

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
2. 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
3. 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)

| | | | | | | | | |
|---------------------|---|-------------------------------|------------------|-----|----------------|------|-------------|-----|
| 20:56:16.292 02.... | 1 | ET POLICY Executable and I... | policy-violation | TCP | 195.239.174.11 | 8010 | 10.10.1.253 | 292 |
| 20:54:19.124 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:19.124 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 220 |
| 20:54:19.114 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:19.114 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 220 |
| 20:54:18.991 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:18.991 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 210 |
| 20:54:18.936 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:18.936 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 210 |
| 20:52:26.703 02.... | 1 | ET POLICY Executable and I... | policy-violation | TCP | 195.239.174.11 | 5556 | 10.10.1.22 | 462 |

(рис. 1)

| | | | | | | | | |
|---------------------|---|-----------------------------|-----------------|-----|----------------|------|-------------|-----|
| 20:54:19.124 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:19.124 02.... | 1 | ET TROJAN Possible Metas... | trojan-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 220 |
| 20:54:19.114 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.2.11 | 216 |
| 20:54:19.114 02.... | 1 | ET INFO PE EXE Download ... | misc-activity | TCP | 195.239.174.11 | 5558 | 10.10.1.253 | 220 |

(рис. 2)

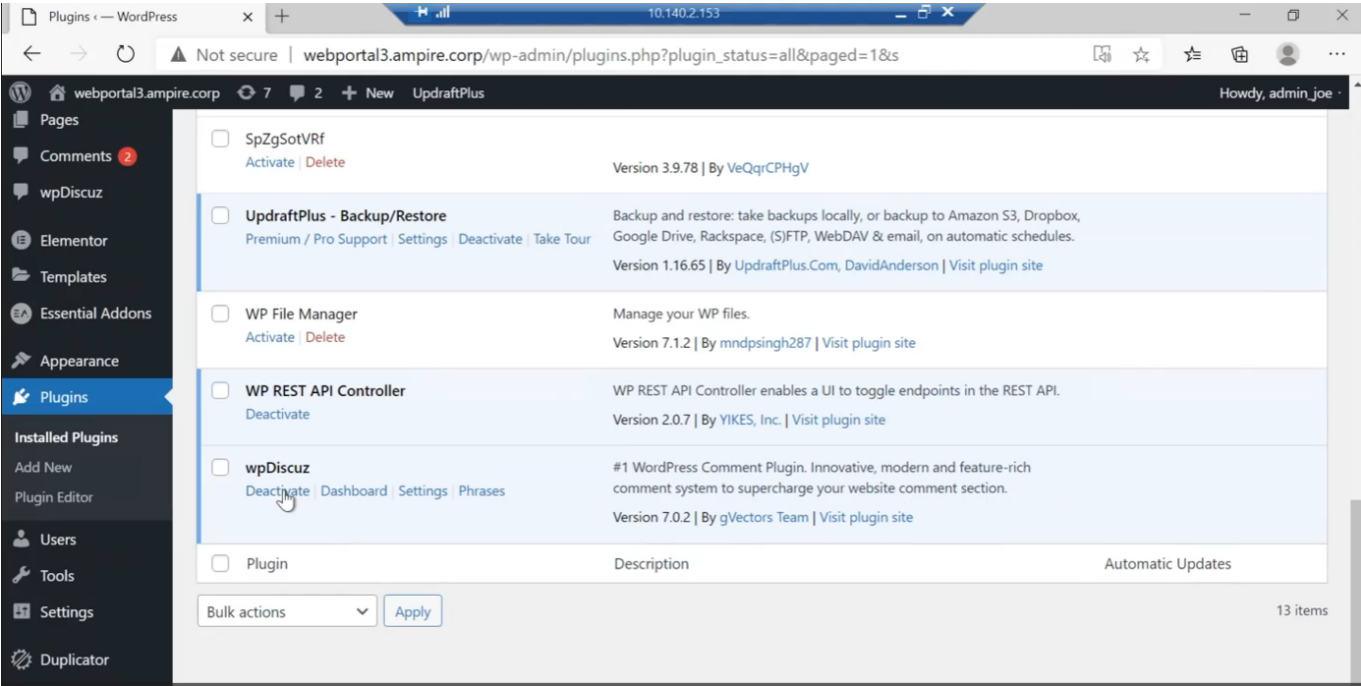
Уязвимость 1. WordPress-wpDiscuz (CVE-2020-24186) (рис. 2)

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.

| Activity Log | | | | | | | |
|---|------|----------------|-------------|---------|----------|----------|--------|
| <div>All Time All Roles All Users All Topics All Actions Filter</div> | | | | | | | Search |
| | | | | | | | 1 item |
| Date | User | IP | Topic | Context | Meta | Action | |
| 51 mins ago 02/10/2025 17:51:58 | N/A | 195.239.174.11 | Attachments | Media | wAeTAAEI | Uploaded | |
| Date | User | IP | Topic | Context | Meta | Action | |
| <div>Export as CSV</div> | | | | | | | 1 item |

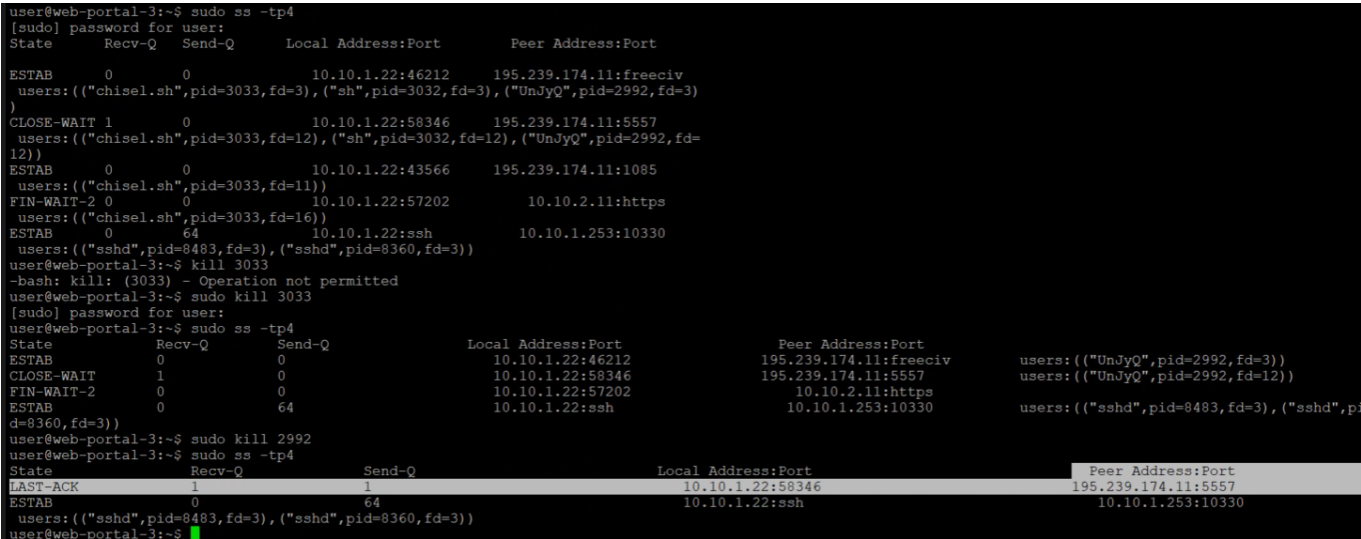
(рис. 3)

Для устранения уязвимости мы деактивировали WordPress.



(рис. 4)

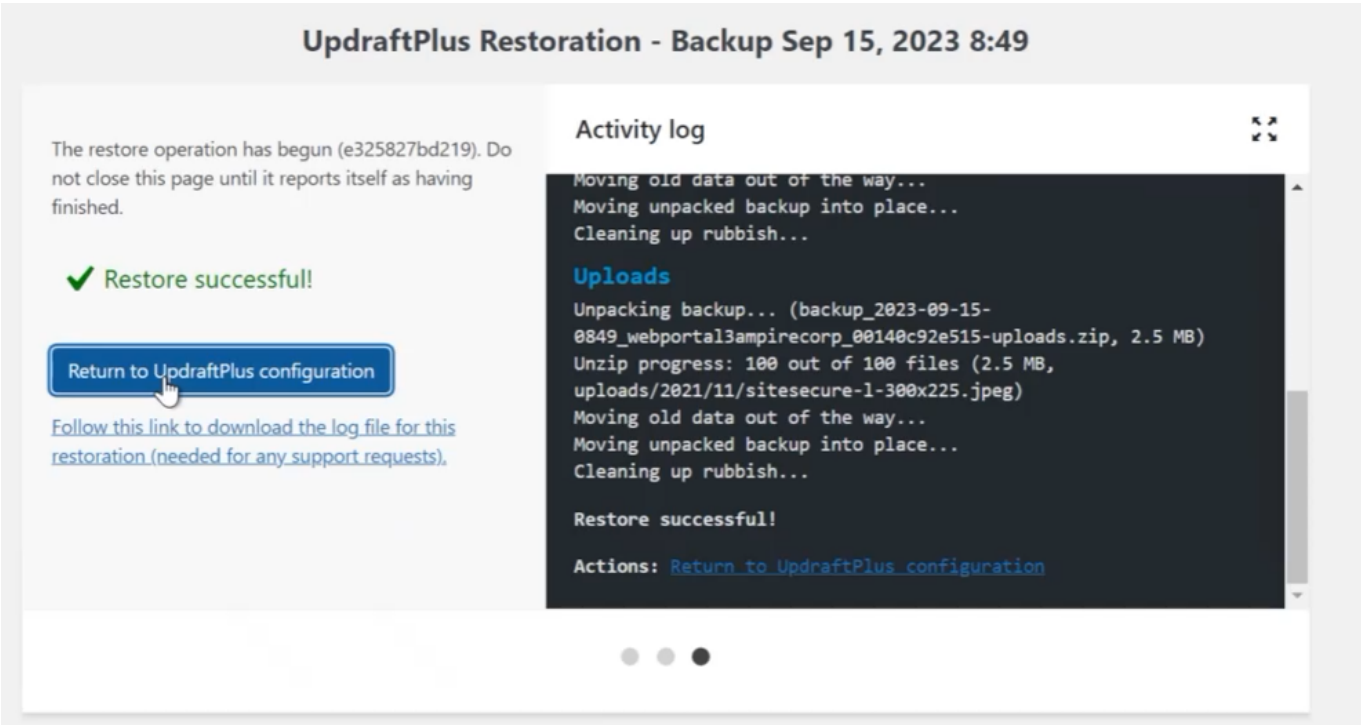
Также для устранения этой уязвимости необходимо удалить meterpreter сессию.



(рис. 5)

Последствие 1. Deface (рис. 6)

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



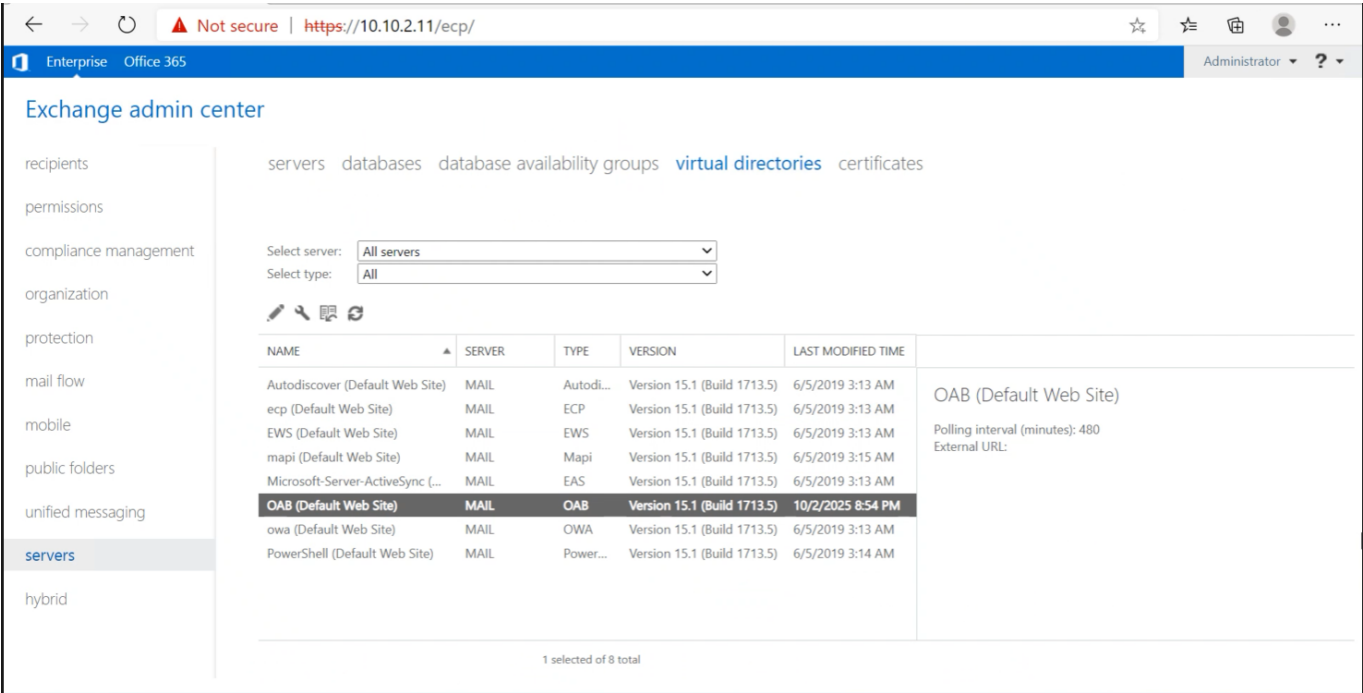
(рис. 6)

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

| У... | Дата и время | К... | Название правила | Класс | Протокол | IP-адрес исто... | Порт ис... | IP-адрес полу... | По |
|------|---------------------|------|-------------------------------|---|----------|------------------|------------|------------------|-----|
| ● | 20:56:26.413 02.... | 1 | ET POLICY Executable and I... | policy-violation | TCP | 195.239.174.11 | 5559 | 10.10.2.22 | 55' |
| ● | 20:56:16.292 02.... | 1 | ET POLICY Executable and | ET POLICY Executable and linking format (ELF) file download var1 | | 239.174.11 | 8010 | 10.10.2.22 | 34' |

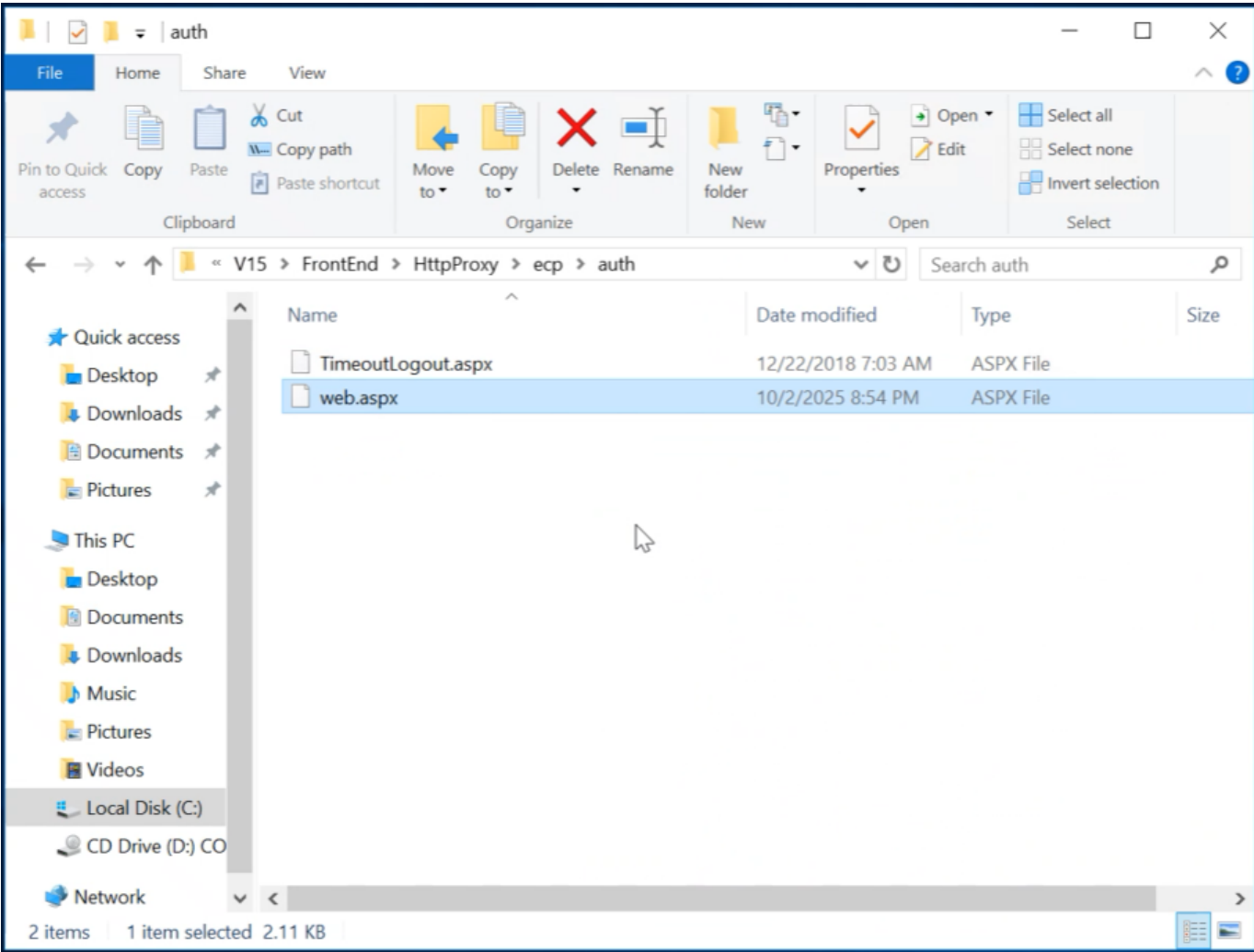
(рис. 7)

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.



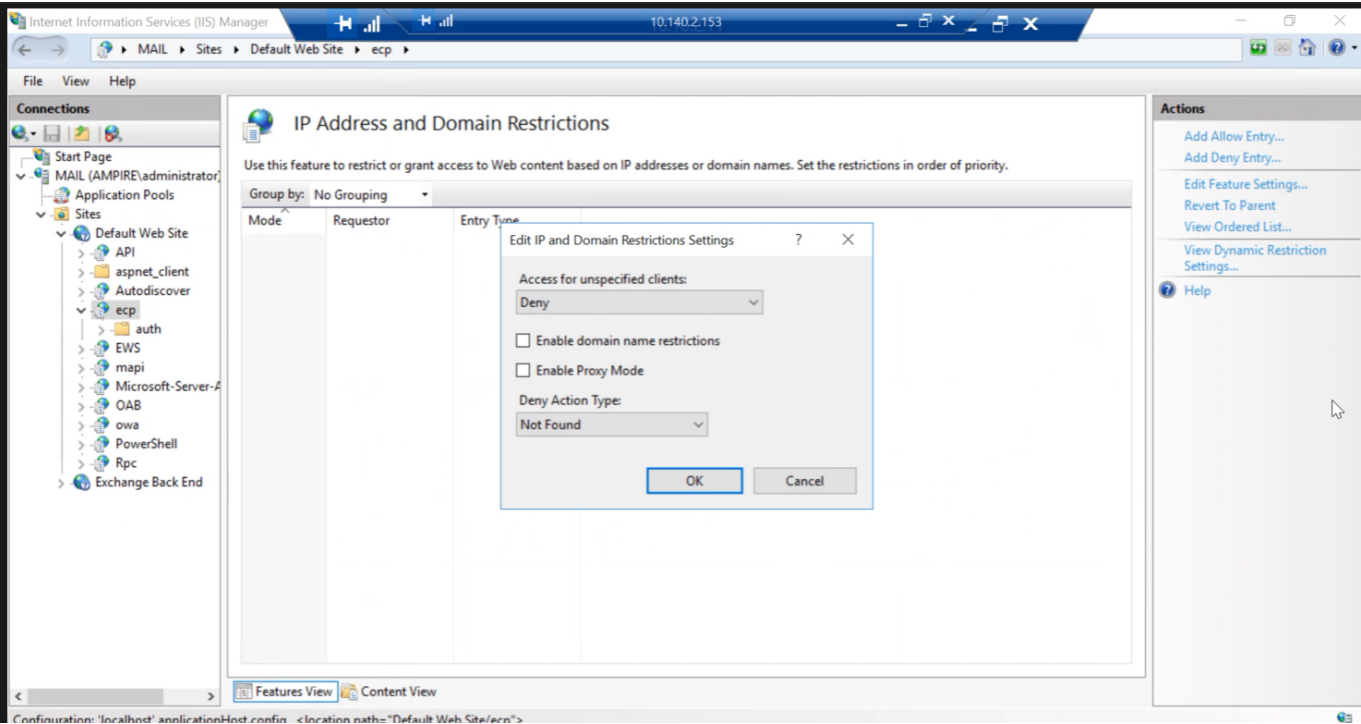
(рис. 8)

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 устранения уязвимости мы ограничили доступ к указанной директории для запрета эксплуатации уязвимости:

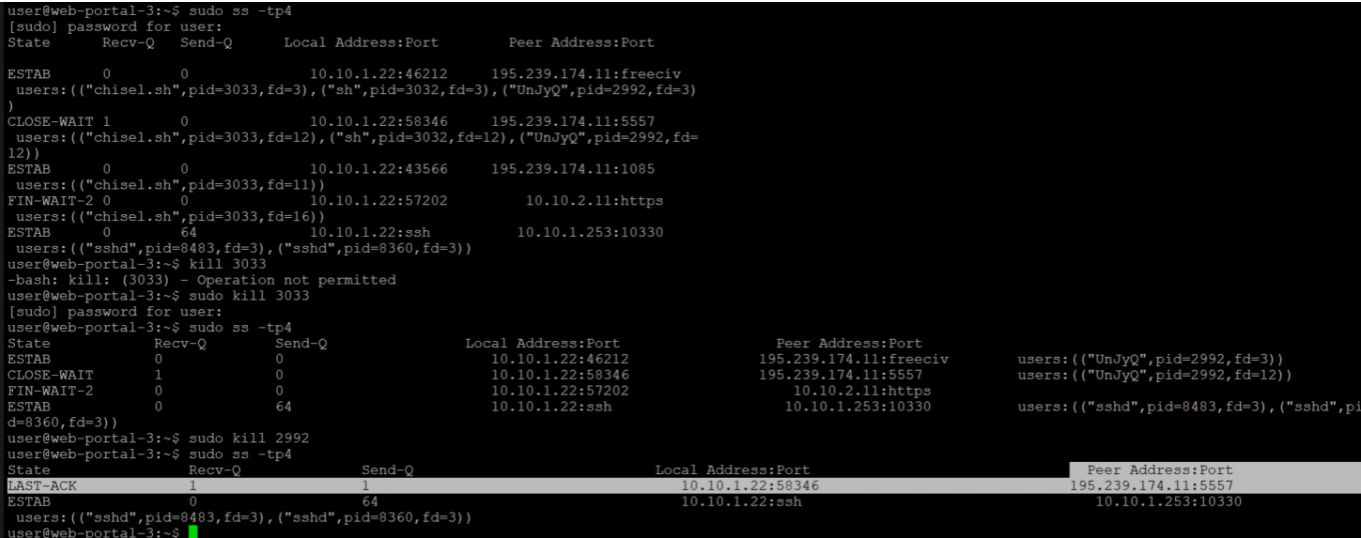


(рис. 10)

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 C:\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:

События

События за последние 24 часа

| У... | Дата и время | Код события | К... | Название правила | Класс |
|------|--------------------|-------------|------|--|----------|
| | 18:08:23.432 12... | 3091878 | 1 | AM EXPLOIT Possible Grandstream ATA HT800 Serie... | attempt |
| | 17:45:37.968 12... | 3049137 | 1 | AM INFO Possible SSH successful connection from E... | bad-unk |
| | 17:45:37.968 12... | 3049137 | 1 | AM INFO Possible SSH successful connection from E... | bad-unk |
| | 17:39:57.622 12... | 3121915 | 1 | ET POLICY Executable and linking format (ELF) file do... | policy-v |
| | 17:39:57.622 12... | 3121915 | 1 | ET POLICY Executable and linking format (ELF) file do... | policy-v |
| | 17:39:47.516 12... | 3129327 | 1 | ET POLICY Executable and linking format (ELF) file do... | policy-v |
| | 17:39:47.516 12... | 3129327 | 1 | ET POLICY Executable and linking format (ELF) file do... | policy-v |
| | 17:37:59.603 12... | 2025644 | 1 | ET TROJAN Possible Metasploit Payload Common Co... | trojan-a |
| | 17:37:59.603 12... | 2025644 | 1 | ET TROJAN Possible Metasploit Payload Common Co... | trojan-a |
| | 17:37:59.600 12... | 2035480 | 1 | ET INFO PE EXE Download over raw TCP | misc-ac |
| | 17:37:59.600 12... | 2035480 | 1 | ET INFO PE EXE Download over raw TCP | misc-ac |
| | 17:37:59.478 12... | 2025644 | 1 | ET TROJAN Possible Metasploit Payload Common Co... | trojan-a |
| | 17:37:59.478 12... | 2025644 | 1 | ET TROJAN Possible Metasploit Payload Common Co... | trojan-a |

Событие 17:39:57.622 12.10.2025

Событие | Источник | Получатель | Пакет

Общая информация

Дата и время

17:39:57.622 12.10.2025

Интерфейс захвата

eth2

Уровень важности

Высокий

Тип события

Сигнатурное событие

Протокол

TCP

Код события

3121915

Правило анализа

Класс

policy-violation

Группа

policy

Название

ET POLICY Executable and linking format (ELF) file download var1

Описание:

Сигнатуры возможного нарушения политики информационной безопасности

(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)

/var/mail/admin - admin@10.10.2.22 - Editor - WinSCP

Encoding | Color | ?

Delivered-To: admin@rocket-local.com
Received: from [127.0.0.1] (localhost [127.0.0.1])
by rocket-chat-server (Postfix) with ESMTP id C0390748BD
for <admin@rocket-local.com>; Thu, 2 Oct 2025 17:55:21 +0000 (UTC)
Content-Type: multipart/alternative;
boundary="--_NmP-76b3d55547bfa5b8-Part_1"
From: "Rocket.Chat" <rocketchat@rocket-local.com>
To: admin@rocket-local.com
Subject: Rocket.Chat - Password Recovery
Message-ID: <2367edf2-0341-c660-1bc0-d8e3c1b63679@rocket-local.com>
Date: Thu, 02 Oct 2025 17:55:21 +0000
MIME-Version: 1.0

-----_NmP-76b3d55547bfa5b8-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/zHvVFiyhsgniFS5Gw6lGnrFcJxLDHhAczuvJx=t9h0D->

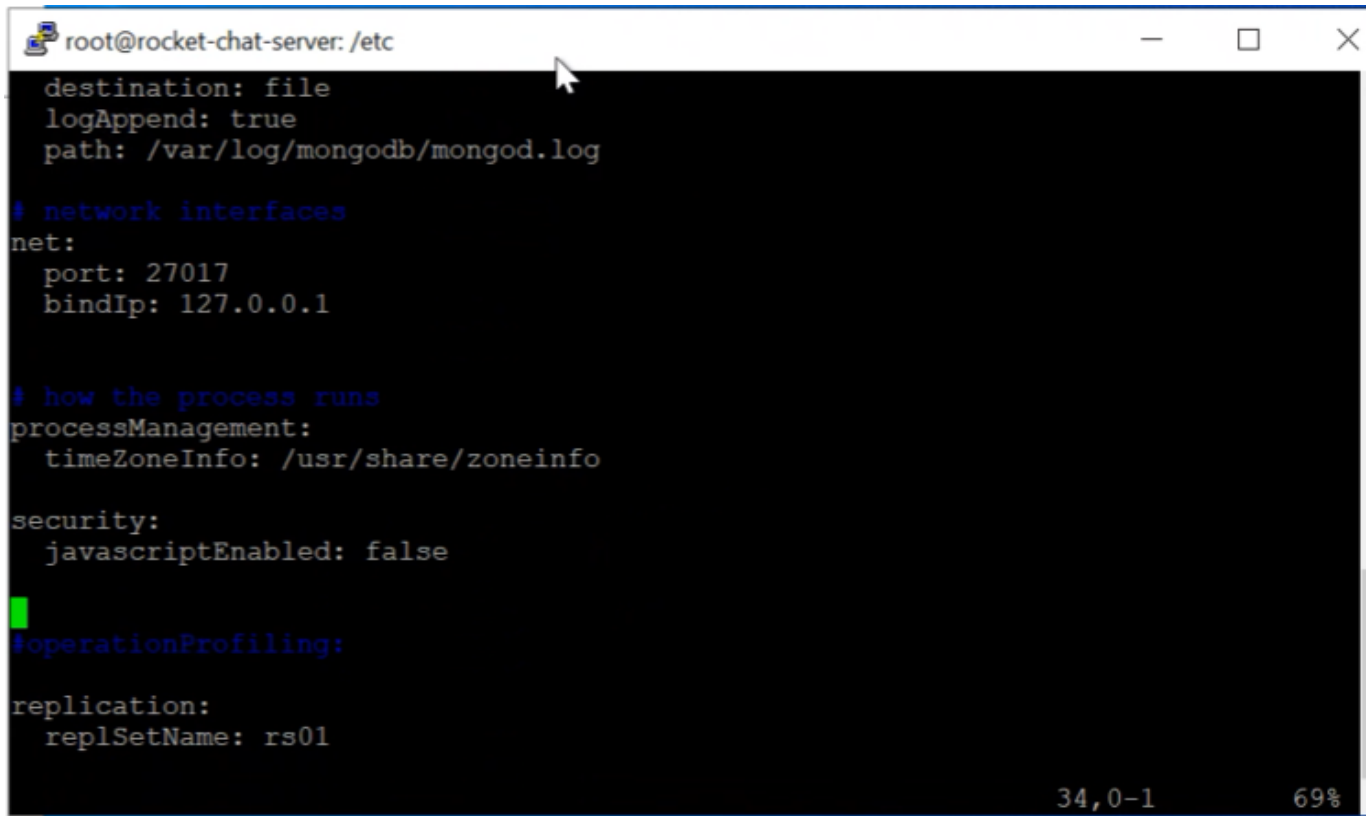
Thanks.

-----_NmP-76b3d55547bfa5b8-Part_1
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable

Line: 27/103 | Column: 85 | Encoding: 1252 (ANSI - L...

(рис. 13)

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

A terminal window titled 'root@rocket-chat-server: /etc' with standard window controls. It displays the configuration for a MongoDB instance. The configuration includes logging settings, network interfaces, process management, security, operation profiling, and replication. A green cursor is visible on the line starting with '#operationProfiling:'.

```
root@rocket-chat-server: /etc
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: rs0l

34,0-1 69%
```

(рис. 14)

Редактировать роль

Сохранено

Роль

user

Описание

Описание

Leave the description field blank if you dont want to show the role

Область

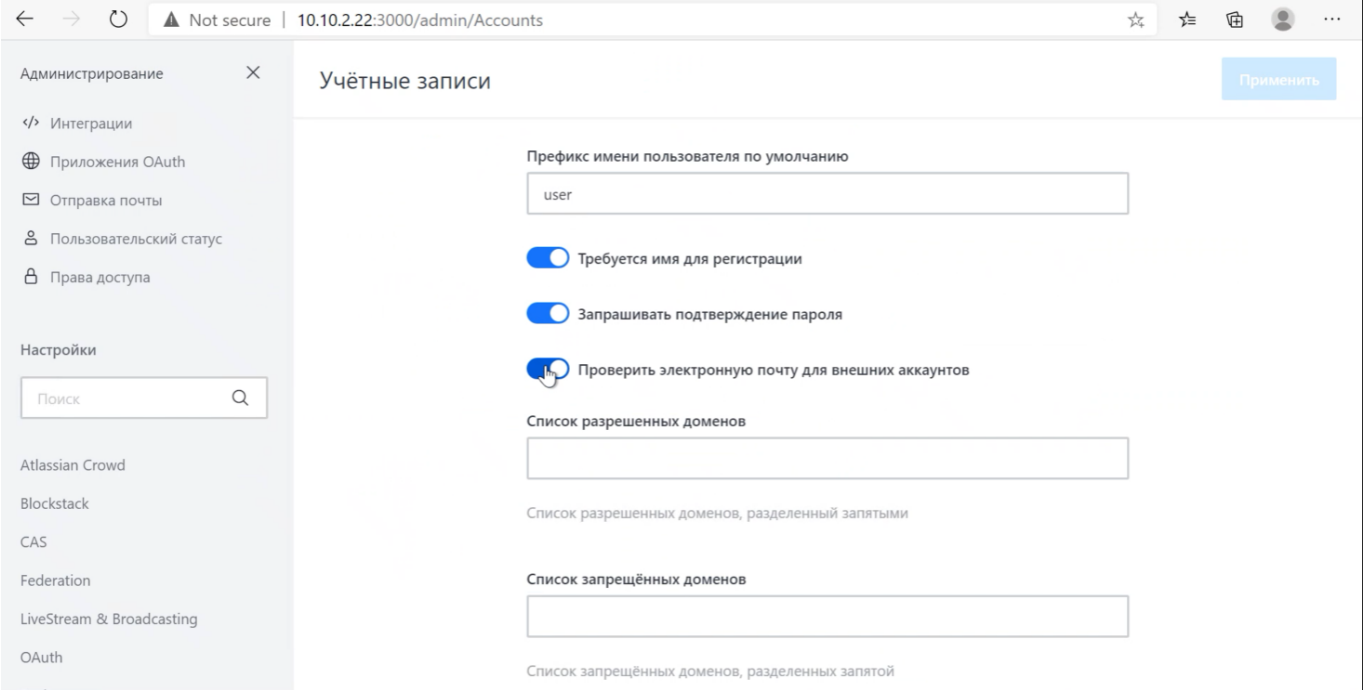
Общие

Пользователи должны использовать двухфакторную аутентификацию

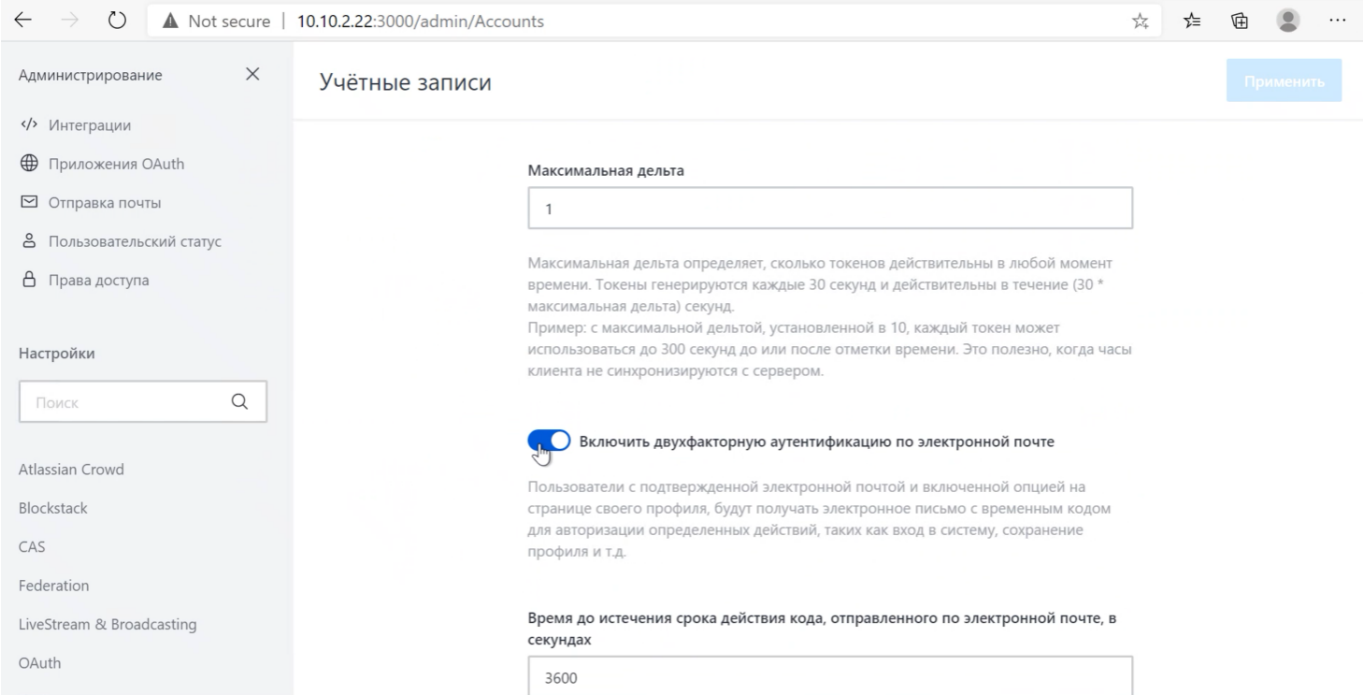
Сохранить

Пользователи с ролью

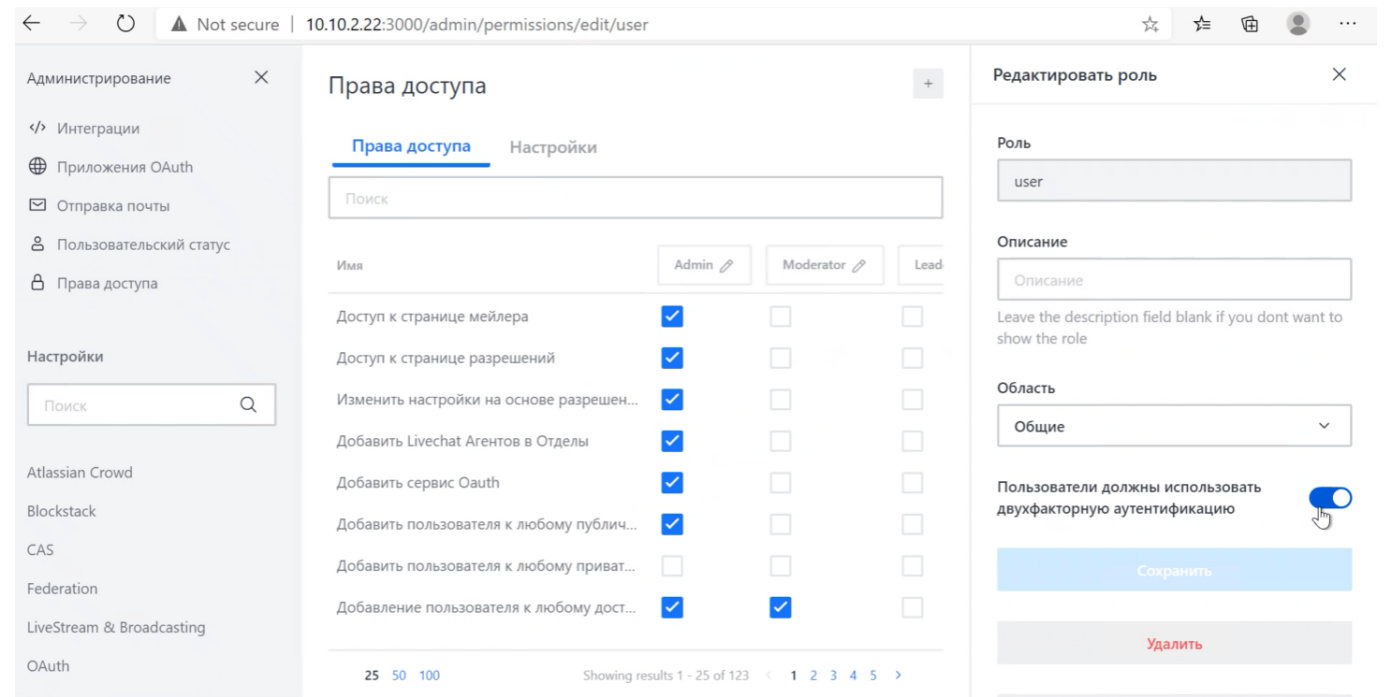
(рис. 15)



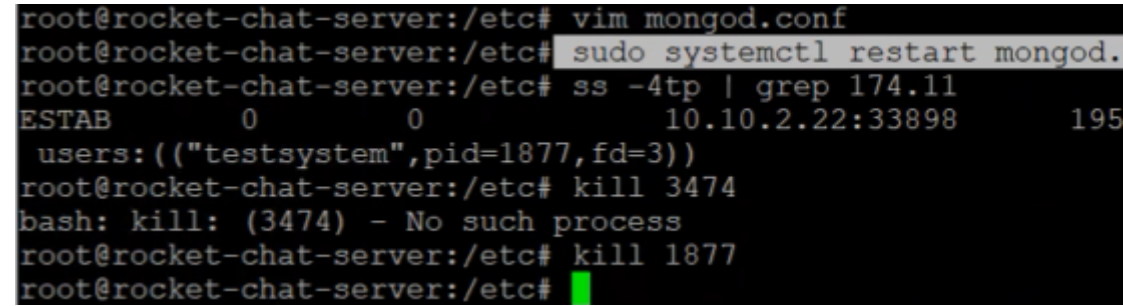
(рис. 16)



(рис. 17)



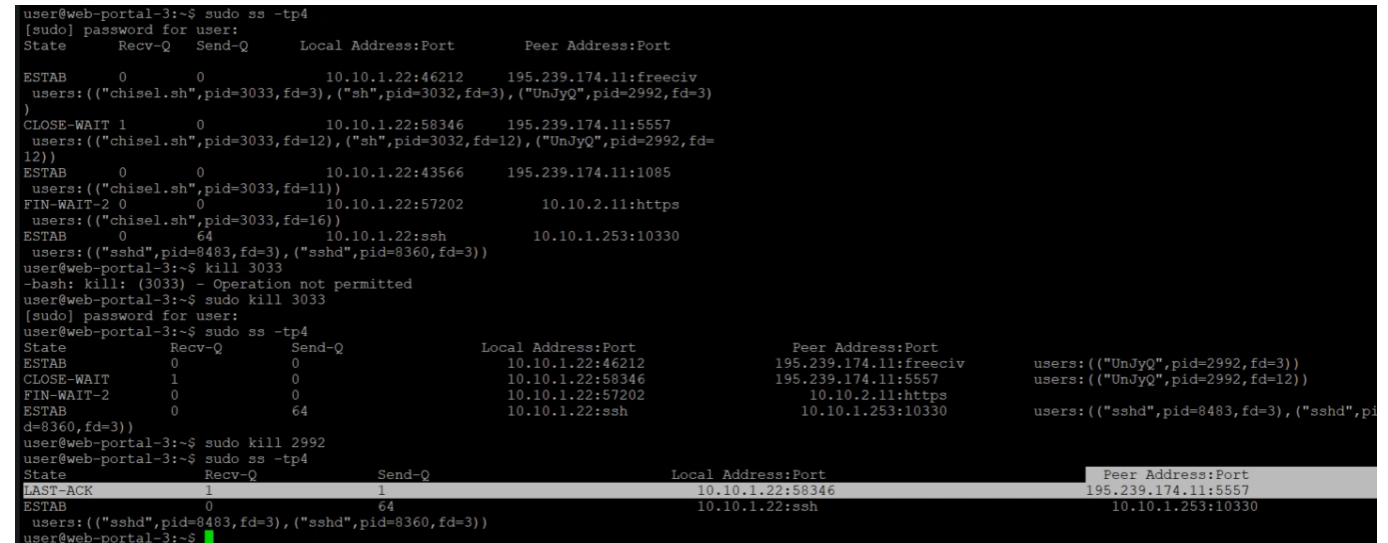
(рис. 18)



(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):

<

WordPress-wpDiscuz (CVE-2020-24186)

Основная информация

Чат

Дата и время события ⓘ

02.10.2025 17:51

Описание ⓘ

устаревшая версия плагина wpDiscuz

Индикаторы компрометации ⓘ

аномально высокое количество обращений к одному файлу

Рекомендации ⓘ

Отключить плагин wpDiscuz или обновить его.

Прикреплённые файлы ⓘ

Не заполнено

(рис. 21)

< **Deface веб-интерфейса**

Основная информация

Чат

Дата и время события ⓘ

02.10.2025 18:02

Описание ⓘ

Данная полезная нагрузка подразумевает изменение интерфейса главной страницы сайта.

Индикаторы компрометации ⓘ

подозрительные файлы, приложения или процессы;

Рекомендации ⓘ

с помощью плагина Updraft Backup/Restore провести рекап и восстановиться на резервную копию

Прикреплённые файлы ⓘ

Не заполнено

(рис. 22)

<

CVE-2021-22911 (NoSQL Injection)

Основная информация

Чат

Дата и время события ⓘ

02.10.2025 20:56

Описание ⓘ

Эксплуатация инъекции сопровождается большим количеством запросов к серверу, так как идет подбор токена для смены пароля непривилегированного пользователя.

Индикаторы компрометации ⓘ

аномально высокое количество обращений к одному файлу;

Рекомендации ⓘ

Для восстановления доступа к аккаунту администратора необходимо сбросить пароль

Прикреплённые файлы ⓘ

Не заполнено

(рис. 23)

<

Proxylogon (CVE 2021-27065)

Основная информация

Чат

Дата и время события ⓘ

02.10.2025 20:03

Описание ⓘ

Данная уязвимость является следствием неэффективного ограничения выбора расположения backup виртуальной директории автономных адресных книг

Индикаторы компрометации ⓘ

подозрительные процессы;

Рекомендации ⓘ

Достаточно ограничить доступ к указанной директории для запрета эксплуатации уязвимости

Прикреплённые файлы ⓘ

Не заполнено

(рис. 24)

<

Web-shell China Chopper

Основная информация

Чат

Дата и время события ⓘ

02.10.2025 20:07

Описание ⓘ

это веб-оболочка размером около 4 килобайт. Этот веб-шелл обычно используется китайскими злоумышленниками для удаленного управления веб-серверами. Эта веб-оболочка состоит из двух частей: клиентского интерфейса (исполняемого файла) и файла хост-приемника на скомпрометированном веб-сервере.

Индикаторы компрометации ⓘ

подозрительные файлы

Рекомендации ⓘ

Для устранения полезной нагрузки необходимо удалить файл веб-оболочки и завершить все соединения между уязвимой машиной и нарушителем

Прикреплённые файлы ⓘ

Не заполнено

(рис. 25)

< **RocketChat meterpreter**

Основная информация **Чат**

Дата и время события ⓘ
12.10.2025 17:39

Описание ⓘ
ель данной полезной нагрузки - получение нарушителем shell-сессии с уязвимым сервером.

Индикаторы компрометации ⓘ
подозрительные SHELL-сессии

Рекомендации ⓘ
Нужно нейтрализовать meterpreter-сессию при помощи утилиты ss с ключом -K, чтобы завершить все сессии с машиной нарушителя необходимо ввести: `sudo ss -K dst HACKER_IP dport = HACKER_PORT`.

Прикреплённые файлы ⓘ
IDS_packet_time-2025-10-12T14_39_57.62295Z_ruleid-3121915.pcap

(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
