

# **Отчёт по лабораторной работе 1-D**

**Кибербезопасность предприятия. 1-D**

Лобанова Полина Иннокентьевна, Лушин Артём Андреевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Легенда</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Вывод</b>	<b>19</b>

# Список иллюстраций

3.1	Начало атаки . . . . .	6
3.2	Просмотр журнала . . . . .	6
3.3	Подозрительное событие . . . . .	7
3.4	Проверка по CVE . . . . .	7
3.5	Схема атаки . . . . .	7
3.6	Создание первого инцидента . . . . .	8
3.7	Подключение к устройству . . . . .	8
3.8	Отключение плагина . . . . .	9
3.9	Изменения на сайте компании . . . . .	9
3.10	Выбор компонентов . . . . .	10
3.11	Успешное выполнение установления . . . . .	10
3.12	Процесс закрытия соединения . . . . .	11
3.13	Проверка первого события . . . . .	11
3.14	Второе событие . . . . .	12
3.15	Второй инцидент . . . . .	12
3.16	Ограничение к директории . . . . .	13
3.17	Закрытие соединения . . . . .	13
3.18	Удаление файла . . . . .	14
3.19	Устранение Proxylogon . . . . .	14
3.20	Проверка журнала . . . . .	14
3.21	Третий инцидент . . . . .	15
3.22	Вход на сайт через администратора . . . . .	16
3.23	Двухфакторная аутентификация . . . . .	16
3.24	Настройки регистрации новых пользователей . . . . .	17
3.25	Отключение javascriptEnabled . . . . .	17
3.26	Завершение всех сессий атакующего . . . . .	18
3.27	Устранение всех последствий . . . . .	18

# **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.

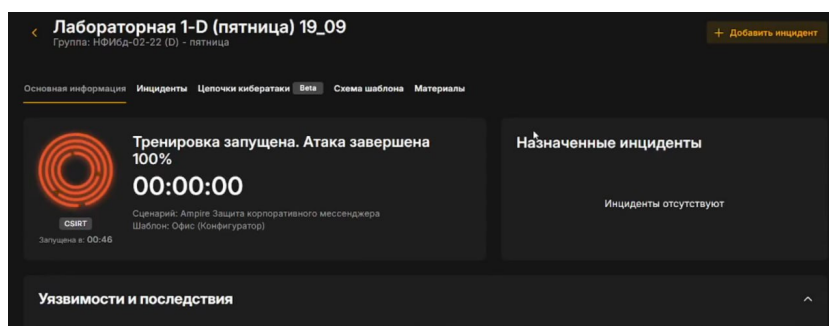


Рис. 3.1: Начало атаки

- 2) Посмотрели журнал событий с интервалом 15 минут.

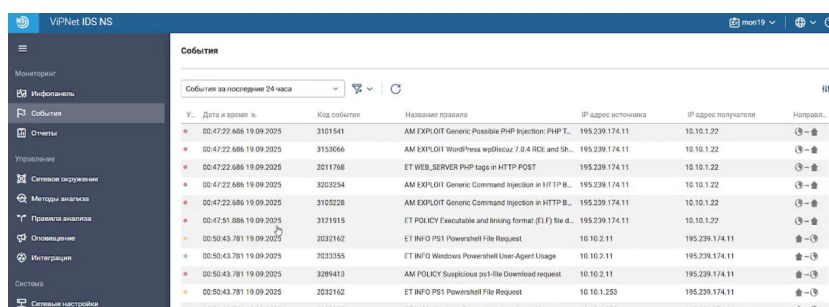


Рис. 3.2: Просмотр журнала

- 3) Увидели подозрительное событие. Согласно нему правило обнаружило в

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

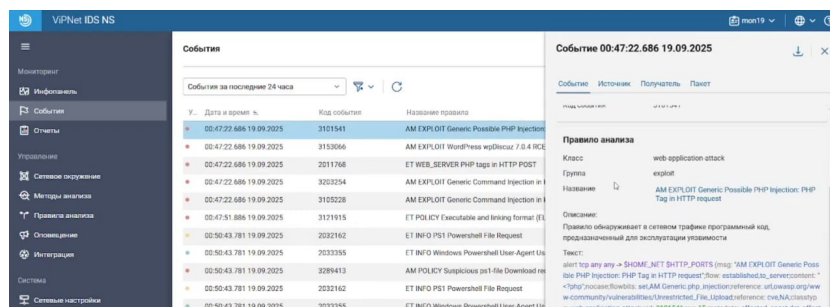


Рис. 3.3: Подозрительное событие

4) Проверил проверку события по CVE.

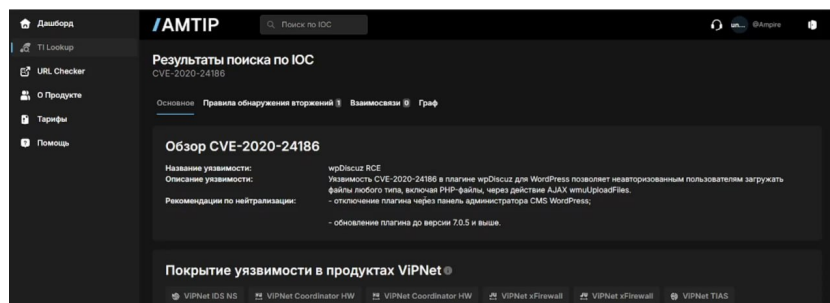


Рис. 3.4: Проерка по CVE

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

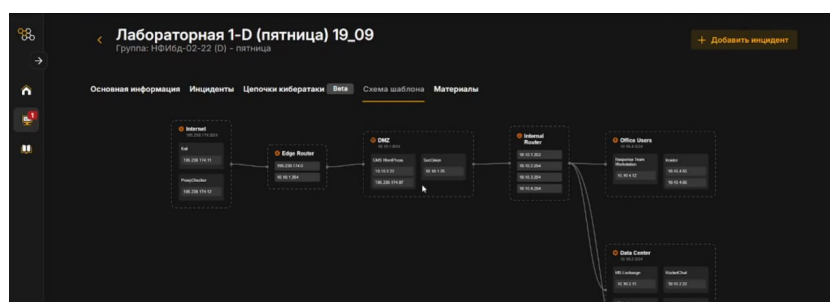


Рис. 3.5: Схема атаки

- 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.

**Добавление инцидента**

Название ⓘ  
Обнаружение в сети программного кода для экспл

Дата и время события ⓘ  
19.09.2025 00:47

Источник ⓘ  
195.239.174.11 (Kali) x

Поражённые активы ⓘ  
10.10.1.22 (CMS WordPress) x

Описание ⓘ  
В сетевом трафике обнаружен программный код, предназначенный для эксплуатации уязвимости. Уязвимость позволяет неавторизованным пользователям загружать файлы любого типа.

Рекомендации ⓘ  
отключение плагина через панель администратора CMS WordPress и обновление плагина до версии 7.0.5 и выше.

Индикаторы компрометации ⓘ  
Подозрительный процесс

Прикрепить файл ⓘ

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.

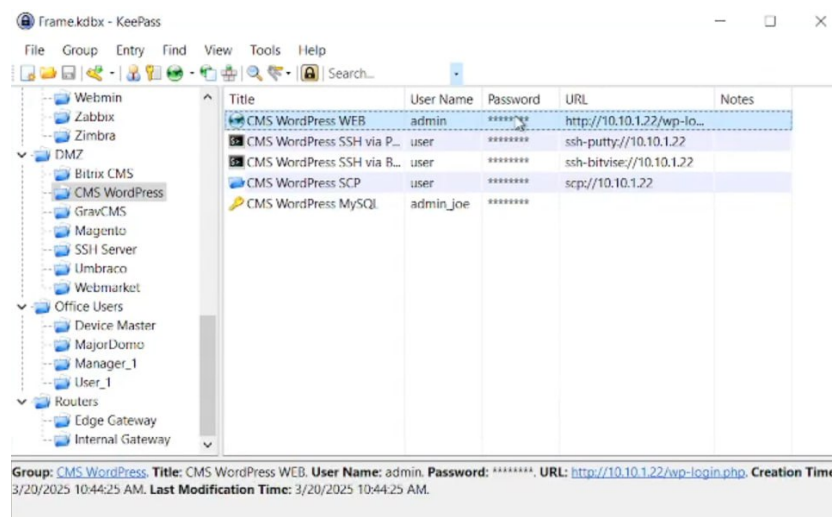


Рис. 3.7: Подключение к устройству



- 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.

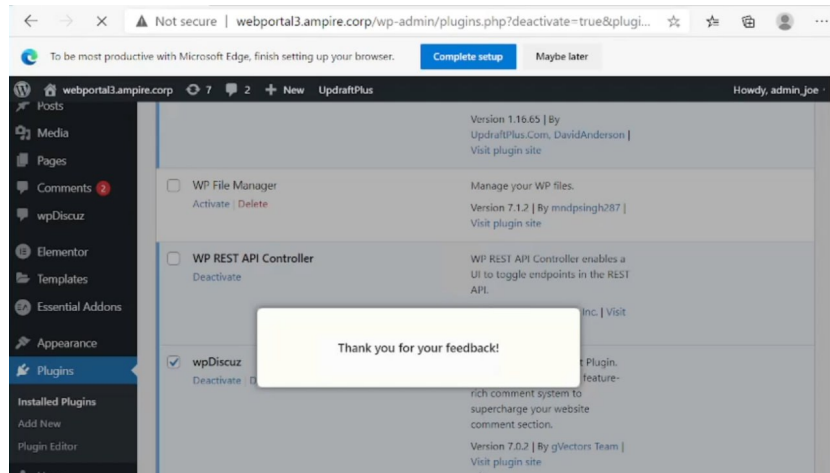


Рис. 3.8: Отключение плагина

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

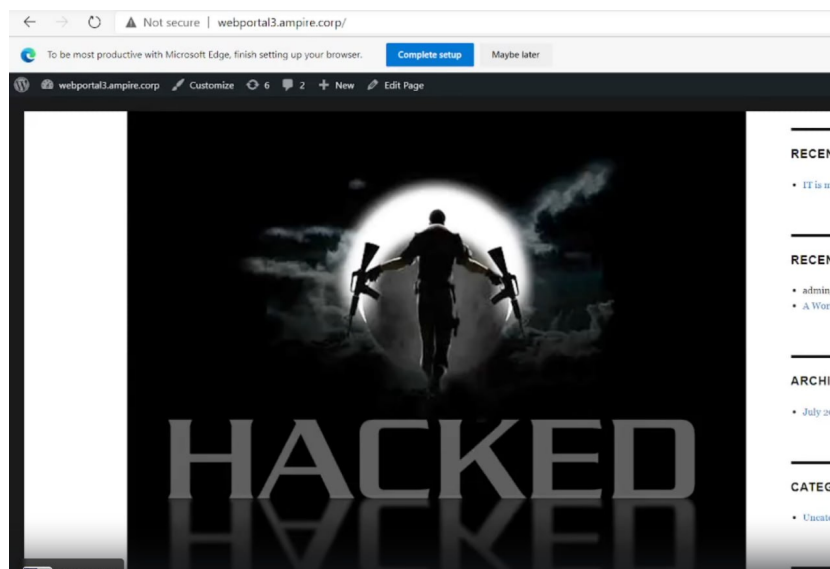


Рис. 3.9: Изменения на сайте компании

- 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.

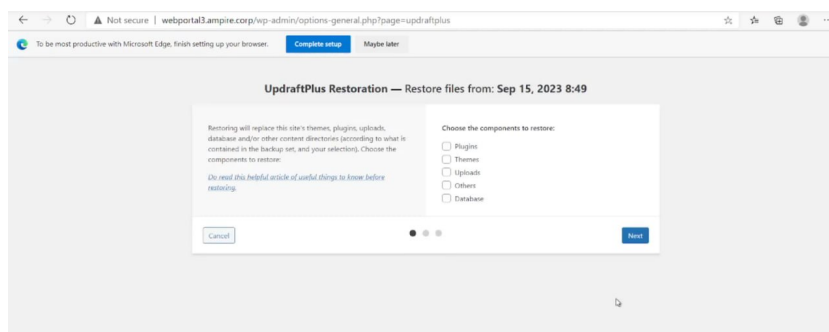


Рис. 3.10: Выбор компонентов

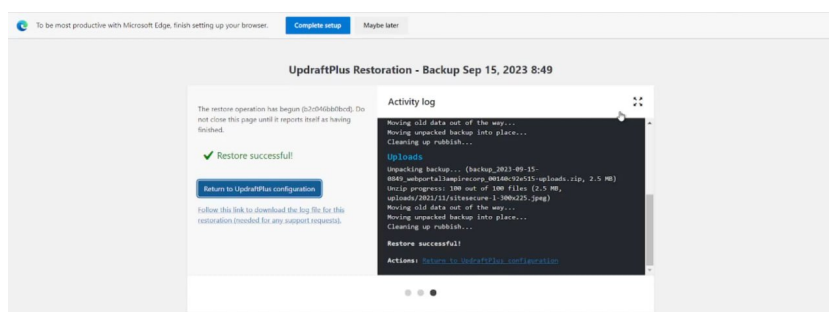


Рис. 3.11: Успешное выполнение установления

- 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.

```

CLOSE-WAIT 0 0 10.10.1.22:37966 195.239.174.11:5557
users:(("chisel.sh",pid=2055,fd=12),("sh",pid=2054,fd=12),("UIGEW",pid=2019,fd=12))
ESTAB 0 0 10.10.1.22:51488 195.239.174.11:5556
users:(("chisel.sh",pid=2055,fd=3),("sh",pid=2054,fd=3),("UIGEW",pid=2019,fd=3))
SYN-SENT 0 1 10.10.1.22:37734 195.239.174.125:8140
users:(("puppet",pid=29584,fd=6))
FIN-WAIT-2 0 0 10.10.1.22:50066 10.10.2.11:443
users:(("chisel.sh",pid=2055,fd=16))
ESTAB 0 0 10.10.1.22:45918 195.239.174.11:1085
users:(("chisel.sh",pid=2055,fd=11))
ESTAB 0 0 10.10.1.22:22 10.10.1.253:42209
users:(("sshd",pid=29984,fd=3),("sshd",pid=29780,fd=3))
FIN-WAIT-2 0 0 [::ffff:10.10.1.22]:80 [::ffff:10.10.1.253]:55912

user@web-portal-3:~$ kill 2055
-bash: kill: (2055) - Operation not permitted
user@web-portal-3:~$ sudo -i
root@web-portal-3:~# kill 2055
root@web-portal-3:~# ss -tnp
State Recv-Q Send-Q Local Address:Port Peer Address:Port
CLOSE-WAIT 0 0 10.10.1.22:37966 195.239.174.11:5557 users:(("UIGEW",p
ESTAB 0 0 10.10.1.22:51488 195.239.174.11:5556 users:(("UIGEW",p
FIN-WAIT-2 0 0 10.10.1.22:50066 10.10.2.11:443
SYN-SENT 0 1 10.10.1.22:38974 195.239.174.125:8140 users:(("puppet",p
ESTAB 0 36 10.10.1.22:22 10.10.1.253:42209 users:(("sshd",pid
FIN-WAIT-2 0 0 [::ffff:10.10.1.22]:80 [::ffff:10.10.1.253]:28186

root@web-portal-3:~# ss -tp4
State Recv-Q Send-Q Local Address:Port Peer Address:Port
CLOSE-WAIT 0 0 10.10.1.22:37966 195.239.174.11:5557
ESTAB 0 0 10.10.1.22:51488 195.239.174.11:freeciv
FIN-WAIT-2 0 0 10.10.1.22:50066 10.10.2.11:https
SYN-SENT 0 1 10.10.1.22:38974 195.239.174.125:puppet
ESTAB 0 36 10.10.1.22:ssh 10.10.1.253:42209

root@web-portal-3:~# kill 2019
root@web-portal-3:~# ss -tp4
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LAST-ACK 1 0 10.10.1.22:37966 195.239.174.11:5557
FIN-WAIT-2 0 0 10.10.1.22:50066 10.10.2.11:https
SYN-SENT 0 1 10.10.1.22:38974 195.239.174.125:puppet
ESTAB 0 36 10.10.1.22:ssh 10.10.1.253:42209

```

Рис. 3.12: Процесс закрытия соединения

12) Проверили, что уязвимость и последствие WordPress устранены.

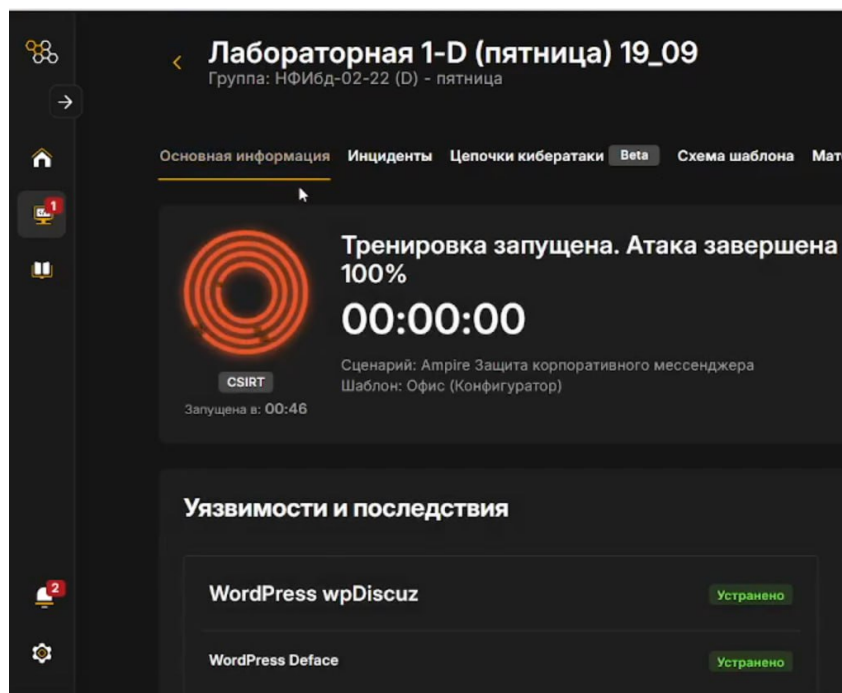


Рис. 3.13: Проверка первого события

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

ТИВНОСТЬ.

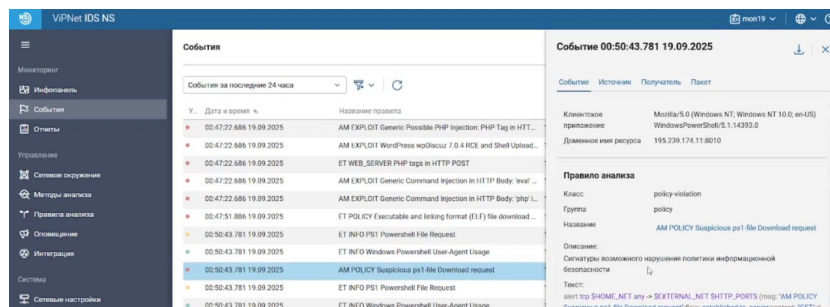


Рис. 3.14: Второе событие

- 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.

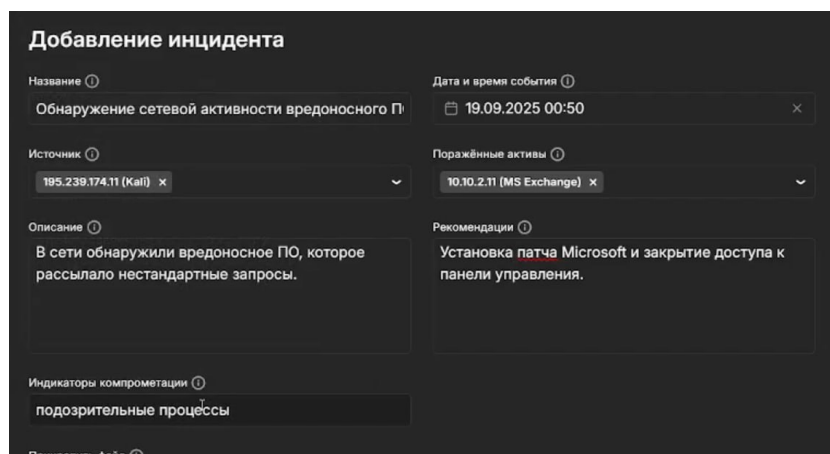


Рис. 3.15: Второй инцидент

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

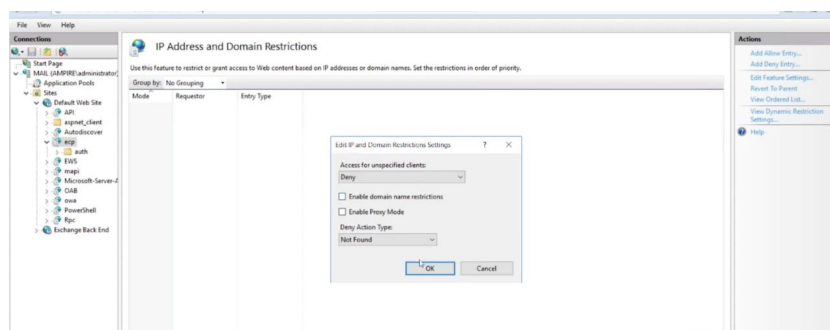


Рис. 3.16: Ограничение к директории

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

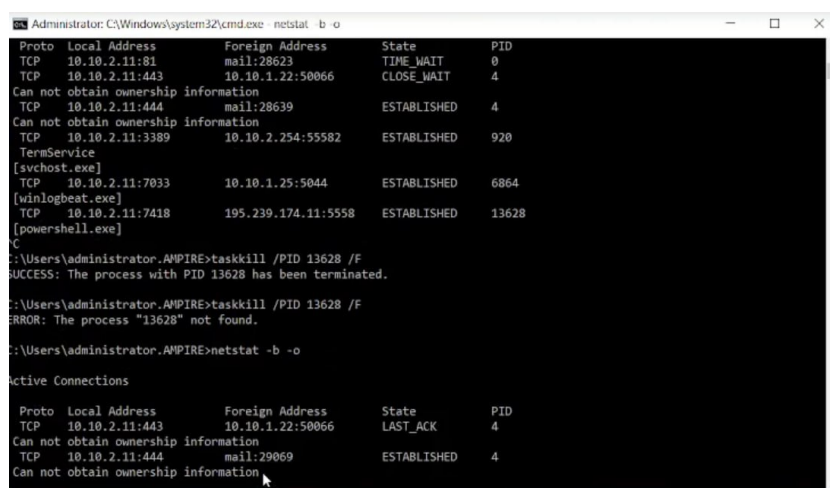


Рис. 3.17: Заккрытие соединения

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

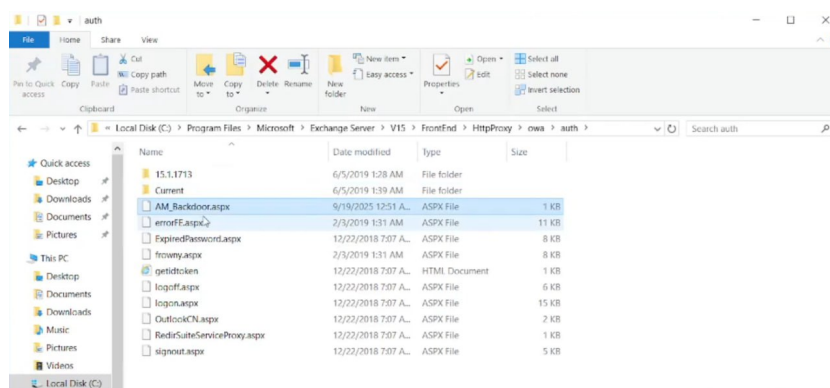


Рис. 3.18: Удаление файла

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

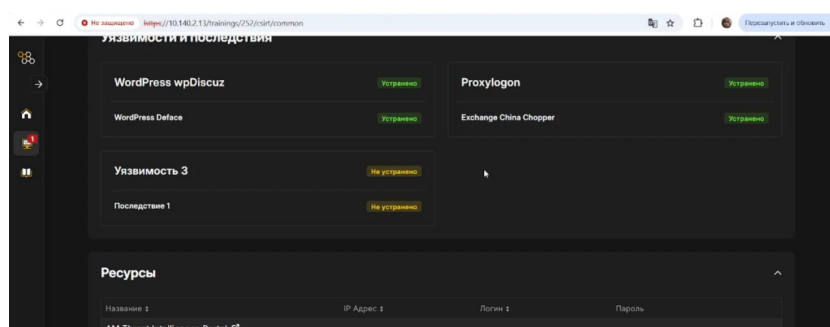


Рис. 3.19: Устранение Proxylogon

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

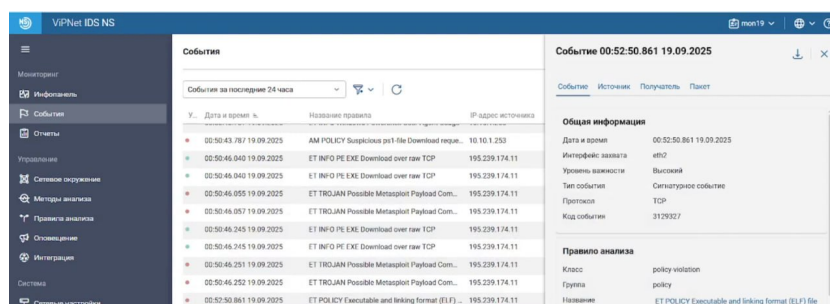


Рис. 3.20: Проверка журнала

- 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.

**Добавление инцидента**

Название ⓘ  
Нарушение политики информационной безопаснос

Дата и время события ⓘ  
19.09.2025 00:52

Источник ⓘ  
195.239.174.11 (Kali) x

Пораженные активы ⓘ  
10.10.2.22 (RocketChat) x

Описание ⓘ  
Нарушение политики информационной безопасности с целью скачивания данных и их использования.

Рекомендации ⓘ  
Обновление версии Rocket.chat или запрет выполнения JavaScript на стороне сервера БД.

Индикаторы компрометации ⓘ  
Ничего не введено

Прикрепить файл ⓘ

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.

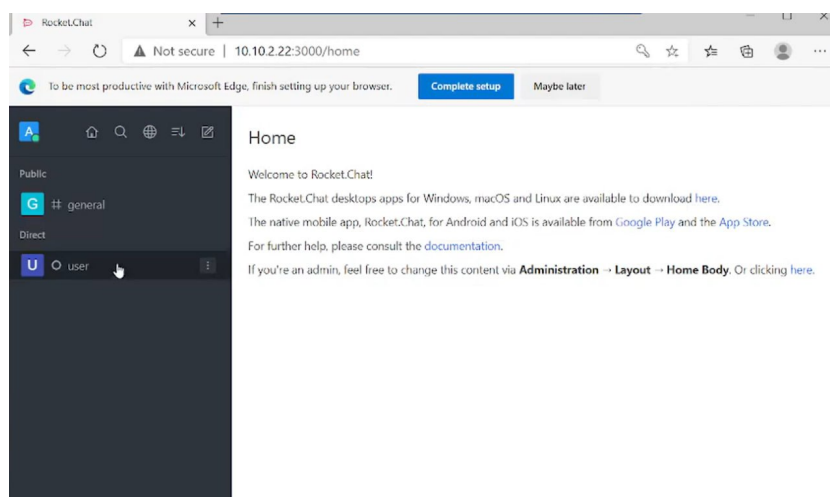


Рис. 3.22: Вход на сайт через администратора

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

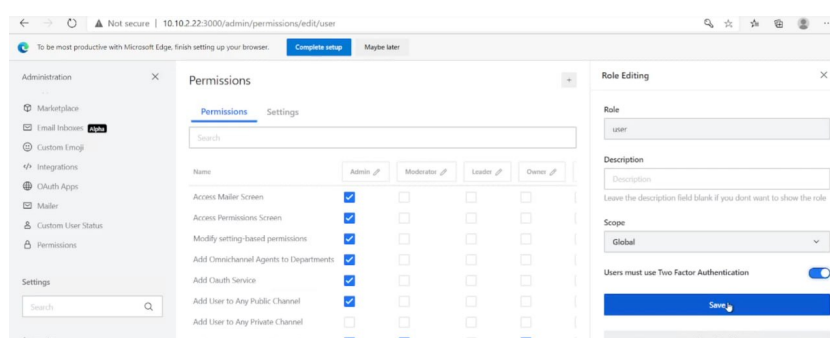


Рис. 3.23: Двухфакторная аутентификация

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



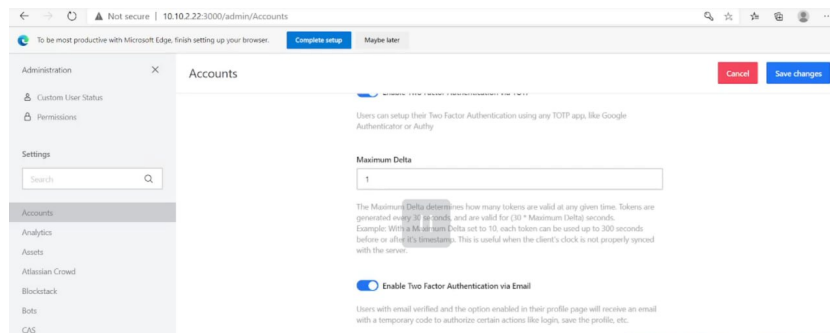


Рис. 3.24: Настройки регистрации новых пользователей

24) Отключили параметр javascriptEnabled и перезапустили службу.

```
admin@10.10.2.22:22 - Bitwise xterm - root@rocket-chat-server: /etc
systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log

# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

# how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo

security:
  javascriptEnabled: false

#operationProfiling:

replication:
  replSetName: rs01

#sharding:

## Enterprise-Only Options:

#auditLog:

#snmp:
root@rocket-chat-server:/etc# $where
root@rocket-chat-server:/etc# mapReduce
mapReduce: command not found
root@rocket-chat-server:/etc# $function
root@rocket-chat-server:/etc# sudo systemctl restart mongod.service
```

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.

```
root@rocket-chat-server:/etc# ss -tp4
State      Recv-Q      Send-Q      Local Address:Port
Process
ESTAB      0            0            10.10.2.22:38842
users:(("testsystem",pid=2042,fd=3))
ESTAB      0            36            10.10.2.22:ssh
users:(("sshd",pid=29578,fd=4),("sshd",pid=29502,fd=4))
ESTAB      0            0            10.10.2.22:ssh
users:(("sshd",pid=29280,fd=4),("sshd",pid=29151,fd=4))
ESTAB      0            0            10.10.2.22:ssh
users:(("sshd",pid=29380,fd=4),("sshd",pid=29302,fd=4))
ESTAB      0            0            10.10.2.22:ssh
users:(("sshd",pid=29481,fd=4),("sshd",pid=29403,fd=4))
ESTAB      0            0            10.10.2.22:3000
users:(("node",pid=688,fd=42))
root@rocket-chat-server:/etc# kill 2042
```

Рис. 3.26: Завершение всех сессий атакующего

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

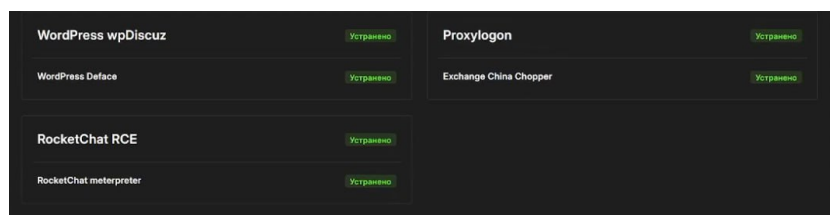


Рис. 3.27: Устранение всех последствий

## 4 Вывод

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