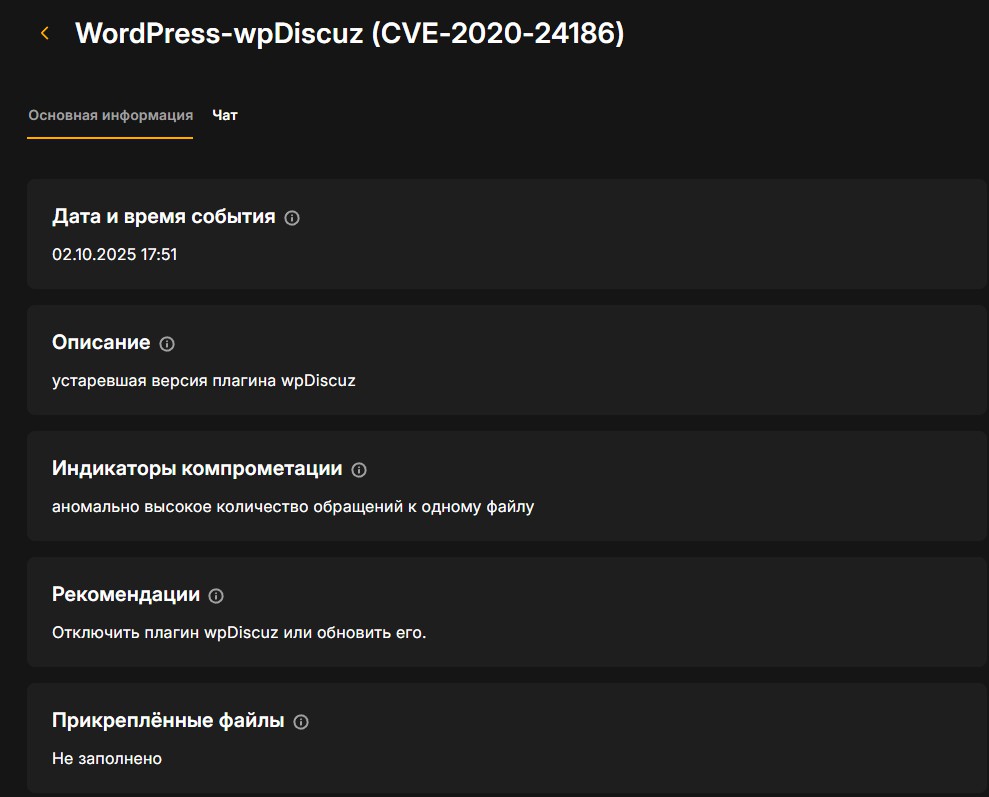
Последствие 3. Meterpreter (рис. 20)

Данная полезная нагрузка заключается в получении нарушителем meterpreter-сессии с уязвимым сервером. Ее можно обнаружить и устранить(рис. 20)

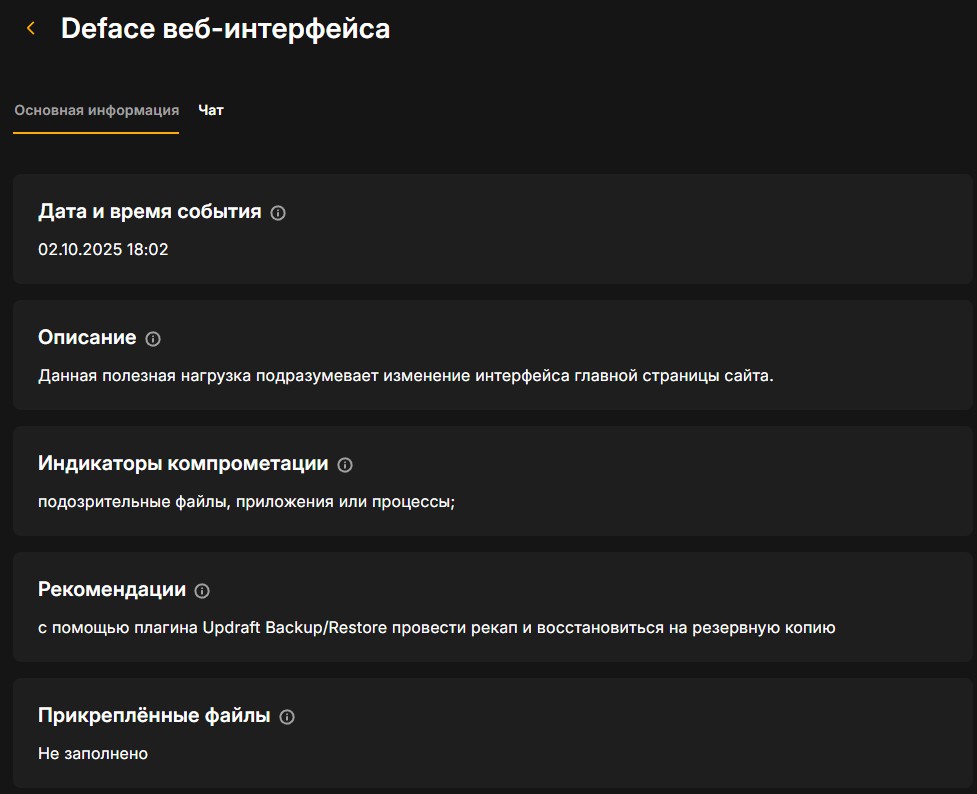


(рис. 20)

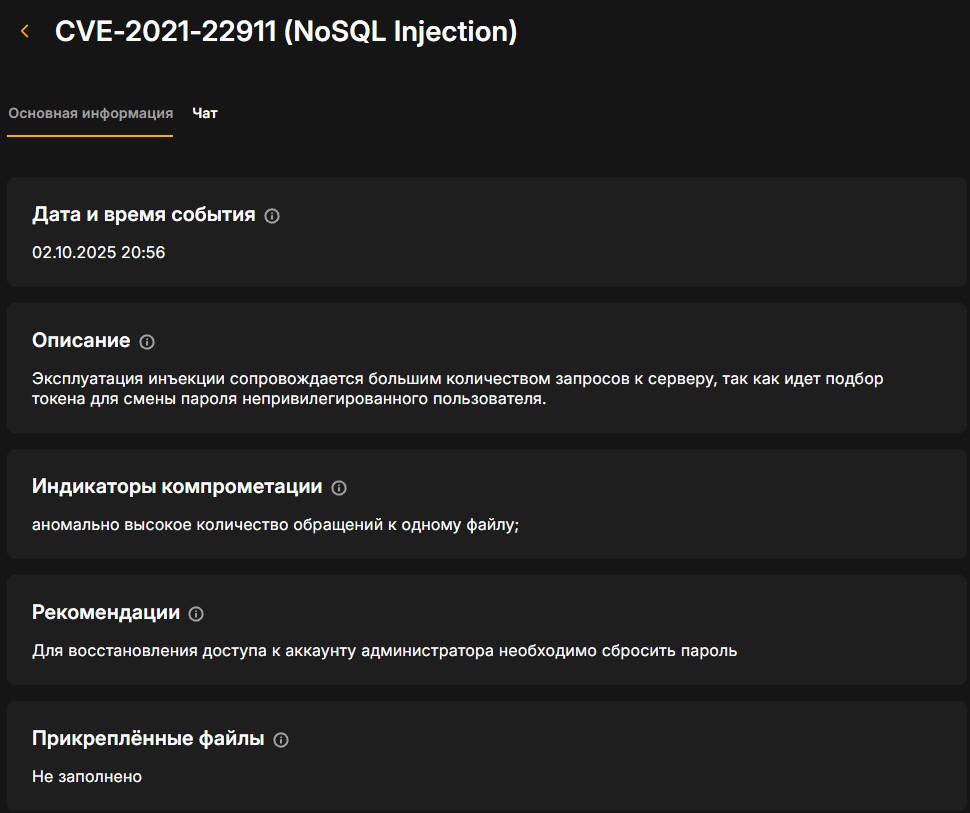
Заполненные инциденты (рис. 21 - 26):



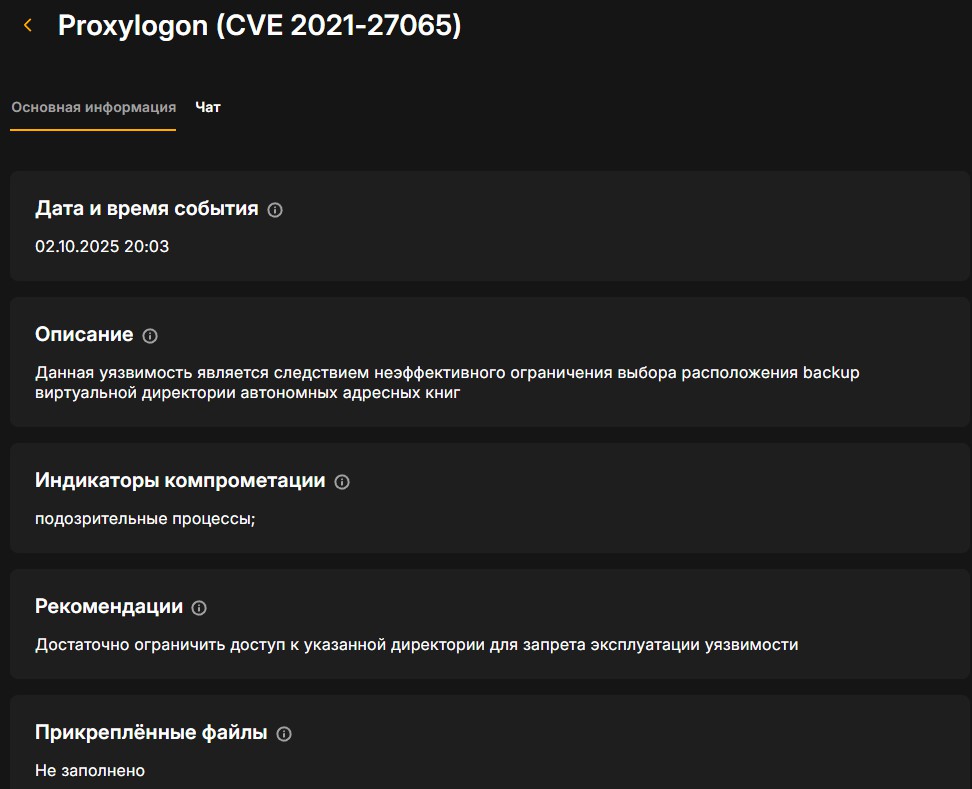
(рис. 21)



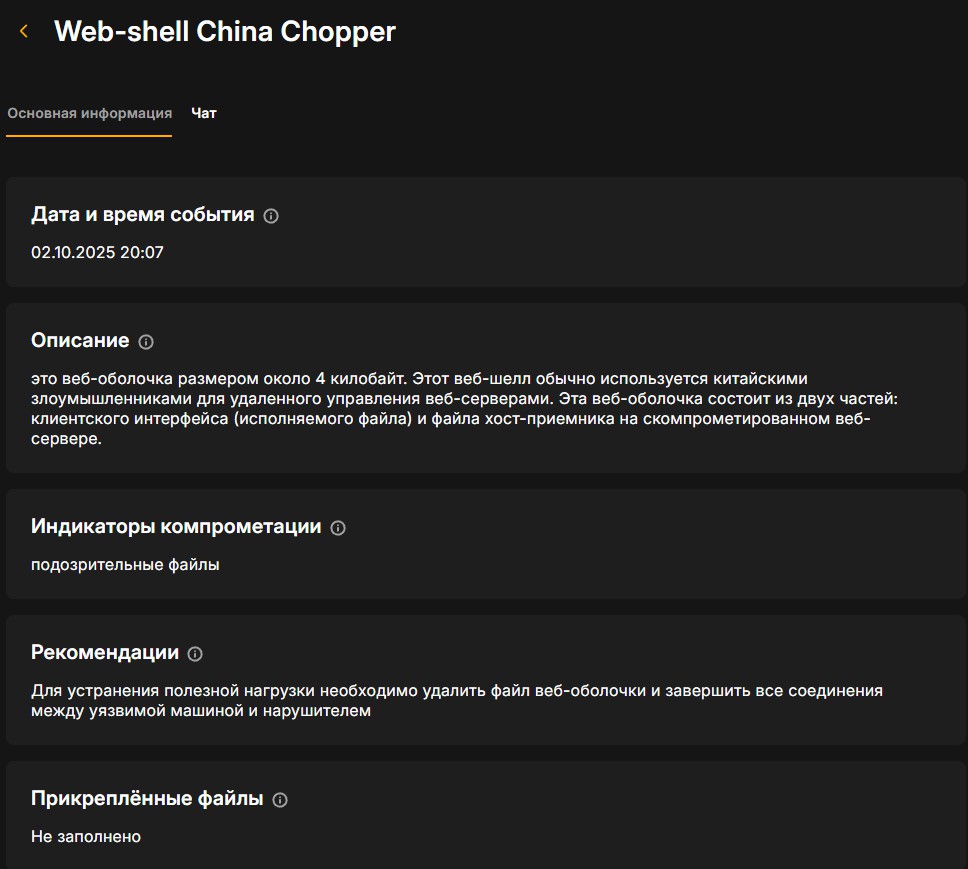
(рис. 22)



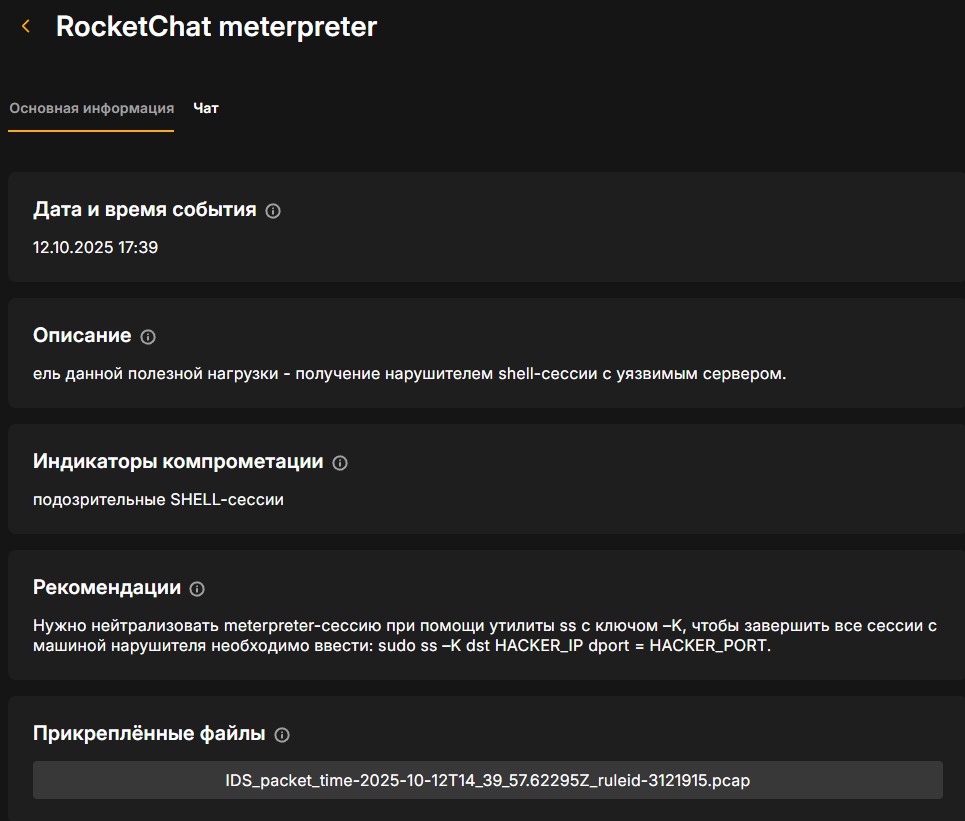
(рис. 23)



(рис. 24)



(рис. 25)



(рис. 26)

# Вывод

В ходе выполнения данной лабораторной работы был изучен сценарий атаки на систему защиты

научно‑технической информации предприятия и способы её нейтрализации. Было рассмотрено, как цепочка уязвимостей может привести к компрометации данных, и какие меры позволяют устранить последствия.

Список литературы