

# **Лабораторная работа № 1-Д**

**Защита корпоративного мессенджера**

Доберштейн А. С., Оразгелдиев Я. О., Барабанова К. А.

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
2.1 Подготовка к выполнению лабораторной работы . . . . .	6
2.2 Уязвимость WordPress-wpDiscuz . . . . .	6
2.3 Уязвимость Proxylogon . . . . .	14
2.4 Уязвимость Rocket.Chat . . . . .	19
2.5 Завершение выполнения лабораторной работы . . . . .	27
<b>3 Выводы</b>	<b>28</b>
<b>Список литературы</b>	<b>29</b>

# Список иллюстраций

2.1	Вектор атаки . . . . .	6
2.2	Вход в ViPNet . . . . .	7
2.3	Журнал событий . . . . .	7
2.4	Обзор уязвимости . . . . .	8
2.5	Подключение к удаленному рабочему столу . . . . .	8
2.6	Вход . . . . .	9
2.7	KeePass . . . . .	10
2.8	Deface . . . . .	10
2.9	Плагин wpDiscuz . . . . .	11
2.10	Плагин UpdraftPlus - Backup/Restore . . . . .	11
2.11	Restore . . . . .	11
2.12	Параметры восстановления . . . . .	11
2.13	Удаление старых директорий . . . . .	12
2.14	Восстановление версии . . . . .	12
2.15	Устранено последствие . . . . .	13
2.16	Проверка процессов . . . . .	13
2.17	Уничтожение вредоносных процессов . . . . .	14
2.18	Успех . . . . .	14
2.19	Журнал событий . . . . .	14
2.20	Обзор уязвимости . . . . .	15
2.21	KeePass . . . . .	15
2.22	inetmgr . . . . .	16
2.23	inetmgr . . . . .	17
2.24	inetmgr . . . . .	18
2.25	Вредоносные процессы . . . . .	18
2.26	Вредоносные процессы . . . . .	18
2.27	Вредоносные процессы . . . . .	19
2.28	Удаление файла .aspx . . . . .	19
2.29	Успех . . . . .	19
2.30	Журнал событий . . . . .	20
2.31	Обзор уязвимости . . . . .	20
2.32	KeePass . . . . .	20
2.33	Сброс пароля . . . . .	21
2.34	Сообщение об отправке email . . . . .	21
2.35	Инструкция по сбросу пароля . . . . .	22
2.36	Сброс пароля . . . . .	22
2.37	Сброс пароля . . . . .	22

2.38 Backup_codes . . . . .	23
2.39 Сброс пароля . . . . .	23
2.40 Вход в учетную запись . . . . .	24
2.41 Права доступа . . . . .	24
2.42 Настройки двухфакторной аутентификации . . . . .	25
2.43 Настройки регистрации . . . . .	25
2.44 Редактирование mongod.conf . . . . .	26
2.45 Restart mongod.service . . . . .	26
2.46 Уничтожение вредоносных соединений . . . . .	26
2.47 Успех . . . . .	26
2.48 Карточки инцидентов . . . . .	27

# **1 Цель работы**

Основной целью работы является получение навыков обнаружения и устранение уязвимостей WordPress-wpDiscuz, Proxylogon, Rocket.Chat и их последствий.

## 2 Выполнение лабораторной работы

### 2.1 Подготовка к выполнению лабораторной работы

Для начала изучили вектор атаки, адреса злоумышленника и атакуемых серверов.(рис. 2.1).



Рис. 2.1: Вектор атаки

### 2.2 Уязвимость WordPress-wpDiscuz

Залогинились в ViPNet для обнаружения уязвимости в журнале событий.(рис. 2.2).



Рис. 2.2: Вход в ViPNet

В “Событиях” обнаружили событие AM Exploit Wordpress с программным кодом, предназначенным для эксплуатации уязвимости(рис. 2.3).

Идентификатор	Код события	Класс	Название правила	Код
16:33:085 29...	203355	1	AM POLICY Suspicious ps...	policy-violation
16:33:085 29...	2032162	1	ET INFO Windows Powershell...	not-suspicious
16:33:084 29...	3289413	1	AM POLICY Suspicious ps...	bad-unknown
16:33:084 29...	203355	1	ET INFO Windows Powershell...	not-suspicious
16:33:084 29...	2032162	1	ET INFO PowerShell Fil...	bad-unknown
14:51:001 29...	3121915	1	ET POLICY Executable and L...	policy-violation
14:23:981 29...	3105228	1	AM EXPLOIT Generic Com...	web-application-attack
14:23:981 29...	3203254	1	AM EXPLOIT Generic Com...	web-application-attack
14:23:981 29...	2011768	1	ET WEB_SERVER PHP tag ...	web-application-attack
14:23:981 29...	3153096	1	AM EXPLOIT WordPress wp...	web-application-attack
14:23:981 29...	3101541	1	AM EXPLOIT Generic Poss...	web-application-attack

Рис. 2.3: Журнал событий

Изучили информацию по CVE-коду об обнаруженной уязвимости, изучили рекомендации понейтрализации. (рис. 2.4).

**Результаты поиска по IOC**  
CVE-2020-24186

Основное Правила обнаружения вторжений 1 Взаимосвязи 0 Граф

**Обзор CVE-2020-24186**

Название уязвимости: wpDiscuz RCE  
Описание уязвимости: Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяет неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles.  
Рекомендации по нейтрализации: - отключение плагина через панель администратора CMS WordPress;  
- обновление плагина до версии 7.0.5 и выше.

Рис. 2.4: Обзор уязвимости

Для устранения уязвимости подключились к удаленному рабочему столу по адресу 10.140.2.180(рис. 2.5).

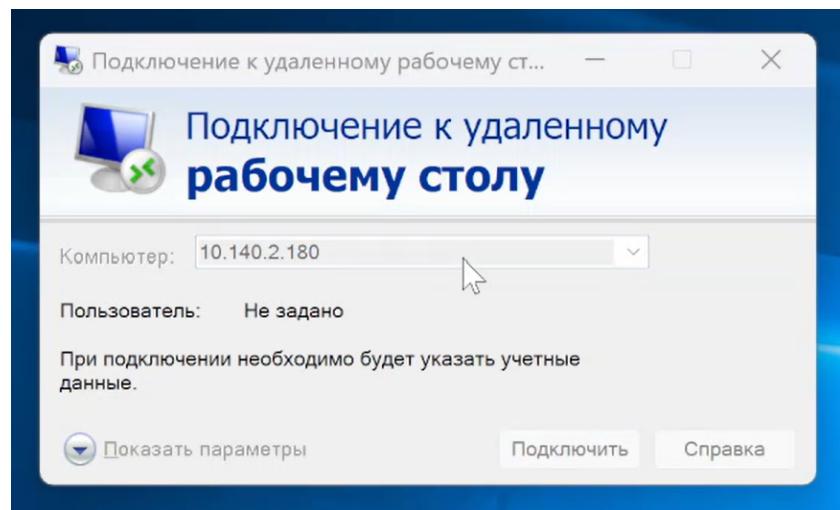


Рис. 2.5: Подключение к удаленному рабочему столу

Вошли под указанной учетной записью. (рис. 2.6).

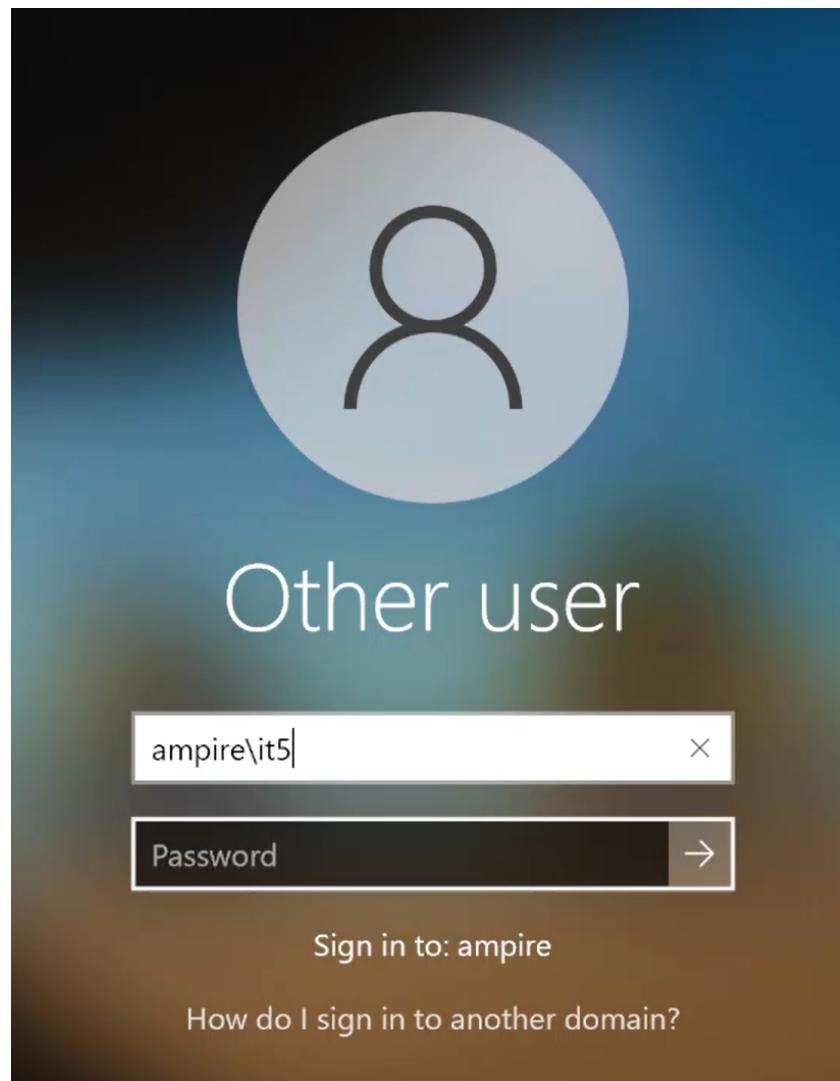


Рис. 2.6: Вход

В соответствии с вектором атаки в KeePass нашли CMS WordPress.(рис. 2.7).

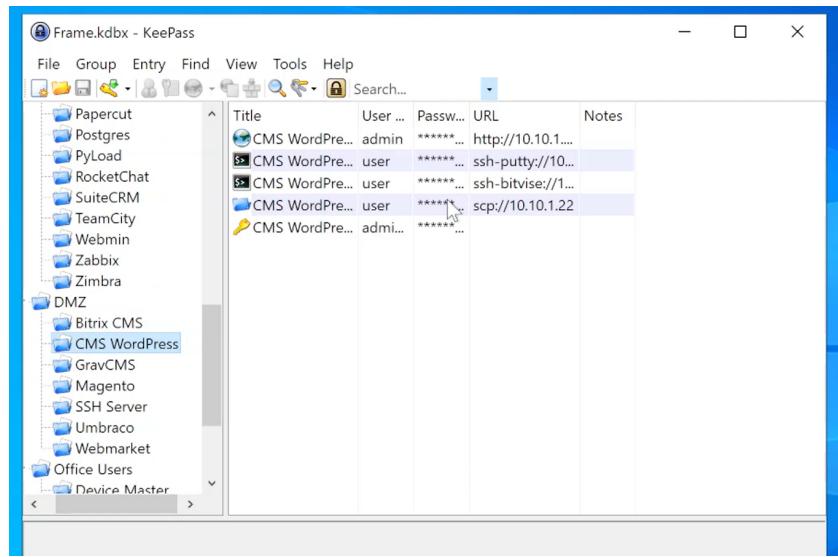


Рис. 2.7: KeePass

Просмотрели сайт WordPress по указанному адресу. Здесь обнаружили последствие - Deface - изменение внешнего вида интерфейса. (рис. 2.8).

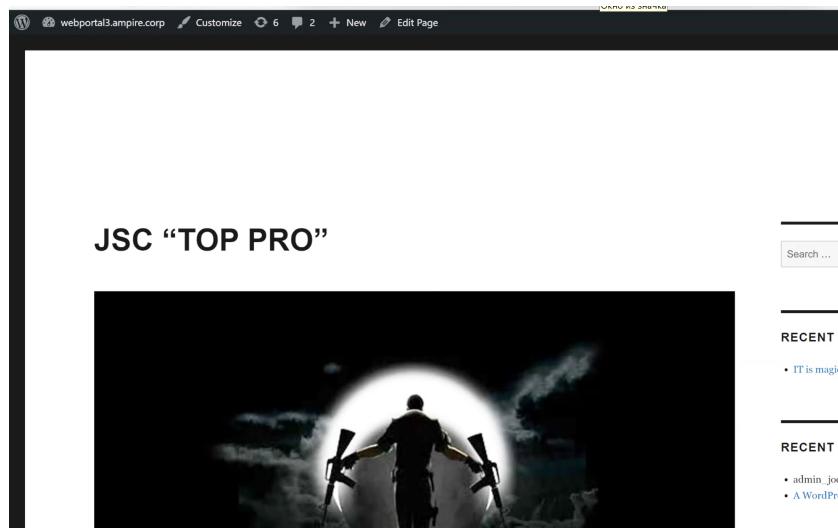


Рис. 2.8: Deface

В панели администрирования перешли во вкладку с плагинами и деактивировали плагин wpDiscuz (рис. 2.9).



Рис. 2.9: Плагин wpDiscuz

Для того, чтобы устранить последствие Deface, необходимо откатить сайт до предыдущей резервной копии. Для этого перешли в панель администрирования и во вкладке с плагинами нашли плагин UpdraftPlus - Backup/Restore, перешли в “Settings”.(рис. 2.10).



Рис. 2.10: Плагин UpdraftPlus - Backup/Restore

Выбрали последнюю резервную копию и нажали “Restore”. (рис. 2.11).

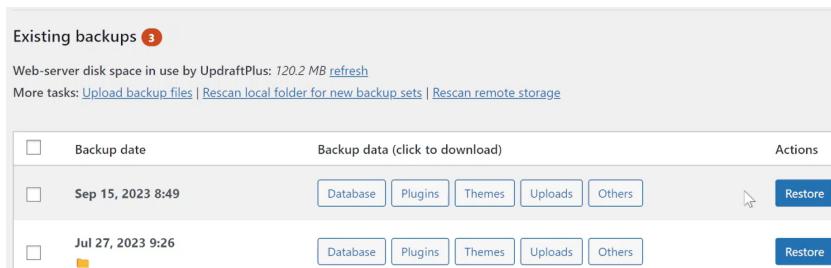


Рис. 2.11: Restore

Поставили флажки у компонентов “Themes” и “Uploads”. (рис. 2.12).

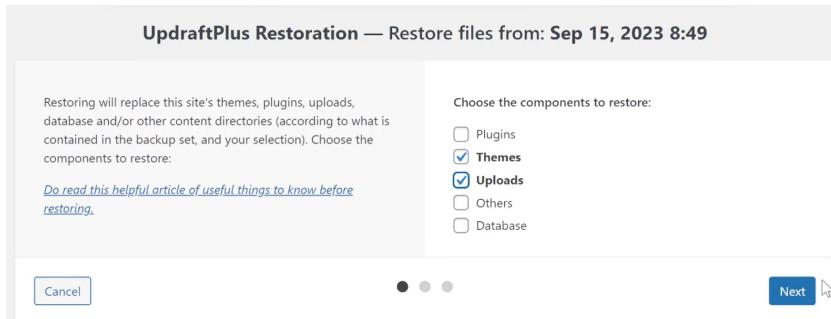


Рис. 2.12: Параметры восстановления

Во всплывшем окне с ошибкой нажали “Удалить старые директории”(рис. 2.13).

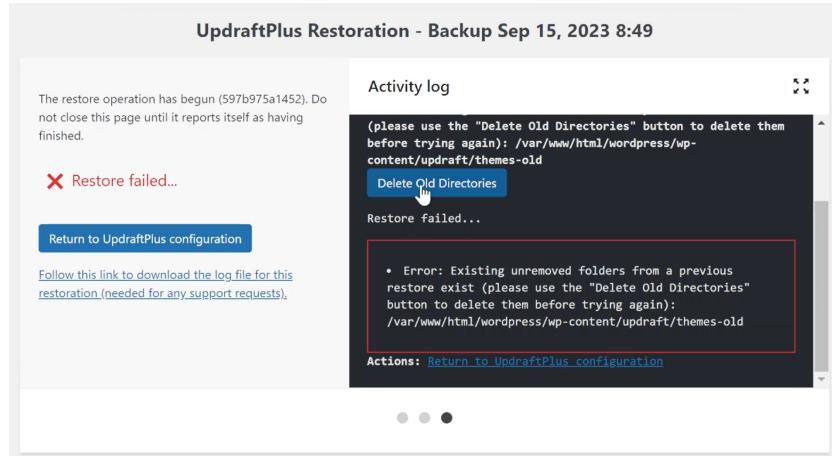


Рис. 2.13: Удаление старых директорий

Когда директории удалились, нажали “Return to UpdraftPlus configuration”(рис. 2.14).

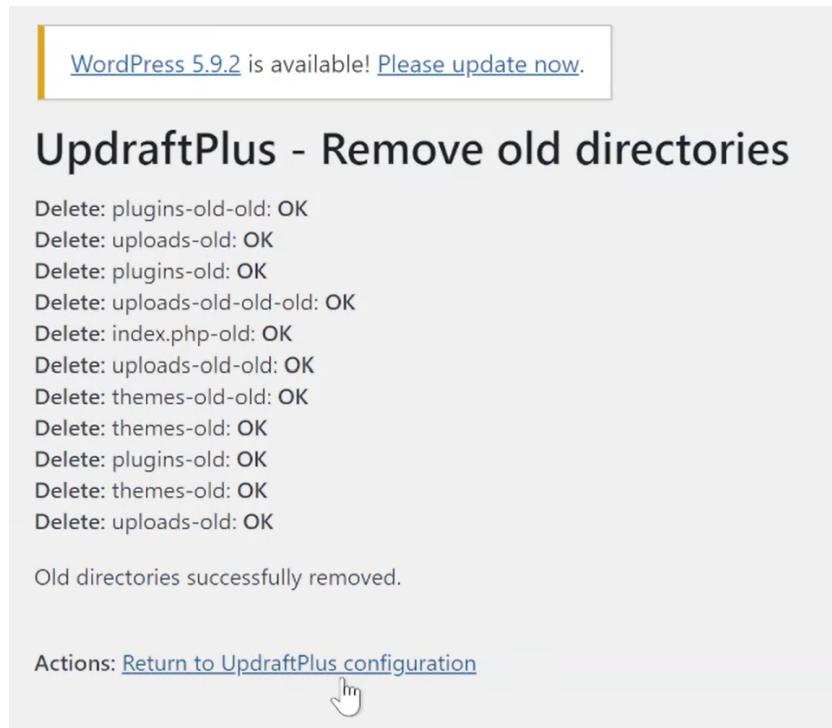


Рис. 2.14: Восстановление версии

Обновили страницу сайта. Убедились, что последствие Deface успешно устранено. (рис. 2.15).



Рис. 2.15: Устранено последствие

Перешли в Putty web-portal, чтобы проверить сокеты на наличие подозрительных процессов с помощью утилиты ss. (рис. 2.16).

```
user@web-portal-3: ~
201 packages can be updated.
120 updates are security updates.

Last login: Mon Jul 21 09:48:28 2025
user@web-portal-3:~$ sudo ss -tnp
[sudo] password for user:
State      Recv-Q    Send-Q      Local Address:Port      Peer Address:Port
FIN-WAIT-2  0          0          10.10.1.22:56234      10.10.2.11:443
users:(("chisel.sh",pid=3607,fd=16))
CLOSE-WAIT  0          0          10.10.1.22:39850      195.239.174.11:5557
users:(("chisel.sh",pid=3607,fd=12), ("sh",pid=3606,fd=12), ("LGnEa",pid=3570,fd=12))
ESTAB      0          0          10.10.1.22:39160      195.239.174.11:1085
users:(("chisel.sh",pid=3607,fd=11))
ESTAB      0          0          10.10.1.22:42002      195.239.174.11:5556
users:(("chisel.sh",pid=3607,fd=3), ("sh",pid=3606,fd=3), ("LGnEa",pid=3570,fd=3))
ESTAB      0          0          10.10.1.22:22        10.10.1.253:30913
users:(("sshd",pid=4929,fd=3), ("sshd",pid=4767,fd=3))
user@web-portal-3:~$
```

Рис. 2.16: Проверка процессов

Уничтожили вредоносные соединения с помощью команды kill {pid}. Убедились в их отсутствии. (рис. 2.17).

```

user@web-portal-3:~$ sudo kill 3607
user@web-portal-3:~$ sudo ss -tnp
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
FIN-WAIT-20      0            10.10.1.22:56234        10.10.2.11:443
CLOSE-WAIT0      0            10.10.1.22:39850        195.239.174.11:5557
ESTAB      0            10.10.1.22:42002        195.239.174.11:5556
users:(("LGnEa",pid=3570,fd=12))
ESTAB      0            10.10.1.22:22           10.10.1.253:30913
users:(("sshd",pid=4929,fd=3),("sshd",pid=4767,fd=3))
FIN-WAIT-20      0            [:ffff:10.10.1.22]:80       [:ffff:10.10.1.253]:45442
user@web-portal-3:~$ sudo kill 3570
user@web-portal-3:~$ █

```

Рис. 2.17: Уничтожение вредоносных процессов

Первая уязвимость с ее последствием успешно устранены (рис. 2.18).

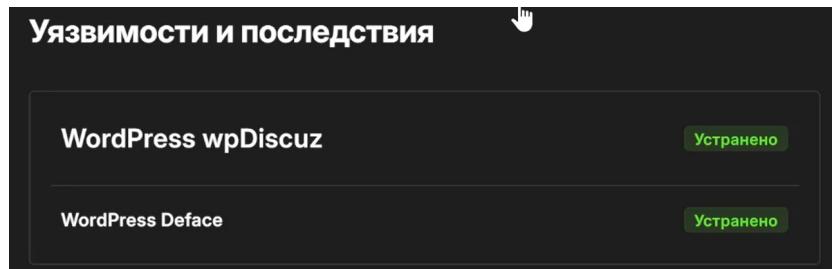


Рис. 2.18: Успех

## 2.3 Уязвимость Proxylogon

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий. (рис. 2.19).

16:33:807 29....	2025644	1	ET TROJAN Possible Metas... trojan-activity
16:33:807 29....	2025644	1	ET TROJAN Possible Metas... trojan-activity
16:33:804 29....	2035480	1	ET INFO PE EXE Download ... misc-activity
16:33:804 29....	2035480	1	ET INFO PE EXE Download ... misc-activity

Рис. 2.19: Журнал событий

Изучили информацию об обнаруженной уязвимости.(рис. 2.20).

Результаты поиска по IOC  
CVE-2021-26855

Основное Правила обнаружения вторжений 3 Взаимосвязи 0 Граф

**Основное**

**Метрики** CVSS версии 3.1

Оценка cvss 9.8 Высокая  
Вектор CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
Дата публикации NVD 03.03.2021 03:15 Последнее изменение NVD 03.03.2021 03:15

**Описание**  
Microsoft Exchange Server Remote Code Execution Vulnerability

**Уровень серьезности**

Оценка воздействия 5.9  
Оценка эксплуатируемости 3.9  
Вектор атаки Сетевой  
Сложность атаки Низкая  
Уровень привилегий Не требуется

Рис. 2.20: Обзор уязвимости

В соответствии с вектором атаки в KeePass нашли MS Exchange.(рис. 2.21).

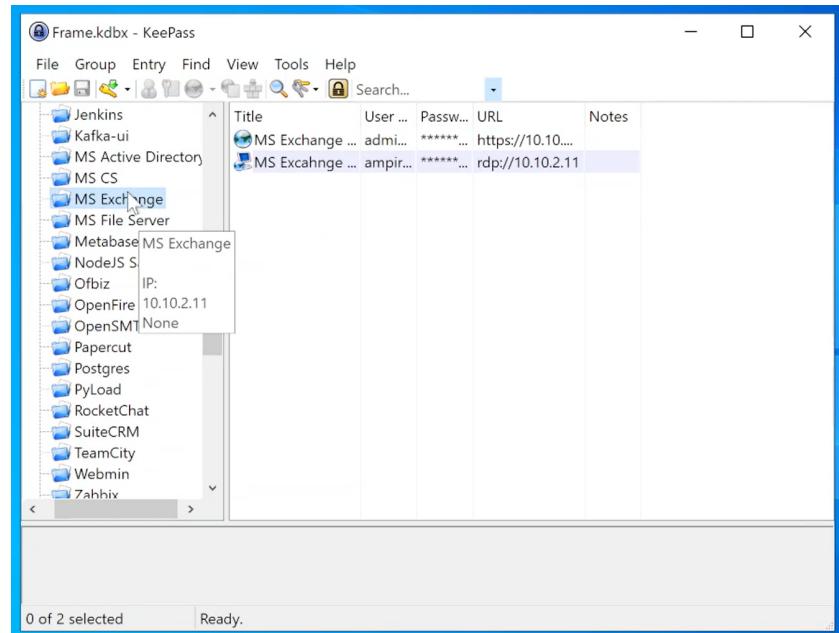


Рис. 2.21: KeePass

Подключились к удаленному рабочему столу по адресу в соответствии с вектором атаки.

Открыли Internet Information Services Manager. (рис. 2.22).

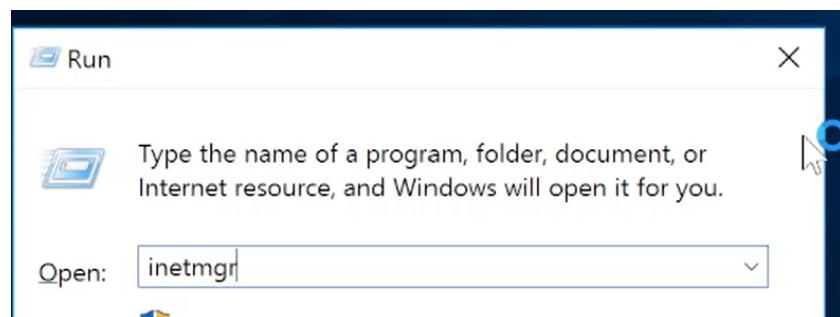


Рис. 2.22: inetmgr

Перешли в /MAIL/Sites/Default Web Site/ecp(рис. 2.23).

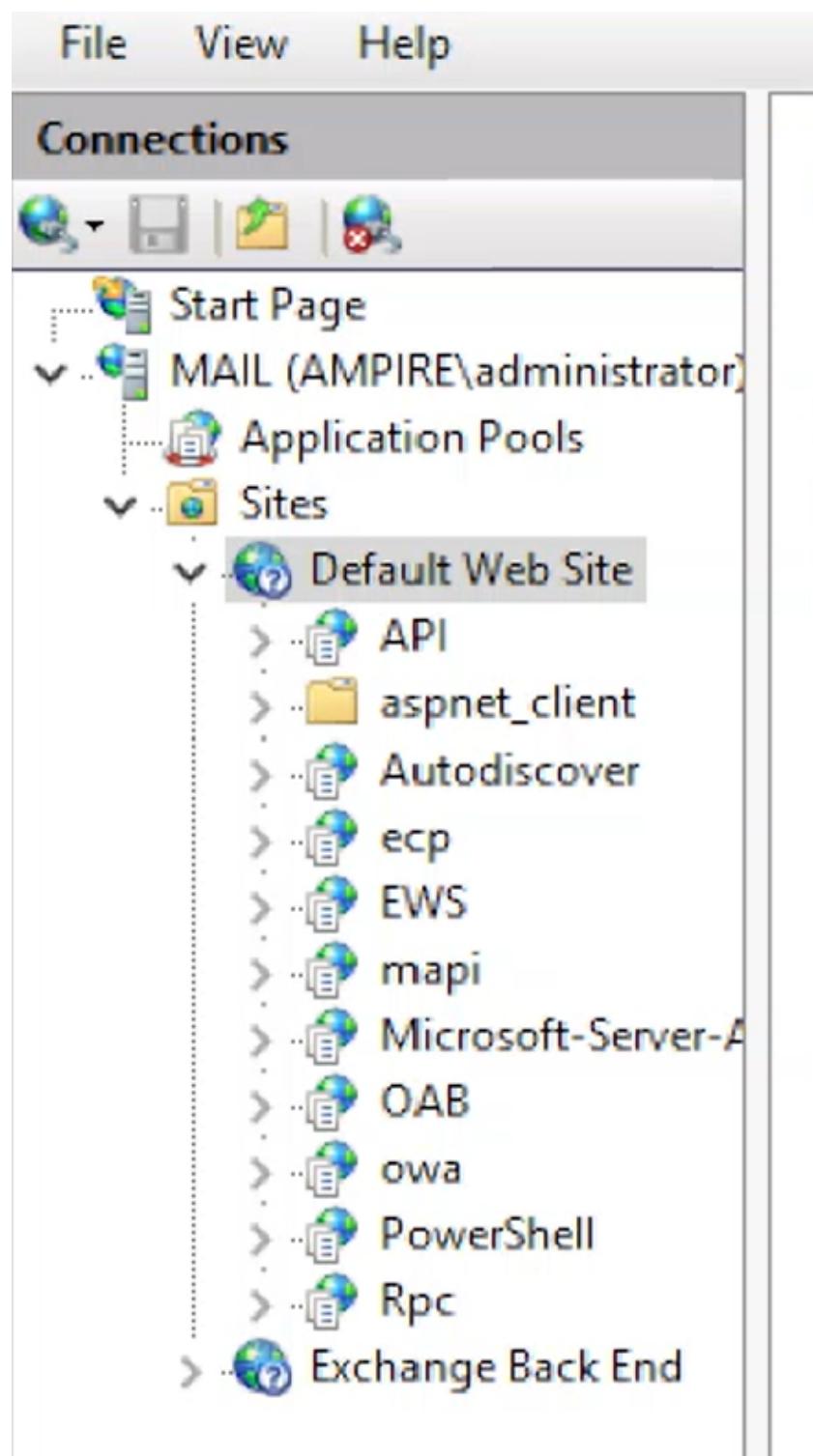


Рис. 2.23: inetmgr

Перешли в IP Address and Domain Restrictions, в “Actions” выбрали “Edit Feature Settings”, в

открывшемся окне в параметре “Access for unspecified clients” выбрали “Deny”.(рис. 2.24).

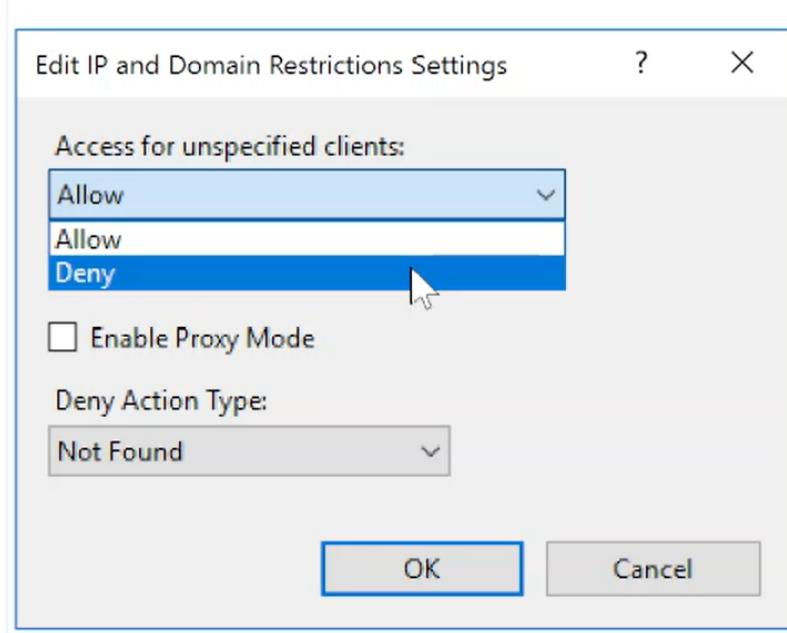


Рис. 2.24: inetmgr

Далее открыли терминал, чтобы обнаружить вредоносные процессы с помощью утилиты netstat. (рис. 2.25-2.26).

```
C:\Users\administrator.АМПИРЕ>netstat -b -o
Active Connections

 Proto  Local Address          Foreign Address        State      PID
 TCP    10.10.2.11:443        10.10.1.22:56234    CLOSE_WAIT  4
```

Рис. 2.25: Вредоносные процессы

```
[w3wp.exe]
TCP    10.10.2.11:13923        195.239.174.11:5558    ESTABLISHED  14832
[powershell.exe]
TCP    10.10.2.11:13924        195.239.174.11:5558    ESTABLISHED  13016
[powershell.exe]
```

Рис. 2.26: Вредоносные процессы

Остановили эти процессы и проверили их отсутствие.(рис. 2.27).

```
C:\Users\administrator.AMPIRE>taskkill /PID 14832 /F
SUCCESS: The process with PID 14832 has been terminated.

C:\Users\administrator.AMPIRE>taskkill /PID 14832 13016 /F
ERROR: Invalid argument/option - '13016'.
Type "TASKKILL /?" for usage.

C:\Users\administrator.AMPIRE>taskkill /PID 13016 /F
ERROR: The process "13016" not found.

C:\Users\administrator.AMPIRE>netstat -b -o
```

Рис. 2.27: Вредоносные процессы

Далее в директории `/C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/owa/auth` удалили файл `AM_Backdoor.aspx`(рис. 2.28).

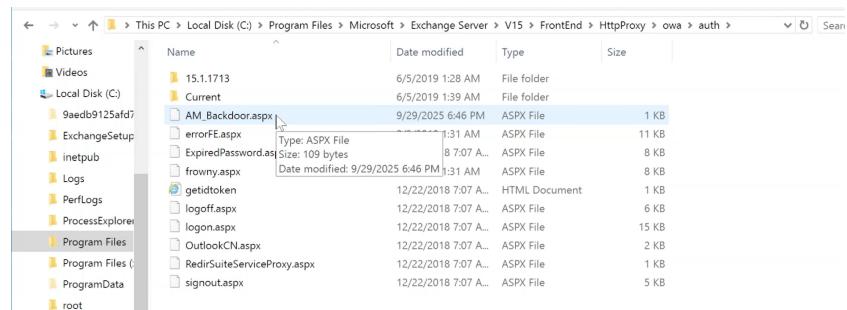


Рис. 2.28: Удаление файла .aspx

Уязвимость Proxylogon и ее последствие China Chopper успешно устраниены.(рис. 2.29).

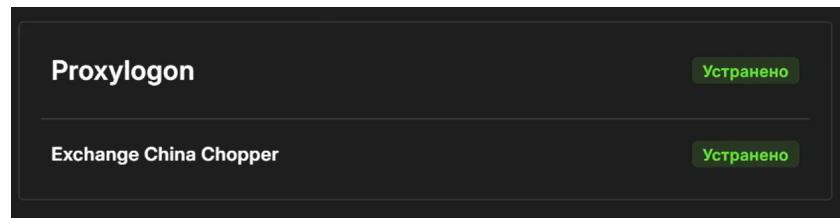


Рис. 2.29: Успех

## 2.4 Уязвимость Rocket.Chat

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий. (рис. 2.30).

18:33:030 29....	3121915	1	ET POLICY Executable and l...	policy-violation	TCP	195.239.174.11	5559	10.10.2.22	45770
18:33:030 29....	3121915	1	ET POLICY Executable and l...	ET POLICY Executable and linking format (ELF)	TCP	195.239.174.11	5559	10.10.1.253	1548
18:22:912 29....	3129327	1	ET POLICY Executable and l...	file download var1	TCP	195.239.174.11	8010	10.10.2.22	47362
18:22:912 29....	3129327	1	ET POLICY Executable and l...	policy-violation	TCP	195.239.174.11	8010	10.10.1.253	37775

Рис. 2.30: Журнал событий

Изучили информацию об обнаруженной уязвимости.(рис. 2.31).

**Обзор CVE-2021-22911**

**Название уязвимости:** RocketChat RCE  
**Описание уязвимости:** CVE-2021-22911 представляет собой две уязвимости NoSQL Injection, эксплуатация которых может позволить злоумышленникам повысить свои привилегии, выполнить произвольные системные команды на хост-сервере и украдь конфиденциальные пользовательские данные и сообщения чата. Обе уязвимости исправлены в версии 3.13.2 и перенесены в старые ветки в версиях 3.12.4 и 3.11.4  
**Рекомендации по нейтрализации:**  
 - обновление версии «RocketChat»;  
 - запрет выполнения JavaScript на стороне сервера БД.

Рис. 2.31: Обзор уязвимости

В соответствии с вектором атаки в KeePass нашли RocketChat.(рис. 2.32).

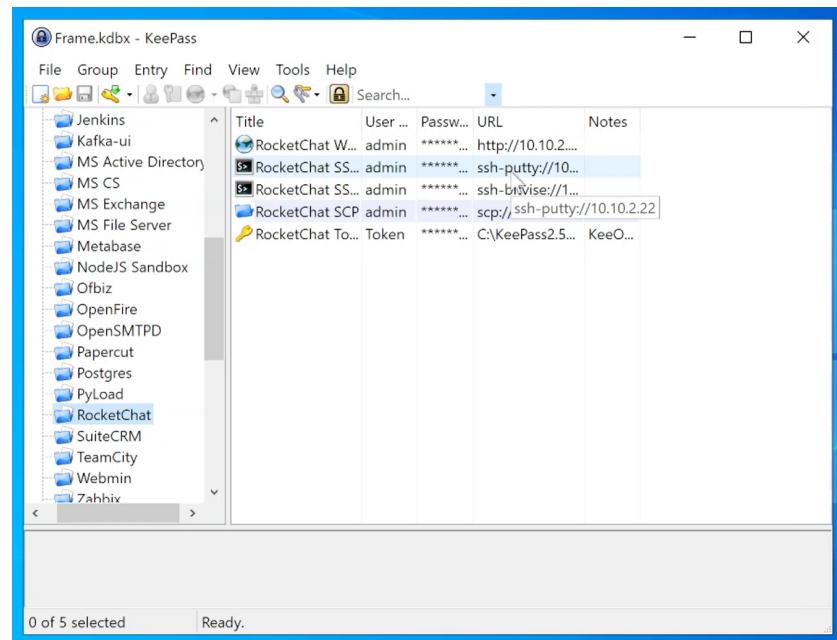


Рис. 2.32: KeePass

Открыли веб-версию Rocket.Chat и нажали на сброс пароля для указанной учетной записи.(рис. 2.33).

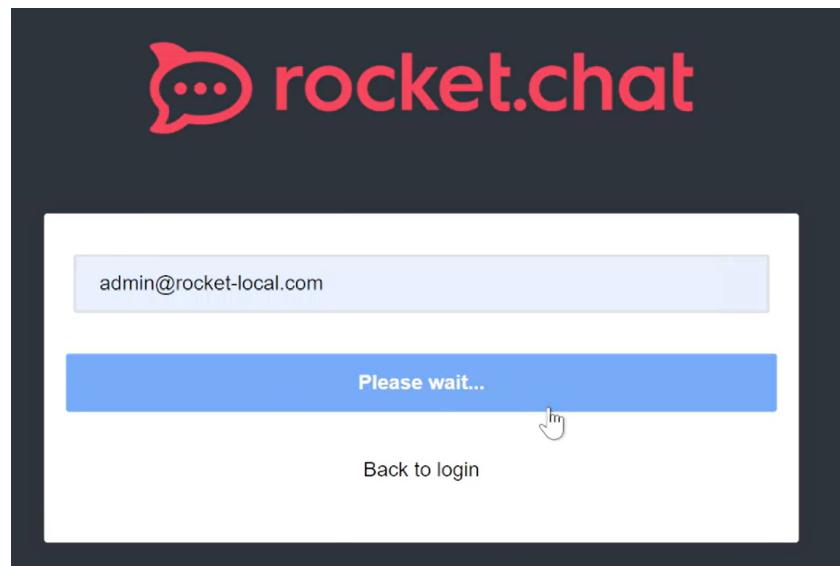


Рис. 2.33: Сброс пароля

На почту администратора Rocket.Chat было направлено email-письмо с инструкциями по сбросу пароля.(рис. 2.34).

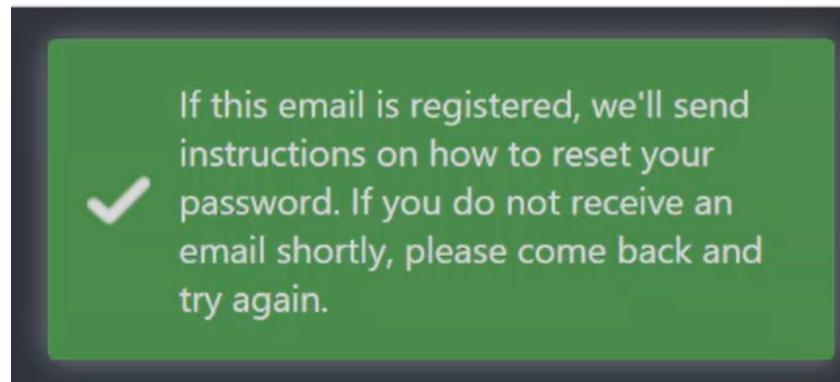
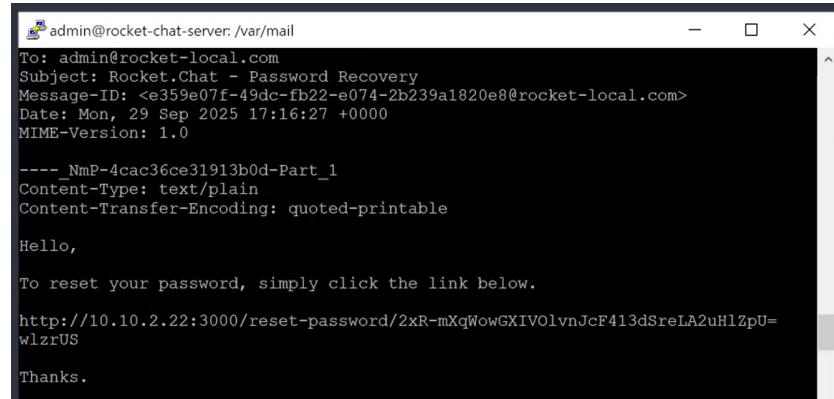


Рис. 2.34: Сообщение об отправке email

В консоли от администратор просмотрели это письмо. Скопировали ссылку со сгенерированным токеном для сброса пароля. (рис. 2.35).



The screenshot shows an email message from admin@rocket-chat-server: /var/mail. The subject is "Rocket.Chat - Password Recovery". The message body contains the following text:

```
To: admin@rocket-local.com
Subject: Rocket.Chat - Password Recovery
Message-ID: <e359e07f-49dc-fb22-e074-2b239a1820e8@rocket-local.com>
Date: Mon, 29 Sep 2025 17:16:27 +0000
MIME-Version: 1.0

----_NmP-4cac36ce31913b0d-Part_1
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable

Hello,

To reset your password, simply click the link below.

http://10.10.2.22:3000/reset-password/2xR-mXqWowGXIVOlvnJcF413dSreLA2uHlZpU=wlrUS

Thanks.
```

Рис. 2.35: Инструкция по сбросу пароля

Перешли по скопированному адресу в браузере(рис. 2.36).



Рис. 2.36: Сброс пароля

Задали новый пароль для пользователя(рис. 2.37).

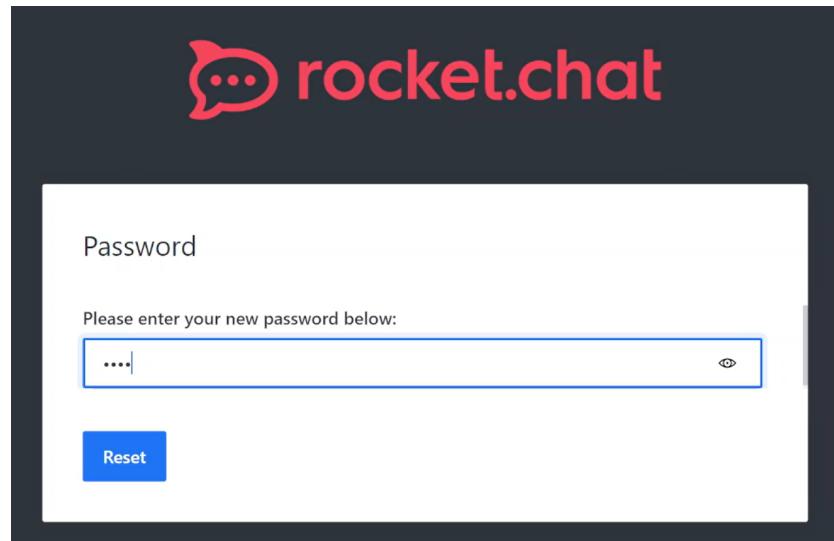


Рис. 2.37: Сброс пароля

Просмотрели /home/user/backup\_codes для прохождения двухфакторной аутентификации при сбросе пароля. (рис. 2.38).

```
admin@rocket-chat-server:/$ cat /home/user/backup_codes
backup codes for admin Rocket Chat:
iFdDR68y kpMifh9E 43PxEyom jho4DGdw RiuwYGrg LohP2b4A 9tiK2Sca THHC87gf mnPEZACy
rdhcBy8B DvPHRnTz ZZPgeko2
admin@rocket-chat-server:/$
```

Рис. 2.38: Backup\_codes

Ввели один из них в соответствующее поле ввода.(рис. 2.39).

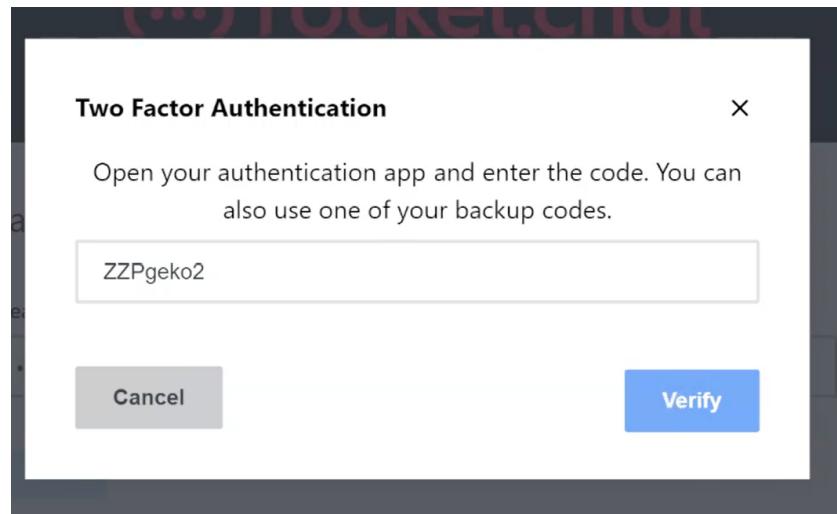


Рис. 2.39: Сброс пароля

Залогинились с измененным паролем. (рис. 2.40).

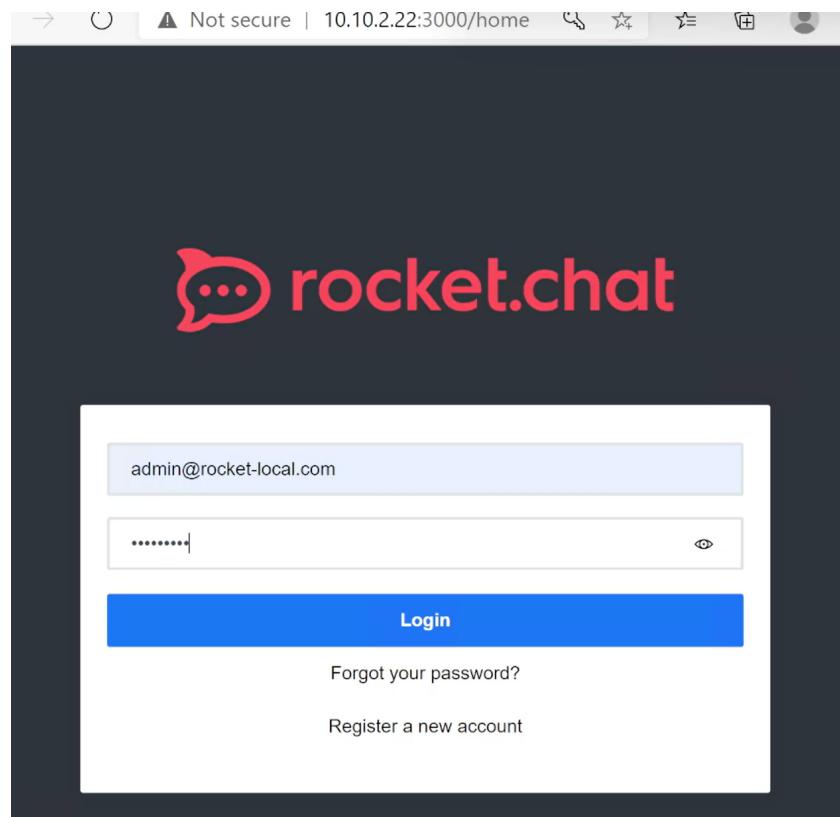


Рис. 2.40: Вход в учетную запись

В панели администрирования перешли в “Права доступа”, и для роли “User” поставили флагок “User must use Two factor Authentication”.(рис. 2.41).

The image shows two side-by-side panels from the Rocket.Chat administration interface. On the left is the "Permissions" panel, which contains a table of permissions with four columns: Admin, Moderator, Leader, and Owner. Most permissions have checkboxes in the Admin column. On the right is the "Role Editing" panel, which is currently set to the "user" role. It includes fields for "Description" (with a note about leaving it blank), "Scope" (set to "Global"), and a checkbox for "Users must use Two Factor Authentication" which is checked. There is also a "Save" button at the bottom.

Рис. 2.41: Права доступа

Перешли во вкладку “Учетные записи” и настроили подтверждение адреса электронной почты при регистрации для роли “User” и автоматическую настройку двухфакторной аутентификации

по электронной почте для новых пользователей.(рис. 2.42-2.43).

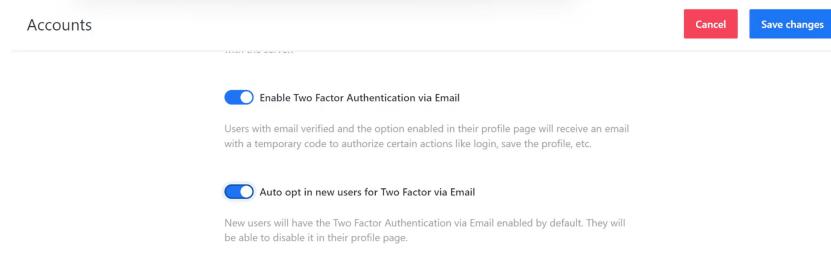


Рис. 2.42: Настройки двухфакторной аутентификации

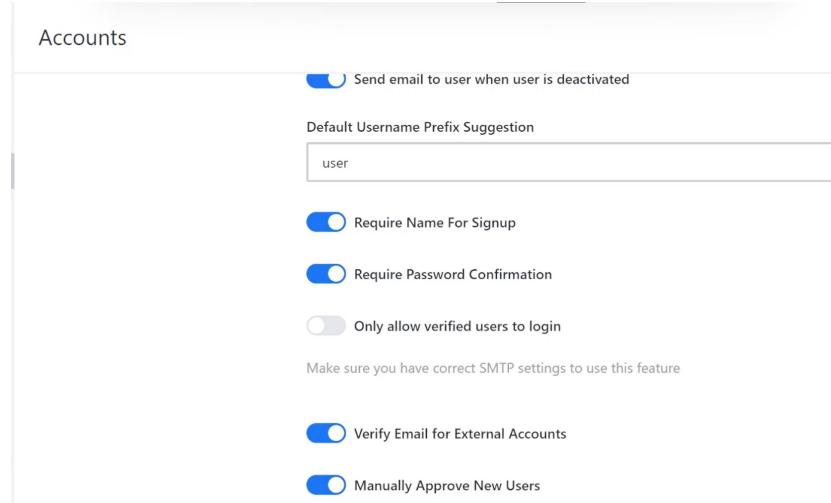
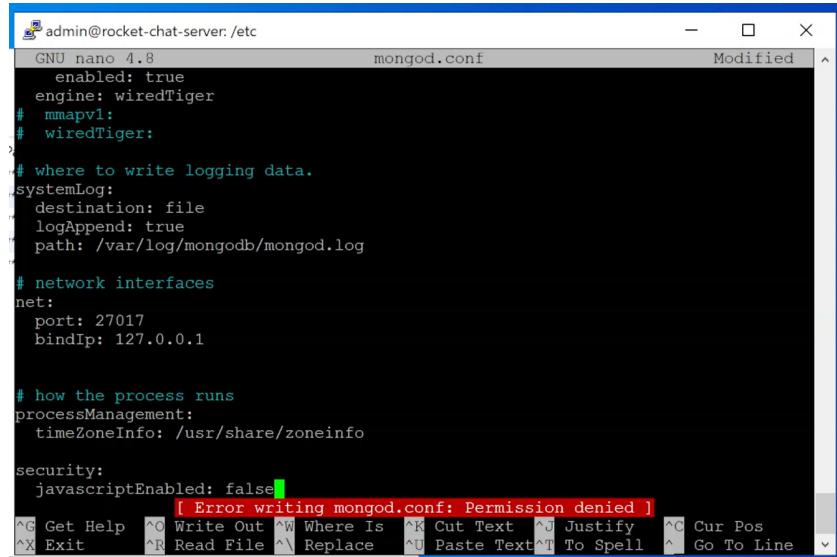


Рис. 2.43: Настройки регистрации

В терминале администратора Rocket.Chat-server отредактировали файл mongod.conf, раскомментировав параметр “security.” и прописав отключение выполнения JavaScript на стороне сервера базы данных “javascriptEnabled: False”.(рис. 2.44).



```
admin@rocket-chat-server: /etc
GNU nano 4.8                                     mongod.conf                                         Modified
enabled: true
engine: wiredTiger
# mmapv1:
# wiredTiger:
#
# where to write logging data.
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
[ Error writing mongod.conf: Permission denied ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text^T To Spell  ^  Go To Line
```

Рис. 2.44: Редактирование mongod.conf

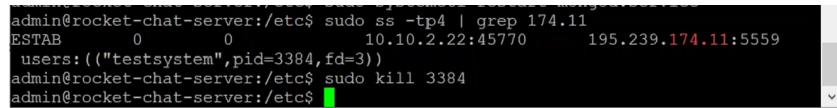
Перезапустили службу mongod.service(рис. 2.45).



```
admin@rocket-chat-server:/etc$ sudo systemctl restart mongod.service
[...]
```

Рис. 2.45: Restart mongod.service

С помощью утилиты ss обнаружили и остановили вредоносные процессы.(рис. 2.46).



```
admin@rocket-chat-server:/etc$ sudo ss -tp4 | grep 174.11
ESTAB      0      0          10.10.2.22:45770      195.239.174.11:5559
users:("testsystem",pid=3384,fd=3)
admin@rocket-chat-server:/etc$ sudo kill 3384
admin@rocket-chat-server:/etc$
```

Рис. 2.46: Уничтожение вредоносных соединений

Уязвимость RocketChat RCE и ее последствие meterpreter успешно устраниены.(рис. 2.47).

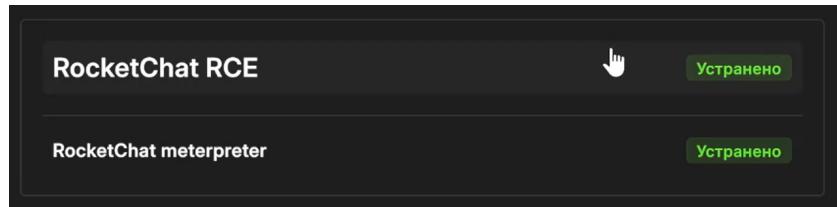


Рис. 2.47: Успех

## 2.5 Завершение выполнения лабораторной работы

Заполнили карточки инцидентов для уязвимостей и их последствий.(рис. 2.48).

The screenshot shows a web-based incident management system with the following details:

- Card 1: Уязвимость WordPress-wpDiscuz**
  - Author: Доберштейн Алина @1132226448@pf...
  - Responsible: Доберштейн Алина @1132226448@pfur.ru
  - Date: 29.09.2025 18:44
  - Status: В работе
  - Risk Rating: ☆☆☆☆☆
- Card 2: Последствие WordPress-wpDiscuz → Deface**
  - Author: Доберштейн Алина @1132226448@pfur.ru
  - Responsible: Доберштейн Алина @1132226448@pf...
  - Date: 29.09.2025 18:44
  - Status: Новый
  - Risk Rating: ☆☆☆☆☆
- Card 3: Уязвимость**
  - Author: Доберштейн Алина @1132226448@pf...
  - Responsible: Доберштейн Алина @1132226448@pf...
  - Date: 0 Сообщений
  - Status: Новый
  - Risk Rating: ☆☆☆☆☆
- Card 4: Последствие Proxylogon → Exchange China Chopper**
  - Author: Доберштейн Алина @1132226448@pf...
  - Responsible: Доберштейн Алина @1132226448@pf...
  - Date: 0 Сообщений
  - Status: Новый
  - Risk Rating: ☆☆☆☆☆
- Card 5: Уязвимость RocketChat**
  - Author: Доберштейн Алина @1132226448@pf...
  - Responsible: Доберштейн Алина @1132226448@pf...
  - Date: 0 Сообщений
  - Status: Новый
  - Risk Rating: ☆☆☆☆☆
- Card 6: Последствие Meterpreter**
  - Author: Доберштейн Алина @1132226448@pf...
  - Responsible: Доберштейн Алина @1132226448@pf...
  - Date: 0 Сообщений
  - Status: Новый
  - Risk Rating: ☆☆☆☆☆

Рис. 2.48: Карточки инцидентов

## **3 Выводы**

В результате выполнения лабораторной работы мы получили навыки обнаружения и устранение уязвимостей WordPress-wpDiscuz, Proxylogon, Rocket.Chat и их последствий.

## **Список литературы**