

# **Лабораторная работа №1**

## **Кибербезопасность предприятия**

НКНБД-01-22; Аристид Жан, Акопян Сатеник,  
Кадров Виктор, Нве Манге Хоце Херсон Мико,  
Эспиноса Висилита Кристина Микаела,  
НПИБД-01-22; Старикив Данила, НФИБД-02-22;  
Чемоданова Ангелина

# Содержание

<b>1 Цель работы</b>	<b>4</b>
<b>2 Теоретическое введение</b>	<b>5</b>
2.1 Легенда “Защита корпоративного мессенджера” . . . . .	5
2.2 Пояснения уязвимостей . . . . .	5
2.2.1 Атака на CMS WordPress-wpDiscuz . . . . .	6
2.2.2 Атака на почтовый сервер(ProxyLogon) . . . . .	6
2.2.3 Атака на RocketChat . . . . .	7
<b>3 Выполнение лабораторной работы</b>	<b>8</b>
3.1 Атака на CMS WordPress-wpDiscuz . . . . .	8
3.1.1 Устранение последствия Deface веб-интерфейса . . . . .	11
3.1.2 Устранение уязвимости . . . . .	14
3.1.3 Устранение последствия Meterpreter-сессия . . . . .	14
3.2 Атака на почтовый сервер(ProxyLogon) . . . . .	16
3.2.1 Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS	16
3.2.2 Обнаружение средствами Security Onion . . . . .	17
3.2.3 Устранение уязвимости ProxyLogon . . . . .	19
3.2.4 Устранение последствия China Chopper . . . . .	21
3.3 Атака на RocketChat (CVE-2021-22911) . . . . .	21
3.3.1 Закрытие уязвимости RocketChat . . . . .	23
3.3.2 Закрытие уязвимости и последствия . . . . .	24
<b>4 Вывод</b>	<b>27</b>
<b>Список литературы</b>	<b>28</b>

# Список иллюстраций

3.1 События VipNet IDS NS . . . . .	8
3.2 Событие CVE-2020-24186 . . . . .	9
3.3 Анализ SecInoin . . . . .	9
3.4 Логи посещения WordPress . . . . .	10
3.5 Карточка первого инцидента . . . . .	11
3.6 Backup-восстановление . . . . .	12
3.7 Backup-восстановление . . . . .	12
3.8 Выбор компонент . . . . .	13
3.9 Успешное восстановление . . . . .	13
3.10 Отклонение плагина WpDiscuz . . . . .	14
3.11 Все активные сети . . . . .	15
3.12 Закрытие активной сессии атакующего . . . . .	16
3.13 Закрытие активной сессии атакующего . . . . .	16
3.14 Список событий, направленных на уязвимый сервер . . . . .	17
3.15 События, зафиксированные Squert . . . . .	18
3.16 Карточка второго инцидента . . . . .	19
3.17 MAIL/Sites/Default Web Site/ecp . . . . .	20
3.18 MAIL/Sites/Default Web Site/ecp/IP Address and Domain Restrictions . . . . .	20
3.19 Удаление файла AM_backdoor . . . . .	21
3.20 Ошибка подтверждения e-mail . . . . .	22
3.21 Письмо со сбросом пароля . . . . .	22
3.22 Ошибки при выполнении сценариев WebHook . . . . .	22
3.23 Карточка третьего инцидента . . . . .	23
3.24 Изначальный файл конфигурации БД /etc/mongod.conf . . . . .	24
3.25 Измененный файл конфигурации БД /etc/mongod.conf . . . . .	24
3.26 Перезапуск службы: sudo systemctl restart mongod.service . . . . .	25
3.27 Закрытие сессии с нарушителем . . . . .	26

# **1 Цель работы**

Основная цель данной лабораторной работы заключается в выполнении тренировки “Защита корпоративного мессенджера” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы необходимо освоить практические навыки выявления, анализа и устранения уязвимостей в корпоративной инфраструктуре, а также освоить навыки отработки действий по нейтрализации последствий успешных атак.

## **2 Теоретическое введение**

### **2.1 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[1].

### **2.2 Пояснения уязвимостей**

Уязвимости:

- WordPress-wpDiscuz (CVE-2020-24186)
- Proxylogon (CVE 2020-26855, CVE 2021-27065)
- Rocket.Chat (CVE-2021-22911, CVE-2022-0847)

## **2.2.1 Атака на CMS WordPress-wpDiscuz**

WpDiscuz – один из плагинов CMS WordPress для создания комментариев на базе Ajax.

Версиях с 7.0.0 по 7.0.4 включительно существует уязвимость File Upload(CVE-2020-24186), которая позволяет получить RCE, если прикрепить любой файл(например, код на php) в поле для комментариев и загрузить на сервер. Данный процесс можно выполнить без аутентификации. После создания файла с полезной нагрузкой нарушитель будет производить POST-запрос с определенными параметрами по ссылке <http://webportal3.ampire.corp/index.php/wp-admin/admin-ajax.php> для загрузки файла.

Факт загрузки будет детектироваться в журнале активности в WordPress, в котором записывается хронологическая запись последовательности изменений и действий[2].

## **2.2.2 Атака на почтовый сервер(ProxyLogon)**

Уязвимость ProxyLogon (CVE 2020-26855 (Server-Side Request Forgery)) представляет собой SSRF в Exchange Server, позволяющую обойти аутентификацию и выдать себя за администратора. В сценарии данная уязвимость используется в связке с CVE2021-27065(запись файла в произвольную директорию).

SSRF - подделка запроса на стороне сервера – это атака, которая позволяет отправлять запросы от имени сервера к внешним или внутренним ресурсам.

При помощи ProxyLogon атакующий может выдать себя, например, за администратора и аутентифицироваться в панели управления Exchange(ECP), после чего перезаписать любой файл в системе при помощи CVE-2021-27065.

Уязвимости ProxyLogon подвержены все Exchange Server 2016 до версии 15.01.2106.013[3].

### **2.2.3 Атака на RocketChat**

Уязвимость CVE-2021-22911 представляет собой сочетание из двух SQL инъекций:

- слепая NoSQL-инъекция (позволяет украдь токен сброса пароля пользователя);
- NoSQL-инъекция№2: повышение привилегий.

Уязвимость CVE-2022-0847 (Dirty Pipe) представляет собой уязвимость повышения привилегий, находящуюся в самом ядре Linux версии 5.8 и выше[4].

# 3 Выполнение лабораторной работы

## 3.1 Атака на CMS WordPress-wpDiscuz

Для начала перейдем в ViPNet IDS NS[5], отфильтруем события и обнаружим атаку на CMS WordPress(рис. 3.1).

Event 00:12:22.30

General information

- Date and time: 00:12:22.306 07/10/2023
- Capture interface: eth2
- Severity: High
- Event type: Signature event
- Protocol: TCP
- Event code: 3011768
- Client application: MySQL 5.0 Windows 8.1 (10.0.6.160) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46
- Resource DNS name: 195.239.174.87

Analysis rule

- Class: web-application-attack
- Group: web\_server
- Name: ET WEB\_SERVER PHP tags in HTTP POST

Description: This rule detects attacks against a web server.

Text:

```
alert tcp $EXTERNAL_NET any->$INTERNAL_NETS_BUT_ME_PORTS ($msg: "ET WEB_SERVER PHP tags in HTTP POST from established connection '$HTTP_PORTS' to '$INTERNAL_NETS_BUT_ME_PORTS' content: '$http["content"]' mismatched pattern only http client body relevance getfa c.eans.edu/diley/infowid-9427/class-type: web-application-attack;id: 203176; $ver: $ruledata; affected_asset_id: affected_product.php.php; affected_vendor_id: 1; attack_target_Web_Server; created_at: 2010-09-28; signature_severity: Informational; $tag: category:Explorator; updated_at: 2013-01-22");
```

Description of vulnerabilities: url: <http://c.eans.edu/diley.htm?stored=9478>

Рис. 3.1: События ViPNet IDS NS

Проанализировав события, поймем, что перед нами уязвимость CVE-2020-24186. Получим дополнительную информацию об этой уязвимости(рис. 3.2).

The screenshot shows the AMpIre-IDS-1 interface for ViPNet IDS NS. On the left is a navigation sidebar with options like Dashboard, Events, Reports, Management, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, and Audit Log. The main area displays a table of events for the last 24 hours. One specific event is highlighted in yellow: "Event 00:12:22.30". This event details a "Signature event" on TCP port 239. The event information includes:

- Date and time: 00:12:22.306 - 201768
- Event code: 3153936
- Rule name: ET WEB\_SERVER.POLICY...
- Class: web-application-attack
- Protocol: TCP
- Source IP: 195.239.174... 45315
- Source port: 10.10.1.22
- Destination IP: 80
- Destination port: 10.10.1.22
- Direction: → ←
- Severity: High
- Event type: Signature event
- Protocol: TCP
- Event code: 3153936
- Client application: Microsoft/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46
- Resource DNS name: 195.239.174.87

The analysis rule is described as "AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)". The text field contains a detailed exploit description, and the description of vulnerabilities points to CVE-2020-24186.

Рис. 3.2: Событие CVE-2020-24186

Через ViPNet IDS NS выявим критические события на почтовом сервере MS Exchange, заметим загрузку подозрительных файлов с использованием фреймворка Metasploit.

Откроем SecInoin[6], увидим подозрительный http-запрос и ответ сервера, изучим полученный пакет и найдем там использование WinAPI-функций, а также байтовый массив для инъектирования кода в память. (рис. 3.3)

The screenshot shows the SecInoin interface. At the top, it displays a summary of 2 events, 1 category, 1 activity, and a timestamp of 21:15:28. The main area shows a table of network events:

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
2	ST	2025-09-14 21:15:28	10.10.2.11	1	RFC1918 (.lo)	195.239.174.11	1	RUSSIAN FEDERATION (.ru)
	RT	2025-09-14 21:15:28	3.25	10.10.2.11	7963	195.239.174.11	8010	ET INFO PS1 Powershell File Request
	RT	2025-09-14 21:15:28	3.29	10.10.2.11	7964	195.239.174.11	8010	ET INFO PS1 Powershell File Request

Below this, another table shows a single event:

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
2	RT	2025-09-14 21:15:28	ET INFO Windows Powershell User-Agent Usage	2033355	6	1.471%		

Рис. 3.3: Анализ SecInoin

Мы можем прийти к выводам по технике атаки:

- Доставка: через http-запрос к скрипту;
- Выполнение: Инжектирование кода в память через VirtualAlloc + CreateThread;
- Цель: Обход антивируса(без записи на диск)

и по индикаторам компрометации(IoC):

- IP-адрес: 195.239.174.11;
- Порт: 8010/TCP; Хэш(SHA-256): Не вычислен(требуется анализ файла);
- Сигнатура кода: Использование VirtualAlloc + шелл-код

Атака оканчивается загрузкой бинарного файла в формате ELF, который, вероятно, содержит вредоносный код или экспloit на узел 10.10.2.22.

Логи посещения WordPress. (рис. 3.4)

```
user@web-portal-3:/var/log/apache2$ grep "195" access.log
195.239.174.11 - - [14/Sep/2025:21:12:17 +0000] "POST /wp-login.php HTTP/1.1" 302 1118 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:17 +0000] "GET /wp-admin/ HTTP/1.1" 302 450 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:18 +0000] "GET /wp-login.php?redirect_to=http%3A%2F%2Fwebportal3.ampire.corp%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 4391 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:18 +0000] "GET /wp-admin/plugins.php HTTP/1.1" 200 27192 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:21 +0000] "GET /wp-content/plugins/wp-discuz/readme.txt HTTP/1.1" 200 54253 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46"
195.239.174.11 - - [14/Sep/2025:21:12:21 +0000] "GET /index.php/2021/07/26/hello-world/ HTTP/1.1" 200 62591 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
```

Рис. 3.4: Логи посещения WordPress

Создадим карточку инцидента[7]. (рис. 3.5)

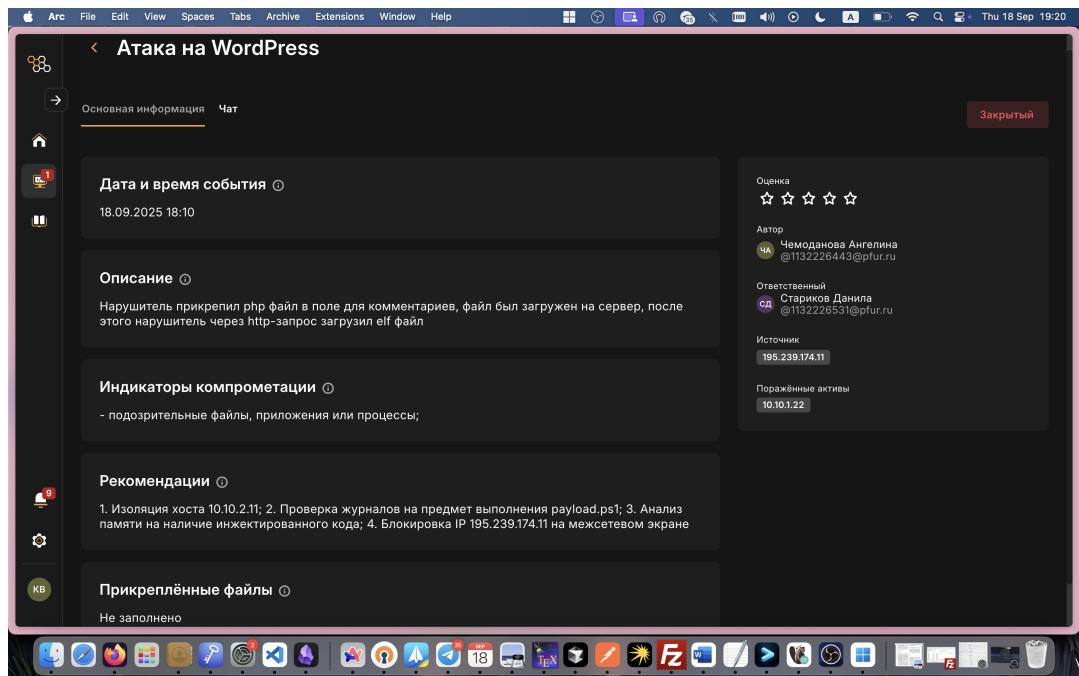


Рис. 3.5: Карточка первого инцидента

### 3.1.1 Устранение последствия Deface веб-интерфейса

Если открыть страницу сайта компании, указать в строке браузера IP-адрес 10.10.1.22 (<http://webportal3.ampire.corp>), то можно заметить, что блог после атаки выглядит следующим образом: до использования полезной нагрузки на странице сайта красный крупнотоннажный грузовой автомобиль и после использования полезной нагрузки картинка “hacked”.

На веб-сервере работает ftp-сервер vsftpd, который дает возможность плагину Updraft сохранять и скачивать backup. Таким образом, можно выполнить backup-восстановление из последнего файла.

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

Этапы восстановления(рис. 3.6 - рис. 3.7):

- в панели управления на странице Plugins найти плагин резервного восстановления UpdraftPlus, открыть настройки.

- для восстановления нажать Restore на последней резервной копии.

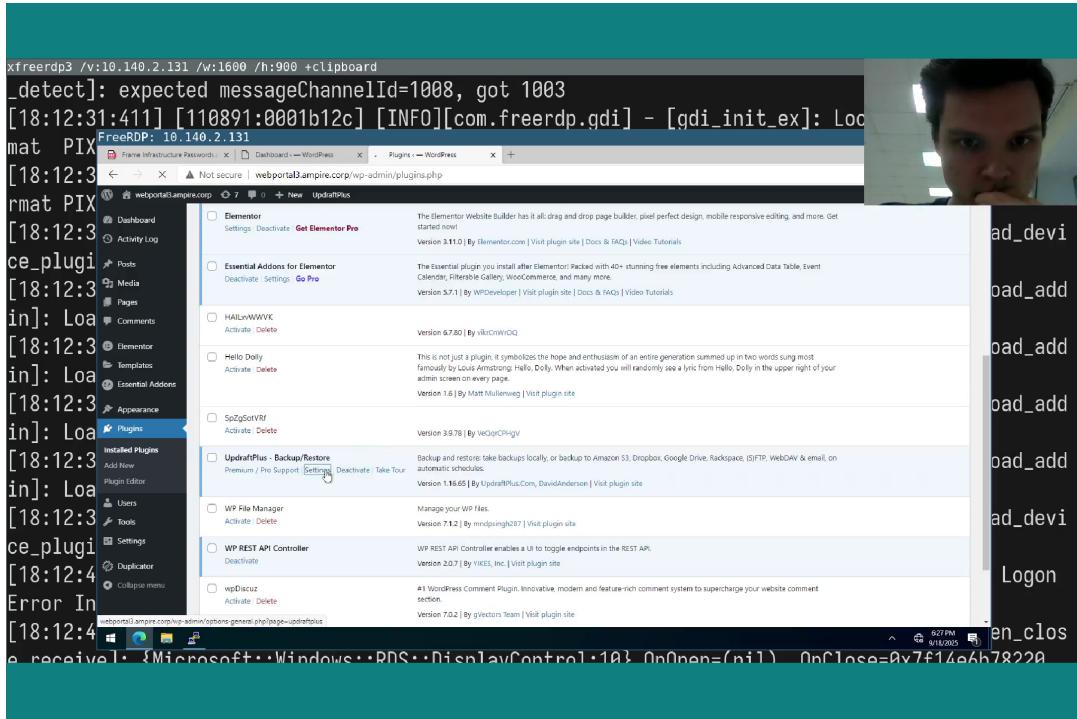


Рис. 3.6: Backup-восстановление

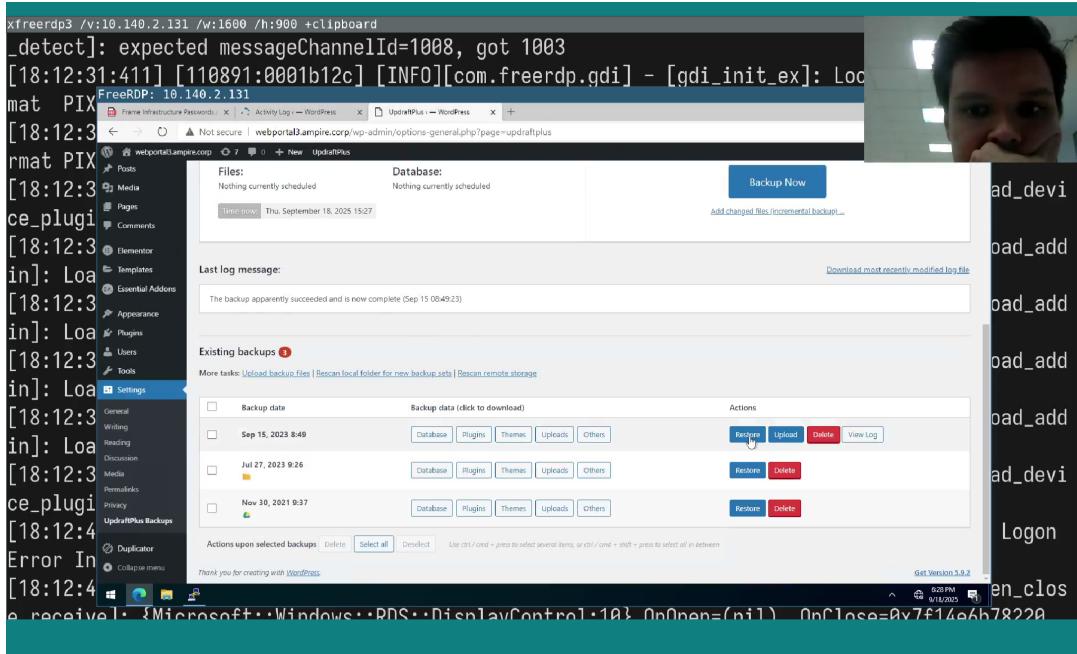


Рис. 3.7: Backup-восстановление

В выпадающем окне выбора компонентов для восстановления выбрать только “Themes” и “Uploads”. (рис. 3.8)

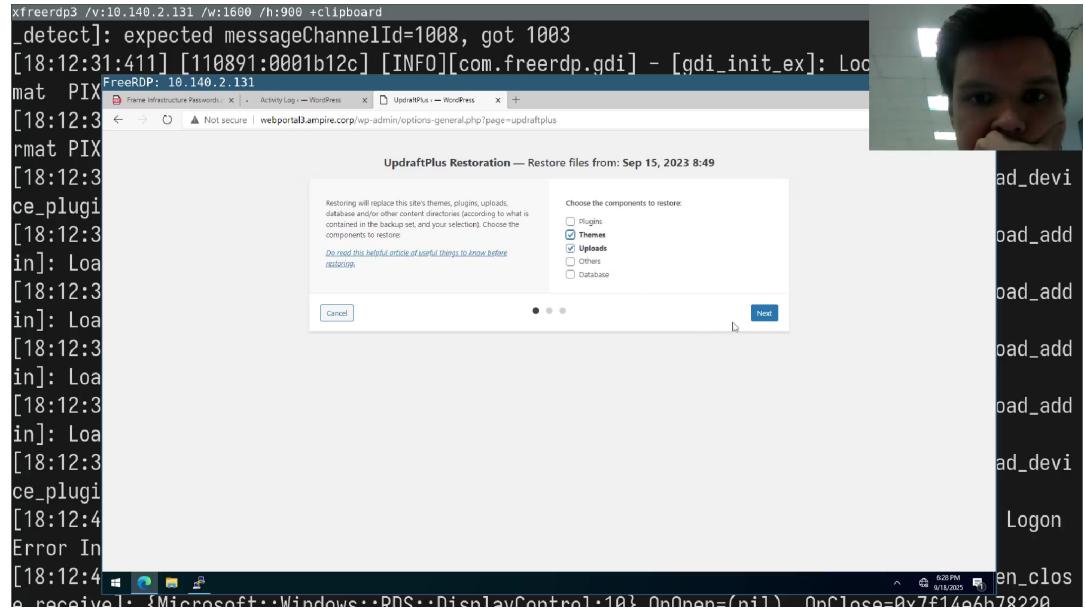


Рис. 3.8: Выбор компонент

Успешное восстановление. (рис. 3.9)

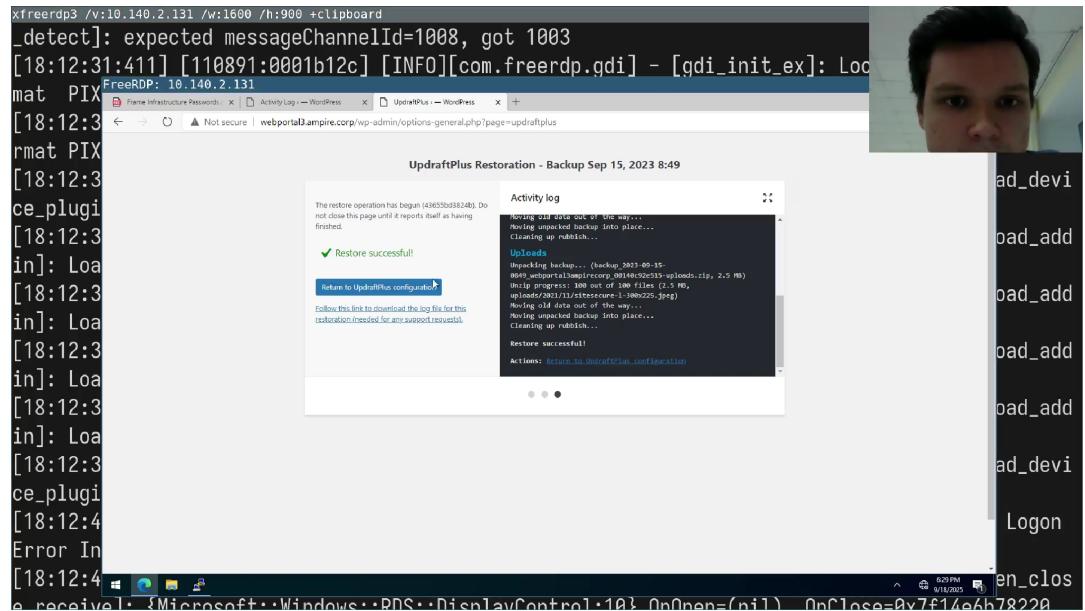


Рис. 3.9: Успешное восстановление

После обновления страницы откроется первоначальная картинка сайта.

### 3.1.2 Устранение уязвимости

Закрытие уязвимости можно осуществить несколькими способами:

- отключение плагина WpDiscuz;
- обновление версии WpDiscuz до версии 7.0.5 и выше(при наличии интернета).

Для отключения плагина в левой части панели инструментов необходимо открыть раздел Plugins, далее нажать на опцию Deactivate. Также можно полностью удалить плагин с сайта аналогичным образом с помощью опции Delete. (рис. 3.10)

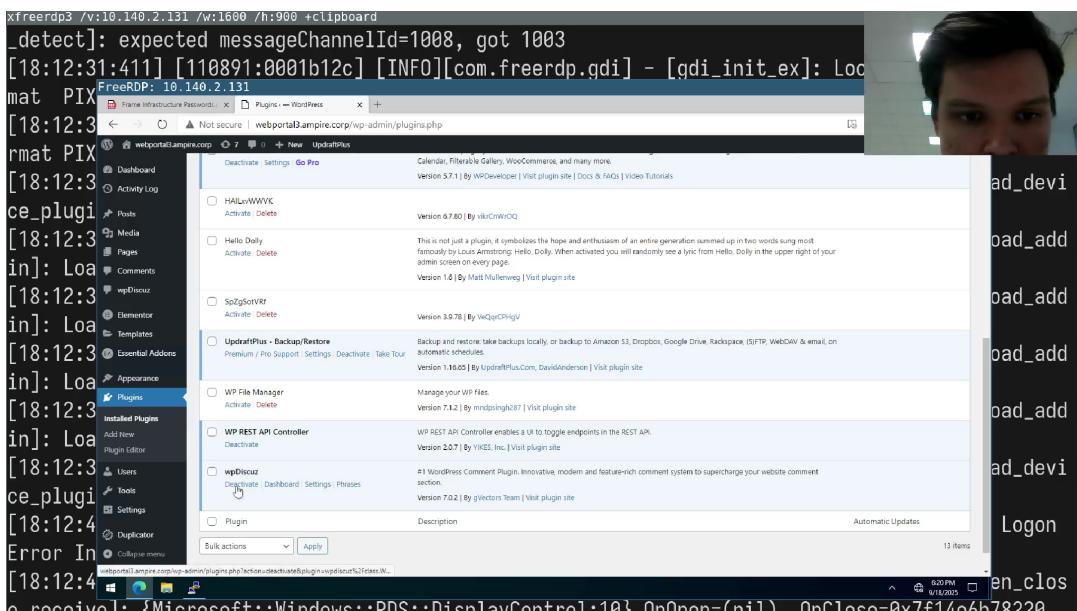


Рис. 3.10: Отключение плагина WpDiscuz

### 3.1.3 Устранение последствия Meterpreter-сессия

Также необходимо закрыть активные сессии с атакующим.

Для обнаружения meterpreter-сессии необходимо проверить сокеты уязвимой машины на подключение к определенному порту машины нарушителя с помощью утилиты ss. Просмотреть сокеты только нужного протокола TCP и

отфильтровать данные (например, вывести только активные TCP-соединения) можно с помощью команды: ss -tnp.

Откроем все активные сессии. Видим там сеть атакующего. (рис. 3.11)

```

xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
_detect]: expected messageChannelId=1008, got 1003
[18:12:31:411] [110891:0001b12c] [INFO][com.freerdp.gdi] - [gdi_init_ex]: Local mat PIX
FreeRDP: 10.140.2.131
mat PIX
[18:12:3 u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 20358
u_str ESTAB 0 0 /run/systemd/journal/stdout 17722
u_str ESTAB 0 0 * 41056
u_str ESTAB 0 0 * 41057
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 17723
u_str ESTAB 0 0 * 17720
u_str ESTAB 0 0 * 17725
u_str ESTAB 0 0 * 18685
u_str ESTAB 0 0 /run/systemd/journal/stdout 14928
u_str ESTAB 0 0 /run/systemd/journal/stdout 20713
[18:12:3 u_str ESTAB 0 0 * 18686
u_str ESTAB 0 0 * 17722
u_str ESTAB 0 0 * 20713
u_str ESTAB 0 0 * 18686
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 20307
u_str ESTAB 0 0 * 18387
u_str ESTAB 0 0 /run/systemd/journal/stdout 20470
u_str ESTAB 0 0 * 17557
u_str ESTAB 0 0 * 18388
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 18389
u_str ESTAB 0 0 * 20831
[18:12:3 u_str ESTAB 0 0 /run/systemd/journal/stdout 20714
u_str ESTAB 0 0 * 21856
u_str ESTAB 0 0 /run/systemd/journal/stdout 17721
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 20352
u_str ESTAB 0 0 /run/systemd/journal/stdout 19306
[18:12:3 u_str ESTAB 0 0 * 17650
u_str ESTAB 0 0 * 14488
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 21316
u_str ESTAB 0 0 * 18611
u_str ESTAB 0 0 * 18615
[18:12:3 u_str ESTAB 0 0 /run/systemd/journal/stdout 15320
u_str ESTAB 0 0 /run/systemd/journal/stdout 14929
u_str ESTAB 0 0 * 16266
u_str ESTAB 0 0 * 18847
u_str ESTAB 0 0 * 19306
ce_plugi
tcp FIN-WAIT-2 0 0 10.10.1.22:58904 10.10.2.11:https
tcp ESTAB 0 0 10.10.1.22:50720 195.239.174.11:6065
tcp ESTAB 0 0 10.10.1.22:38910 195.239.174.11:freeniciv
tcp CLOSE-WAIT 0 0 10.10.2.21:38944 195.239.174.11:5557
Error In
admin@web-portal-3:~$ ^ 521PM 9/18/2015
e_receive. {Microsoft::Windows::RDS::DisplayControl.101 OnOpen=(nil) OnClose=0x7f14a6b78220

```

Рис. 3.11: Все активные сети

Для закрытия вредоносного сокета необходимо завершить процесс, использующийся для поддержания соединения. При завершении процесса определить уникальный идентификатор процесса (PID) и прописать команду kill с соответствующими параметрами.

Закрываем активную сессию атакующего. (рис. 3.12 - рис. 3.13)

```

xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
[18:12:31:411] [110891:0001b12c] [INFO][com.freerdp.gdi] - [gdi_init_ex]: Local
mat PIX
[admin@web-portal-3 ~]
[18:12:31] --query=QUERY --socket=QUERY
    QUERY := (all|inet|tcp|udp|raw|unix|unix_dgram|unix_stream|unix_segpocket|packet|netlink|vsock_stream|vsock_dgram),Q
rmat PIX
-D, --diagFILE   Dump raw information about TCP sockets to FILE
-E, --filterFILE read filter information from FILE
[18:12:31] STATE-FILTER := (all|connected|synthesized|listen|closed|recv-Q|fin-wait-[1,2]|time-wait|closed|close-wait|last-ack|listening|closing)
TCP-FILTER := (all|established|syn-sent|syn-recv|fin-wait-[1,2]|time-wait|close-wait|last-ack|closing)
connected := (established|syn-sent|syn-recv|fin-wait-[1,2]|time-wait|close-wait|last-ack|closing)
synthesized := (established|syn-recv|fin-wait-[1,2]|time-wait|close-wait|last-ack|closing)
bucket := (syn-recv|time-wait)
big := (syn-sent|fin-wait-[1,2]|closed|close-wait|last-ack|listening|closing)
admin@web-portal-3:~$ ss -R dst 195.239.174.11
SOCK_DESTROY answers: Operation not permitted
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31] Error: an inet prefix is expected rather than "195.239.174.". Cannot parse dst/src address.
in]: Loo
[18:12:31] admin@web-portal-3:~$ ss -tp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31] FIN-WAIT-2      0          0          10.10.1.22:59004      10.10.2.11:https
[18:12:31] ESTAB      0          0          10.10.1.22:590720     195.239.174.11:1085
[18:12:31] ESTAB      210         0          10.10.1.22:33136     195.239.174.12:https
[18:12:31] ESTAB      0          64         10.10.1.22:sshd      10.10.1.253:59827
[18:12:31] ESTAB      0          0          10.10.1.22:39210     195.239.174.11:freeciv
[18:12:31] CLOSE-WAIT      0          0          10.10.1.22:38944     195.239.174.11:5557
admin@web-portal-3:~$ ss -R dst 195.239.174.11
Error: an inet prefix is expected rather than "195.239.174.". Cannot parse dst/src address.
[18:12:31] admin@web-portal-3:~$ ss -R dst 195.239.174.11
SOCK_DESTROY answers: Operation not permitted
[18:12:31] admin@web-portal-3:~$ sudo ss -K dst 195.239.174.11
[18:12:31] [sudo] password for admin:
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31] tcp      ESTAB      0          0          10.10.1.22:59020     195.239.174.11:1085
[18:12:31] tcp      ESTAB      0          0          10.10.1.22:39210     195.239.174.11:freeciv
[18:12:31] Error In      CLOSE-WAIT      0          0          10.10.1.22:38944     195.239.174.11:5557
admin@web-portal-3:~$ 

```

Рис. 3.12: Закрытие активной сессии атакующего

```

user@web-portal-3:~$ sudo ss --kill dst 195.239.174.11
[18:12:31] [sudo] password for user:
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31] tcp      CLOSE-WAIT      1          0          10.10.1.22:51092     195.239.174.11:5557
[18:12:31] tcp      ESTAB      0          0          10.10.1.22:48244     195.239.174.11:1085
[18:12:31] tcp      ESTAB      0          0          10.10.1.22:60528     195.239.174.11:freeciv

```

Рис. 3.13: Закрытие активной сессии атакующего

Таким образом, meterpreter-сессия между машиной нарушителя и уязвимым хостом будет успешно завершена.

## 3.2 Атака на почтовый сервер(ProxyLogon)

### 3.2.1 Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS

#### NS

Proxylogon представляет собой SSRF в Exchange Server, позволяющую обойти аутентификацию и выдать себя за администратора. В сценарии данная уязвимость используется в связке с CVE 2021-27065 (запись файла в произвольную директорию). Уязвимости Proxylogon подвержены все Exchange Server 2016, до версии 15.01.2106.013.

Сетевой сенсор ViPNet IDS NS[5] во время атаки детектирует несколько событий, которые потенциально могут быть связаны с эксплуатацией уязвимости на уязвимом хосте(рис. 3.14)

The screenshot shows the ViPNet IDS NS web interface. On the left is a sidebar with navigation links: Monitoring, Dashboard, Events (selected), Reports, Management, Network Environment, Analysis Methods, Rules, Notifications, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit logs. The main area has a title 'Events' and a sub-section 'Events for recent 24 hours'. It lists several events with columns: Date and time, Event code, Q., Rule name, and Class. Some events are highlighted in red, indicating suspicious or malicious activity. To the right, a specific event is detailed: 'Event 00:15:30.2025644'. The details pane includes sections for 'Capture interface', 'Severity' (Signature event), 'Event type' (TCP), 'Protocol' (TCP), 'Event code' (2025644), and 'Analysis rule'. The analysis rule is named 'ET TROJAN Possible Metasploit Payload Common Construct Bind API (from server)' and describes it as detecting malware activity. Below the rule is a 'Text' section containing a complex alert rule definition. At the bottom of the details pane, there is a timestamp '20:27:47 15.09.2025'.

Рис. 3.14: Список событий, направленных на уязвимый сервер

В списке событий присутствуют признаки загрузки на уязвимый хост подозрительных файлов в формате .exe. Также зафиксирована активность вредоносного программного обеспечения Metasploit.

### 3.2.2 Обнаружение средствами Security Onion

Для обнаружения последствий эксплуатации в Security Onion[6] следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. Для просмотра данных о событиях нужно открыть ссылку на веб-приложение Squert на главной странице Security Onion.

На скриншоте представлены события, зафиксированные веб-приложением Squert(рис. 3.15). Данные события аналогичны событиям, зафиксированным сетевым сенсором ViPNet IDS NS.

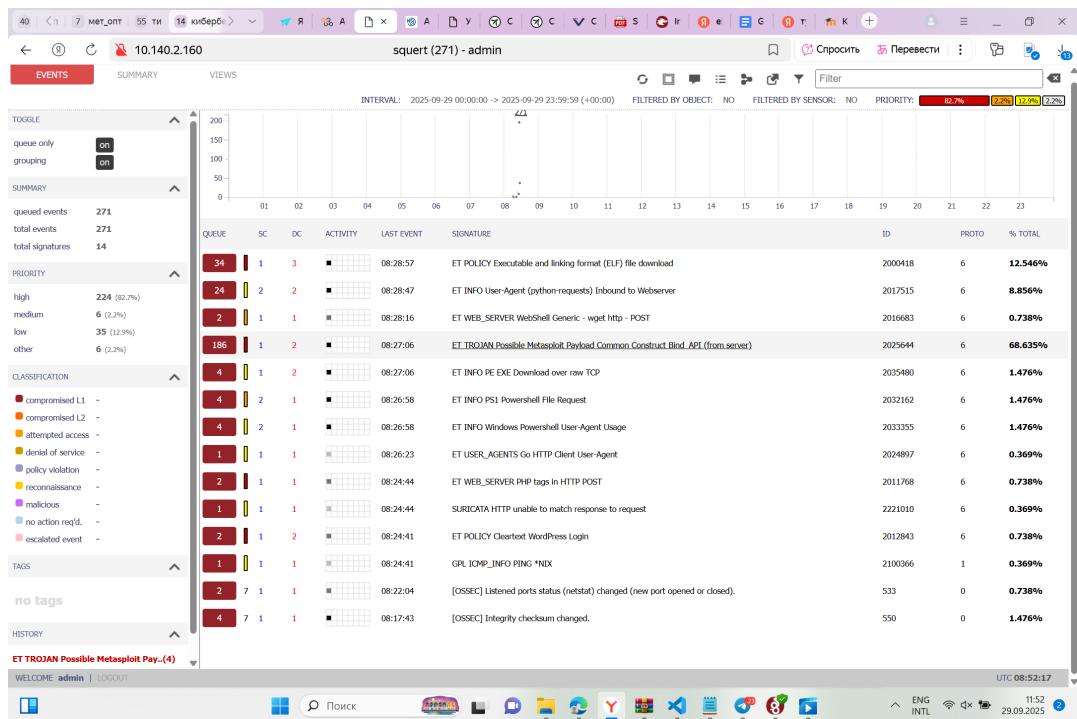


Рис. 3.15: События, зафиксированные Squert

Необходимо выбрать любое из событий и нажать соответствующий «EVENT ID». Событие подробнее приведено в содержимом сетевых пакетов, которые использует нарушитель для работы с уязвимым хостом и эксплуатации уязвимости.

Заполним карточку второго инцидента. (рис. 3.16)

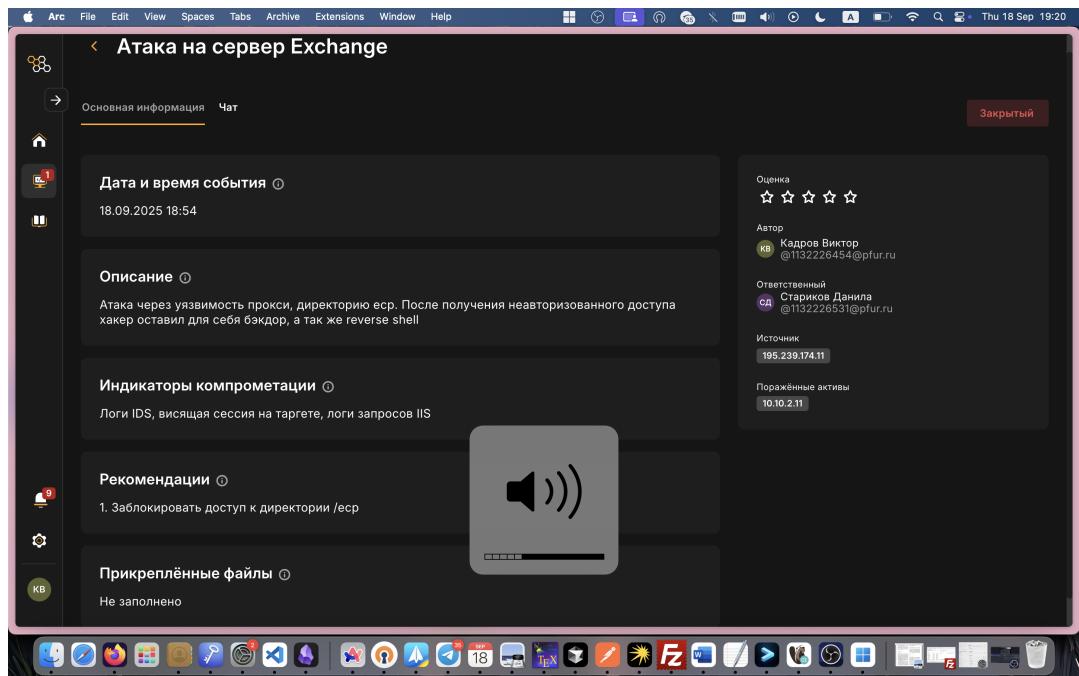


Рис. 3.16: Карточка второго инцидента

### 3.2.3 Устранение уязвимости ProxyLogon

Во время эксплуатации уязвимости ProxyLogon нарушитель совершает GET и POST запросы к /ecp. Достаточно ограничить доступ к вышеуказанной директории чтобы уязвимость не эксплуатировалась.

Открыть Internet Information Services (IIS) Manager. Для этого необходимо нажать сочетание клавиш «Win+R», ввести «inetmgr» и нажать «Enter». В открывшемся окне перейти во вкладку MAIL/Sites/Default Web Site/ecp и нажать на IP Address and Domain Restrictions. Далее в «Edit Feature Settings» – «Access for unspecified clients» выбрать пункт «Deny» и нажать «OK»(рис. 3.17 - рис. 3.18)

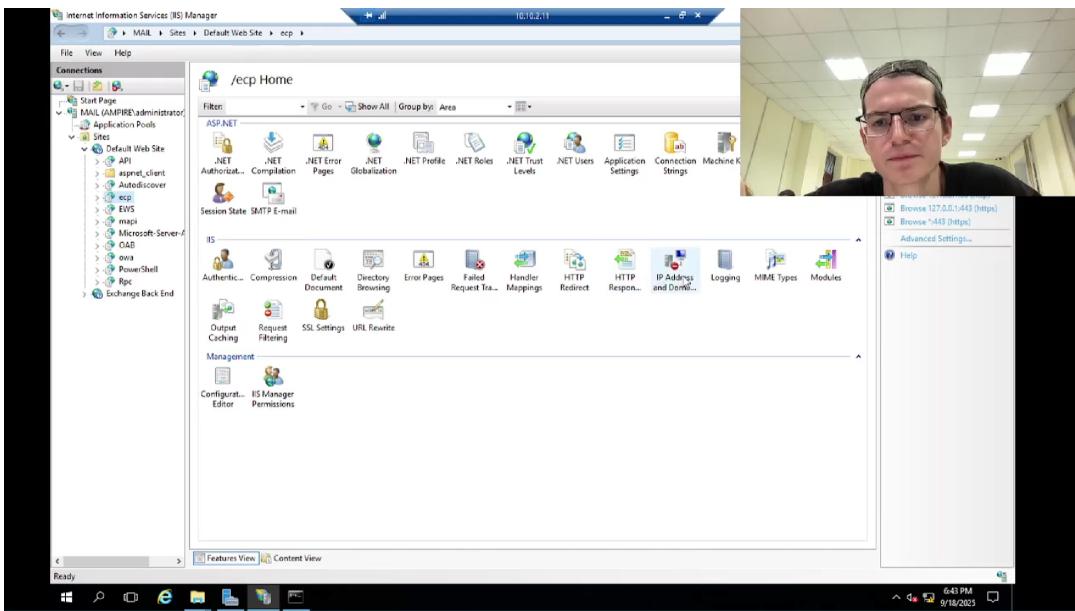


Рис. 3.17: MAIL/Sites/Default Web Site/ecp

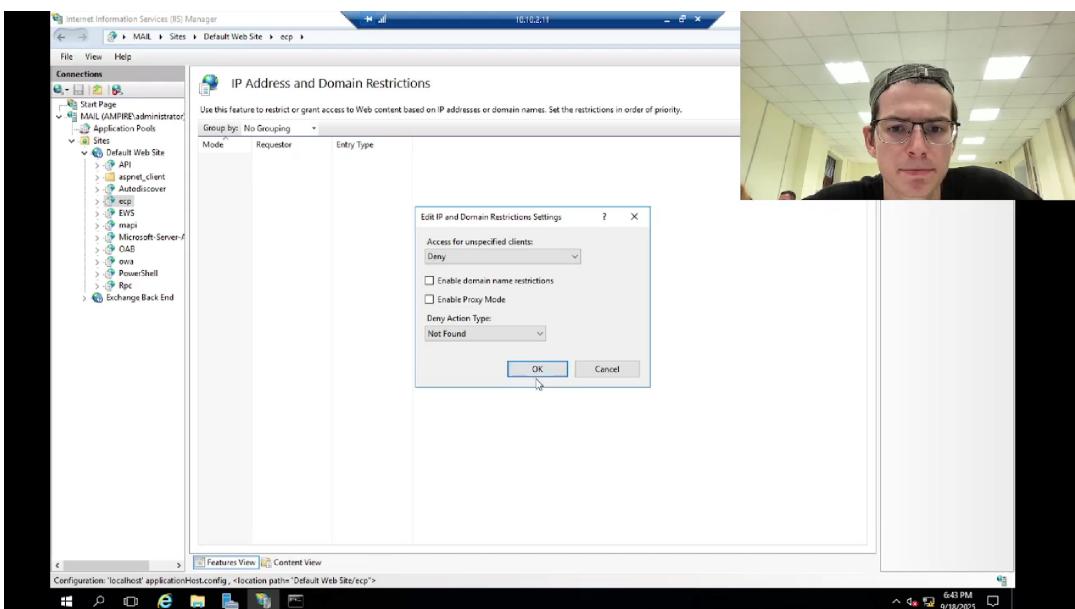


Рис. 3.18: MAIL/Sites/Default Web Site/ecp/IP Address and Domain Restrictions

Следует отметить, что индикатор устранения уязвимости не изменится, пока не устранено последствие в виде вредоносного meterpreter-соединения. Рекомендации по закрытию вредоносного соединения представлены ниже.

### 3.2.4 Устранение последствия China Chopper

Backdoor “China Chopper” можно найти в очевидной для таких атак директории C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/owa/auth/AM\_backdoor.aspx. Большинство РОС (проверок концепций) эксплуатации уязвимости Proxylogon записывают файл именно по данному адресу, что выполняется для доступа backdoor(backdoor — «чёрный ход», дословно «задняя дверь» — уязвимость, которая даёт несанкционированный доступ к компьютеру, смартфону и т. п..) без авторизации из веб-директории owa/auth. При необходимости последствие можно записать в другую директорию.

Для устранения последствия необходимо: - удалить файл веб-оболочки по пути C:/ProgramFiles/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/..auth/;(рис. 3.19)

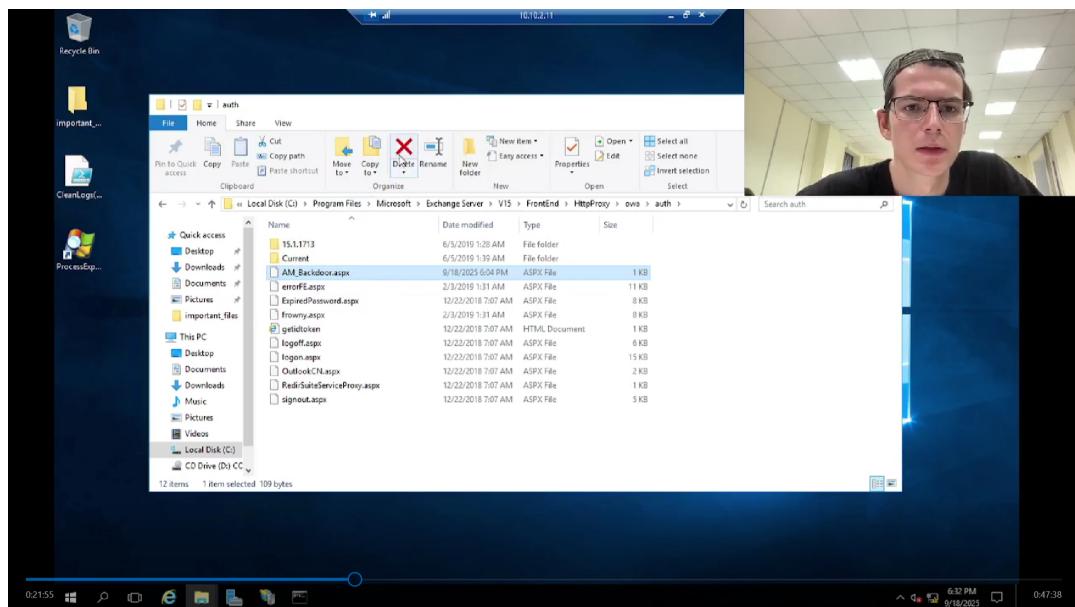


Рис. 3.19: Удаление файла AM\_backdoor

## 3.3 Атака на RocketChat (CVE-2021-22911)

Признак эксплуатации NoSQL-инъекции[8] - это невозможность осуществления входа на веб-интерфейс под учетными данными администратора (логин:

admin@rocket-local.com, пароль: qwe123!@#). В syslog пишутся следующие строчки:

- ошибка отправки приветственного сообщения при регистрации нового аккаунта(рис. 3.20);
- письмо для сброса пароля админа(рис. 3.21);
- ошибки при выполнении сценариев WebHook(рис. 3.22).

```
root@rocket-chat-server:~# less /var/log/syslog | grep smtpd
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: NOQUEUE: reject: RCPT from localhost[127.0.0.1]: 550 5.1.1 <hacker@hacker.com>; Recipient address rejected: hacker.com; from=<rocketchat@rocket-local.com> to=<hacker@hacker.com> proto=ESMTP helo=<[127.0.0.1]>
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: lost connection after RCPT from localhost[127.0.0.1]
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=0/1 commands=2/3
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: ECAC1748BD: client=localhost[127.0.0.1]
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 commands=4
root@rocket-chat-server:~#
```

Рис. 3.20: Ошибка подтверждения e-mail

```
root@rocket-chat-server:/var/log# less /var/log/syslog | grep -n postfix
29:Sep 29 08:17:34 rocket-chat-server postfix/postfix-script[1279]: warning: symlink leaves directory: /etc/postfix//.makefiles.out
32:Sep 29 08:17:34 rocket-chat-server postfix/postfix-script[1463]: starting the Postfix mail system
33:Sep 29 08:17:34 rocket-chat-server postfix/master[1465]: daemon started -- version 3.4.13, configuration /etc/postfix
254:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
255:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: NOQUEUE: reject: RCPT from localhost[127.0.0.1]: 550 5.1.1 <hacker@hacker.com>; Recipient address rejected: hacker.com; from=<rocketchat@rocket-local.com> to=<hacker@hacker.com> proto=ESMTP helo=<[127.0.0.1]>
256:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: lost connection after RCPT from localhost[127.0.0.1]
257:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=0/1 commands=2/3
260:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
261:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: ECAC1748BD: client=localhost[127.0.0.1]
262:Sep 29 08:27:55 rocket-chat-server postfix/cleanup[1882]: ECAC1748BD: message-id=<83dc9a2b-d7a7-39de-e94b-58eb84dcdb88@rocket-local.com>
263:Sep 29 08:27:55 rocket-chat-server postfix/qmgr[1468]: ECAC1748BD: from=<rocketchat@rocket-local.com>, size=5870, nrcpt=1 (queue active)
264:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 commands=4
265:Sep 29 08:27:56 rocket-chat-server postfix/local[1883]: ECAC1748BD: to=<admin@rocket-local.com>, relay=local, delay=0.06, delays=0.03/0.02/0.0, dsn=2.0.0, status=sent (delivered to mailbox)
266:Sep 29 08:27:56 rocket-chat-server postfix/qmgr[1468]: ECAC1748BD: removed
root@rocket-chat-server:/var/log#
```

Рис. 3.21: Письмо со сбросом пароля

```
Sep 29 08:28:22 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" not in Trigger rce ]
Sep 29 08:28:34 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" not in Trigger rce ]
Sep 29 08:28:48 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" not in Trigger rce ]
```

Рис. 3.22: Ошибки при выполнении сценариев WebHook

Создадим карточку инцидента. (рис. 3.23)

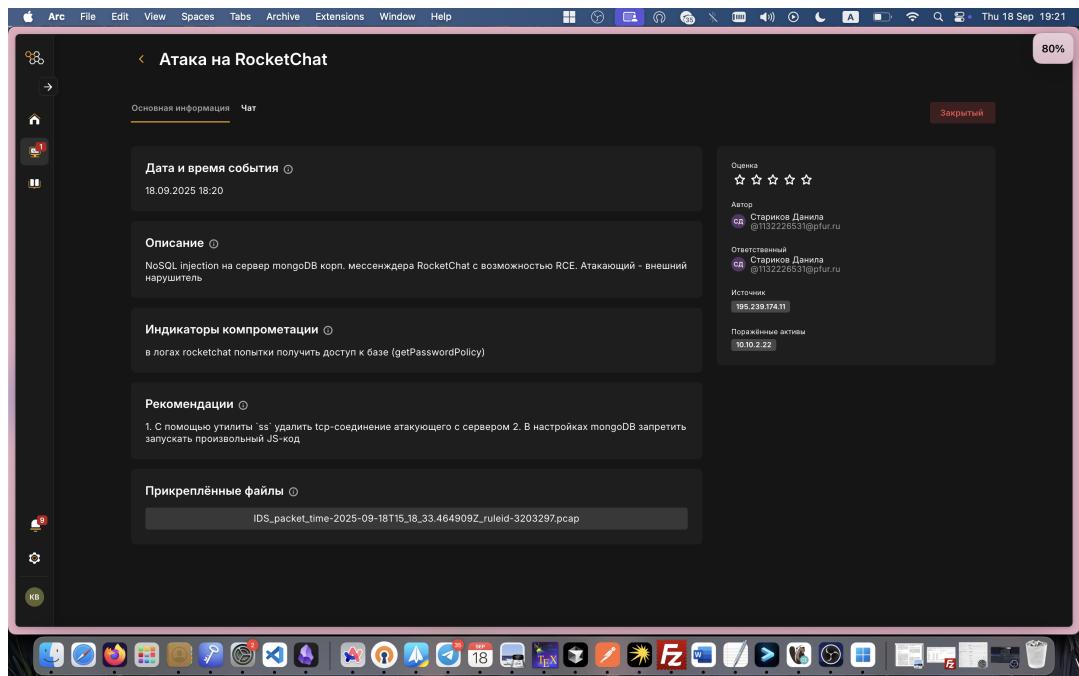
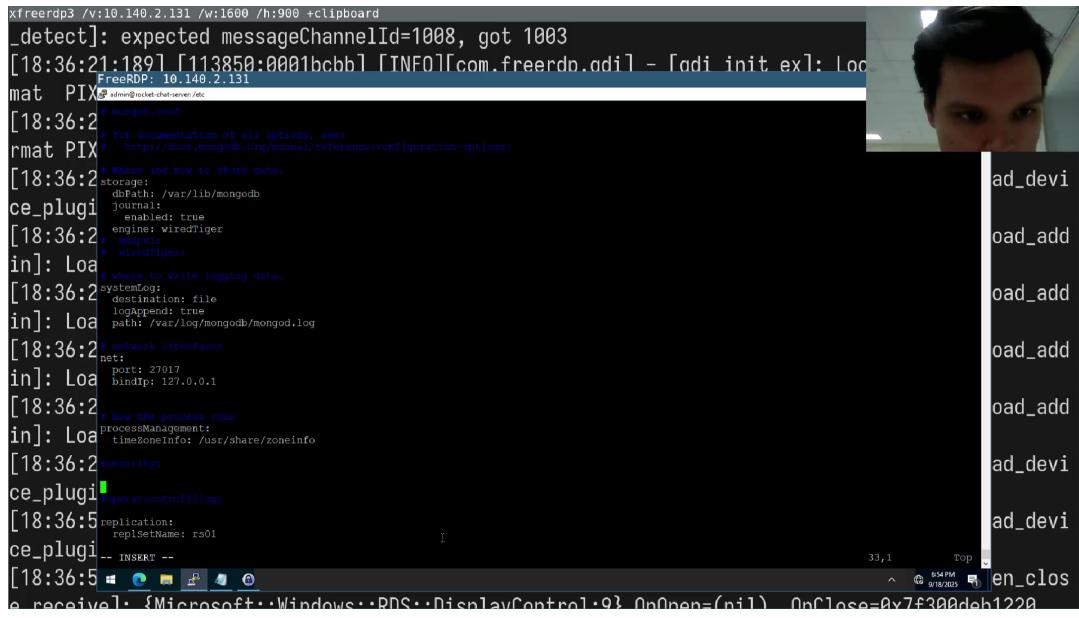


Рис. 3.23: Карточка третьего инцидента

### 3.3.1 Закрытие уязвимости RocketChat

Так как NoSQL-инъекция для повышения привилегий использует высокоуровневый оператор БД \$where, временной, смягчающей мерой, может стать отключение выполнения JavaScript на стороне сервера базы данных.

Для этого необходимо отредактировать файл конфигурации БД /etc/mongod.conf, добавив строчку javascriptEnabled: false. (рис. 3.24 - рис. 3.25)

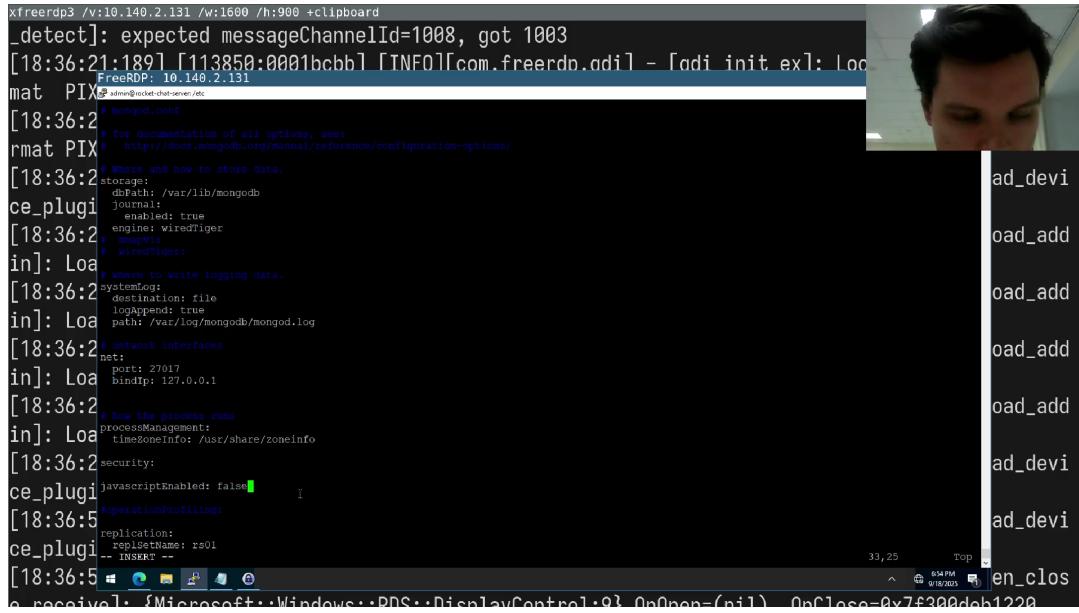


```

xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
[18:36:21:189] [113850:0001bcbb] [INFO][com.freerdp.adil - adi_init_ex]: LocalFree: 10.140.2.131
mat PIX
# mongod.conf
# for documentation of all options, see:
# http://docs.mongodb.org/manual/reference/configuration-options/
[18:36:2 storage:
  dbPath: /var/lib/mongodb
  journal:
    enabled: true
  engine: wiredTiger
  mmapv1:
  # wiredTiger:
in]: Loo
  # where to write logging data.
[18:36:2 systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log
[18:36:2 network interfaces:
net:
  port: 27017
  bindIp: 127.0.0.1
[18:36:2 # how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo
[18:36:2 #security:
ce_plugi
  #operationProfiling:
[18:36:5 replication:
  replSetName: rs01
ce_plugi -- INSERT --
[18:36:5
e received: {Microsoft::Windows::PDS::DisplayControl::OnOpen-(nil)} OnClose=0x7f300dcb1220

```

Рис. 3.24: Изначальный файл конфигурации БД /etc/mongod.conf



```

xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
[18:36:21:189] [113850:0001bcbb] [INFO][com.freerdp.adil - adi_init_ex]: LocalFree: 10.140.2.131
mat PIX
# mongod.conf
# for documentation of all options, see:
# http://docs.mongodb.org/manual/reference/configuration-options/
[18:36:2 storage:
  dbPath: /var/lib/mongodb
  journal:
    enabled: true
  engine: wiredTiger
  mmapv1:
  # wiredTiger:
in]: Loo
  # where to write logging data.
[18:36:2 systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log
[18:36:2 network interfaces:
net:
  port: 27017
  bindIp: 127.0.0.1
[18:36:2 # how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo
[18:36:2 #security:
ce_plugi
  javascriptEnabled: false
  #operationProfiling:
[18:36:5 replication:
  replSetName: rs01
ce_plugi -- INSERT --
[18:36:5
e received: {Microsoft::Windows::PDS::DisplayControl::OnOpen-(nil)} OnClose=0x7f300dcb1220

```

Рис. 3.25: Измененный файл конфигурации БД /etc/mongod.conf

### 3.3.2 Закрытие уязвимости и последствия

Для применения настроек необходимо перезапустить службу: sudo systemctl restart mongod.service. (рис. 3.26)

```
xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
[xfreerdp3]: expected messageChannelId=1008, got 1003
[18:36:21+189] [113850:0001:bccb1] [INFO][com.freerdp.adil] - [adi init ex]: Loc
FreeRDP: 10.140.2.131
mat PIX
[18:36:2 LoadAll: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
Active: failed (Result: exit-code) since Thu 2025-09-18 15:54:55 UTC; 1min 3s ago
Docs: https://docs.mongodb.org/manual
Process: 3497 ExecStart=/usr/bin/mongod --config /etc/mongod.conf (code=exited, status=2)
Main PID: 3497 (code=exited, status=2)
[18:36:2 Sep 18 15:54:55 rocketchat-server systemd[1]: Stopped MongoDB Database Server.
Sep 18 15:54:55 rocketchat-server mongod[3497]: Started MongoDB Database Server.
Sep 18 15:54:55 rocketchat-server mongod[3497]: Unrecognized option: security
Sep 18 15:54:55 rocketchat-server mongod[3497]: try '/usr/bin/mongod --help' for more information
Sep 18 15:54:55 rocketchat-server mongod[3497]: mongod.service: Main process exited, code=exited, status=2/INVALIDARGUMENT
Sep 18 15:54:55 rocketchat-server mongod[3497]: mongod.service: Failed with result 'exit-code'.
[18:36:2 admin@rocketchat-server:~$ sudo systemctl status mongod.service
[18:36:2 mongod.service - MongoDB Database Server
[18:36:2 Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
[18:36:2 Active: failed (Result: exit-code) since Thu 2025-09-18 15:54:55 UTC; 1min 5s ago
[18:36:2 Docs: https://docs.mongodb.org/manual
[18:36:2 Process: 3497 ExecStart=/usr/bin/mongod --config /etc/mongod.conf (code=exited, status=2)
[18:36:2 Main PID: 3497 (code=exited, status=2)
[18:36:2 Sep 18 15:54:55 rocketchat-server systemd[1]: Stopped MongoDB Database Server.
[18:36:2 Sep 18 15:54:55 rocketchat-server mongod[3497]: Started MongoDB Database Server.
[18:36:2 Sep 18 15:54:55 rocketchat-server mongod[3497]: Unrecognized option: security
[18:36:2 Sep 18 15:54:55 rocketchat-server mongod[3497]: try '/usr/bin/mongod --help' for more information
[18:36:2 Sep 18 15:54:55 rocketchat-server mongod[3497]: mongod.service: Main process exited, code=exited, status=2/INVALIDARGUMENT
[18:36:2 Sep 18 15:54:55 rocketchat-server mongod[3497]: mongod.service: Failed with result 'exit-code'.
[18:36:2 admin@rocketchat-server:~$ sudo systemctl status mongod.service
[18:36:2 mongod.service - MongoDB Database Server
[18:36:2 Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
[18:36:2 Active: active (running) Since Thu 2025-09-18 15:56:04 UTC; 1s ago
[18:36:2 Docs: https://docs.mongodb.org/manual
[18:36:2 Main PID: 3544 (mongod)
[18:36:2 Memory: 175.6M
[18:36:2 CGroup: /system.slice/mongod.service
└─3544 /usr/bin/mongod --config /etc/mongod.conf
[18:36:5 Sep 18 15:56:04 rocketchat-server systemd[1]: Started MongoDB Database Server.
[18:36:5 admin@rocketchat-server:~$ █
e-receive: {Microsoft::Windows::PDS::DisplayControl1::OnOpen=(nil), OnClose=0x7f300deb1220}
```

Рис. 3.26: Перезапуск службы: sudo systemctl restart mongod.service

Данное последствие можно обнаружить при выводе сетевой статистики с помощью утилиты ss и параметрами -tp (позволяет просматривать сведения по TCP-соединениям, список процессов в данный момент). В случае установления соединения, на уязвимой машине появится сокет с машиной нарушителя.

Нейтрализовать meterpreter-сессию также можно 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.

И закрыть сессию с нарушителем. (рис. 3.27)

Рис. 3.27: Закрытие сессии с нарушителем

## **4 Вывод**

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Задача корпоративного мессенджера” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы освоили практические навыки выявления, анализа и устранения уязвимостей в корпоративной инфраструктуре, а также освоили навыки отработки действий по нейтрализации последствий успешных атак.

# **Список литературы**

1. Сценарий Защита корпоративного мессенджера [Электронный ресурс].
2. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «WPDISCUZ» [Электронный ресурс].
3. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «PROXYLOGON» (CVE 2020-26855) [Электронный ресурс].
4. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «ROCKETCHAT» [Электронный ресурс].
5. Сетевой сенсор системы обнаружения атак программно-аппаратный комплекс ViPNet IDS NS 3 Руководство администратора [Электронный ресурс].
6. Security Onion Documentation Release 16.04.7.2 [Электронный ресурс].
7. AM Threat Intelligence Portal [Электронный ресурс].
8. NoSQL Injections in Rocket.Chat 3.12.1: How A Small Leak Grounds A Rocket [Электронный ресурс]. URL: <https://www.sonarsource.com/blog/nosql-injections-in-rocket-chat/>.