

Лабораторная работа №1

Кибербезопасность предприятия

Аскеров Александр Эдуардович; Замбалова Дина Владимировна;
Кузнецова София Вадимовна; Поляков Глеб Сергеевич;
Скандарова Полина Юрьевна; Тарутина Кристина Еленовна;
Цвелев Сергей Андреевич; Шулугужук Айраана Вячеславовна

Российский университет дружбы народов, Москва, Россия

Учебная группа НПИбд-01-22

01.10.2025

Цель лабораторной работы

Целью лабораторной работы является исследование сценария целенаправленной атаки на корпоративный мессенджер и сопутствующие сервисы, выявить и продемонстрировать эксплуатацию реальных уязвимостей (WpDiscuz, ProxyLogon, RocketChat), а также отработать методы обнаружения, локализации и нейтрализации последствий компрометации для восстановления безопасности информационной инфраструктуры организации.

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.

Теоретическое введение

Описание уязвимостей

WpDiscuz

CVE-2020-24186 – это уязвимость в плагине для создания комментариев WpDiscuz версии с 7.0.0 по 7.0.4 включительно. Уязвимость позволяет получить RCE (удаленное выполнение кода).

Proxylogon

Proxylogon представляет собой SSRFуязвимость, позволяющую обойти аутентификацию и выдать себя за администратора.

Следующий шаг после SSRF – эксплуатация CVE 2020-27065. Данная уязвимость является следствием неэффективного ограничения выбора расположения backup виртуальной директории автономных адресных книг.

Описание уязвимостей

RocketChat

CVE-2021-22911 представляет собой сочетание из двух SQL-инъекций: - слепая NoSQL-инъекция, - NoSQL-инъекция №2: повышение привилегий.

CVE-2022-0847 (Dirty Pipe) представляет собой уязвимость повышения привилегий, находящаяся в самом ядре Linux версии 5.8 и выше.

Ход выполнения лабораторной работы

The screenshot shows a terminal window titled "dandelion@vbox:~". The terminal displays the following command sequence:

```
dandelion@vbox:~$ sudo wg-quick up wg0
[sudo] password for dandelion:
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.77.198.76/32 dev wg0
[#] ip -6 address add fd42:42:42::76/128 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] resolvconf -a tun.wg0 -m 0 -x
[#] ip -4 route add 10.0.0.0/8 dev wg0
dandelion@vbox:~$ gnome-connections
```

Below this, several warning messages from the "gnome-connections" application are listed:

```
(gnome-connections:7335): Gtk-WARNING **: 20:04:01.175: GtkFlowBox with a model will ignore sort and filter functions
[20:04:34:864] [7335:7357] [WARN][com.freerdp.core.nego] - Error: SSL_NOT_ALLOWED_BY_SERVER
[20:04:34:890] [7335:7357] [WARN][com.freerdp.core.nego] - Error: SSL_NOT_ALLOWED_BY_SERVER
[20:04:35:330] [7335:7357] [ERROR][com.winpr.timezone] - Unable to get current timezone rule
[20:04:35:065] [7335:7357] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRA32
[20:04:35:065] [7335:7357] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[20:04:36:418] [7335:7335] [ERROR][com.freerdp.core.rdp] - WARNING: invalid pack
```

Рис. 1: Подключение к серверу

Ход выполнения лабораторной работы

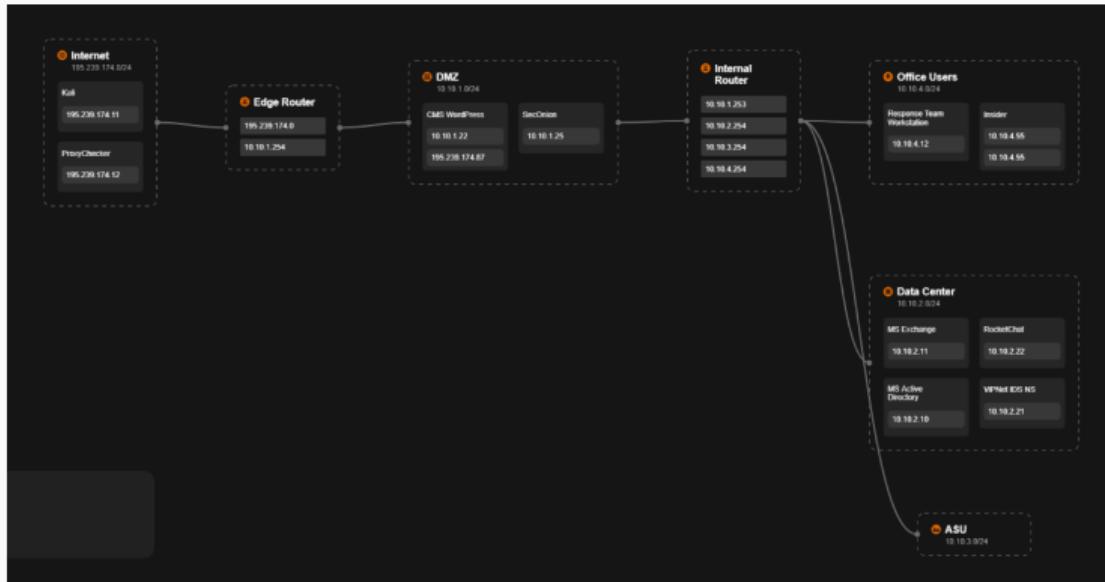


Рис. 2: Вектор атаки

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

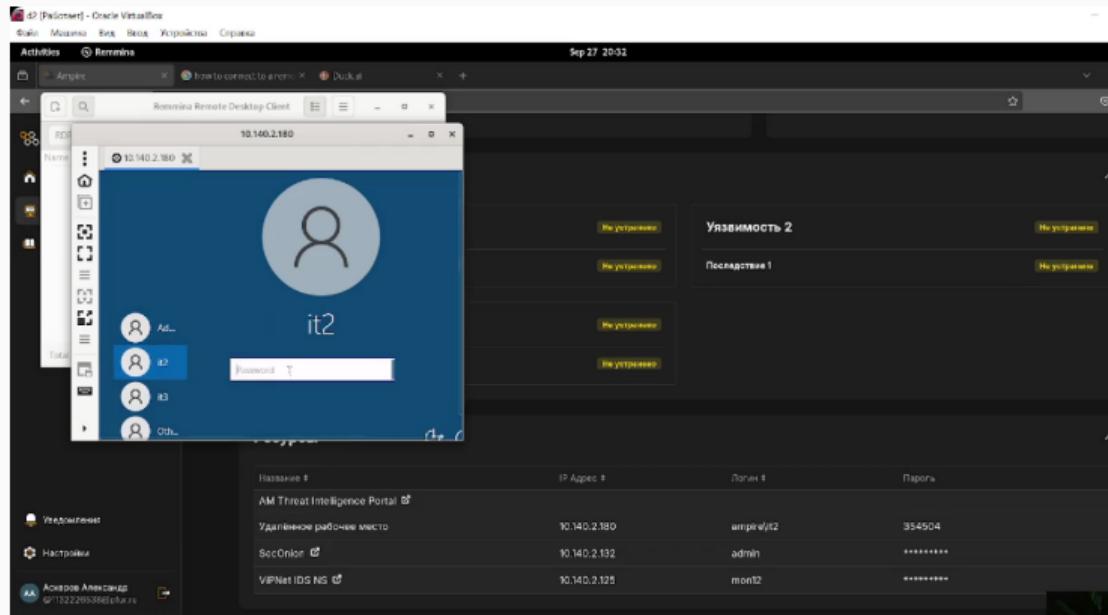


Рис. 3: Подключение к удаленному рабочему столу

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

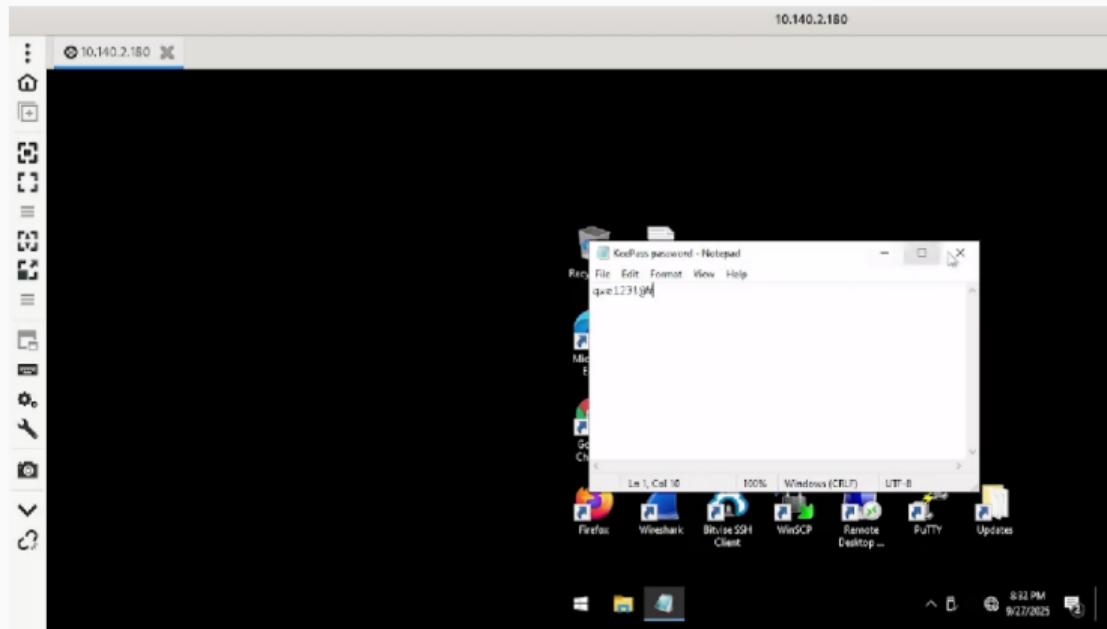


Рис. 4: Просмотр пароля

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок



Рис. 5: Вход в KeyPass 2

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

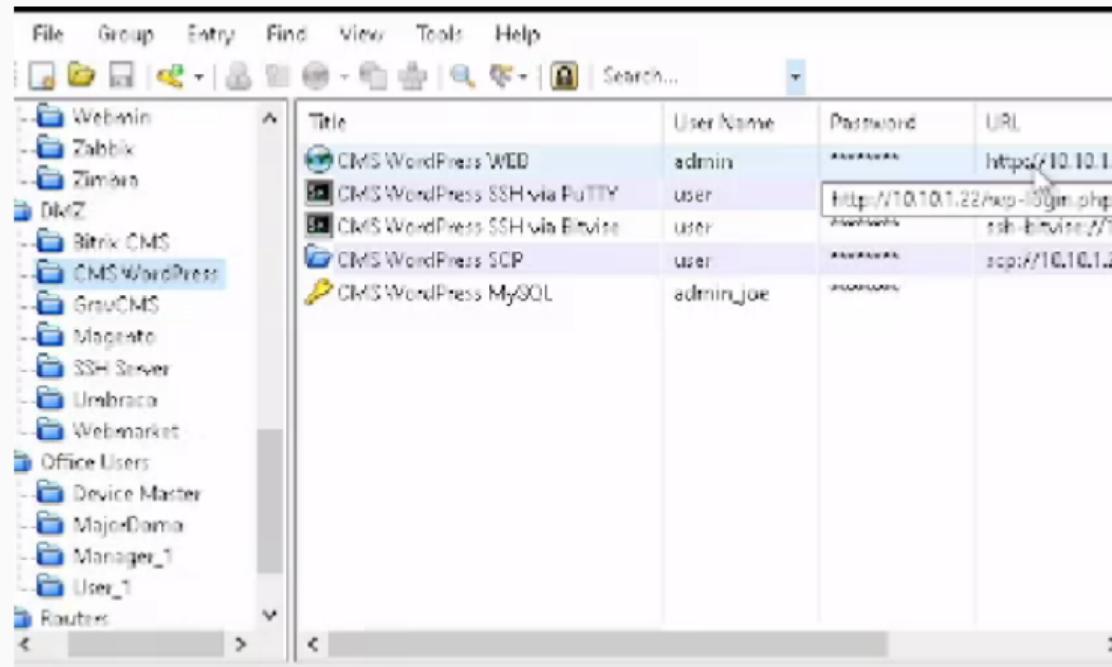


Рис. 6: Папка атакованного сервера

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок



Рис. 7: Атакованный сервер

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

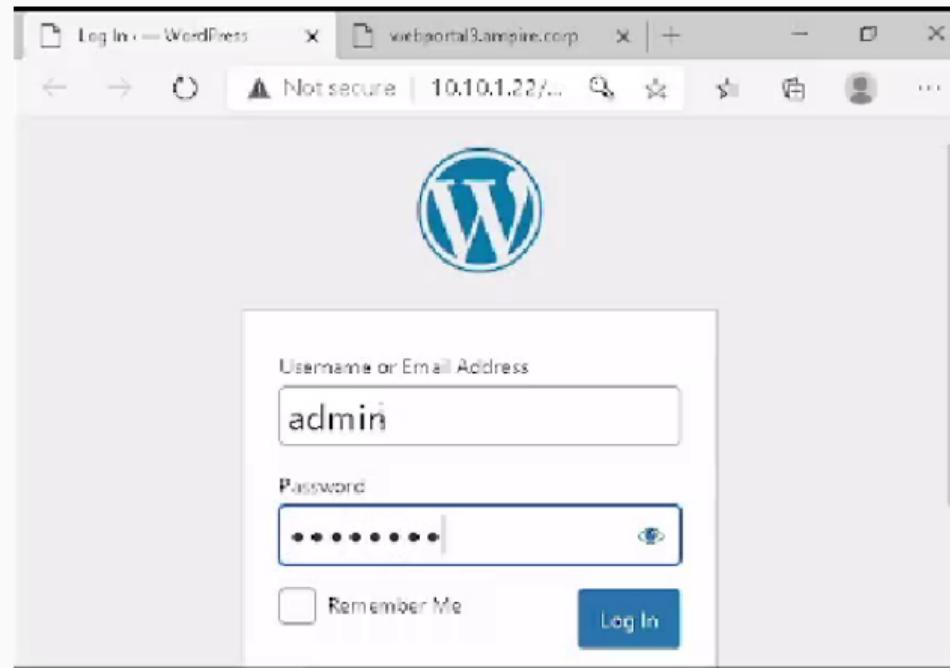


Рис. 8: Авторизация

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

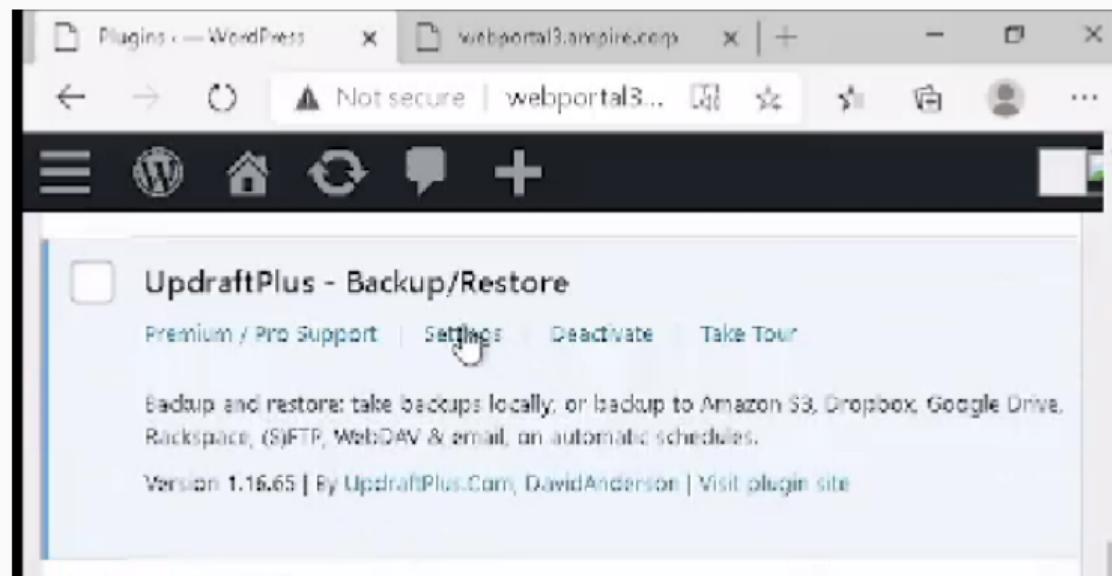


Рис. 9: Плагин UpdraftPlus в репозитории WordPress

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

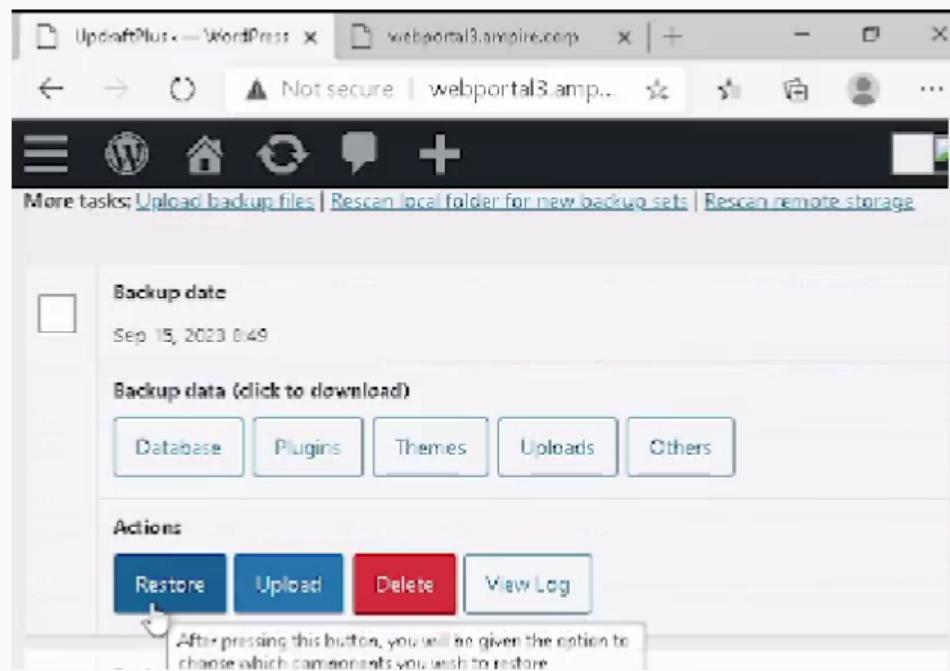


Рис. 10: Существующие резервные копии UpdraftPlus

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

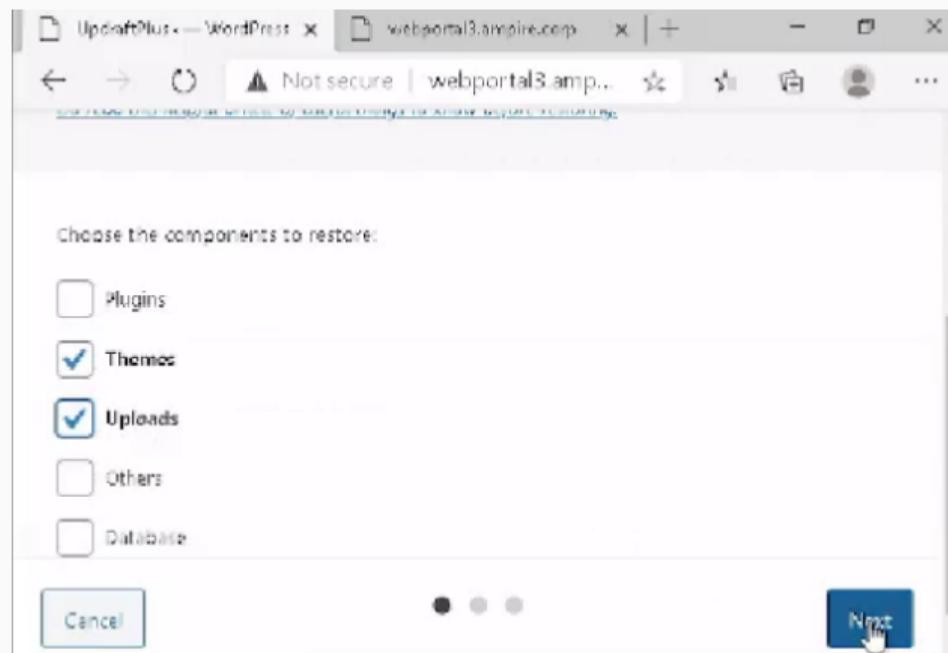


Рис. 11: Компоненты для восстановления

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

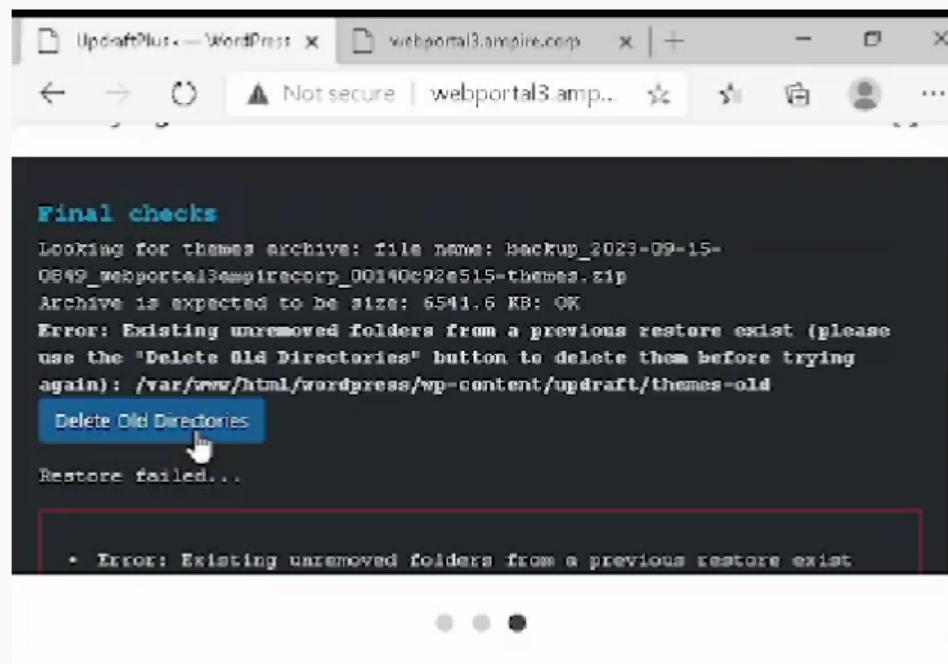


Рис. 12: Ошибка восстановления

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

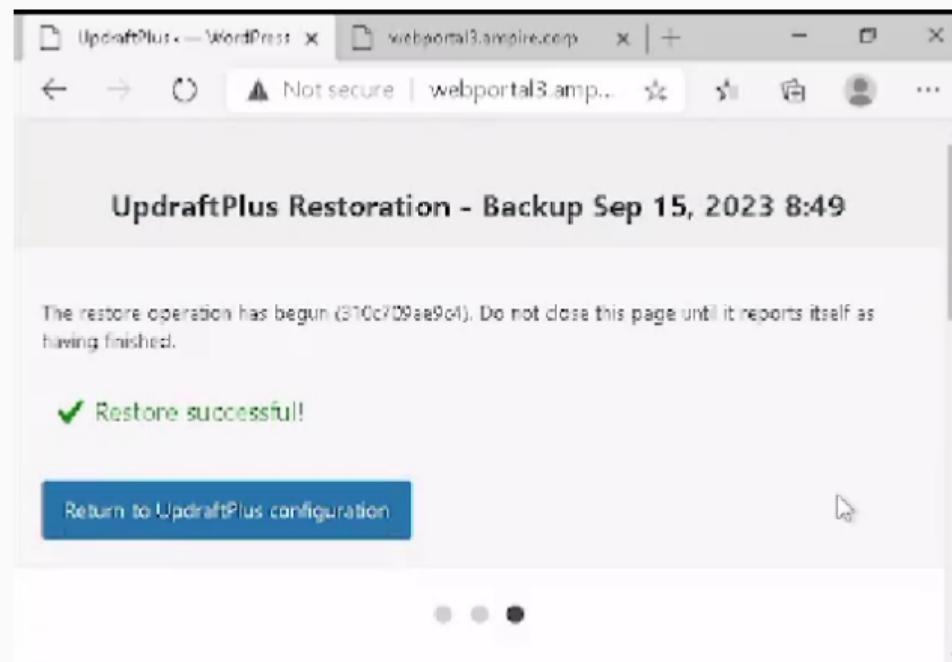


Рис. 13: Успешное выполнение восстановления

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

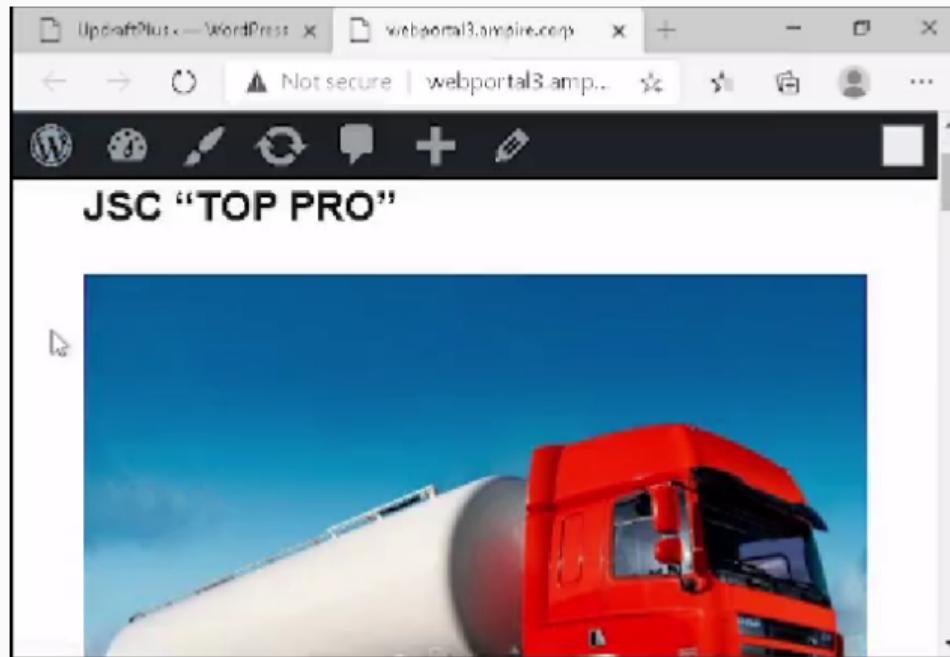


Рис. 14: Обновленная страница сайта

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

```
user@web-portal-3:~$ sudo ss -tnp
State      Recv-Q  Send-Q      Local Address:Port      Peer Address:Port
CLOSE-WAIT  0        0          10.10.1.22:39654    195.239.174.11:5557  users:(("chisel.sh",pid=1923,fd=12),("sh",pid=1922,fd=12),("KLoWi",pid=1889,fd=12))
FIN-WAIT-2  0        0          10.10.1.22:55518    10.10.2.11:443   users:(("chisel.sh",pid=1923,fd=16))
ESTAB     0        0          10.10.1.22:53386    195.239.174.11:5556  users:(("chisel.sh",pid=1923,fd=3),("sh",pid=1922,fd=3),("KLoWi",pid=1889,fd=3))
ESTAB     0        0          10.10.1.22:34892    195.239.174.11:1085 users:(("chisel.sh",pid=1923,fd=11))
ESTAB     0       64          10.10.1.22:22      10.10.1.253:51756  users:(("sshd",pid=10666,fd=3),("sshd",pid=10545,fd=3))

user@web-portal-3:~$ kill 1889
-bash: kill: (1889) - Operation not permitted
user@web-portal-3:~$ sudo kill 1889
user@web-portal-3:~$ sudo ss -tpq
State      Recv-Q  Send-Q      Local Address:Port      Peer Address:Port
CLOSE-WAIT  0        0          10.10.1.22:39654    195.239.174.11:5557  users:(("chisel.sh",pid=1923,fd=12),("sh",pid=1922,fd=12))
FIN-WAIT-2  0        0          10.10.1.22:55519    10.10.2.11:https   users:(("chisel.sh",pid=1923,fd=16))
ESTAB     0        0          10.10.1.22:53386    195.239.174.11:freecciv users:(("chisel.sh",pid=1923,fd=3),("sh",pid=1922,fd=3))
ESTAB     0        0          10.10.1.22:34892    195.239.174.11:1085 users:(("chisel.sh",pid=1923,fd=11))
ESTAB     0       64          10.10.1.22:ssh      10.10.1.253:51756  users:(("sshd",pid=10666,fd=3),("sshd",pid=10545,fd=3))

user@web-portal-3:~$ sudo kill 1923
user@web-portal-3:~$ sudo ss -tpq
State      Recv-Q  Send-Q      Local Address:Port      Peer Address:Port
LAST-ACK   0        1          10.10.1.22:39654    195.239.174.11:5557
FIN-WAIT-2  0        0          10.10.1.22:55518    10.10.2.11:https   users:(("sshd",pid=10666,fd=3),("sshd",pid=10545,fd=3))
```

Рис. 15: Отображение информации о TCP-соединениях. Процесс закрытия meterpreter-сессии

Уязвимый узел WpDiscuz

Обнаружение и нейтрализация полезных нагрузок

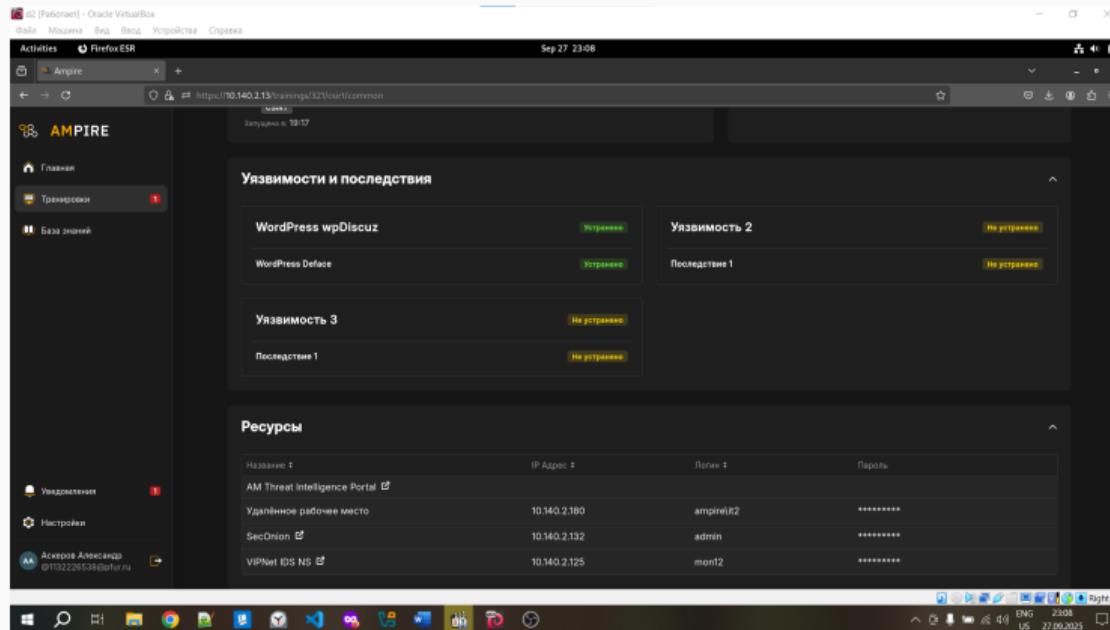


Рис. 16: Уязвимость и последствия устраниены

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ОС

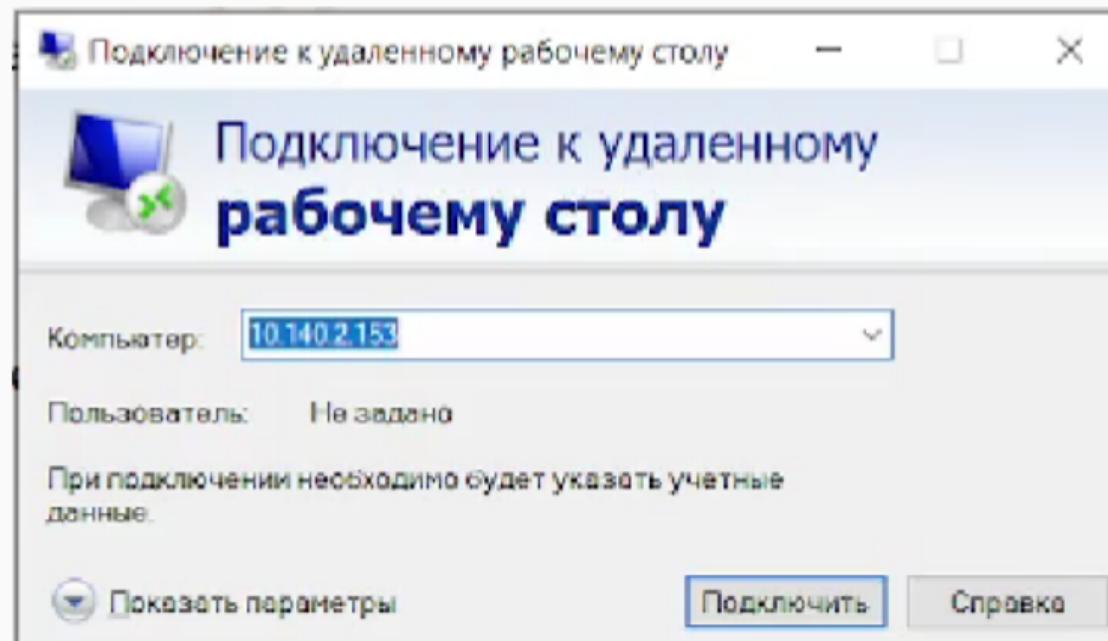


Рис. 17: Подключение к удаленному рабочему столу

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ОС

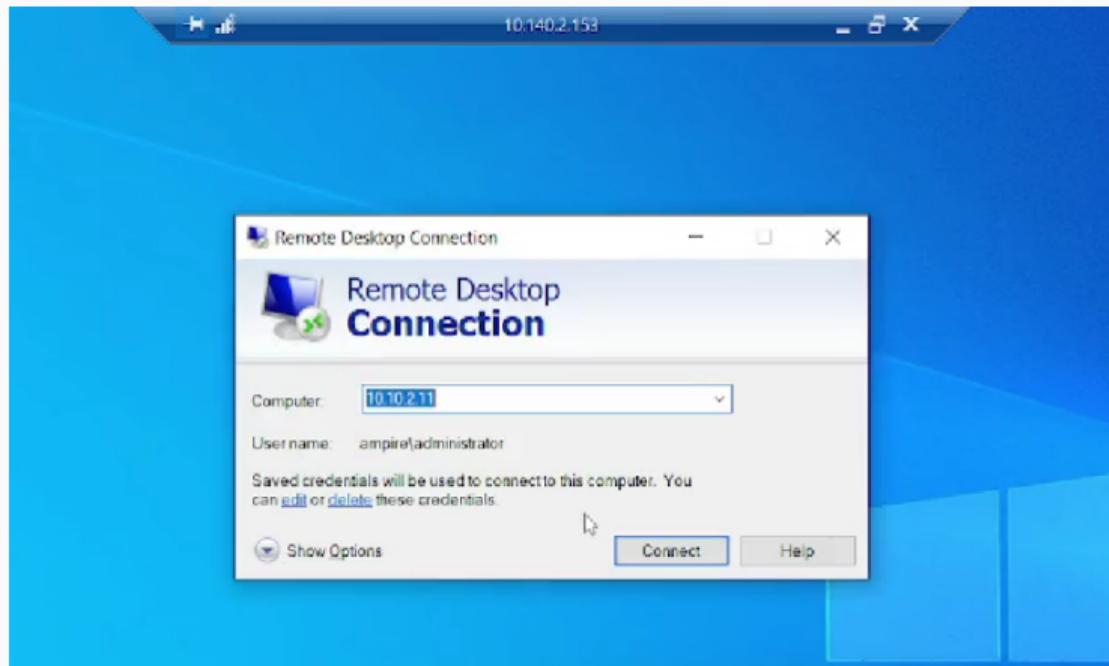


Рис. 18: Подключение к удаленному рабочему столу

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ОС

```
2025-09-30 12:29:10 10.10.2.11 POST /favicon.ico &correlationId=empty>;&cafe80qqd-25e38b91-a139-4dae-b5bd-c3f3f06c0c02; 443 - 10.10.1.22 User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 - 200 0 0 1951
2025-09-30 12:29:10 10.10.2.11 POST /favicon.ico &correlationId=empty>;&cafe80qqd-25e38b91-a139-4dae-b5bd-c3f3f06c0c02; 443 - 10.10.1.22 User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 - 200 0 0 115
2025-09-30 12:29:15 10.10.2.11 POST /appth/web.aspx &correlationId=empty>;&cafe80qqd-25e38b91-a139-4dae-b5bd-c3f3f06c0c02; 443 - 10.10.1.22 python-requests/2.28.1 - 200 0 0 1938
2025-09-30 12:29:23 fe80::b1c5:df9f:940d:153C%3 POST /powershell
```

Рис. 19: Артефакты, оставленные атакой в журнале «IIS»

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ОС

```
2025-09-28 12:38:33 19.10.2.11 POST /api/emsmdb/mailboxId=/d82dbca-f50f-42c4-acbd-eb6ba1564ee@empire.corp&correlationId=<empty>;&ClientRequestInfo=<id:423255e2-bc6a-4c5a-abbe-c9b7cd3061b1:1>RT:Connect;CI:cef40ff6-795f-4ba3-b160-adf5d8aa015:1;CID:adff23f4-1da8-4b6f-8590-20f599f07519;cafeReqId=699f6375-dc3-423f-9221-219b5182eckj;443 AMP;URL=\\healthMailbox\84te8a710.10.2.11 MapIISHttpclient - 200 0 0 7
2025-09-28 12:38:33 19.10.2.11 POST /api/emsmdb/mailboxId=/d82dbca-f50f-42c4-acbd-eb6ba1564ee@empire.corp&correlationId=<empty>;&ClientRequestInfo=<id:423255e2-bc6a-4c5a-abbe-c9b7cd3061b1:2>RT:Execute;CI:cef40ff6-795f-4ba3-b160-adf5d8aa015:1;CID:da2ff0c03-0f26-4ff6-8eb-5596c1754c1b8;cafeReqId=b20c3667-86e9-4303-87d4-47810b4cd85f;443 AMP;URL=\\healthMailbox\84te8a710.10.2.11 MapIISHttpclient - 200 0 0 7
2025-09-28 12:38:33 19.10.2.11 POST /api/emsmdb/mailboxId=/d82dbca-f50f-42c4-acbd-eb6ba1564ee@empire.corp&correlationId=<empty>;&ClientRequestInfo=<id:423255e2-bc6a-4c5a-abbe-c9b7cd3061b1:3>RT:Disconnect;CI:cef40ff6-795f-4ba3-b160-adf5d8aa015:1;CID:c5026c09-21ee-4f11-8a6c-c6f02635d115&cafeReqId=788c7c4d-d8a9-4d88-8926-d6da3666e50a;443 AMP;URL=\\healthMailbox\84te8a710.10.2.11 MapIISHttpclient - 200 0 0 12
2025-09-28 12:38:33 127.0.0.1 GET /api/emsmdb/mailboxId=/d82dbca-f50f-42c4-acbd-eb6ba1564ee@empire.corp&correlationId=<empty>;&cafeReqId=d8cbfc1b-e772-4cc9-adb6-9c5c6564861b;443 AMP;URL=\\healthMailbox\84te8a7127.0.0.1 AMP;Verb=\\ClientAccess - 200 0 0 1
2025-09-28 12:38:53 19.10.2.11 POST /powershell
```

Рис. 20: Артефакты, оставленные атакой в журнале «IIS»

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS

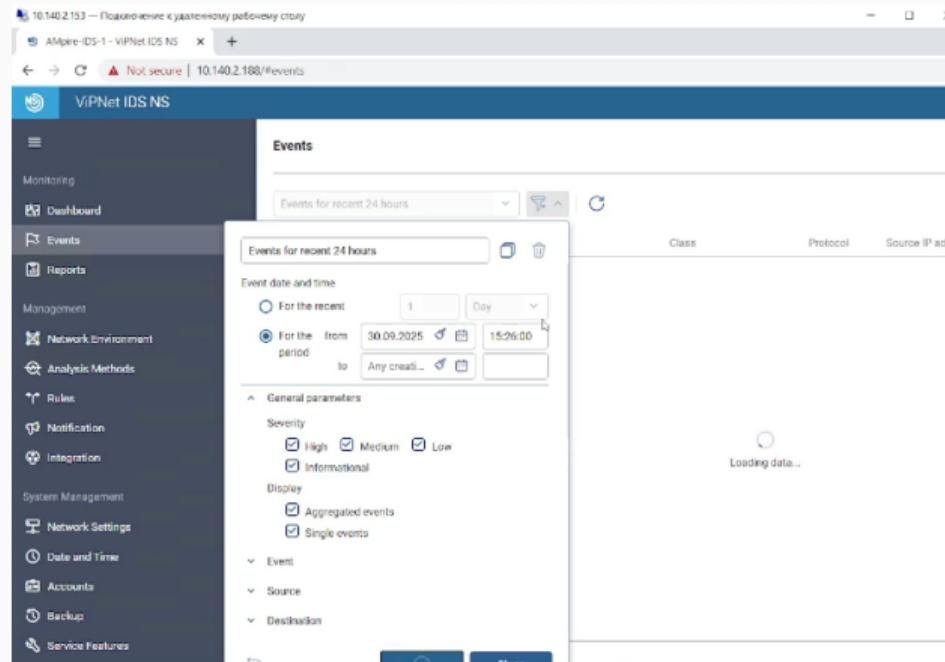


Рис. 21: Вход в ViPNet IDS NS

Уязвимый узел Proxylogon

Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS

●	15:29:16.556 09/...	2025644	1	ET TROJAN Possible Metasp...	trojan-activity	TCP	195.239.174.11
●	15:29:16.557 09/...	2025644	1	ET TROJAN Possible Metasp...	trojan-activity	TCP	195.239.174.11
●	15:29:16.555 09/...	2035480	1	ET INFO PE EXE Download o...	misc-activity	TCP	195.239.174.11
●	15:29:16.555 09/...	2035480	1	ET INFO PE EXE Download o...	misc-activity	TCP	195.239.174.11

Рис. 22: Список событий, направленных на уязвимый сервер

Уязвимый узел Proxylogon

Устранение уязвимостей

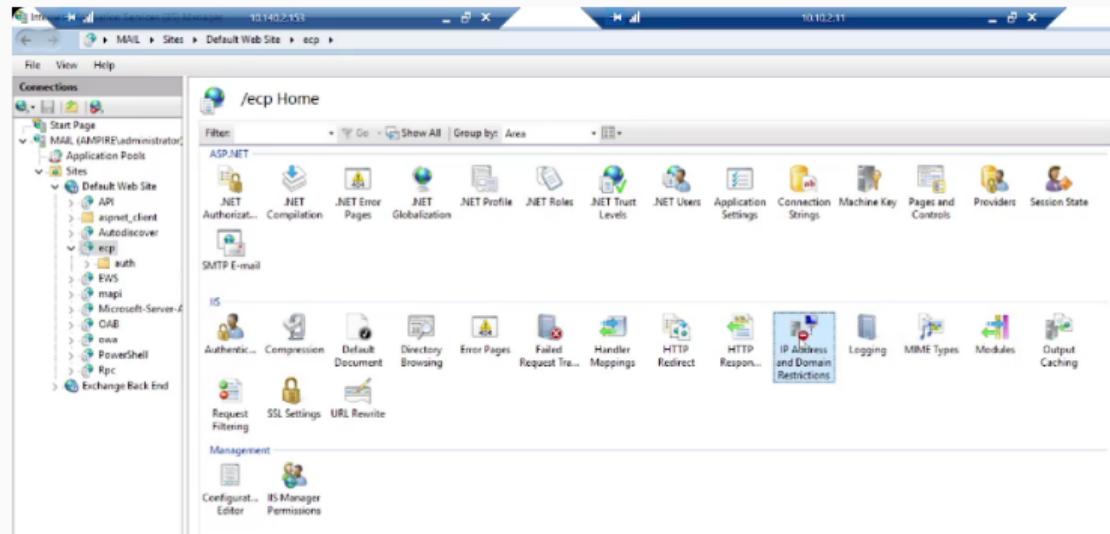


Рис. 23: Окно Internet Information Services (IIS) Manager

Уязвимый узел Proxylogon

Устранение уязвимостей

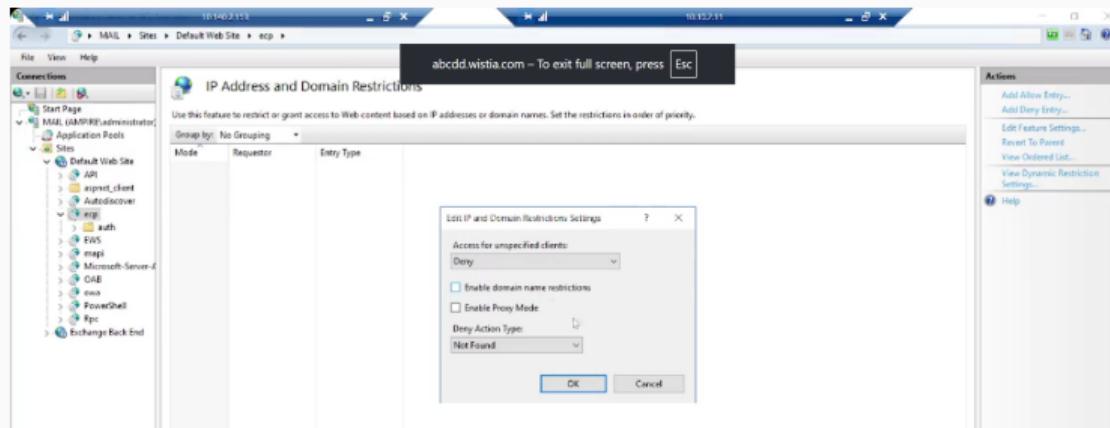


Рис. 24: «IP Address and Domain Restrictions»

Уязвимый узел Proxylogon

Устранение уязвимостей

```
TCP 10.10.2.11:7206 195.239.174.11:5558 ESTABLISHED 4260  
[powershell.exe]  
TCP 10.10.2.11:7207 195.239.174.11:5558 ESTABLISHED 13136  
[powershell.exe]
```

Рис. 25: Сокет с узлом нарушителя

Уязвимый узел Proxylogon

Устранение уязвимостей

```
C:\Users\administrator.АМPIRE>taskkill /PID 4260 /F  
SUCCESS: The process with PID 4260 has been terminated.  
  
C:\Users\administrator.АМPIRE>taskkill /PID 13136 /F  
SUCCESS: The process with PID 13136 has been terminated.  
  
C:\Users\administrator.АМPIRE>
```

Рис. 26: Завершение процессов

Уязвимый узел Proxylogon

Устранение уязвимостей

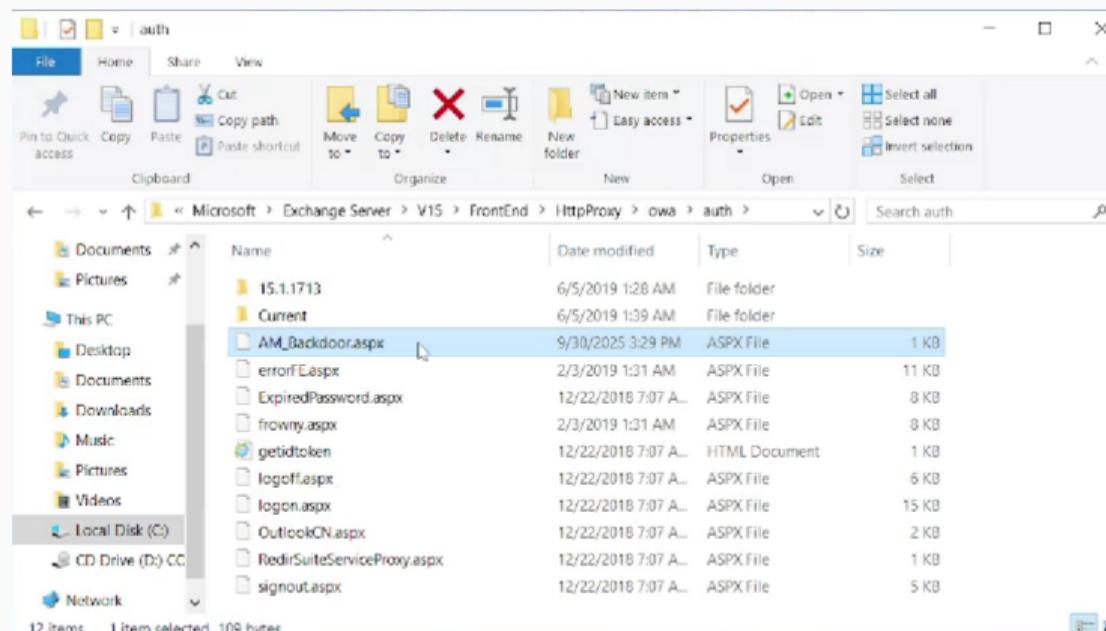


Рис. 27: Удаление файла

Уязвимый узел Proxylogon

Устранение уязвимостей

The screenshot shows the Proxylogon application interface. At the top, there's a navigation bar with tabs: Основная информация, Инциденты, Цепочки кибератаки, Beta, Схема шаблона, and Материалы. On the left, there's a sidebar with icons for Home, Training (with a '1' notification), and Settings (with a '2' notification).

Main content area:

- Тренировка запущена. Атака завершена 100% 00:00:00**
Сценарий: Amphi Защита корпоративного мессенджера
Шаблон: Офис [Конфигуратор]
Запущена в 16-26
- Нераспределенные инциденты**
Инциденты отсутствуют
- Уязвимости и последствия**

Уязвимость 1	Не устранено
Последствие 1	Не устранено
Уязвимость 3	Не устранено
Последствие 1	Не устранено
- Proxylogon**

Exchange China Chopper	Устранено
------------------------	-----------

Рис. 28: Уязвимость и последствия устраниены

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)

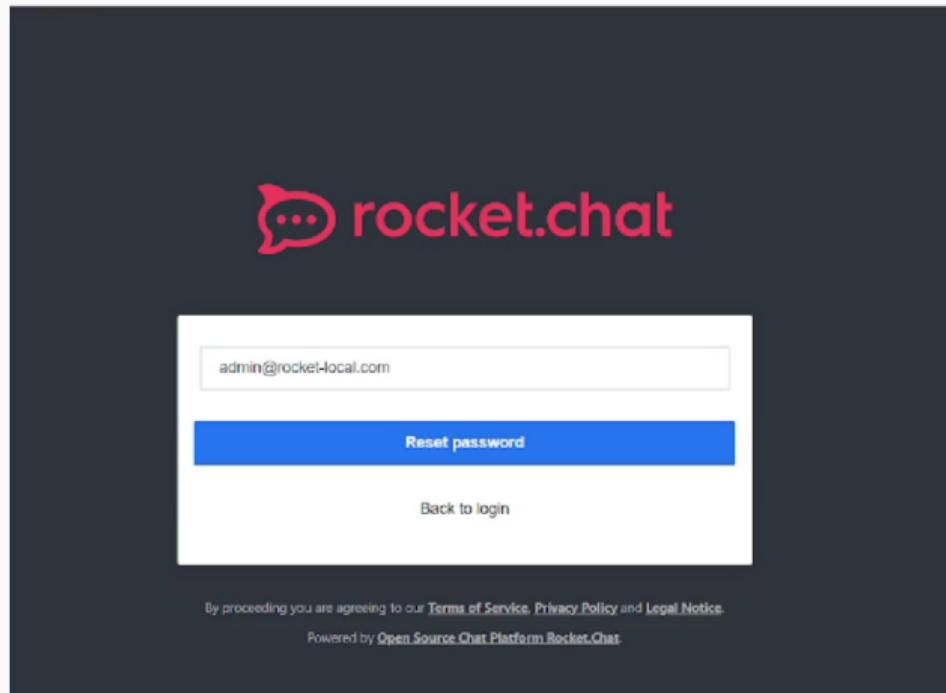
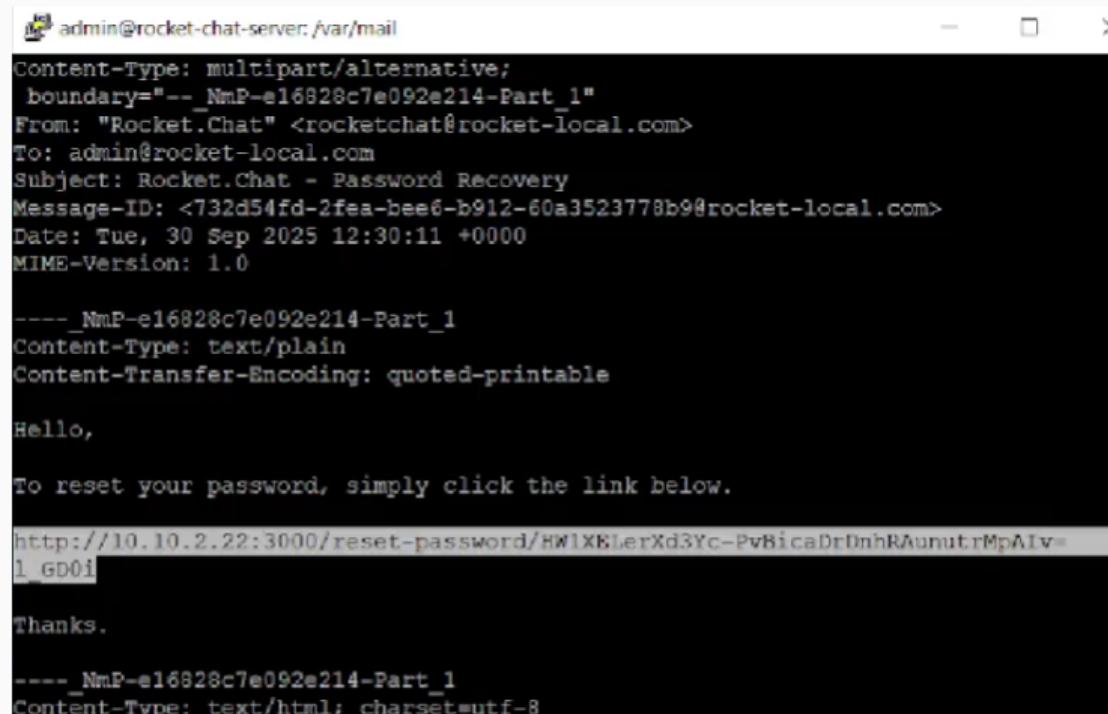


Рис. 29: Восстановление пароля

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)



```
admin@rocket-chat-server:/var/mail
Content-Type: multipart/alternative;
boundary="--_NmP-e16828c7e092e214-Part_1"
From: "Rocket.Chat" <rocketchat@rocket-local.com>
To: admin@rocket-local.com
Subject: Rocket.Chat - Password Recovery
Message-ID: <732d54fd-2fea-bee6-b912-60a3523778b9@rocket-local.com>
Date: Tue, 30 Sep 2025 12:30:11 +0000
MIME-Version: 1.0

-----_NmP-e16828c7e092e214-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/HW1XElterXd3Yc-PvBicaDrDnhRAunutrMpAIV=1\_gD0i

Thanks.

-----_NmP-e16828c7e092e214-Part_1
Content-Type: text/html; charset=utf-8
```

Рис. 30: Ссылка для сброса пароля

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)

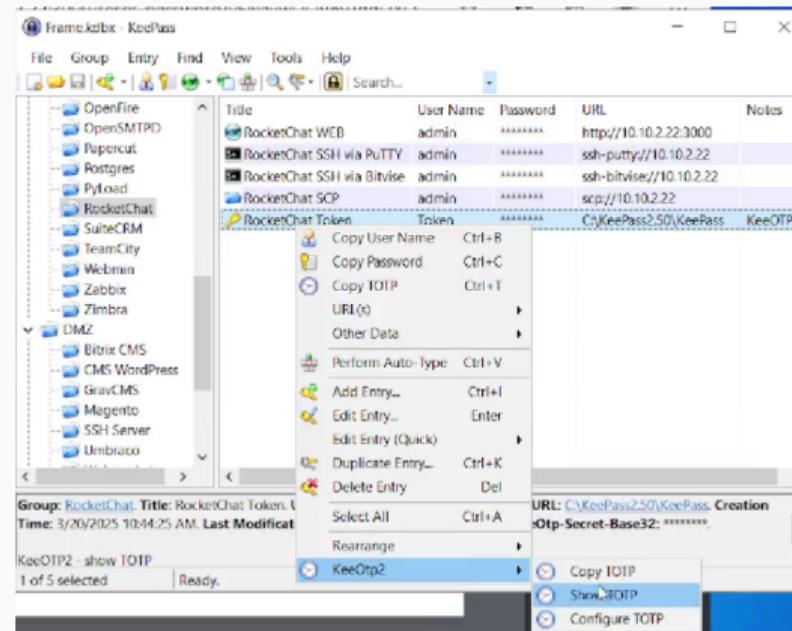


Рис. 31: Генерация одноразового пароля

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)



Рис. 32: Генерация одноразового пароля

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)

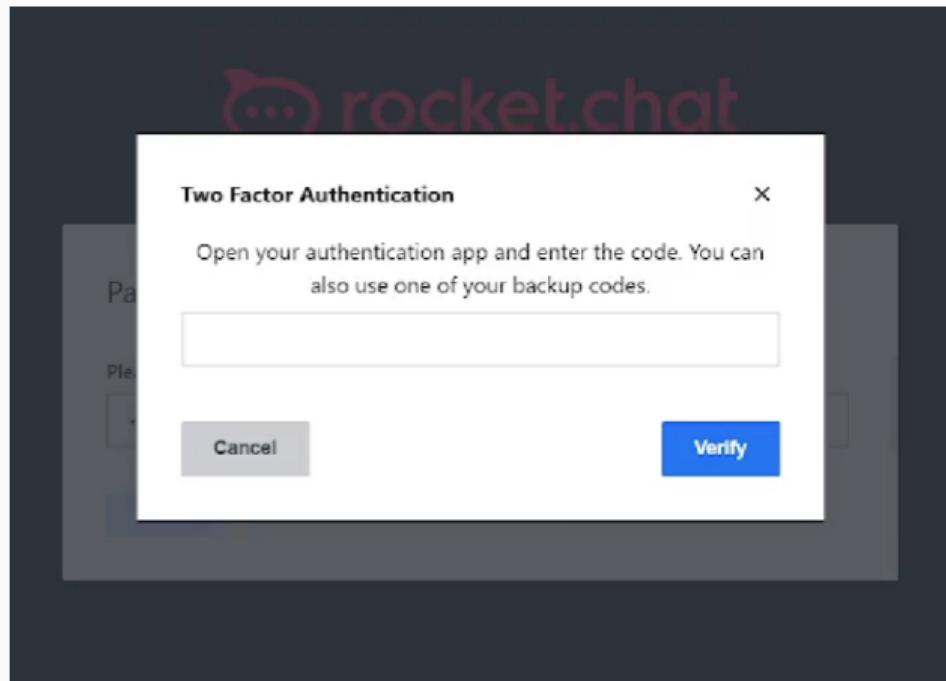
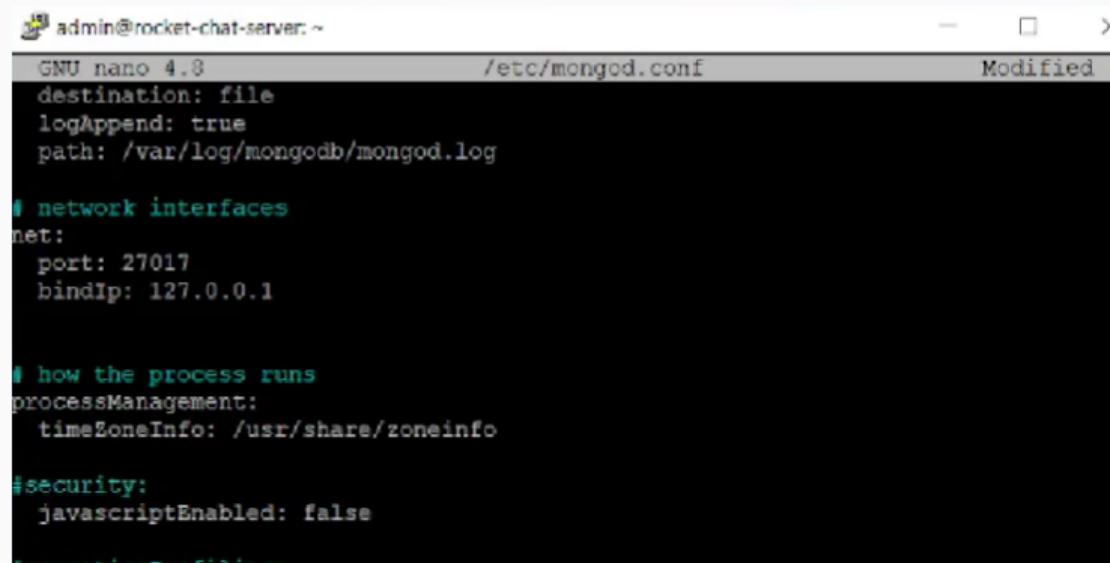


Рис. 33: Двухфакторная аутентификация

Уязвимый узел RocketChat

Устранение CVE-2021-22911 (NoSQL Injection)



```
GNU nano 4.8          /etc/mongod.conf          Modified
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
```

Рис. 34: Настройка конфигурации БД

Уязвимый узел RocketChat

Обнаружение и нейтрализация полезных нагрузок

```
root@rocket-chat-server:~# ss -tp
State Recv-Q Send-Q      Local Address:Port          Peer Address:Port
Process
ESTAB  0        0          10.10.2.22:57212        195.239.174.11:5559
  users:(("testsystem",pid=1848,fd=3))
ESTAB  0        0          10.10.2.22:ssh           10.10.2.254:5837
  users:(("sshd",pid=9088,fd=4),("sshd",pid=8967,fd=4))
ESTAB  0        64         10.10.2.22:ssh           10.10.2.254:47014
  users:(("sshd",pid=7236,fd=4),("sshd",pid=7148,fd=4))
ESTAB  0        0          10.10.2.22:3000          10.10.2.254:5604
  users:(("node",pid=681,fd=21))
root@rocket-chat-server:~# ss -K dst 195.239.174.11 dport=5559
Error: an inet prefix is expected rather than "dport=5559".
Cannot parse dst/src address.
root@rocket-chat-server:~# ss -K dst 195.239.174.11 dport = 5559
Netid State Recv-Q Send-Q      Local Address:Port          Peer Address:Port Process
tcp   ESTAB  0        0          10.10.2.22:57212        195.239.174.11:5559
root@rocket-chat-server:~#
```

Рис. 35: Пример сокета с узлом нарушителя

Уязвимый узел RocketChat

Обнаружение и нейтрализация полезных нагрузок

The screenshot shows a user interface for managing vulnerabilities. On the left, there's a sidebar titled 'Уязвимости и последствия' (Vulnerabilities and Consequences). Below it, two main sections are displayed:

- Уязвимость 1**: A card with 'Последствие 1' (Consequence 1) below it. To the right of each item is a button labeled 'Не устранено' (Not fixed).
- Proxylogon**: A card with 'Exchange China Chopper' listed below it. To its right is a button labeled 'Устранено' (Fixed).
- RocketChat RCE**: A card with 'RocketChat meterpreter' listed below it. To its right is a button labeled 'Устранено' (Fixed).

Рис. 36: Уязвимость и последствия устраниены

Карточки инцидентов

The screenshot shows a card incident page with the following details:

- Название:** WP Discuz RCE
- Статус:** Закрытый
- Основная информация:** Чат
- Дата и время события:** 27.09.2025 20:34
- Описание:** Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяет неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles.
- Индикаторы компрометации:** AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)
- Рекомендации:** - отключение плагина через панель администратора CMS WordPress; - обновление плагина до версии 7.0.5 и выше.
- Оценка:** ☆☆☆☆☆
- Автор:** Аскеров Александр @#1132226538@ptur.ru
- Ответственный:** Аскеров Александр @#1132226538@ptur.ru
- Источник:** 195.239.174.11
- Пораженные активы:** 10.30.1.22

Рис. 37: WP Discuz RCE

Карточки инцидентов

The screenshot shows a card incident view for the vulnerability 'Proxylogon'. The card has a dark background with white text. At the top left is the title 'Proxylogon'. Below it are tabs for 'Основная информация' (selected) and 'Чат'. On the right is a red button labeled 'Закрытый'.

Основная информация

Дата и время события ①
30.09.2025 15:29

Описание ①
Proxylogon представляет собой SSRF уязвимость, позволяющую обойти аутентификацию и выдать себя за Администратора.

Индикаторы компрометации ①
ET TROJAN

Рекомендации ①
- закрыть доступ к Панели управления Exchange (Exchange Control Panel); - установить обновление из каталога центра обновлений Microsoft.)

Оценка
☆ ☆ ☆ ☆ ☆

Автор
Асхеров Александр
@1132226538@yftr.ru

Ответственный
Асхеров Александр
@1132226538@yftr.ru

Источник
195.239.174.11

Пораженные активы
10.30.2.12

Рис. 38: Proxylogon

Карточки инцидентов

The screenshot shows a card-based incident report interface. At the top, there's a back arrow and the title "Rocketchat RCE". Below the title, there are two tabs: "Основная информация" (selected) and "Чат". A red button labeled "Закрытый" (Closed) is on the right. The main content area has several sections:

- Дата и время события**: 30.09.2025 21:21
- Описание**: 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.
- Индикаторы компрометации**: AM EXPLOIT Token BruteForce in RocketChat 3.12.1
- Рекомендации**: - обновление версии «RocketChat»; - запрет выполнения JavaScript на стороне сервера БД.

On the right side, there are additional details:

- Оценка**: Five stars
- Автор**: Аскеров Александр @1132226538@rtu.ru
- Ответственный**: Аскеров Александр @1132226538@rtu.ru
- Источник**: 195.239.374.11
- Пораженные активы**: 10.30.2.22

Рис. 39: Rocketchat RCE

Вывод

В ходе выполнения данной лабораторной работы мы исследовали сценарии целенаправленной атаки на корпоративный мессенджер и сопутствующие сервисы, выявили и продемонстрировали эксплуатацию реальных уязвимостей (WpDiscuz, ProxyLogon, RocketChat), а также отработали методы обнаружения, локализации и нейтрализации последствий компрометации для восстановления безопасности информационной инфраструктуры организации.