

Отчёт по лабораторной работе №2 по кибербезопасности.

Презентация

Дурдалыев Максат

10 октября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Дурдалыев Максат
- студент 4 курса
- Российский университет дружбы народов
- 1032205337@pfur.ru
- <https://github.com/mdurdalyyev>

Выполнение лабораторной работы

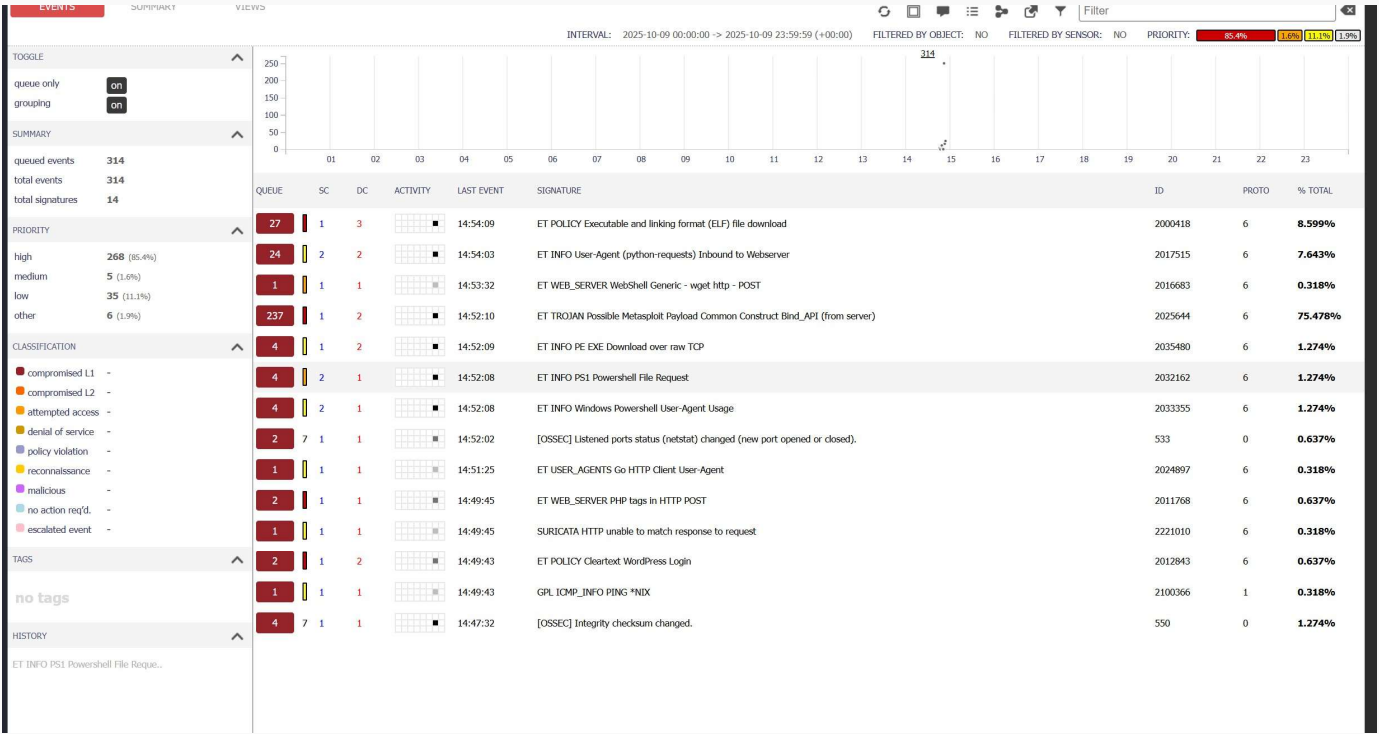


Рис. 1: События, связанные с эксплуатацией уязвимости.

Выполнение лабораторной работы

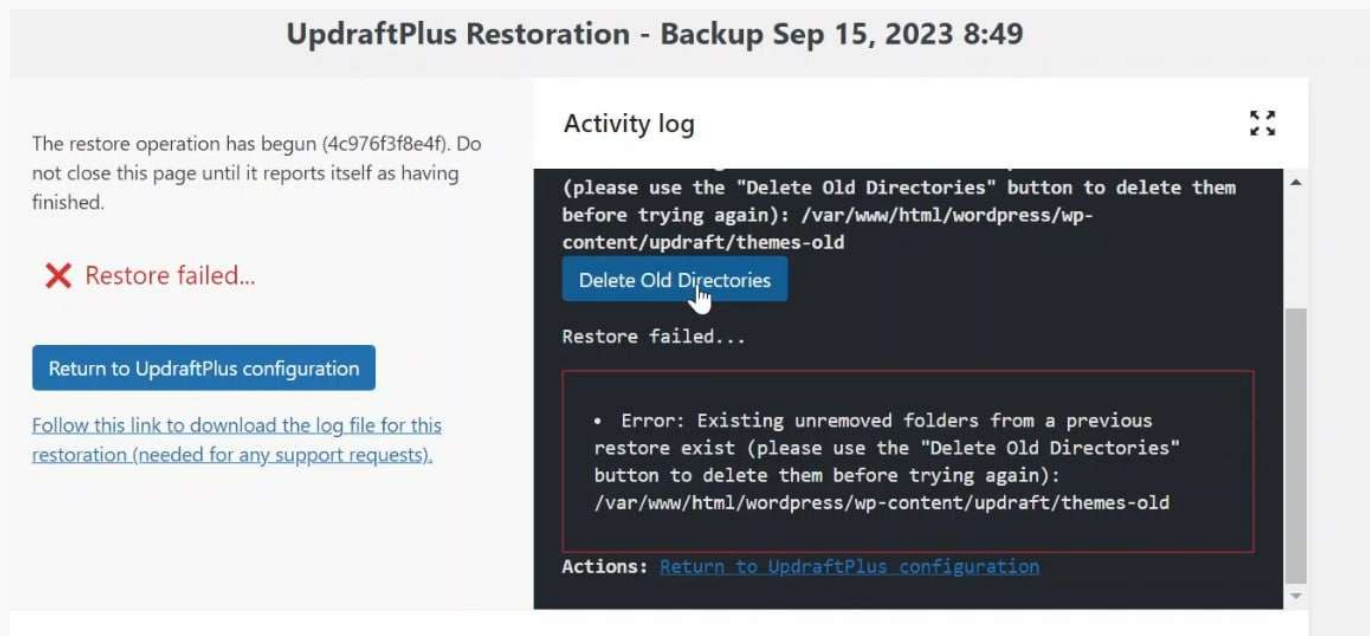


Рис. 2: Ошибка восстановления.

Выполнение лабораторной работы

UpdraftPlus Restoration - Backup Sep 15, 2023 8:49

The restore operation has begun (c24bd7d71516). Do not close this page until it reports itself as having finished.

✓ Restore successful!

[Return to UpdraftPlus configuration](#)

[Follow this link to download the log file for this restoration \(needed for any support requests\).](#)

Activity log

```
Moving old data out of the way...
Moving unpacked backup into place...
Cleaning up rubbish...

Uploads
Unpacking backup... (backup_2023-09-15-0849_webportal3ampirecorp_00140c92e515-uploads.zip, 2.5 MB)
Unzip progress: 100 out of 100 files (2.5 MB, uploads/2021/11/sitesecure-1-300x225.jpeg)
Moving old data out of the way...
Moving unpacked backup into place...
Cleaning up rubbish...

Restore successful!

Actions: Return to UpdraftPlus configuration
```

Рис. 3: Успешное выполнение восстановления.

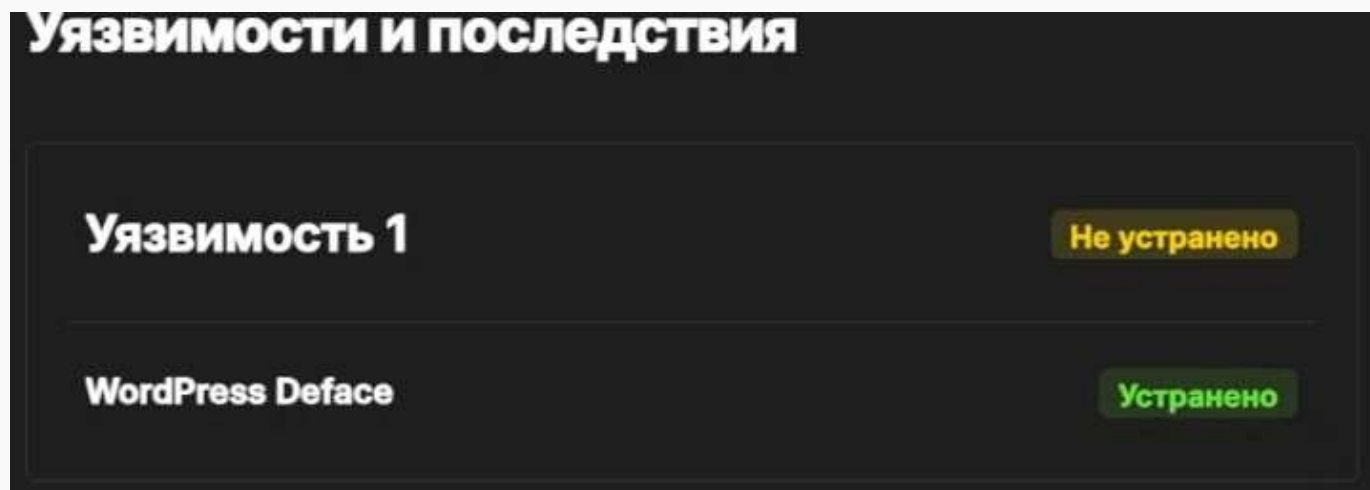


Рис. 4: Последствие WordPress Deface устранено.

Выполнение лабораторной работы

```
n64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.67 Safari/537.36 Edg/87.0.664.47"
root@web-portal-3:/var/log/apache2# ss -tp4
state      Recv-Q      Send-Q               Local Address:Port               Peer Address:Port
STAB              0             36                  10.10.1.22:ssh                    10.10.1.253:20929
users:(("sshd",pid=3058,fd=3),("sshd",pid=2909,fd=3))
CLOSE-WAIT      1             0                  10.10.1.22:60792                  195.239.174.11:5557
users:(("chisel.sh",pid=1745,fd=12),("sh",pid=1744,fd=12),("FkAaL",pid=1709,fd=12))
STAB              0             0                  10.10.1.22:38774                  195.239.174.11:freeciv
users:(("chisel.sh",pid=1745,fd=3),("sh",pid=1744,fd=3),("FkAaL",pid=1709,fd=3))
IN-WAIT-2       0             0                  10.10.1.22:37242                  10.10.2.11:https
users:(("chisel.sh",pid=1745,fd=16))
STAB              0             0                  10.10.1.22:37822                  195.239.174.11:1085
users:(("chisel.sh",pid=1745,fd=11))
root@web-portal-3:/var/log/apache2# kill 1745
root@web-portal-3:/var/log/apache2# ss -tp4
state      Recv-Q      Send-Q               Local Address:Port               Peer Address:Port               users:
STAB              0             36                  10.10.1.22:ssh                    10.10.1.253:20929                users:(("sshd",pid=3058,fd=3),("sshd",pid=2909,fd=3))
CLOSE-WAIT      1             0                  10.10.1.22:60792                  195.239.174.11:5557                users:(("FkAaL",pid=1709,fd=12))
STAB              0             0                  10.10.1.22:38774                  195.239.174.11:freeciv            users:(("FkAaL",pid=1709,fd=3))
IN-WAIT-2       0             0                  10.10.1.22:37242                  10.10.2.11:https
root@web-portal-3:/var/log/apache2# kill 1709
root@web-portal-3:/var/log/apache2#
```

Рис. 5: Закрытие сессии.

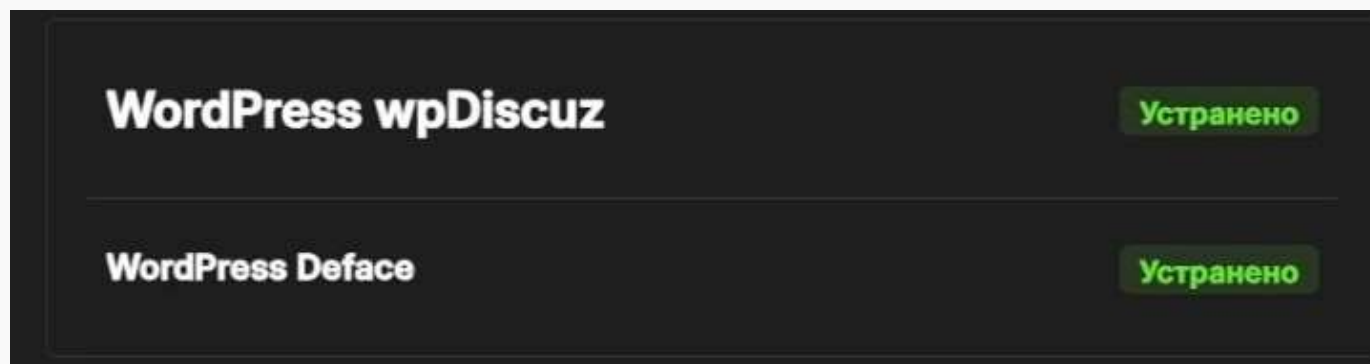
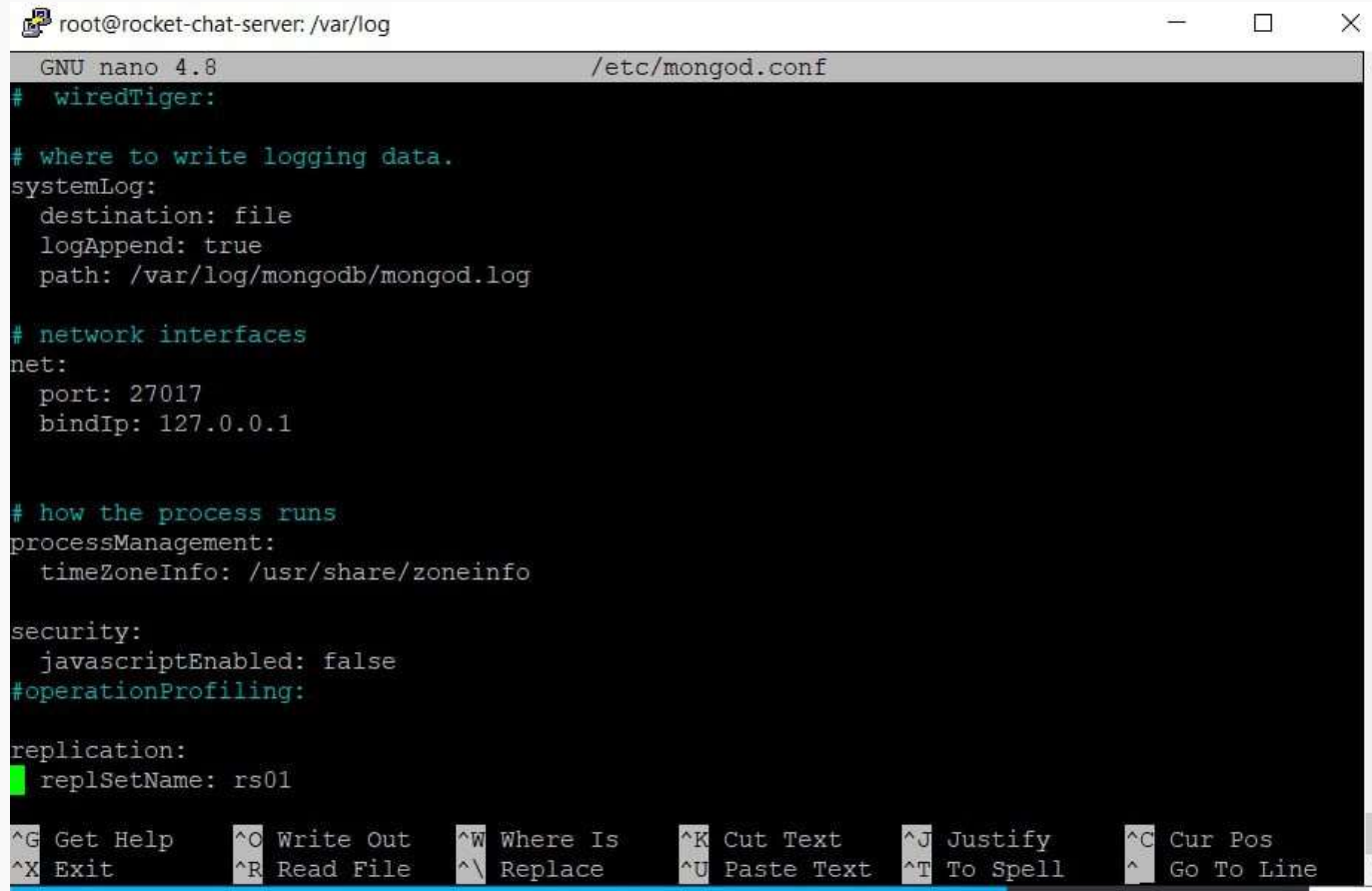


Рис. 6: Уязвимость WordPress wpDiscuz устранена.

Выполнение лабораторной работы



```
root@rocket-chat-server: /var/log
GNU nano 4.8 /etc/mongod.conf
# 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
#operationProfiling:

replication:
  replSetName: rs01

^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. 7: Настройка конфигурации БД для отключения операций с кодами на JavaScript на стороне сервера.

Выполнение лабораторной работы

```
root@rocket-chat-server:/var/log# systemctl restart mongod.service
root@rocket-chat-server:/var/log# systemctl status mongod.service
● mongod.service - MongoDB Database Server
   Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-10-13 16:02:07 UTC; 6s ago
     Docs: https://docs.mongodb.org/manual
   Main PID: 3795 (mongod)
    Memory: 184.1M
    CGroup: /system.slice/mongod.service
            └─3795 /usr/bin/mongod --config /etc/mongod.conf

Oct 13 16:02:07 rocket-chat-server systemd[1]: mongod.service: Succeeded.
Oct 13 16:02:07 rocket-chat-server systemd[1]: Stopped MongoDB Database Server.
Oct 13 16:02:07 rocket-chat-server systemd[1]: Started MongoDB Database Server.
root@rocket-chat-server:/var/log#
```

Рис. 8: Перезагрузка RocketChat.

Выполнение лабораторной работы

```
root@rocket-chat-server:/# ss -tp4 | grep 174.11
ESTAB  0      0      10.10.2.22:51100      195.239.174.11:5559  users: ("t
estsystem",pid=2066,fd=3))
root@rocket-chat-server:/# kill 2066
```

Рис. 9: Заккрытие сессии с нарушителем.

Выполнение лабораторной работы

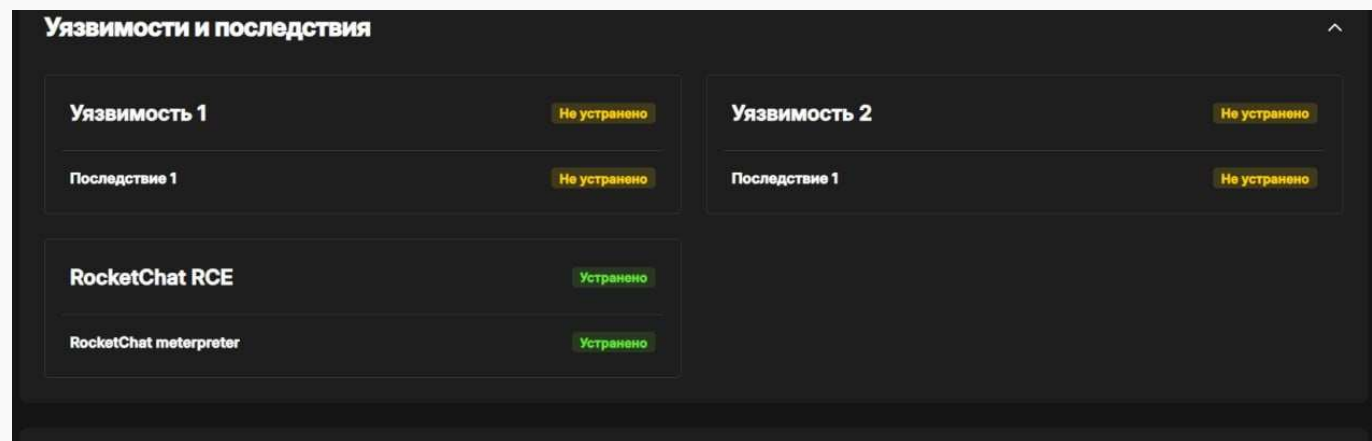


Рис. 10: Уязвимость RocketChat RCE и последствие RocketChat meterpreter устранены.

Выполнение лабораторной работы

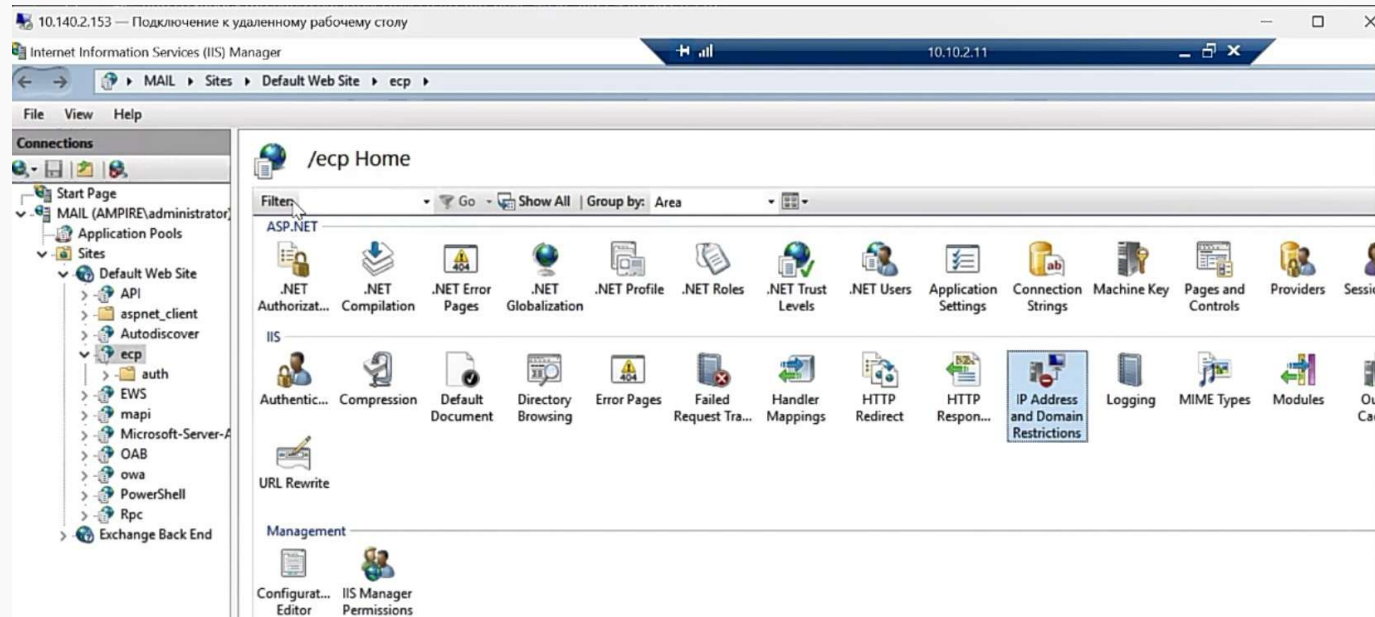


Рис. 11: Окно Internet Information Services (ISS) Manager.

Выполнение лабораторной работы

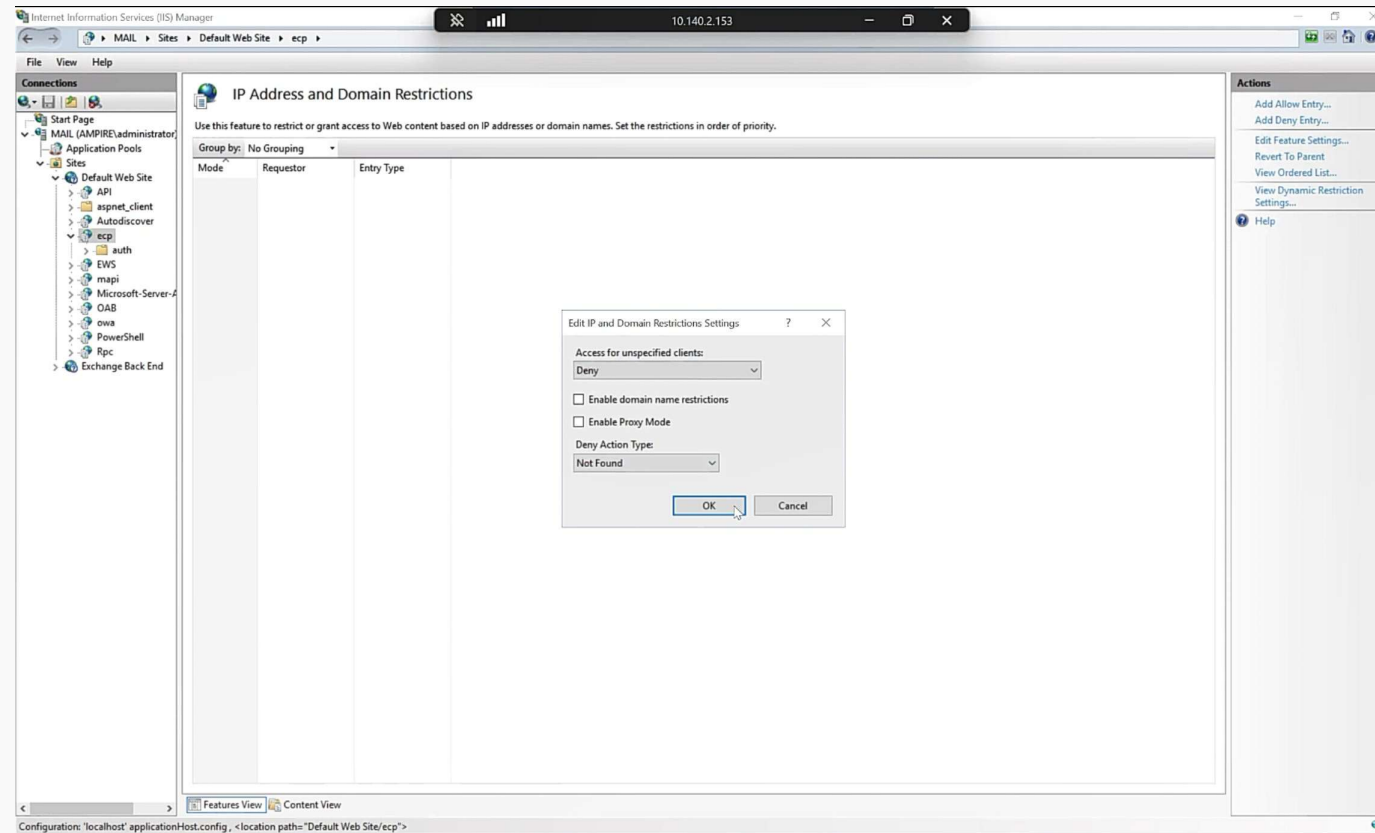
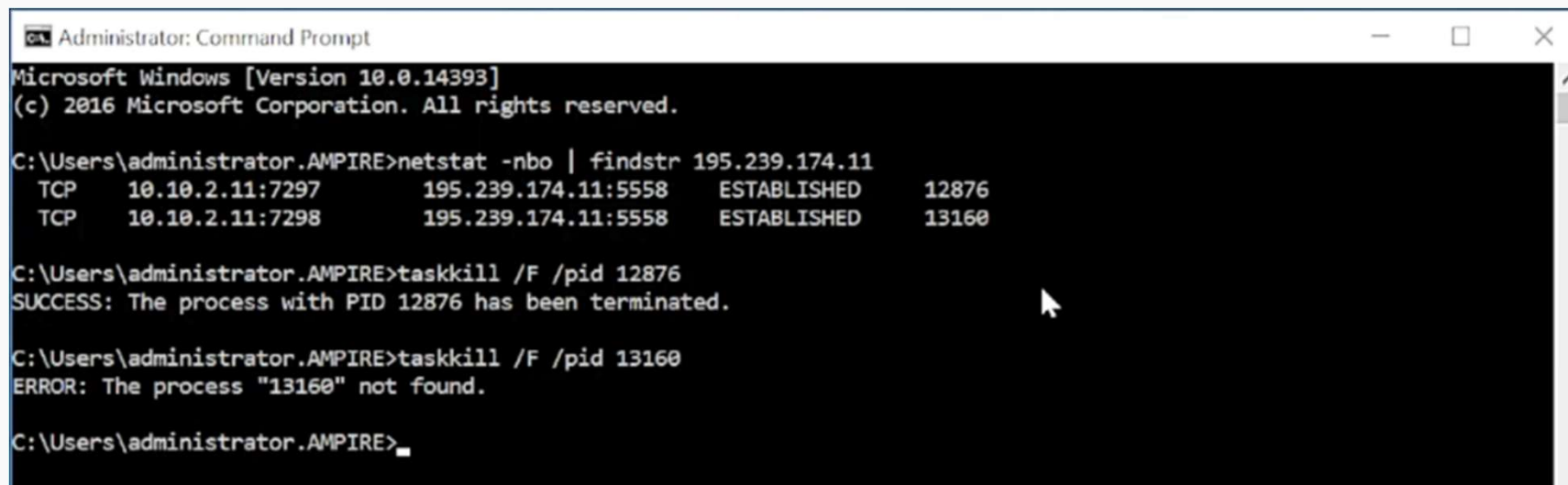


Рис. 12: IP Address and Domain Restrictions.

Выполнение лабораторной работы



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\administrator.AMPIRE>netstat -nbo | findstr 195.239.174.11
TCP    10.10.2.11:7297      195.239.174.11:5558  ESTABLISHED    12876
TCP    10.10.2.11:7298      195.239.174.11:5558  ESTABLISHED    13160

C:\Users\administrator.AMPIRE>taskkill /F /pid 12876
SUCCESS: The process with PID 12876 has been terminated.

C:\Users\administrator.AMPIRE>taskkill /F /pid 13160
ERROR: The process "13160" not found.

C:\Users\administrator.AMPIRE>
```

Рис. 13: Устранение последствия Exchange China Chopper.

Выполнение лабораторной работы

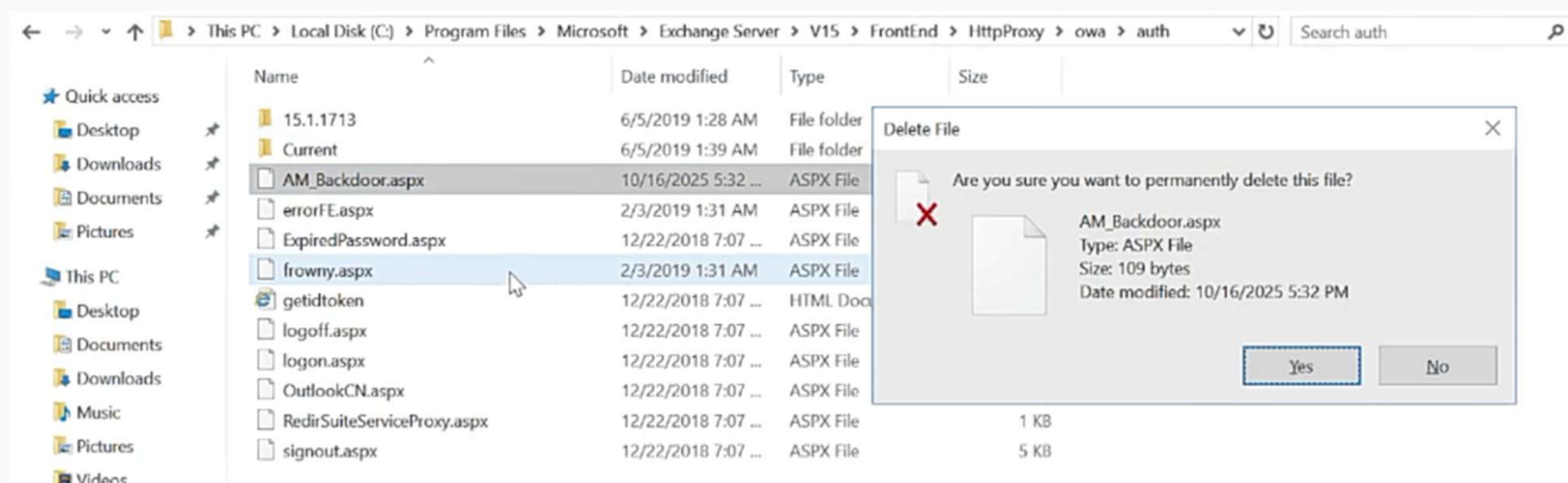



Рис. 14: Обнаружение Exchange China Chopper последствия в приведенном на скриншоте пути.

Выполнение лабораторной работы



Тренировка запущена. Атака завершена 100%

00:02:49

Сценарий: Amprige Защита корпоративного мессенджера
Шаблон: Офис (Конфигуратор)

CSIRT

Запущена в: 17:29

Назначенные инциденты

Инциденты отсутствуют

Уязвимости и последствия

Уязвимость 1	Не устранено	Proxylogon	Устранено
Последствие 1	Не устранено	Exchange China Chopper	Устранено
Уязвимость 3	Не устранено		
Последствие 1	Не устранено		

Рис. 15: Устранение уязвимости Proxylogon и последствия Exchange China Chopper.

Выводы

В ходе данной лабораторной мы устранили 3 уязвимости и 3 последствия.