Лабораторная работа №3

Защита корпоративного мессенджера

Панченко Д.Д. 1132229056

Савурская П.А. 1132222827

Кочарян Н.Р. 1132221541

Чистякова Д.В. 1132220820

Содержание

# 1 Цель работы

Защитить корпортивный мессенджер от атаки. Найти и устранить уязвимости и последствия от них.

# 2 Выполнение лабораторной работы

## 2.1 Уязвимость WordPress wpDiscuz и последствие WordPress Deface

### 2.1.1 Обнаружение уязвимости WordPress wpDiscuz

Детектируем эксплуатацию уязвимости CVE-2020-24186 с помощью сетевого сенсора ViPNet IDS NS (рис. 1, рис. 2).

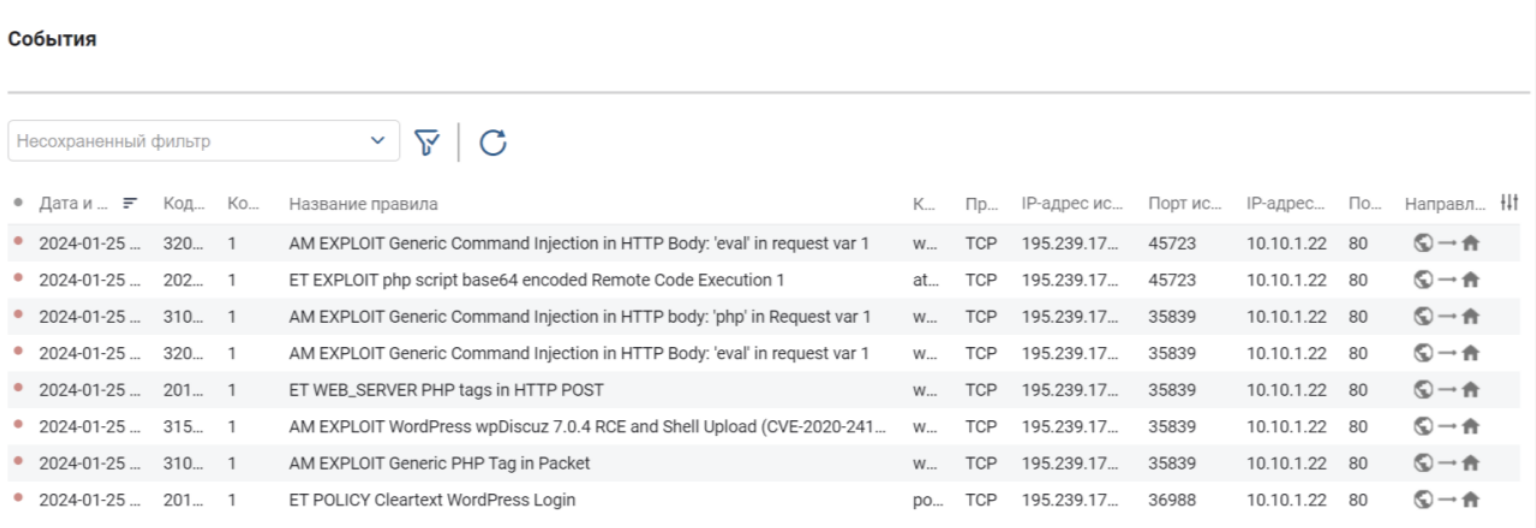


Рис. 1: Журнал событий сетевого сенсора ViPNet IDS NS

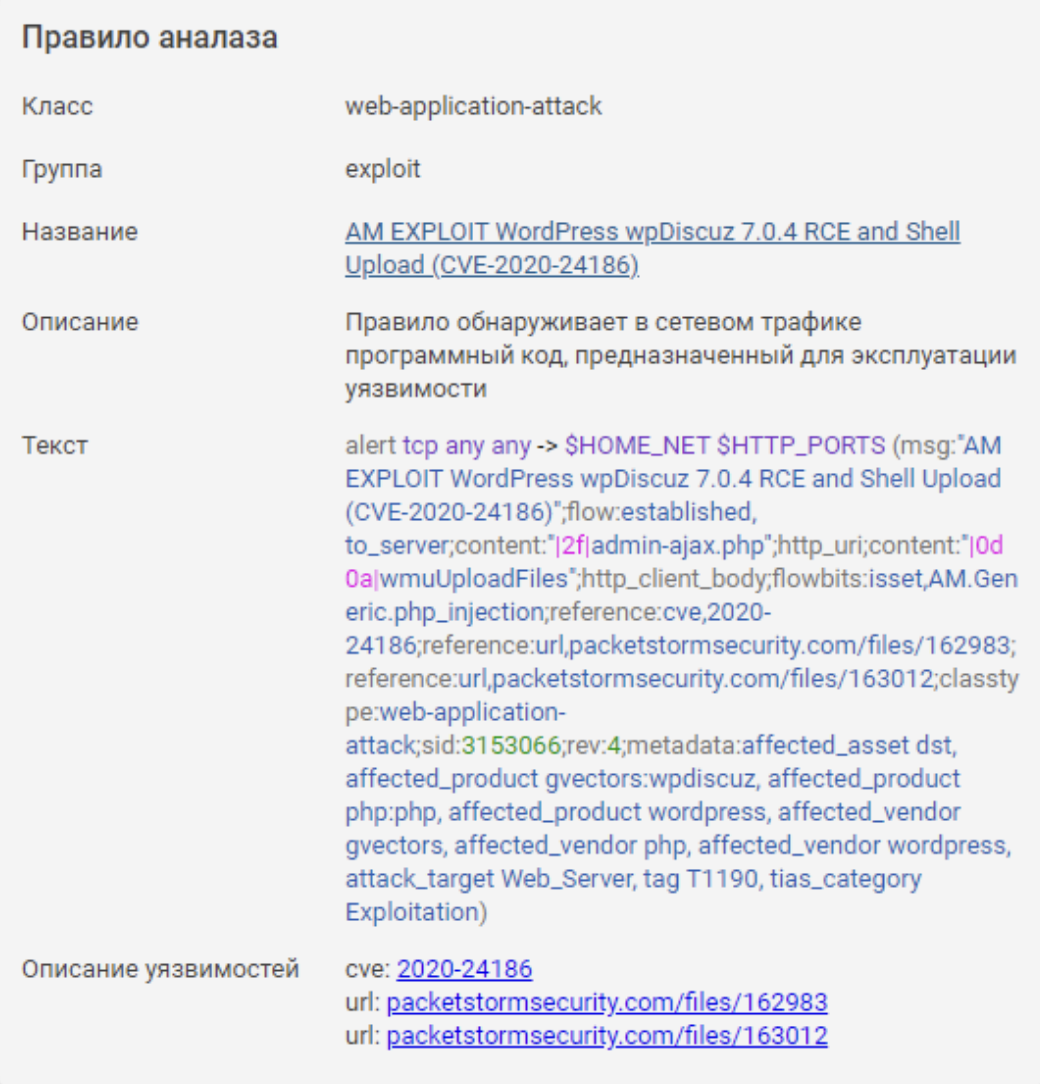


Рис. 2: Карточка события ИБ

С помощью «WP Activity Log» проверяем журнал и обнаруживаем авторизацию внешнего пользователя и загрузку файла (рис. 3).

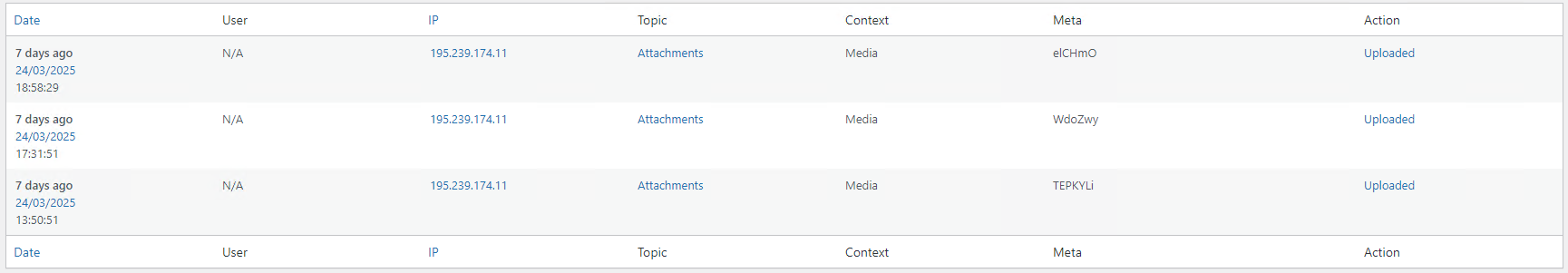


Рис. 3: Окно пользовательской активности в WordPress

### 2.1.2 Устранение уязвимости WordPress wpDiscuz

Закрытие уязвимости можно осуществить с помощью отключения плагина WpDiscuz. Для отключения плагина в панели инструментов заходим в раздел «Plugins» и далее отключаем нужный плагин (рис. 4).

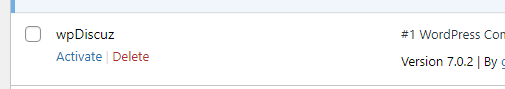


Рис. 4: Отключение плагина в панели управления в WordPress

Данная нагрузка заключается в том, что нарушитель устанавливает shell сессию с уязвимой машиной. Для обнаружения meterpreter-сессии проверим сокеты уязвимой машины на подключение с помощью утилиты ss (рис. 5).

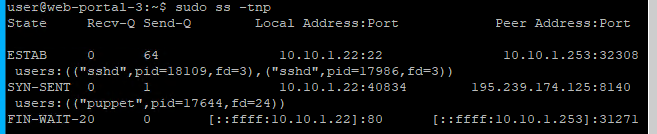


Рис. 5: Отображение информации о TCP-соединениях

Для закрытия вредоносного сокета завершим процесс с помощью команды kill (рис. 6).

Рис. 6: Процесс закрытия meterpreter-сессии

Рис. 6: Процесс закрытия meterpreter-сессии

Уязвимость WordPress wpDiscuz устранена (рис. 7).

Рис. 7: Устранение уязвимости WordPress wpDiscuz

Рис. 7: Устранение уязвимости WordPress wpDiscuz

### 2.1.3 Устранение последствия WordPress Deface

Данная нагрузка подразумевает изменение внешнего вида сайта путем изменения главной страницы сайта на картинку «hacked» (рис. 8).

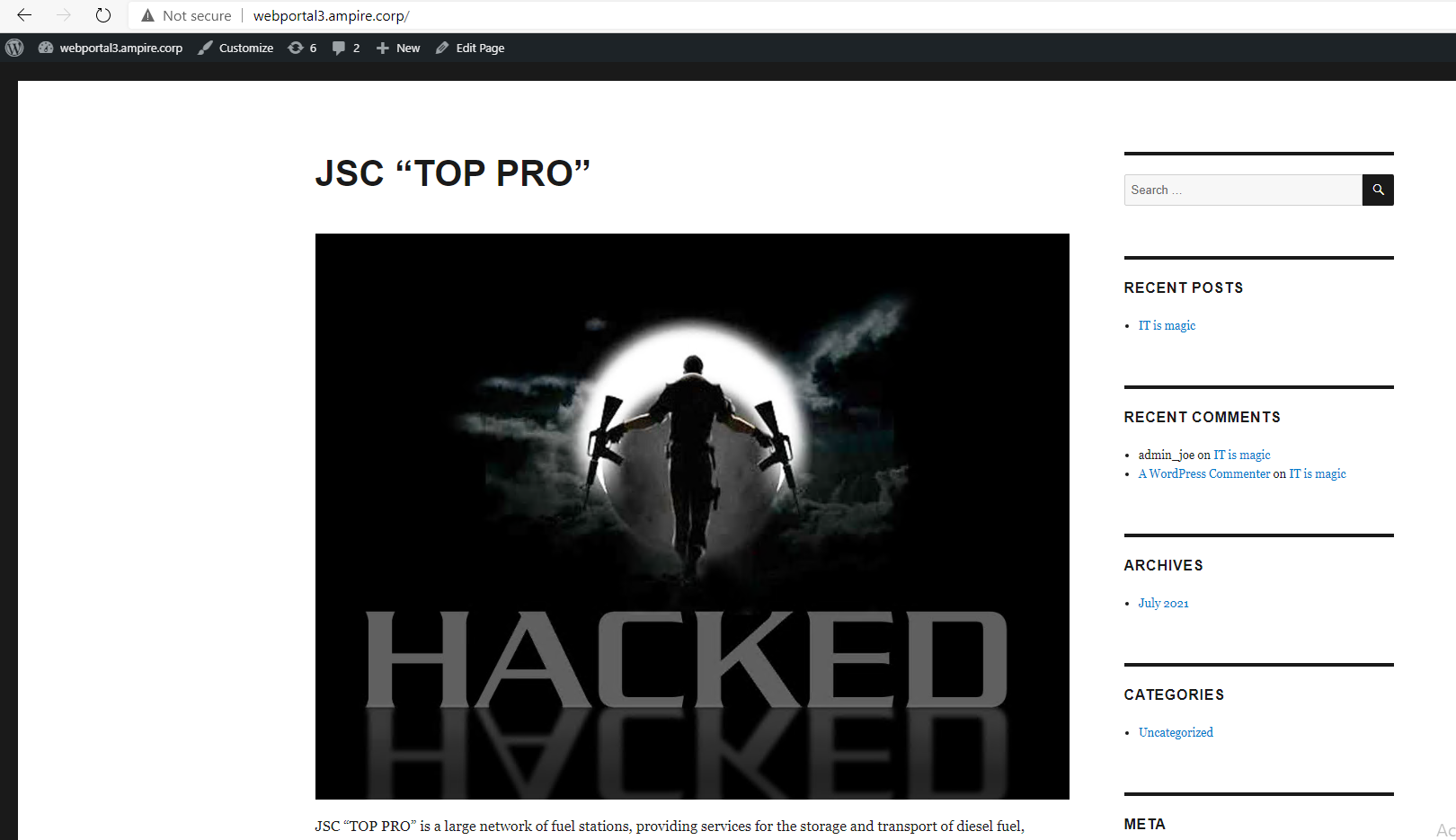


Рис. 8: Страничка сайта

Для нейтрализации данной нагрузки сформируем backup с помощью плагина Updraft Backup/Restore (рис. 9).

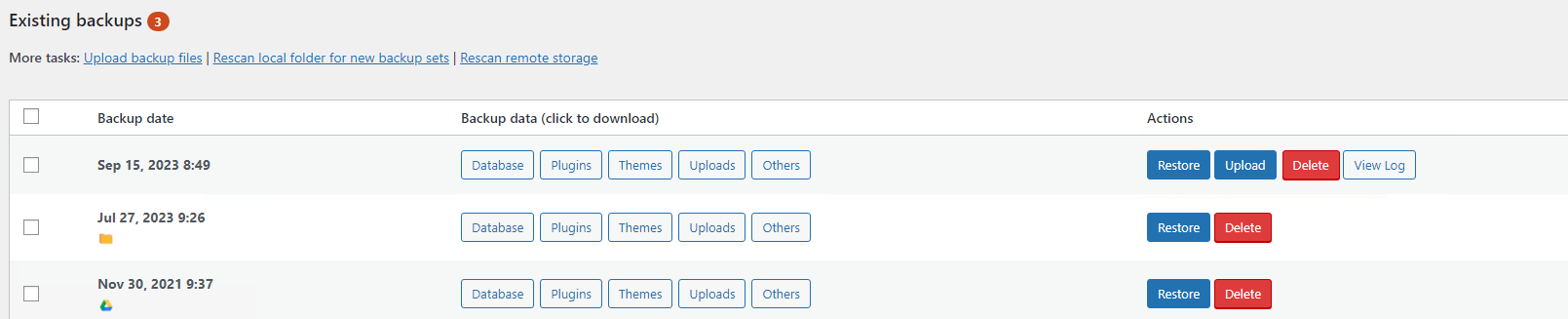


Рис. 9: Существующие резервные копии UpdraftPlus

Выберем самую последнию резервную копию и проведем восстановление (рис. 10).

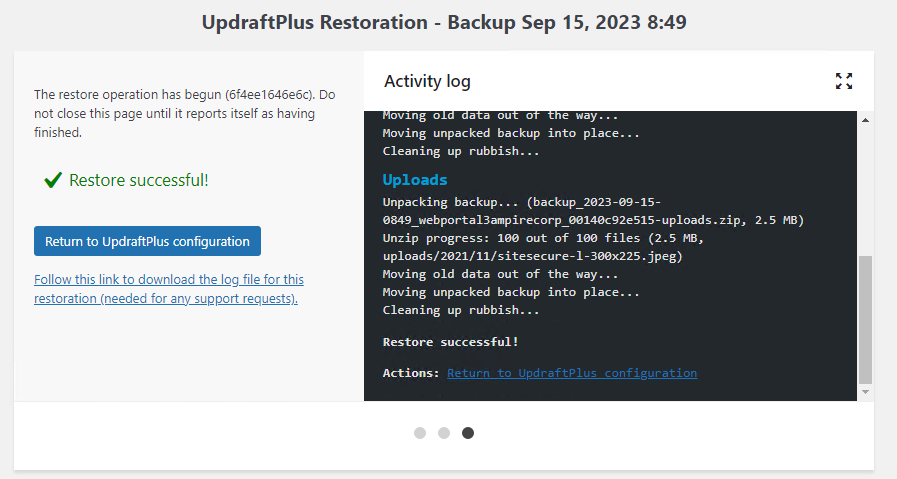


Рис. 10: Успешное выполнение восстановления

Последствие «Deface» веб-интерфейса успешно устранено (рис. 11).

Рис. 11: Устранение последствия WordPress Deface

Рис. 11: Устранение последствия WordPress Deface

## 2.2 Уязвимость RocketChat RCE и последствие RocketChat meterpreter

### 2.2.1 Обнаружение уязвимости RocketChat RCE

Детектируем скачивание вредоносного файла в формате «.elf» для установки TCP-соединения (рис. 12).

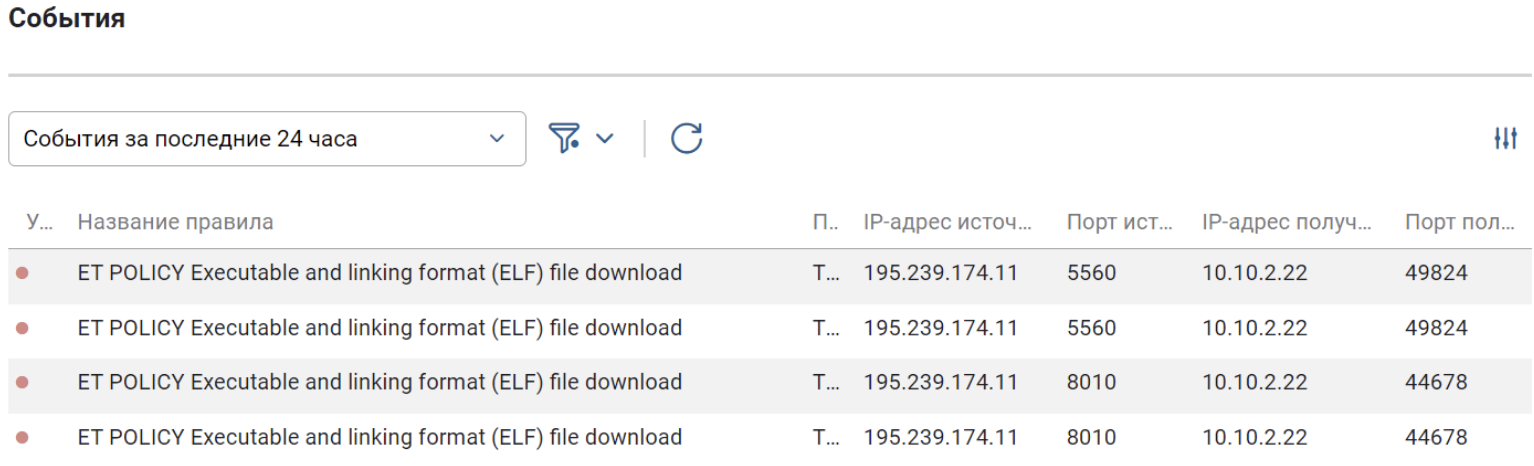


Рис. 12: События ИБ в сетевом сенсоре ViPNet IDS NS

После восстановления пароля администратора (см. следующий пункт) в веб-интерфейсе RocketChat можем увидеть добавленные сценарии (рис. 13, рис. 14).

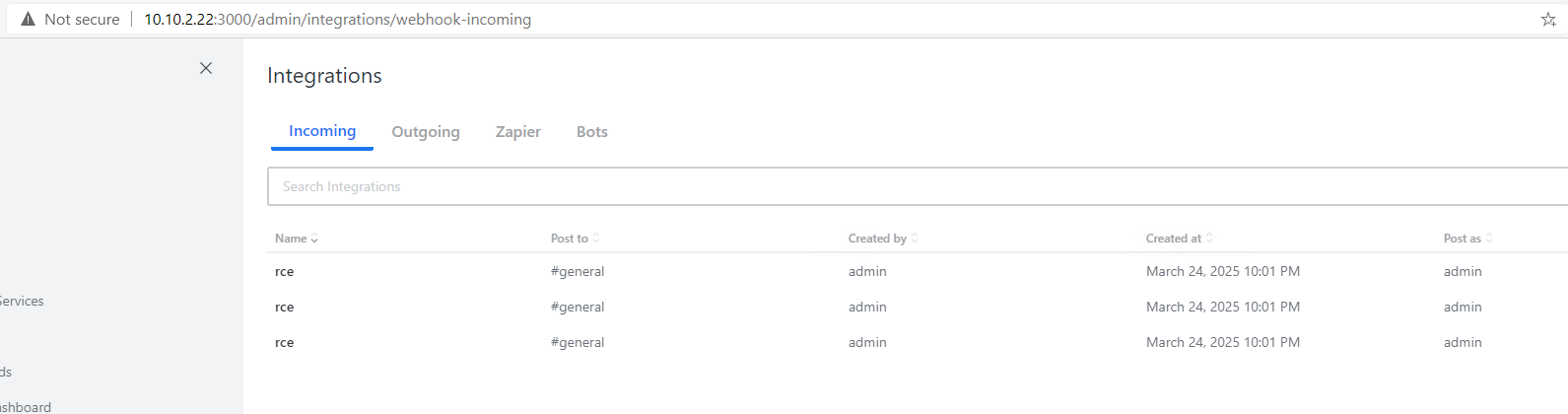


Рис. 13: Выполнение сценариев

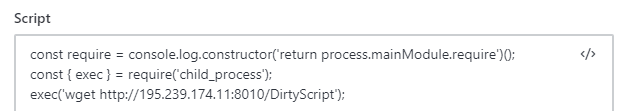


Рис. 14: Сценарий

### 2.2.2 Устранение уязвимости RocketChat RCE

Для восстановления доступа к аккаунту администратора сбросим пароль. Письмо с инструкциями для сброса пароля читаем в файле /var/mail/admin (рис. 15, рис. 16)

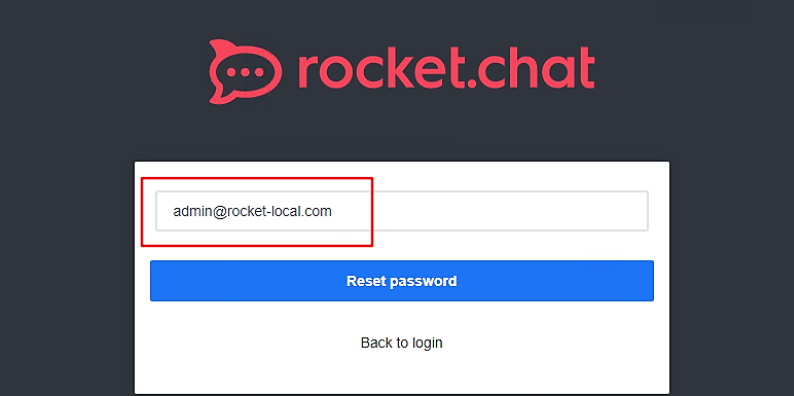


Рис. 15: Восстановление пароля

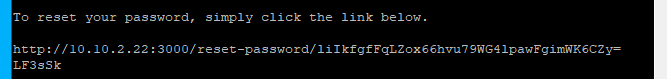


Рис. 16: Ссылка для сброса пароля

Переходим по ссылке и вводим новый пароль. Также для учетной записи администратора настроена двухфакторная аутентификация, воспользуемся кодами восстановления, которые записаны в файле /home/user/backup\_codes (рис. 17, рис. 18).

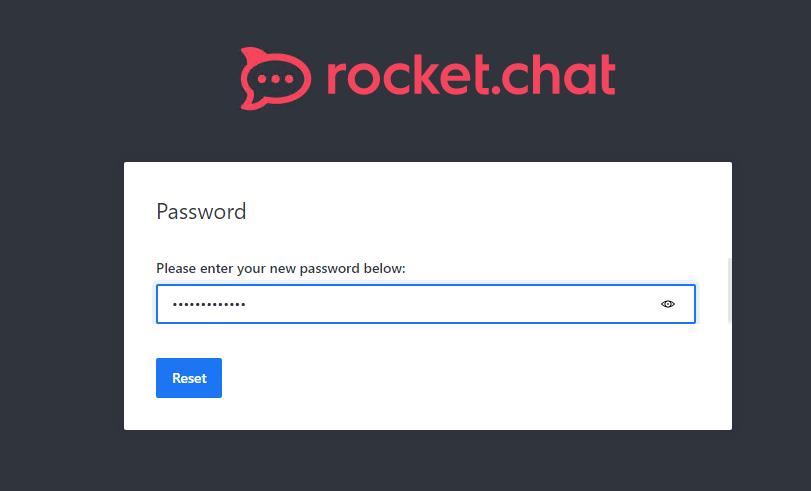


Рис. 17: Восстановление пароля

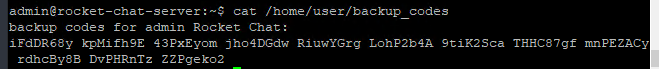


Рис. 18: Коды восстановления

Включим обязательный второй фактор для всех пользователей. Зайдем в «Администрирование», выберем роль и активируем параметр «Пользователи должны использовать двухфакторную аутентификацию» (рис. 19).

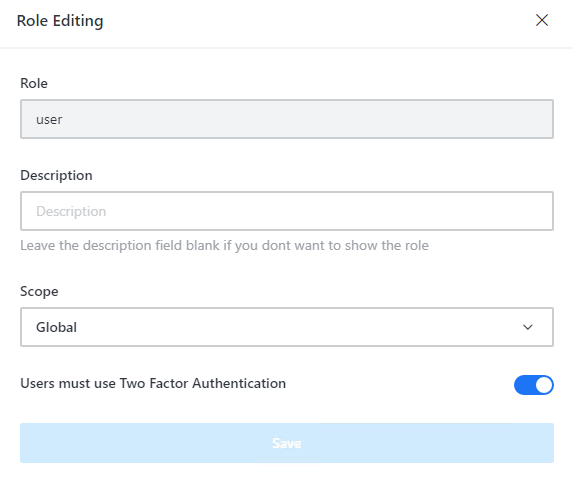


Рис. 19: Настройка обязательной двухфакторной аутентификации

Настроим автоматическое подтверждение почты во вкладке «Администрирование» (рис. 20).

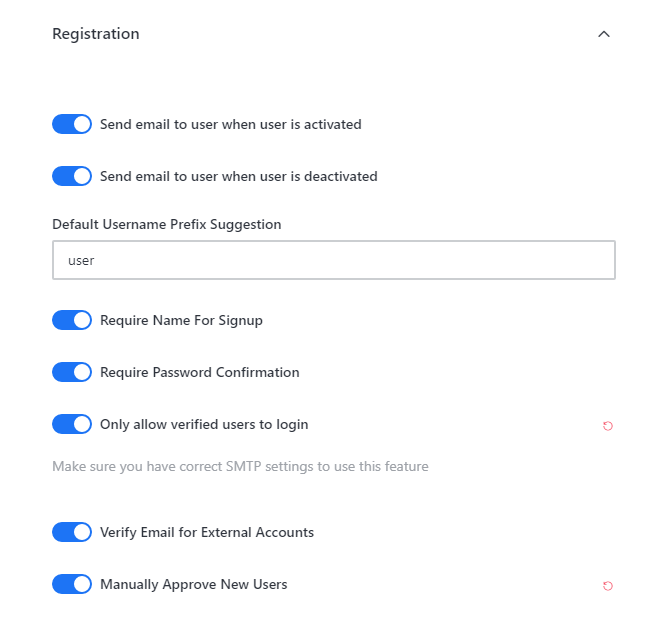


Рис. 20: Настройка регистрации новых пользователей

Настроим автоматическую двухфакторную аутентификацию по электронной почте для новых пользователей во вкладке «Администрирование» (рис. 21).

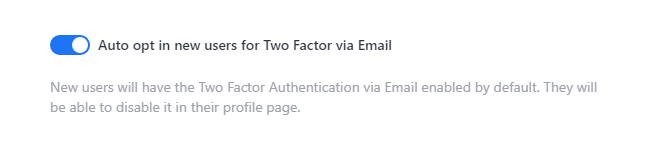


Рис. 21: Настройка автоматической двухфакторной аутентификации

Вторая NoSQL инъекция для повышения привилегий использует высокоуровневый оператор БД $where, то отключим выполнения JavaScript на стороне сервера базы данных. Для этого отредактируем файл конфигурации БД /etc/mongod.conf (рис. 22).

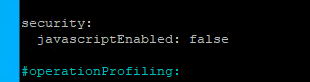


Рис. 22: Настройка конфигурации БД

Для применения настроек перезапустим службу (рис. 23).

Рис. 23: Перезапуск службы

Рис. 23: Перезапуск службы

Уязвимость RocketChat RCE устранена (рис. 24).

Рис. 24: Устранение уязвимости RocketChat RCE

Рис. 24: Устранение уязвимости RocketChat RCE

### 2.2.3 Устранение последствия RocketChat meterpreter

Для устранения meterpreter-сессии сначала выполним команду ss -tp для обнаружения активных соединений, а после командой sudo kill завершим процесс, устанавливающий соединение с хостом злоумышленника (рис. 25, рис. 26).

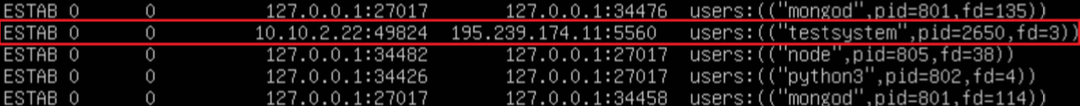


Рис. 25: Сокет с узлом нарушителя

Рис. 26: Завершение процесса

Рис. 26: Завершение процесса

Последствие RocketChat meterpreter успешно устранено (рис. 27).

Рис. 27: Устранение последствия RocketChat meterpreter

Рис. 27: Устранение последствия RocketChat meterpreter

## 2.3 Уязвимость Proxylogon и последствие Exchange China Chopper

### 2.3.1 Обнаружение уязвимости Proxylogon

С помощью ViPNet IDS NS обнаруживаем несколько событий, которые связаны с эксплуатацией уязвимости Proxylogon (рис. 28).

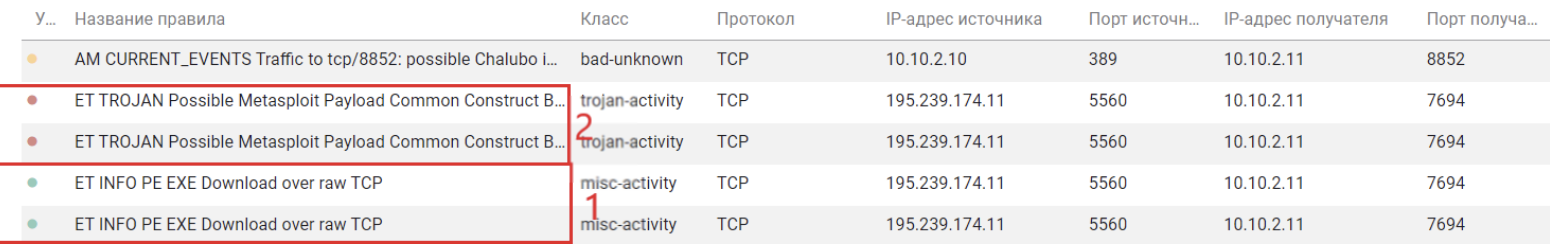


Рис. 28: Список событий, направленных на уязвимый сервер

### 2.3.2 Устранение уязвимости Proxylogon

Во время эксплуатации уязвимости Proxylogon нарушитель совершает GET и POST запросы к /ecp. Ограничим доступ к директории, чтобы уязвимость не эксплуатировалась, с помощью Internet Information Services Manager (рис. 29, рис. 30).

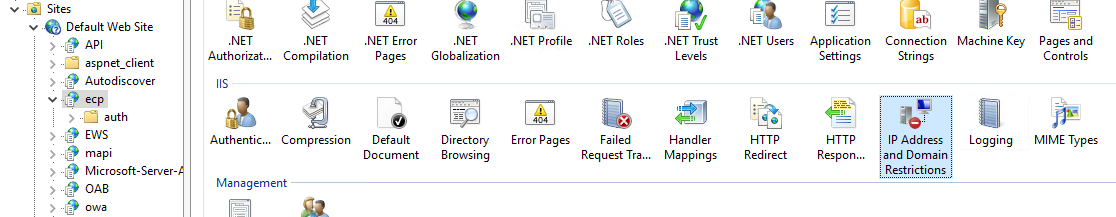


Рис. 29: Окно IIS

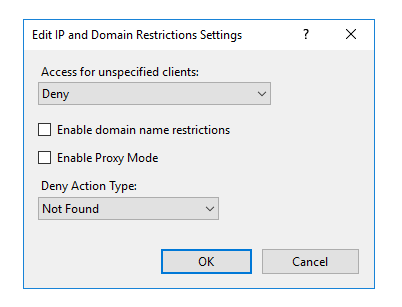


Рис. 30: IP Address and Domain Restrictions

Также обнаруживаем meterpreter-сессию нарушителя с уязвимым сервером при помощи утилиты netstat с ключами -b и -o (рис. 31).

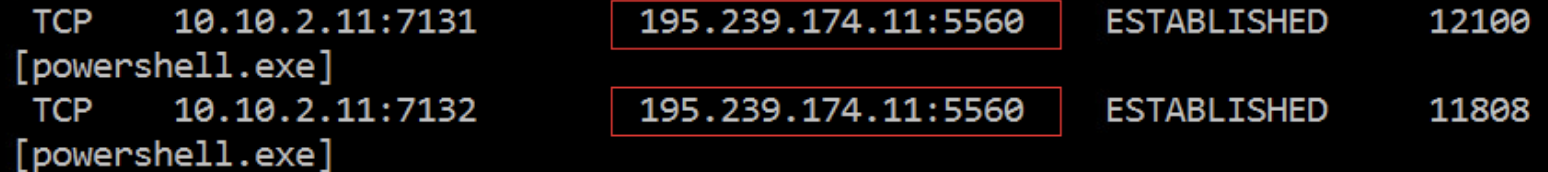


Рис. 31: Сокет с узлом нарушителя

Завершим meterpreter-сессию нарушителя с уязвимым сервером (рис. 32, рис. 33).

Рис. 32: Завершение процесса

Рис. 32: Завершение процесса

Рис. 33: Завершение процесса

Рис. 33: Завершение процесса

Уязвимость Proxylogon устранена (рис. 34).

Рис. 34: Устранение уязвимости Proxylogon

Рис. 34: Устранение уязвимости Proxylogon

### 2.3.3 Устранение последствия Exchange China Chopper

Backdoor China Chopper установлен в самую очевидную для таких атак директорию. Находим его в С:\ProgramFiles\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\AM\_backdoor.aspx (рис. 35).

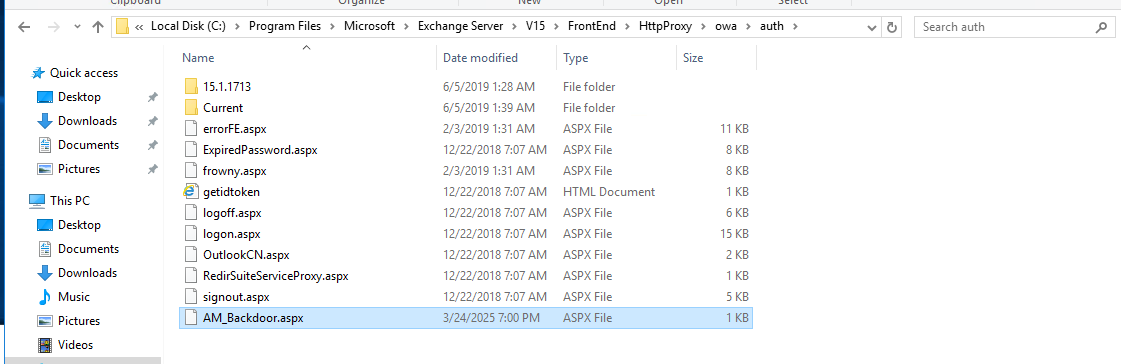


Рис. 35: Backdoor China Chopper

Для устранения нагрузки Backdoor China Chopper удаляем файл веб-оболочки и завершаем meterpreter-сессию, что уже было сделано в предыдущем пункте (рис. 36).

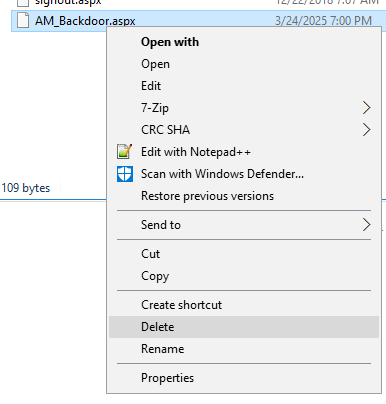


Рис. 36: Backdoor China Chopper

Последствие Exchange China Chopper успешно устранено (рис. 37).

Рис. 37: Устранение последствия Exchange China Chopper

Рис. 37: Устранение последствия Exchange China Chopper

# 3 Вывод

В результате выполнения работы мы успешно устранили три уязвимости и три последствия (рис. 38):  
1) Уязвимость WordPress wpDiscuz и последствие WordPress Deface;  
2) Уязвимость RocketChat RCE и последствие RocketChat meterpreter;  
3) Уязвимость Proxylogon и последствие Exchange China Chopper.

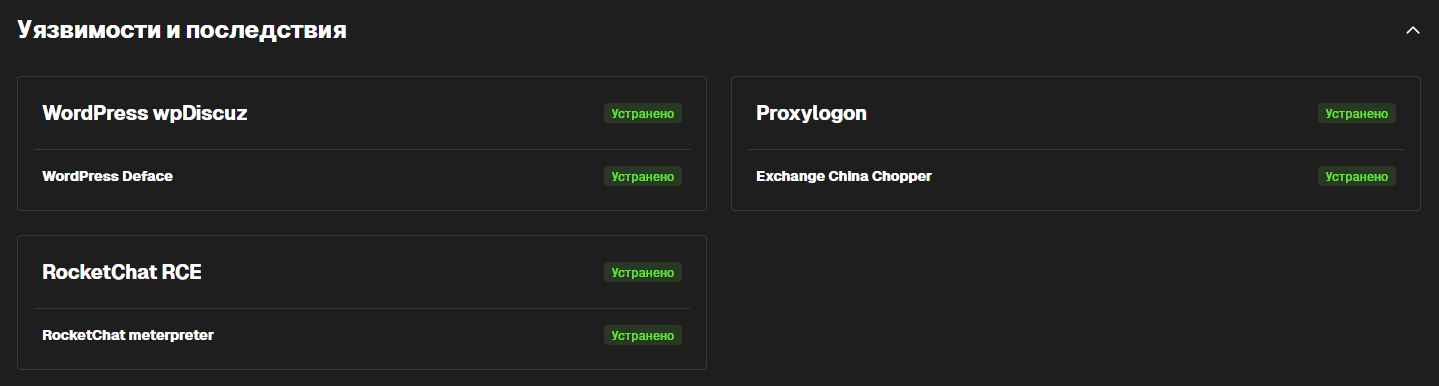


Рис. 38: Успешное устранение уязвимостей и последствий