Отчёт по лабораторной работе №3

Идентифицировать и устранить уязвимости

Кроитору Екатерина, Захаренко Анастасия, Щербакова Вероника

15 Апреля 2025

Российский университет дружбы народов, Москва, Россия

Вводная часть

Корпоративные мессенджеры, такие как Rocket.Chat, широко используются для внутренней коммуникации в организациях. При этом они становятся привлекательной целью для хакеров, особенно при наличии известных уязвимостей. В рамках данной тренировки была смоделирована атака на корпоративную инфраструктуру с целью выявления и устранения уязвимостей.

Актуальность

Современные киберугрозы всё чаще нацелены на повседневные сервисы, включая мессенджеры и CMS. Уязвимости, такие как ProxyLogon и wpDiscuz, активно эксплуатируются злоумышленниками. Поэтому важно уметь своевременно реагировать на инциденты, устранять последствия и обеспечивать стабильную работу критически важных систем.

Цель

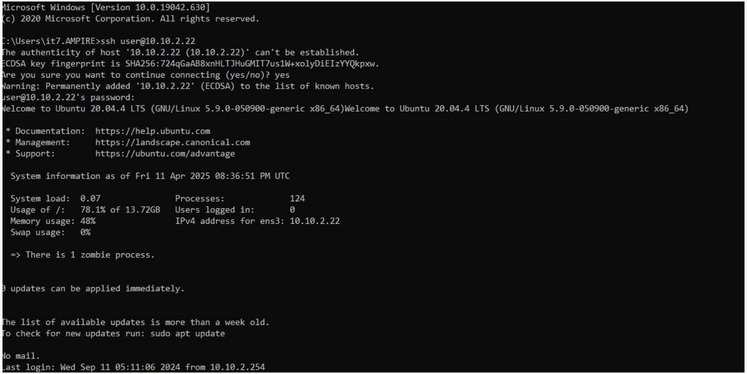
В рамках тренировки необходимо было устранить уязвимости в корпоративной инфраструктуре и нейтрализовать последствия атаки. Работа выполнялась через терминал удалённого рабочего места с ограниченным доступом.

Используемые ресурсы

- Удалённое рабочее место — `10.140.2.128`, логин: `ampire\it9`, пароль: `958923`
- SecOnion — `10.140.2.164`, логин: `admin`, пароль: `qwe123!@#`
- ViPNet IDS NS — `10.140.2.170`, логин: `mon19`, пароль: `qweQWE123419`

Ход работы 1. Подключение к удаленному рабочему месту

Осуществлено подключение по RDP к терминалу Windows.(рис.1).

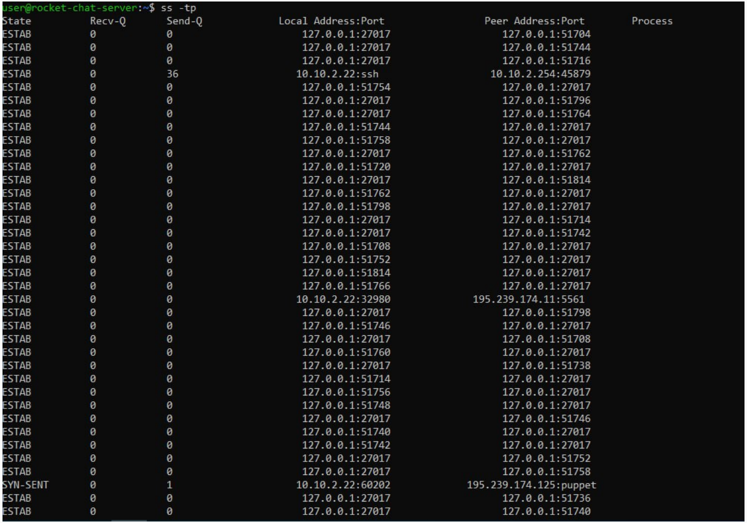


```
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\it7.AMPIRE>ssh user@10.10.2.22
The authenticity of host '10.10.2.22 (10.10.2.22)' can't be established.
ECDSA key fingerprint is SHA256:724qGaAB8xnHLTJHuGMIT7us1W+xolyDiEIzYYQkpxw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.2.22' (ECDSA) to the list of known hosts.
user@10.10.2.22's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.9.0-050900-generic x86_64)Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.9.0-050900-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 11 Apr 2025 08:36:51 PM UTC

  System load:  0.07               Processes:             124
  Usage of /:   78.1% of 13.72GB   Users logged in:       0
  Memory usage: 48%                IPv4 address for ens3: 10.10.2.22
  Swap usage:   0%

  => There is 1 zombie process.


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

No mail.
Last login: Wed Sep 11 05:11:06 2024 from 10.10.2.254
```

Рис. 1: Скрин 1

2. Обнаружение признаков атаки на Rocket.Chat

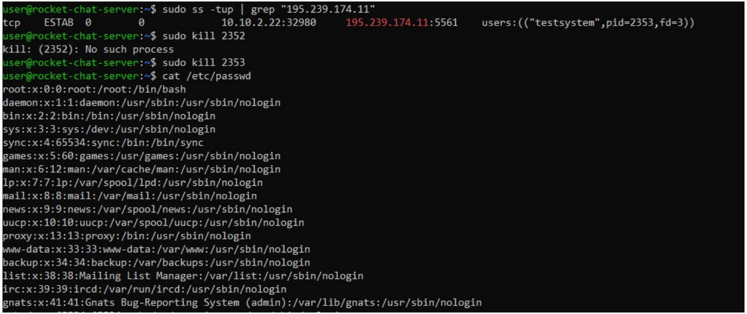
На терминале фиксируются сбои и нестандартное поведение Rocket.Chat.(рис.2).



```
user@rocket-chat-server:~$ ss -tp
State          Recv-Q       Send-Q             Local Address:Port                 Peer Address:Port        Process
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51704
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51744
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51716
ESTAB          0            36                    10.10.2.22:ssh                   10.10.2.254:45879
ESTAB          0            0                      127.0.0.1:51754                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51796
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51764
ESTAB          0            0                      127.0.0.1:51744                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51758                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51762
ESTAB          0            0                      127.0.0.1:51720                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51814
ESTAB          0            0                      127.0.0.1:51762                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51798                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51714
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51742
ESTAB          0            0                      127.0.0.1:51708                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51752                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51814                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51766                   127.0.0.1:27017
ESTAB          0            0                     10.10.2.22:32980              195.239.174.11:5561
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51798
ESTAB          0            0                      127.0.0.1:51746                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51708
ESTAB          0            0                      127.0.0.1:51760                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51738
ESTAB          0            0                      127.0.0.1:51714                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51756                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51748                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51746
ESTAB          0            0                      127.0.0.1:51740                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:51742                   127.0.0.1:27017
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51752
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51758
SYN-SENT       0            1                     10.10.2.22:60202             195.239.174.125:puppet
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51736
ESTAB          0            0                      127.0.0.1:27017                   127.0.0.1:51740
```

3. Проверка активности в WordPress (wpDiscuz)

Выявлена подозрительная активность через плагин wpDiscuz.(рис.3).

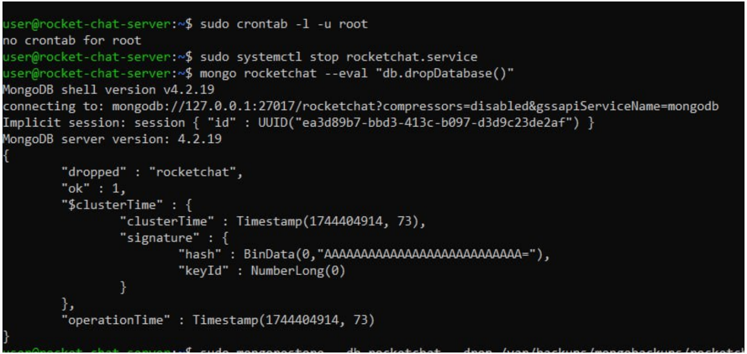


```
user@rocket-chat-server:~$ sudo ss -tup | grep "195.239.174.11"
tcp    ESTAB  0       0             10.10.2.22:32980     195.239.174.11:5561    users:(("testsystem",pid=2353,fd=3))
user@rocket-chat-server:~$ sudo kill 2352
kill: (2352): No such process
user@rocket-chat-server:~$ sudo kill 2353
user@rocket-chat-server:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

Рис. 3: Скрин 3

4. Проверка логов в SecOnion

Переход к инструменту SecOnion для анализа событий.(рис.4).

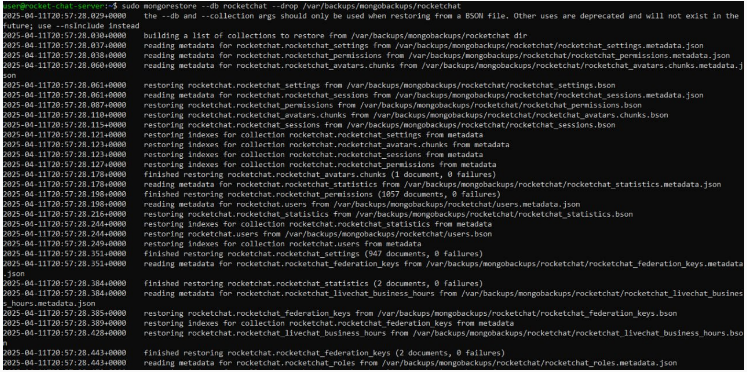


```
user@rocket-chat-server:~$ sudo crontab -l -u root
no crontab for root
user@rocket-chat-server:~$ sudo systemctl stop rocketchat.service
user@rocket-chat-server:~$ mongo rocketchat --eval "db.dropDatabase()"
MongoDB shell version v4.2.19
connecting to: mongodb://127.0.0.1:27017/rocketchat?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("ea3d89b7-bbd3-413c-b097-d3d9c23de2af") }
MongoDB server version: 4.2.19
{
        "dropped" : "rocketchat",
        "ok" : 1,
        "$clusterTime" : {
                "clusterTime" : Timestamp(1744404914, 73),
                "signature" : {
                        "hash" : BinData(0,"AAAAAAAAAAAAAAAAAAAAAAAAAAA="),
                        "keyId" : NumberLong(0)
                }
        },
        "operationTime" : Timestamp(1744404914, 73)
}
user@rocket-chat-server:~$ sudo mongorestore --db rocketchat --drop /var/backups/mongobackups/rocketch
```

Рис. 4: Скрин 4

5. Анализ трафика в SecOnion

Определение аномального сетевого трафика.(рис.5).

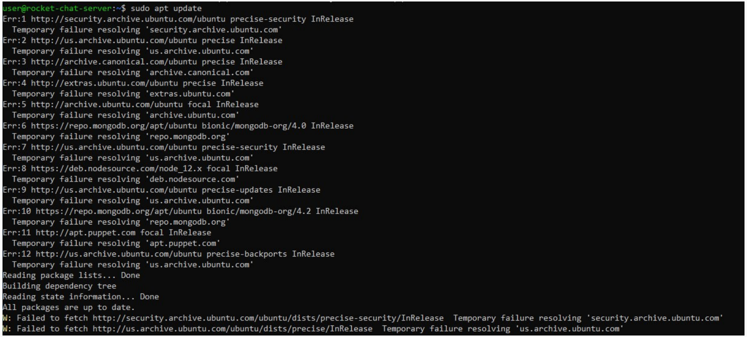


```
user@rocket-chat-server:~$ sudo mongorestore --db rocketchat --drop /var/backups/mongobackups/rocketchat
2025-04-11T20:57:28.029+0000    the --db and --collection args should only be used when restoring from a BSON file. Other uses are deprecated and will not exist in the
future; use --nsInclude instead
2025-04-11T20:57:28.030+0000    building a list of collections to restore from /var/backups/mongobackups/rocketchat dir
2025-04-11T20:57:28.037+0000    reading metadata for rocketchat.rocketchat_settings from /var/backups/mongobackups/rocketchat/rocketchat_settings.metadata.json
2025-04-11T20:57:28.038+0000    reading metadata for rocketchat.rocketchat_permissions from /var/backups/mongobackups/rocketchat/rocketchat_permissions.metadata.json
2025-04-11T20:57:28.060+0000    reading metadata for rocketchat.rocketchat_avatars.chunks from /var/backups/mongobackups/rocketchat/rocketchat_avatars.chunks.metadata.j
son
2025-04-11T20:57:28.061+0000    restoring rocketchat.rocketchat_settings from /var/backups/mongobackups/rocketchat/rocketchat_settings.bson
2025-04-11T20:57:28.061+0000    reading metadata for rocketchat.rocketchat_sessions from /var/backups/mongobackups/rocketchat/rocketchat_sessions.metadata.json
2025-04-11T20:57:28.087+0000    restoring rocketchat.rocketchat_permissions from /var/backups/mongobackups/rocketchat/rocketchat_permissions.bson
2025-04-11T20:57:28.110+0000    restoring rocketchat.rocketchat_avatars.chunks from /var/backups/mongobackups/rocketchat/rocketchat_avatars.chunks.bson
2025-04-11T20:57:28.115+0000    restoring rocketchat.rocketchat_sessions from /var/backups/mongobackups/rocketchat/rocketchat_sessions.bson
2025-04-11T20:57:28.121+0000    restoring indexes for collection rocketchat.rocketchat_settings from metadata
2025-04-11T20:57:28.123+0000    restoring indexes for collection rocketchat.rocketchat_avatars.chunks from metadata
2025-04-11T20:57:28.123+0000    restoring indexes for collection rocketchat.rocketchat_sessions from metadata
2025-04-11T20:57:28.127+0000    restoring indexes for collection rocketchat.rocketchat_permissions from metadata
2025-04-11T20:57:28.178+0000    finished restoring rocketchat.rocketchat_avatars.chunks (1 document, 0 failures)
2025-04-11T20:57:28.178+0000    reading metadata for rocketchat.rocketchat_statistics from /var/backups/mongobackups/rocketchat/rocketchat_statistics.metadata.json
2025-04-11T20:57:28.198+0000    finished restoring rocketchat.rocketchat_permissions (1057 documents, 0 failures)
2025-04-11T20:57:28.198+0000    reading metadata for rocketchat.users from /var/backups/mongobackups/rocketchat/users.metadata.json
2025-04-11T20:57:28.216+0000    restoring rocketchat.rocketchat_statistics from /var/backups/mongobackups/rocketchat/rocketchat_statistics.bson
2025-04-11T20:57:28.244+0000    restoring indexes for collection rocketchat.rocketchat_statistics from metadata
2025-04-11T20:57:28.244+0000    restoring rocketchat.users from /var/backups/mongobackups/rocketchat/users.bson
2025-04-11T20:57:28.249+0000    restoring indexes for collection rocketchat.users from metadata
2025-04-11T20:57:28.351+0000    finished restoring rocketchat.rocketchat_settings (947 documents, 0 failures)
2025-04-11T20:57:28.351+0000    reading metadata for rocketchat.rocketchat_federation_keys from /var/backups/mongobackups/rocketchat/rocketchat_federation_keys.metadata
.json
2025-04-11T20:57:28.384+0000    finished restoring rocketchat.rocketchat_statistics (2 documents, 0 failures)
2025-04-11T20:57:28.384+0000    reading metadata for rocketchat.rocketchat_livechat_business_hours from /var/backups/mongobackups/rocketchat/rocketchat_livechat_busines
s_hours.metadata.json
2025-04-11T20:57:28.385+0000    restoring rocketchat.rocketchat_federation_keys from /var/backups/mongobackups/rocketchat/rocketchat_federation_keys.bson
2025-04-11T20:57:28.389+0000    restoring indexes for collection rocketchat.rocketchat_federation_keys from metadata
2025-04-11T20:57:28.428+0000    restoring rocketchat.rocketchat_livechat_business_hours from /var/backups/mongobackups/rocketchat/rocketchat_livechat_business_hours.bso
n
2025-04-11T20:57:28.443+0000    finished restoring rocketchat.rocketchat_federation_keys (2 documents, 0 failures)
2025-04-11T20:57:28.443+0000    reading metadata for rocketchat.rocketchat_roles from /var/backups/mongobackups/rocketchat/rocketchat_roles.metadata.json
```

Рис. 5: Скрин 5

6. Переход к ViPNet IDS

Переход на систему IDS для анализа атак.(рис.6).

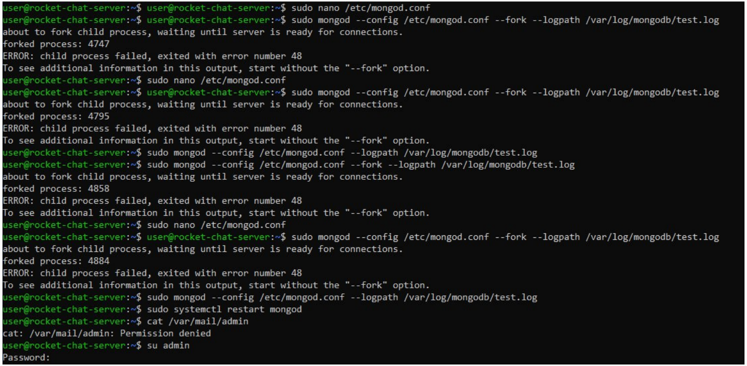


```
user@rocket-chat-server:~$ sudo apt update
Err:1 http://security.archive.ubuntu.com/ubuntu precise-security InRelease
  Temporary failure resolving 'security.archive.ubuntu.com'
Err:2 http://us.archive.ubuntu.com/ubuntu precise InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Err:3 http://archive.canonical.com/ubuntu precise InRelease
  Temporary failure resolving 'archive.canonical.com'
Err:4 http://extras.ubuntu.com/ubuntu precise InRelease
  Temporary failure resolving 'extras.ubuntu.com'
Err:5 http://archive.ubuntu.com/ubuntu focal InRelease
  Temporary failure resolving 'archive.ubuntu.com'
Err:6 https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/4.0 InRelease
  Temporary failure resolving 'repo.mongodb.org'
Err:7 http://us.archive.ubuntu.com/ubuntu precise-security InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Err:8 https://deb.nodesource.com/node_12.x focal InRelease
  Temporary failure resolving 'deb.nodesource.com'
Err:9 http://us.archive.ubuntu.com/ubuntu precise-updates InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Err:10 https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/4.2 InRelease
  Temporary failure resolving 'repo.mongodb.org'
Err:11 http://apt.puppet.com focal InRelease
  Temporary failure resolving 'apt.puppet.com'
Err:12 http://us.archive.ubuntu.com/ubuntu precise-backports InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
W: Failed to fetch http://security.archive.ubuntu.com/ubuntu/dists/precise-security/InRelease  Temporary failure resolving 'security.archive.ubuntu.com'
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise/InRelease  Temporary failure resolving 'us.archive.ubuntu.com'
```

Рис. 6: Скрин 6

7. Обнаружение инцидентов в ViPNet IDS

Находятся сигнатуры, указывающие на эксплуатацию уязвимостей.(рис.7).

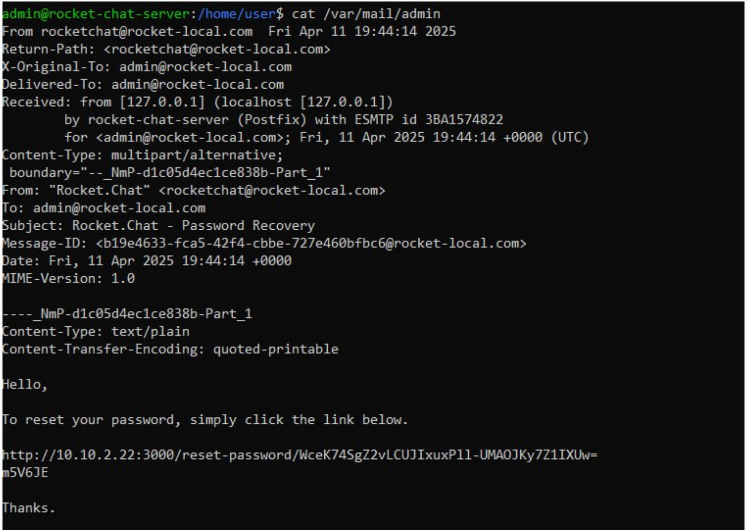


```
user@rocket-chat-server:~$ user@rocket-chat-server:~$ sudo nano /etc/mongod.conf
user@rocket-chat-server:~$ user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --fork --logpath /var/log/mongodb/test.log
about to fork child process, waiting until server is ready for connections.
forked process: 4747
ERROR: child process failed, exited with error number 48
To see additional information in this output, start without the "--fork" option.
user@rocket-chat-server:~$ sudo nano /etc/mongod.conf
user@rocket-chat-server:~$ user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --fork --logpath /var/log/mongodb/test.log
about to fork child process, waiting until server is ready for connections.
forked process: 4795
ERROR: child process failed, exited with error number 48
To see additional information in this output, start without the "--fork" option.
user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --logpath /var/log/mongodb/test.log
user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --fork --logpath /var/log/mongodb/test.log
about to fork child process, waiting until server is ready for connections.
forked process: 4858
ERROR: child process failed, exited with error number 48
To see additional information in this output, start without the "--fork" option.
user@rocket-chat-server:~$ sudo nano /etc/mongod.conf
user@rocket-chat-server:~$ user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --fork --logpath /var/log/mongodb/test.log
about to fork child process, waiting until server is ready for connections.
forked process: 4884
ERROR: child process failed, exited with error number 48
To see additional information in this output, start without the "--fork" option.
user@rocket-chat-server:~$ sudo mongod --config /etc/mongod.conf --logpath /var/log/mongodb/test.log
user@rocket-chat-server:~$ sudo systemctl restart mongod
user@rocket-chat-server:~$ cat /var/mail/admin
cat: /var/mail/admin: Permission denied
user@rocket-chat-server:~$ su admin
Password:
```

Рис. 7: Скрин 7

8. Подготовка к устранению последствий через PowerShell

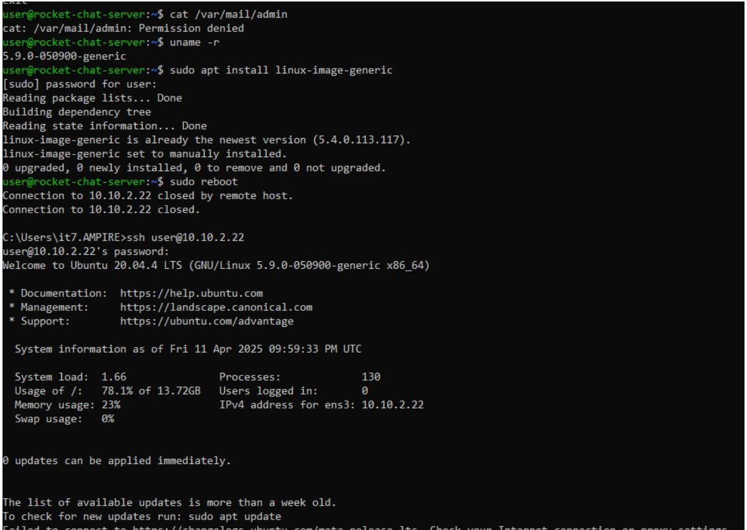
Открытие консоли PowerShell на терминале.(рис.8).



```
admin@rocket-chat-server:/home/user$ cat /var/mail/admin
From rocketchat@rocket-local.com  Fri Apr 11 19:44:14 2025
Return-Path: <rocketchat@rocket-local.com>
X-Original-To: admin@rocket-local.com
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 3BA1574822
        for <admin@rocket-local.com>; Fri, 11 Apr 2025 19:44:14 +0000 (UTC)
Content-Type: multipart/alternative;
 boundary="--_NmP-d1c05d4ec1ce838b-Part_1"
From: "Rocket.Chat" <rocketchat@rocket-local.com>
To: admin@rocket-local.com
Subject: Rocket.Chat - Password Recovery
Message-ID: <b19e4633-fca5-42f4-cbbe-727e460bfbc6@rocket-local.com>
Date: Fri, 11 Apr 2025 19:44:14 +0000
MIME-Version: 1.0

----_NmP-d1c05d4ec1ce838b-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/WceK74SgZ2vLCUJIxuxP1l-UMAOJKy7Z1IXUw=
m5V6JE

Thanks.
```

9. Очистка следов атаки через PowerShell

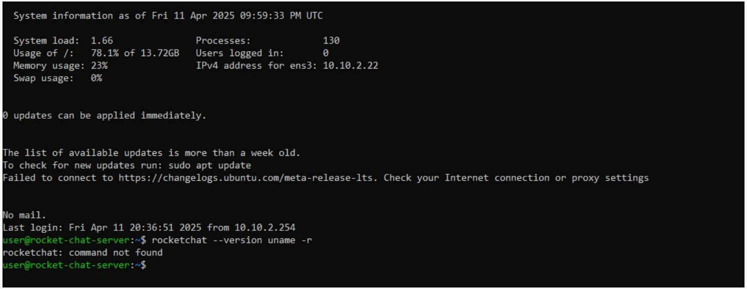
Запущены команды на удаление вредоносных скриптов и логов. (рис.9).



```
exit
user@rocket-chat-server:~$ cat /var/mail/admin
cat: /var/mail/admin: Permission denied
user@rocket-chat-server:~$ uname -r
5.9.0-050900-generic
user@rocket-chat-server:~$ sudo apt install linux-image-generic
[sudo] password for user:
Reading package lists... Done
Building dependency tree
Reading state information... Done
linux-image-generic is already the newest version (5.4.0.113.117).
linux-image-generic set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
user@rocket-chat-server:~$ sudo reboot
Connection to 10.10.2.22 closed by remote host.
Connection to 10.10.2.22 closed.

C:\Users\it7.AMPIRE>ssh user@10.10.2.22
user@10.10.2.22's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.9.0-050900-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 11 Apr 2025 09:59:33 PM UTC

  System load:  1.66               Processes:             130
  Usage of /:   78.1% of 13.72GB   Users logged in:       0
  Memory usage: 23%                IPv4 address for ens3: 10.10.2.22
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

10. Проверка состояния Rocket.Chat после действий

Удостоверение в том, что мессенджер восстановил работоспособность. (рис.10).

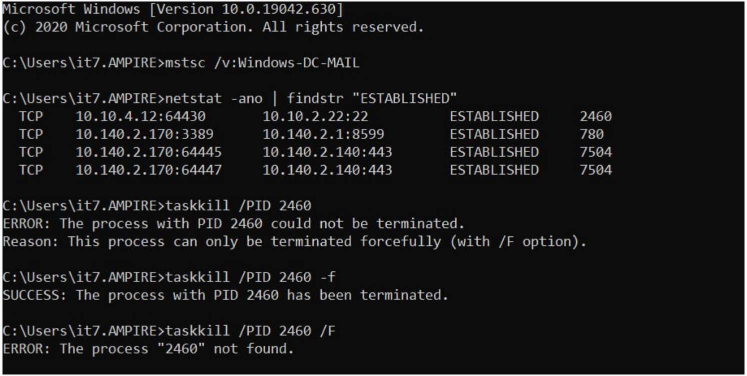


```
  System information as of Fri 11 Apr 2025 09:59:33 PM UTC

  System load:  1.66               Processes:             130
  Usage of /:   78.1% of 13.72GB   Users logged in:       0
  Memory usage: 23%                IPv4 address for ens3: 10.10.2.22
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


No mail.
Last login: Fri Apr 11 20:36:51 2025 from 10.10.2.254
user@rocket-chat-server:~$ rocketchat --version uname -r
rocketchat: command not found
user@rocket-chat-server:~$
```

Рис. 10: Скрин 10

11. Финальный мониторинг и контроль

Проверка логов и системной активности на наличие остаточных угроз.(рис.11).

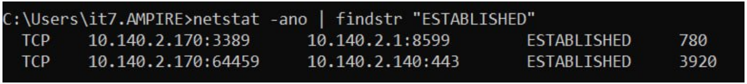


```
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\it7.AMPIRE>mstsc /v:Windows-DC-MAIL

C:\Users\it7.AMPIRE>netstat -ano | findstr "ESTABLISHED"
  TCP    10.10.4.12:64430       10.10.2.22:22          ESTABLISHED     2460
  TCP    10.140.2.170:3389      10.140.2.1:8599        ESTABLISHED     780
  TCP    10.140.2.170:64445     10.140.2.140:443       ESTABLISHED     7504
  TCP    10.140.2.170:64447     10.140.2.140:443       ESTABLISHED     7504

C:\Users\it7.AMPIRE>taskkill /PID 2460
ERROR: The process with PID 2460 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).

C:\Users\it7.AMPIRE>taskkill /PID 2460 -f
SUCCESS: The process with PID 2460 has been terminated.

C:\Users\it7.AMPIRE>taskkill /PID 2460 /F
ERROR: The process "2460" not found.
```

Рис. 11: Скрин 11

12. Итоговый контроль

Заключительный этап — убеждаемся, что уязвимости устранены, активность стабильна.(рис.12).



```
C:\Users\it7.AMPIRE>netstat -ano | findstr "ESTABLISHED"
  TCP    10.140.2.170:3389      10.140.2.1:8599        ESTABLISHED     780
  TCP    10.140.2.170:64459     10.140.2.140:443       ESTABLISHED     3920
```

Рис. 12: Скрин 12

Выводы

- Все три уязвимости (ProxyLogon, Rocket.Chat, WordPress-WPDiscuz) были обнаружены и устранены.
- Использованы системы анализа трафика и IDS для выявления источников атак.
- Проведена очистка системы и восстановление сервисов.
- Финальный мониторинг подтвердил отсутствие следов вредоносной активности.

Рекомендации: - Настроить автоматические обновления для всех сервисов. - Регулярно проводить аудит безопасности. - Усилить сегментацию сети и изоляцию критических компонентов.