

Лабораторная работа №2

Кибербезопасность предприятия

Крутова Екатерина Дмитриевна, Прасолов Валерий Сергеевич | НПИ-22

30.09.2025

Российский университет дружбы народов

Москва, Россия

Цель лабораторной работы

Показать этапы реализации атак и контрмер в сценарии защиты корпоративного мессенджера, определить уязвимости, продемонстрировать доказательства успешной эксплуатации и предложить практические способы устранения.

Сценарий №5

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

Обнаружение атак:

●	20:56:16.292 02....	1	ET POLICY Executable and L...	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 L...	policy-violation	TCP	195.239.174.11	5556	10.10.1.22	462

Рис. 1: Серия атак

- **Уязвимость 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).

Последствие 1: Deface.

- **Уязвимость 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.

Последствие 2: Exchange China Chopper.

- **Уязвимость 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

Для устранения уязвимости 1 мы деактивировали WordPress.

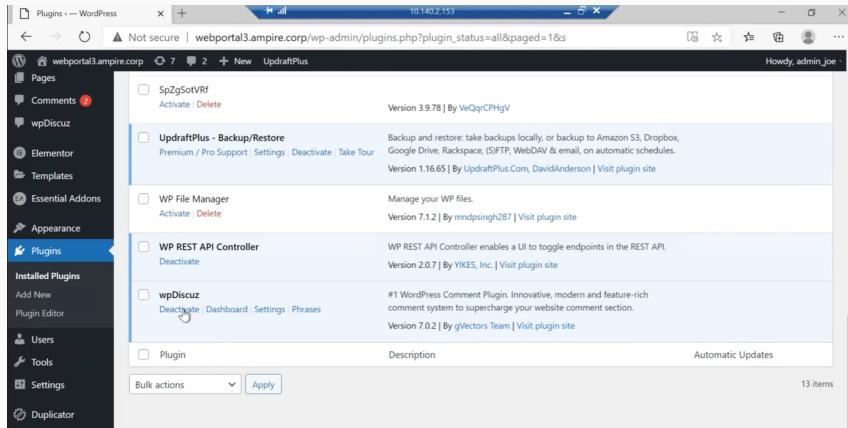


Рис. 2: Деактивация WordPress

Решение последствия 1

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

UpdraftPlus Restoration - Backup Sep 15, 2023 8:49

The restore operation has begun (e325827bd219). 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...

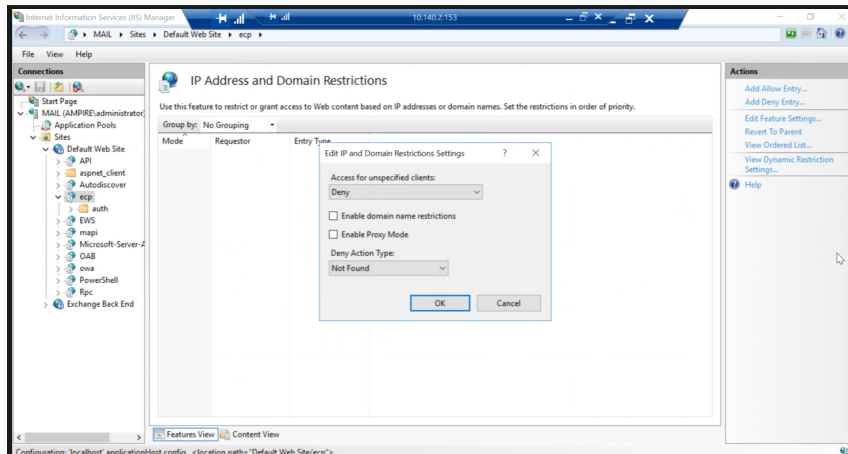
Uploads
Unpacking backup... (backup_2023-09-15-0849_webportal3ampirecorp_00140c92e515-uploads.zip, 2.5 MB)
Unzip progress: 100 out of 100 files (2.5 MB, uploads/2021/11/sitesecure-1-300x225.jpeg)
Moving old data out of the way...
Moving unpacked backup into place...
Cleaning up rubbish...

Restore successful!

Actions: Return to UpdraftPlus configuration
```

Уязвимость 2

Для устранения уязвимости 2 мы ограничили доступ к указанной директории для запрета эксплуатации уязвимости:



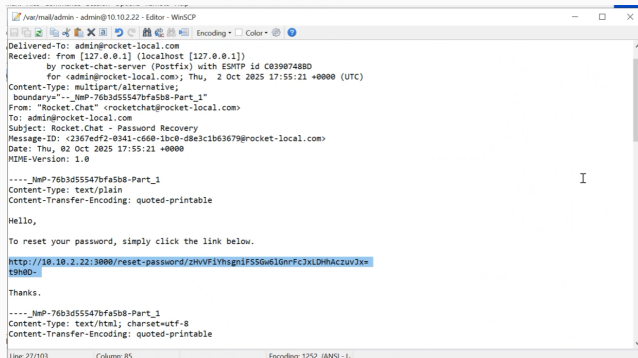
Решение последствий 2

Для устранения полезной нагрузки мы удалили файл веб-оболочки по пути C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\..\auth\ и завершили все соединения между уязвимой машиной и нарушителем.

```
user@web-portal-3i:~$ sudo ss -tp4
[sudo] password for user:
State      Recv-Q   Send-Q   Local Address:Port      Peer Address:Port
ESTAB      0         0        10.10.1.22:46212        195.239.174.11:freeciv
users: (("chisel.sh",pid=3033,fd=3), ("sh",pid=3032,fd=3), ("UnJyQ",pid=2992,fd=3)
)
CLOSE-WAIT 1         0        10.10.1.22:58346        195.239.174.11:5557
users: (("chisel.sh",pid=3033,fd=12), ("sh",pid=3032,fd=12), ("UnJyQ",pid=2992,fd=
12))
ESTAB      0         0        10.10.1.22:43566        195.239.174.11:1085
users: (("chisel.sh",pid=3033,fd=11))
FIN-WAIT-2 0         0        10.10.1.22:57202        10.10.2.11:https
users: (("chisel.sh",pid=3033,fd=16))
ESTAB      0         64       10.10.1.22:ssh          10.10.1.253:10330
users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
user@web-portal-3i:~$ kill 3033
-bash: kill: (3033) - Operation not permitted
user@web-portal-3i:~$ sudo kill 3033
[sudo] password for user:
user@web-portal-3i:~$ sudo ss -tp4
State      Recv-Q   Send-Q   Local Address:Port      Peer Address:Port
ESTAB      0         0        10.10.1.22:46212        195.239.174.11:freeciv
users: (("UnJyQ",pid=2992,fd=3))
CLOSE-WAIT 1         0        10.10.1.22:58346        195.239.174.11:5557
users: (("UnJyQ",pid=2992,fd=12))
FIN-WAIT-2 0         0        10.10.1.22:57202        10.10.2.11:https
ESTAB      0         64       10.10.1.22:ssh          10.10.1.253:10330
users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
user@web-portal-3i:~$ sudo kill 2992
user@web-portal-3i:~$ sudo ss -tp4
State      Recv-Q   Send-Q   Local Address:Port      Peer Address:Port
LAST-ACK   1         1        10.10.1.22:58346        195.239.174.11:5557
ESTAB      0         64       10.10.1.22:ssh          10.10.1.253:10330
users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
user@web-portal-3i:~$
```

Рис. 5: Соединения с машиной нарушителя

Для восстановления доступа к аккаунту администратора необходимо сбросить пароль.



```
/var/mail/admin - admin@10.10.2.22 - Editor - WinSCP
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/zHvVFiyhsnIF55Gw6lGnFcJxLDHhAczuvJx=t9h0D-

Thanks.

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

Рис. 6: /var/mail/admin

Решение последствий 3

Данная полезная нагрузка заключается в получении нарушителем meterpreter-сессии с уязвимым сервером.

Её можно обнаружить и устранить (рис. @fig:020).

```
user@web-portal-3:~$ sudo ss -tp4
[sudo] password for user:
State      Recv-Q      Send-Q           Local Address:Port      Peer Address:Port
ESTAB      0            0                10.10.1.22:46212        195.239.174.11:freeciv
users: (("chisel.sh",pid=3033,fd=3), ("sh",pid=3032,fd=3), ("UnJyQ",pid=2992,fd=3)
)
CLOSE-WAIT 1            0                10.10.1.22:58346        195.239.174.11:5557
users: (("chisel.sh",pid=3033,fd=12), ("sh",pid=3032,fd=12), ("UnJyQ",pid=2992,fd=
12))
ESTAB      0            0                10.10.1.22:43566        195.239.174.11:1085
users: (("chisel.sh",pid=3033,fd=11))
FIN-WAIT-2 0            0                10.10.1.22:57202        10.10.2.11:https
users: (("chisel.sh",pid=3033,fd=16))
ESTAB      0            64               10.10.1.22:ssh          10.10.1.253:10330
users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
user@web-portal-3:~$ sudo kill 3033
-bash: kill: (3033) - Operation not permitted
user@web-portal-3:~$ sudo kill 3033
[sudo] password for user:
user@web-portal-3:~$ sudo ss -tp4
State      Recv-Q      Send-Q           Local Address:Port      Peer Address:Port
ESTAB      0            0                10.10.1.22:46212        195.239.174.11:freeciv      users: (("UnJyQ",pid=2992,fd=3))
CLOSE-WAIT 1            0                10.10.1.22:58346        195.239.174.11:5557      users: (("UnJyQ",pid=2992,fd=12))
FIN-WAIT-2 0            0                10.10.1.22:57202        10.10.2.11:https
ESTAB      0            64               10.10.1.22:ssh          10.10.1.253:10330      users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
d=8360,fd=3))
user@web-portal-3:~$ sudo kill 2992
user@web-portal-3:~$ sudo ss -tp4
State      Recv-Q      Send-Q           Local Address:Port      Peer Address:Port
LAST-ACK   1            1                10.10.1.22:58346        195.239.174.11:5557
ESTAB      0            64               10.10.1.22:ssh          10.10.1.253:10330
users: (("sshd",pid=8483,fd=3), ("sshd",pid=8360,fd=3))
user@web-portal-3:~$
```

Рис. 8: Соединения с машиной нарушителя