

Выполнение лабораторной работы 1

Цель работы

Цель работы

Закрепить практические навыки устранения уязвимостей и защиты корпоративных сервисов.

Задание

Провести анализ уязвимостей и устраниить их на примере MS Exchange и сопутствующих сервисов.

Выполнение лабораторной работы

Уязвимость «PROXYLOGON»

Proxylogon представляет собой SSRF- уязвимость, позволяющую обойти аутентификацию и выдать себя за администратора

Сначала мы завели карточку с описание уязвимости, ее индикаторами и рекомендациями по устранению

The screenshot shows a dark-themed web interface for managing vulnerabilities. At the top, there are tabs for 'Основная информация' (Main Information) and 'Чат' (Chat), with 'Основная информация' being active. A status indicator 'В работе' (In Progress) is shown with a dropdown arrow. On the left side, there are four main sections: 'Дата и время события' (Event Date and Time) showing '25.09.2025 18:59'; 'Описание' (Description) containing the text 'Атака на MS Exchange на базе Kali с попыткой эксплуатации уязвимости Proxylogon. Атакующий - внешний нарушитель'; 'Индикаторы компрометации' (Compromise Indicators) listing '- необычные DNS-запросы; - подозрительные файлы, приложения или процессы'; and 'Рекомендации' (Recommendations) with the note '- установить патч от Microsoft (KBS000871); - закрыть доступ к Панели управления Exchange (Exchange Control Panel)'. To the right, there are sections for 'Оценка' (Rating) with a 5-star icon, 'Автор' (Author) listed as 'Гузева Ирина @1132226441@pfur.ru' with a GitHub icon, 'Ответственный' (Responsible) also listed as 'Гузева Ирина @1132226441@pfur.ru' with a dropdown arrow, 'Источник' (Source) showing '195.239.174.11', and 'Поражённые активы' (Affected Assets) showing '10.10.2.11'.

Figure 1: карточка

Устранием уязвимость, ограничиваем доступ к панели управления

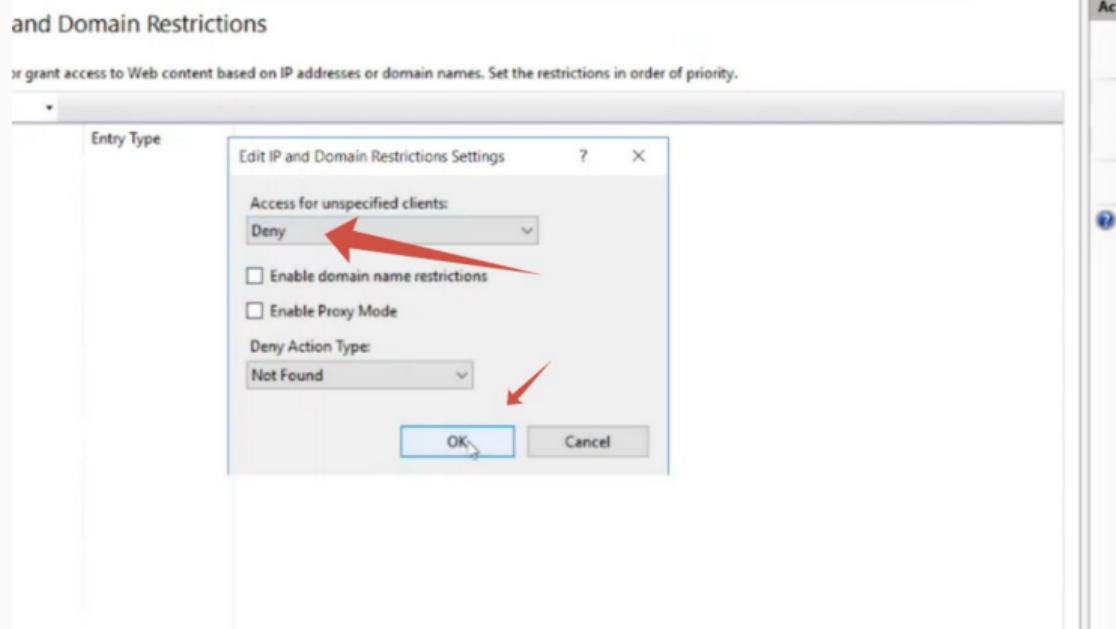
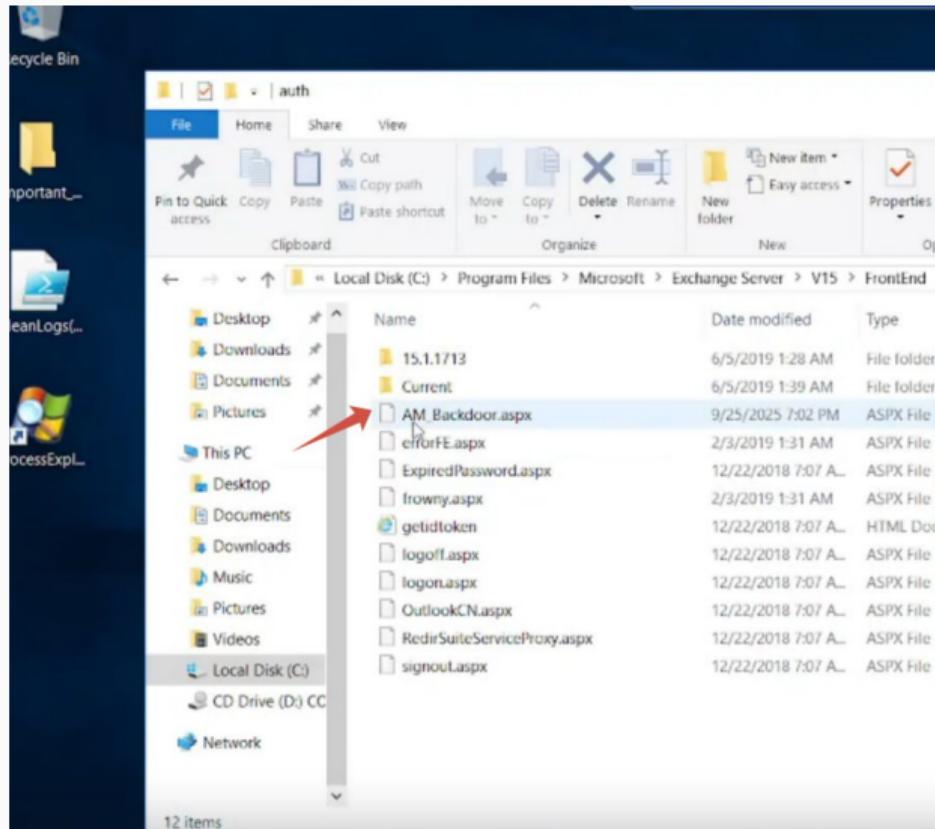


Figure 2: 1.1

Далее нужно обнаружить последствия и убрать их. В нашем случае это - Exchange China Chopper



Уязвимости «ROCKETCHAT»

CVE-2021-22911 представляет собой сочетание из двух SQL-инъекций. CVE-2022-0847(Dirty Pipe) представляет собой уязвимость повышения привилегий, находящаяся в самом ядре Linux версии 5.8 и выше

Завели карточку с описание уязвимости, ее индикаторами и рекомендациями по устраниению

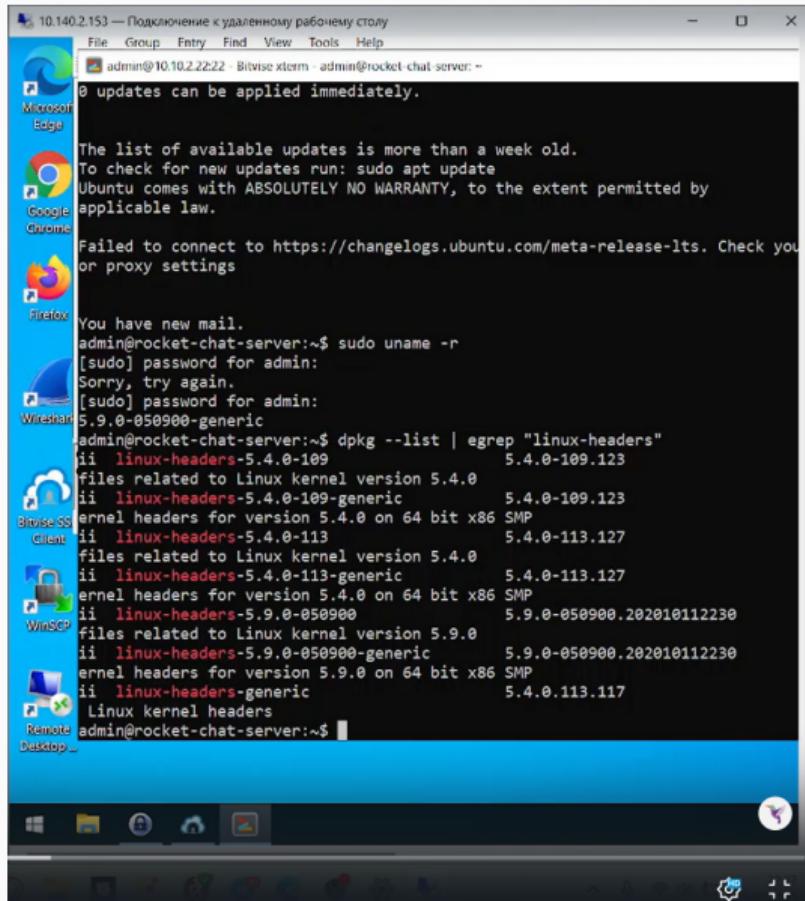
The screenshot shows a detailed view of a vulnerability tracking card. The card is divided into several sections:

- Дата и время события**: 25.09.2025 19:59
- Описание**: Атака на RocketChat на базе Kali с попыткой эксплуатации уязвимости NoSQL-инъекция. Атакующий - внешний нарушитель
- Индикаторы компрометации**: - необычные DNS-запросы; - подозрительные файлы, приложения или процессы;
- Рекомендации**: обновление версии Rocket.Chat; запрет выполнения JavaScript на стороне сервера БД (запрет использования \$where); обновление ядра Linux до новой версии; загрузка с более старой версии ядра <5.8, установленной в системе
- Прикреплённые файлы**: Не заполнено

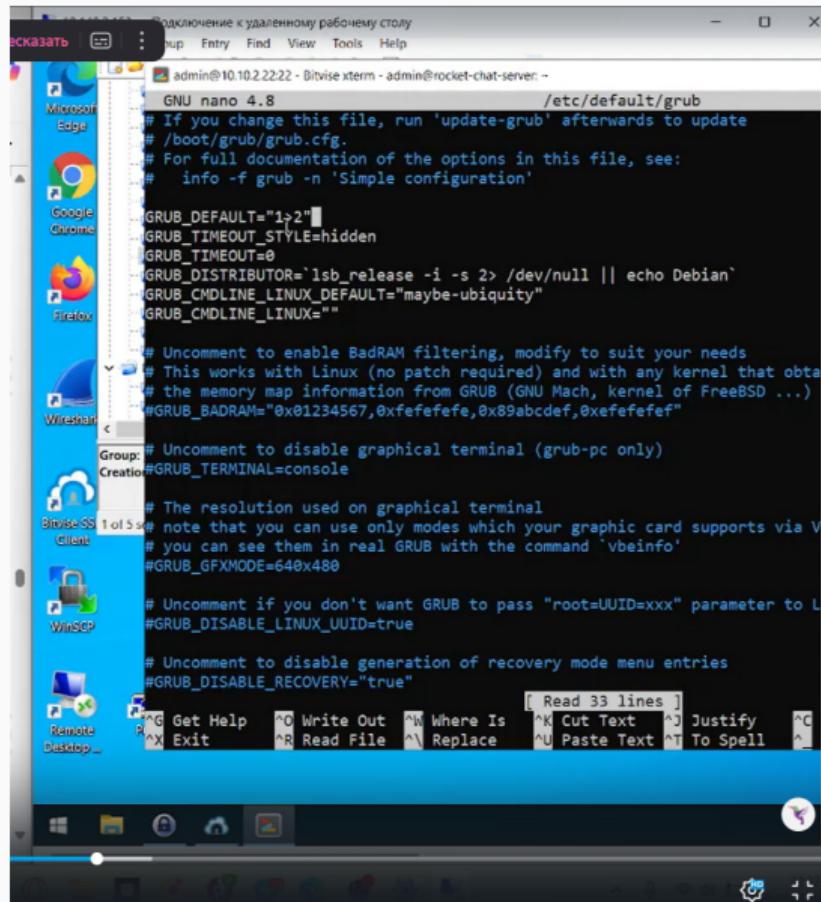
On the right side of the card, there are additional details:

- Оценка**: ☆☆☆☆☆
- Автор**: Гузева Ирина (@1132226441@ppfur.ru)
- Ответственный**: Ничего не выбрано
- Источник**: 195.239.174.11
- Пораженные активы**: 10.10.2.22

После обнаружения уязвимости (Dirty Pipe) , проверяем версию ядра Линукс.



Далее меняем в файле конфигурации строку GRUB_DEFAULT=0 на GRUB_DEFAULT="1>X"



```
admin@10.10.2.22- Bitvise xterm - admin@rocket-chat-server: ~
GNU nano 4.8 /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT="1>2"
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRO='lsb_release -i -s 2> /dev/null || echo Debian'
GRUB_CMDLINE_LINUX_DEFAULT="maybe-ubiquity"
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, Kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command 'vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"
[ Read 33 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell
```

Перезагружаем систему и проверяем версию ядра

```
Sorry, try again.  
[sudo] password for admin:  
5.9.0-050900-generic  
admin@rocket-chat-server:~$ dpkg --list | egrep "linux-headers"  
ii  linux-headers-5.4.0-109           5.4.0-109.123      all  
files related to Linux kernel version 5.4.0  
ii  linux-headers-5.4.0-109-generic   5.4.0-109.123      amd64  
ernel headers for version 5.4.0 on 64 bit x86 SMP  
ii  linux-headers-5.4.0-113           5.4.0-113.127      all  
files related to Linux kernel version 5.4.0  
ii  linux-headers-5.4.0-113-generic   5.4.0-113.127      amd64  
ernel headers for version 5.4.0 on 64 bit x86 SMP  
ii  linux-headers-5.9.0-050900       5.9.0-050900.202010112230  all  
files related to Linux kernel version 5.9.0  
ii  linux-headers-5.9.0-050900-generic 5.9.0-050900.202010112230  amd64  
ernel headers for version 5.9.0 on 64 bit x86 SMP  
ii  linux-headers-generic          5.4.0.113.117      amd64  
Linux kernel headers  
admin@rocket-chat-server:~$ cd /etc/default/grub  
-bash: cd: /etc/default/grub: Not a directory  
admin@rocket-chat-server:~$ sudo nano /etc/default/grub  
admin@rocket-chat-server:~$ sudo nano /etc/default/grub  
admin@rocket-chat-server:~$ sudo update-grub  
Sourcing file '/etc/default/grub'  
Sourcing file '/etc/default/grub.d/init-select.cfg'  
Generating grub configuration file ...  
Found linux image: /boot/vmlinuz-5.9.0-050900-generic  
Found initrd image: /boot/initrd.img-5.9.0-050900-generic  
Found linux image: /boot/vmlinuz-5.4.0-113-generic  
Found initrd image: /boot/initrd.img-5.4.0-113-generic  
Found linux image: /boot/vmlinuz-5.4.0-109-generic  
Found initrd image: /boot/initrd.img-5.4.0-109-generic  
done  
admin@rocket-chat-server:~$
```

Пересказать | PDF

```
admin@10.10.2.22- Bitvise xterm - admin@rocket-chat-server: ~
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-113-generic x86_64)

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

System information as of Thu 25 Sep 2025 07:38:56 PM UTC

System load: 1.35           Processes:      138
Usage of /: 78.4% of 13.72GB Users logged in: 0
Memory usage: 14%           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
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conn
or proxy settings

You have new mail.

Last login: Thu Sep 25 19:34:20 2025 from 10.10.2.254
admin@rocket-chat-server:~$ sudo uname -r
[sudo] password for admin:
5.4.0-113-generic
admin@rocket-chat-server:~$
```

Figure 8: 10

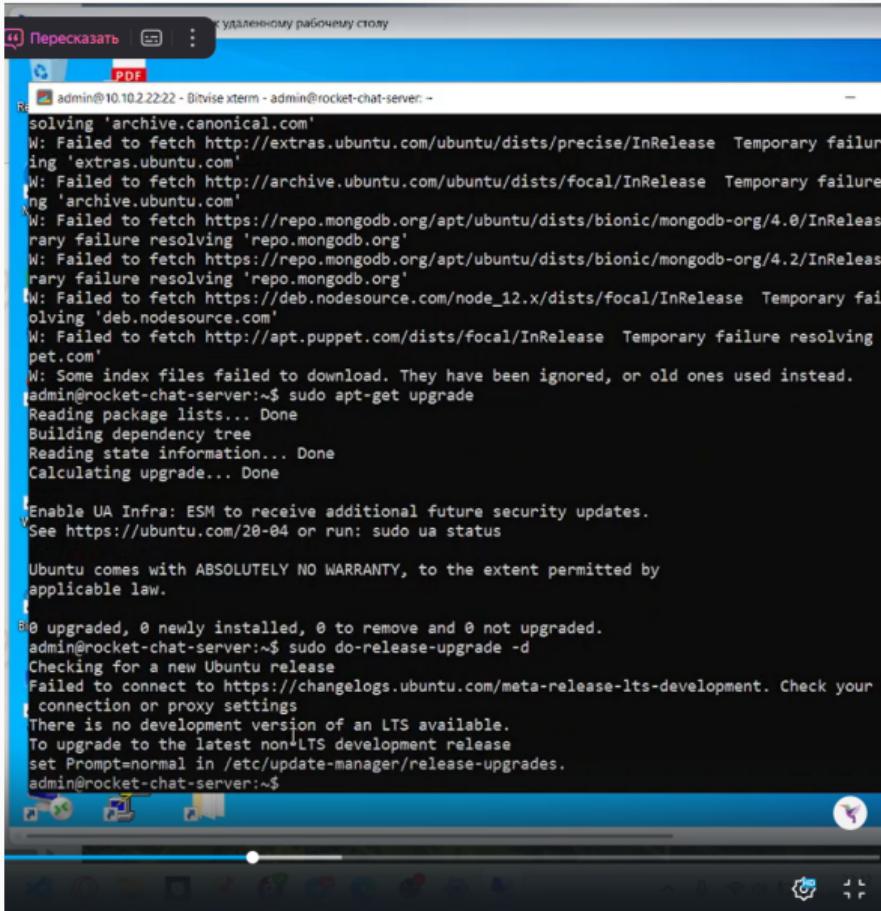


Figure 9: 11

10.140.2.153 — Подключение к удаленному рабочему столу

```
admin@10.10.2.22:22 - Bitvise xterm - admin@rocket-chat-server: ~
Checking for a new Ubuntu release
  failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection.
  new release found.
min@rocket-chat-server:~$ lsb_release -a
lsb_release: command not found
min@rocket-chat-server:~$ apt show ubuntu-release
  Unable to locate package ubuntu-release
  Unable to locate package ubuntu-release
  No packages found
min@rocket-chat-server:~$ ss -tp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56960
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56998
LISTEN      0            36          10.10.2.22:ssh         10.10.2.254:42568
LISTEN      0            0           127.0.0.1:57040        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:57040
LISTEN      0            0           127.0.0.1:56992        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56992
LISTEN      0            0           127.0.0.1:56984        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56952
LISTEN      0            0           127.0.0.1:57058        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:57006        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:57000
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56984
LISTEN      0            0           127.0.0.1:57002        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:57042
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56964
LISTEN      0            0           127.0.0.1:56952        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:56996        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:57010        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:56958
LISTEN      0            0           127.0.0.1:56998        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:27017        127.0.0.1:57008
LISTEN      0            0           127.0.0.1:56980        127.0.0.1:27017
LISTEN      0            0           127.0.0.1:57004        127.0.0.1:27017
```

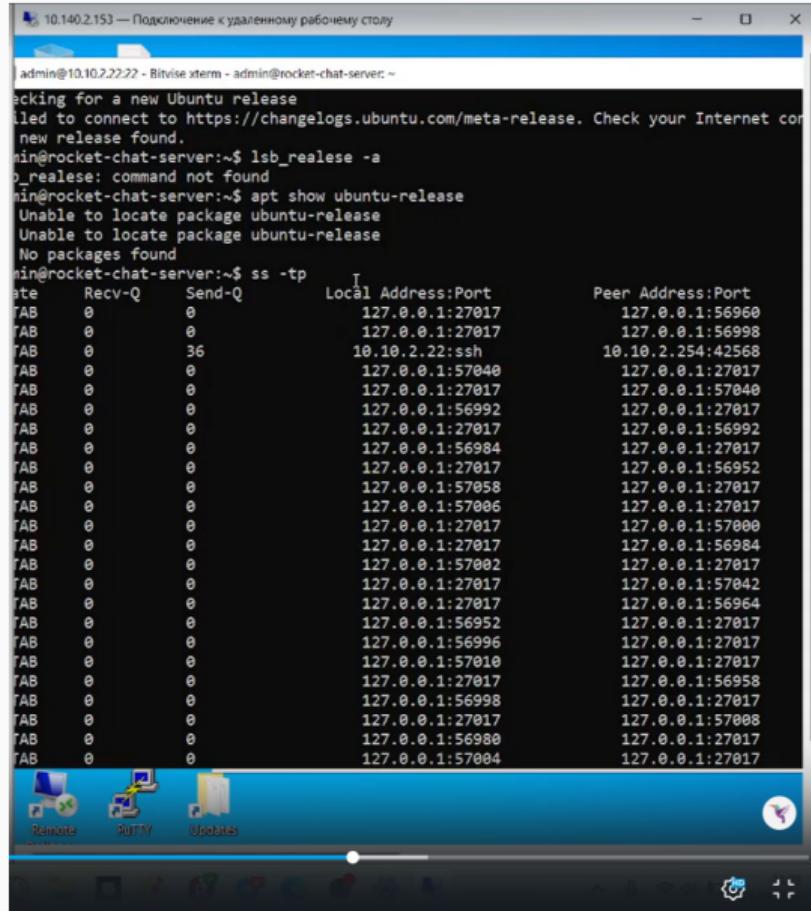
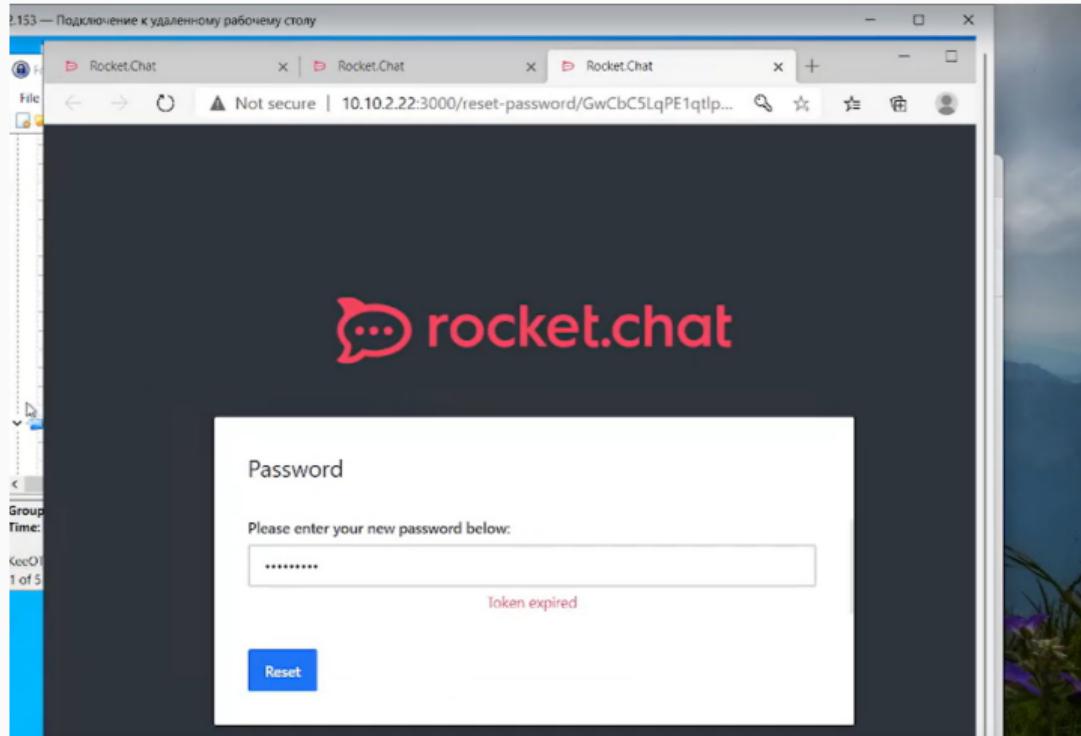


Figure 10: 12

Также нам нужно было сбросить пароль, используя данную почту, мы сбросили пароль и и через терминал получили ссылку для сброса пароля. далее мы столкнулись с проблемой непринятия токена, но эту проблему можно было проигнорировать и войти уже с новым паролем, после чего предстагается пройти двухфакторную аутентификацию.



Для устранения второй уязвимости мы ставим запрет выполнения JavaScript на стороне сервера БД, для этого мы отредактировали файл конфигурации БД /etc/mongod.conf, добавив строчку javascriptEnabled: False

<5.8, установленной в системе	
Способы проверки статуса уязвимости	<ul style="list-style-type: none">– проверка версии Rocket.Chat;– проверка mongod.conf (запрет выполнения JavaScript);– проверка перезапуска служб.– проверка текущей версии ядра Linux
Полезная нагрузка	

Figure 12: 14

```
... Новая Я дипси grok DeepS Устрани + - ×

ранного режима — подключение к удаленному рабочему столу
2025-09-25T19:38:59.045+0000 I CONTROL [initandlisten]
2025-09-25T19:38:59.045+0000 I CONTROL [initandlisten] ** WARNING: Access
2025-09-25T19:38:59.046+0000 I CONTROL [initandlisten] ** Read ar
2025-09-25T19:38:59.046+0000 I CONTROL [initandlisten]
---

Enable MongoDB's free cloud-based monitoring service, which will then receive
metrics about your deployment (disk utilization, CPU, operation statistics,
The monitoring data will be available on a MongoDB website with a unique URL
and anyone you share the URL with. MongoDB may use this information to make
improvements and to suggest MongoDB products and deployment options to you.

To enable free monitoring, run the following command: db.enableFreeMonitoring()
To permanently disable this reminder, run the following command: db.disableFreeMonitoring()
---

иен
rs01:PRIMARY> db.users.update({username: "admin"}, {$set: {services: {password: "1234567890"}}, upsert: true)
1 document updated.
rs01:PRIMARY> db.users.find({username: "admin"})
{
  "_id": "5f37399b40a9005400540054",
  "username": "admin",
  "services": {
    "password": "1234567890"
  }
}
rs01:PRIMARY> admin@rocket-chat-server:~$ sudo nano /etc/mongod.conf
rs01:PRIMARY> admin@rocket-chat-server:~$ sudo systemctl restart mongod
rs01:PRIMARY> admin@rocket-chat-server:~$
```

Figure 13: 15

Готово! Уязвимость и последствия на данный узел устраниены

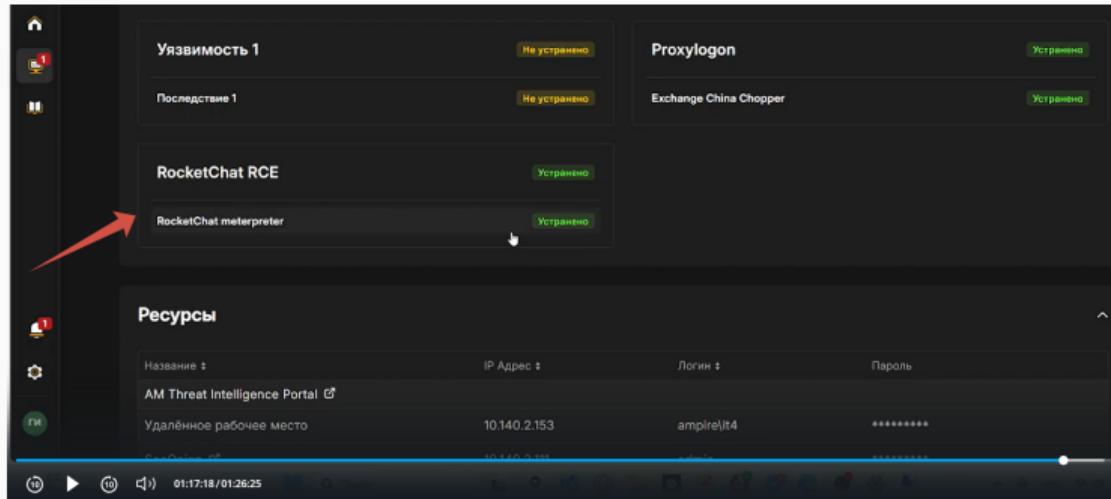


Figure 14: 16

Уязвимость «WPDISCUZ»

Это уязвимость в плагине для создания комментариев WpDiscuz версии с 7.0.0 по 7.0.4 включительно. Уязвимость позволяет получить (удаленное RCE выполнение кода)

Обнаружив уязвимость, мы отключили плагин WpDiscuz, точнее мы его полностью удалили.

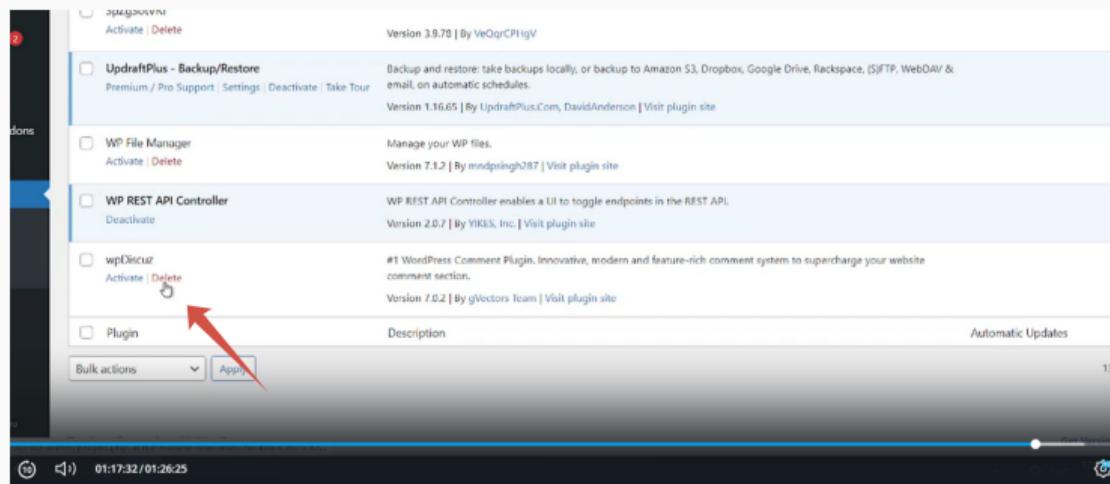


Figure 15: 17

Далее нам нужно обновить плагин, мы обновили до версии 7.6.34

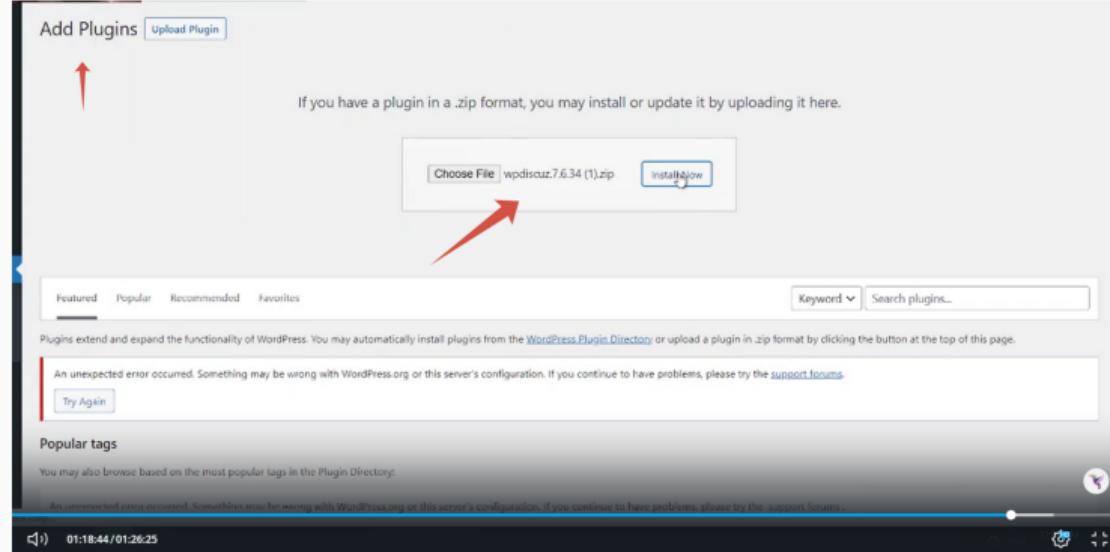


Figure 16: 18

После этого требуется нейтрализовать последствие, для того необходимо сформировать резервную копию с помощью плагина Updraft Backup/Restore

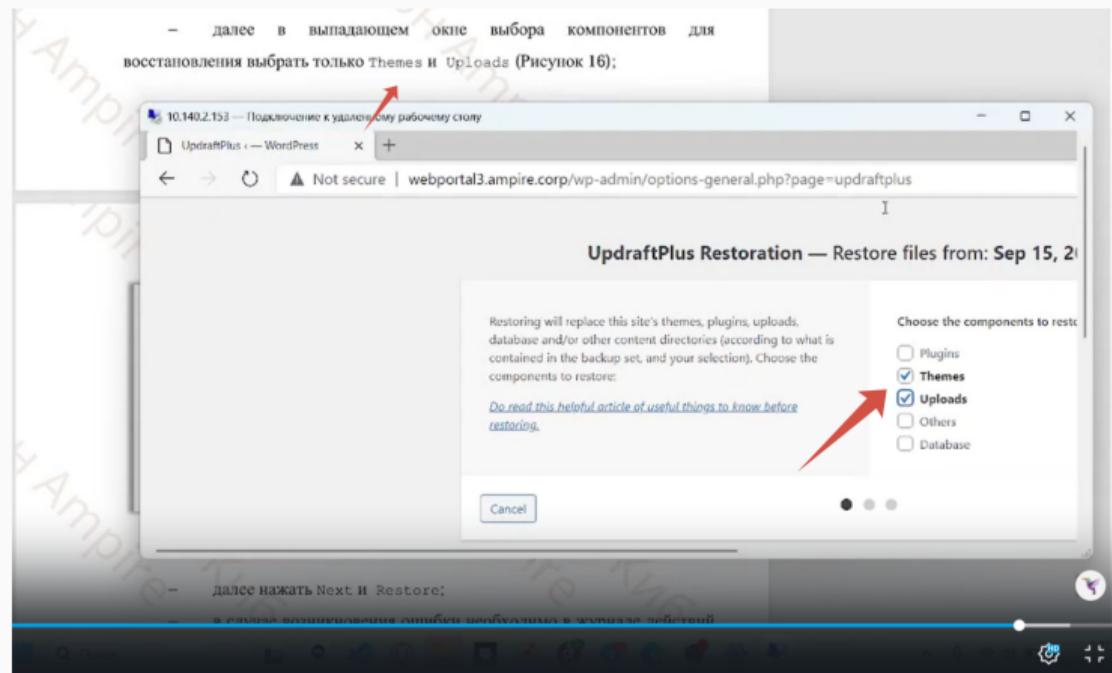


Figure 17: 19

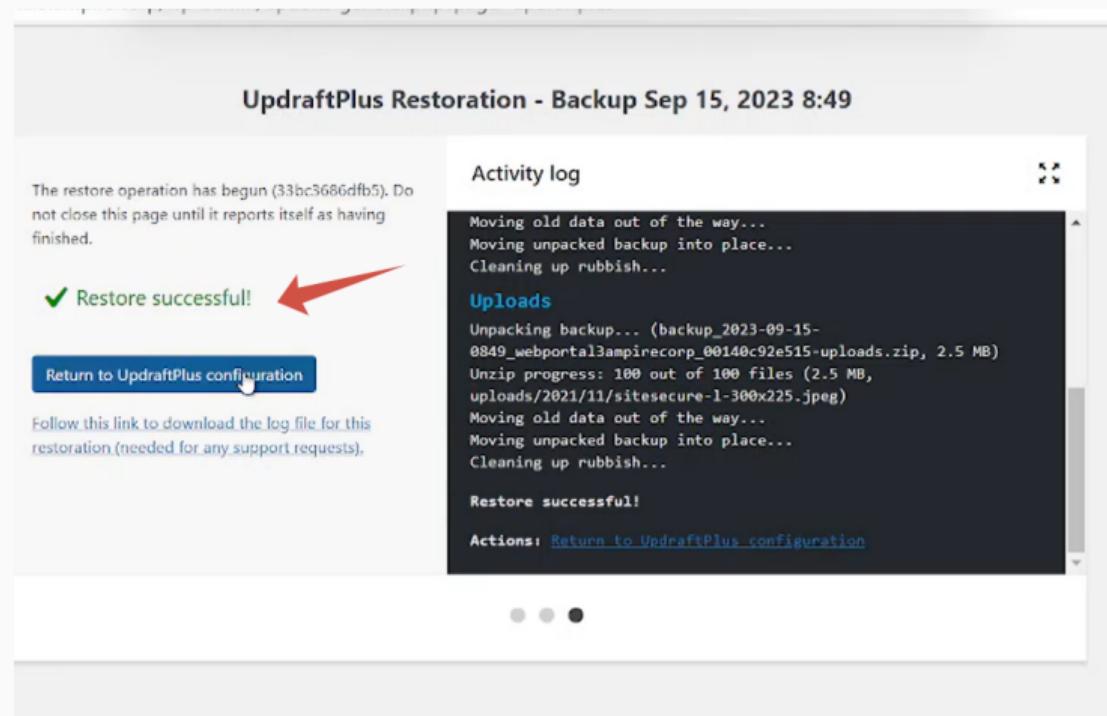


Figure 18: 20

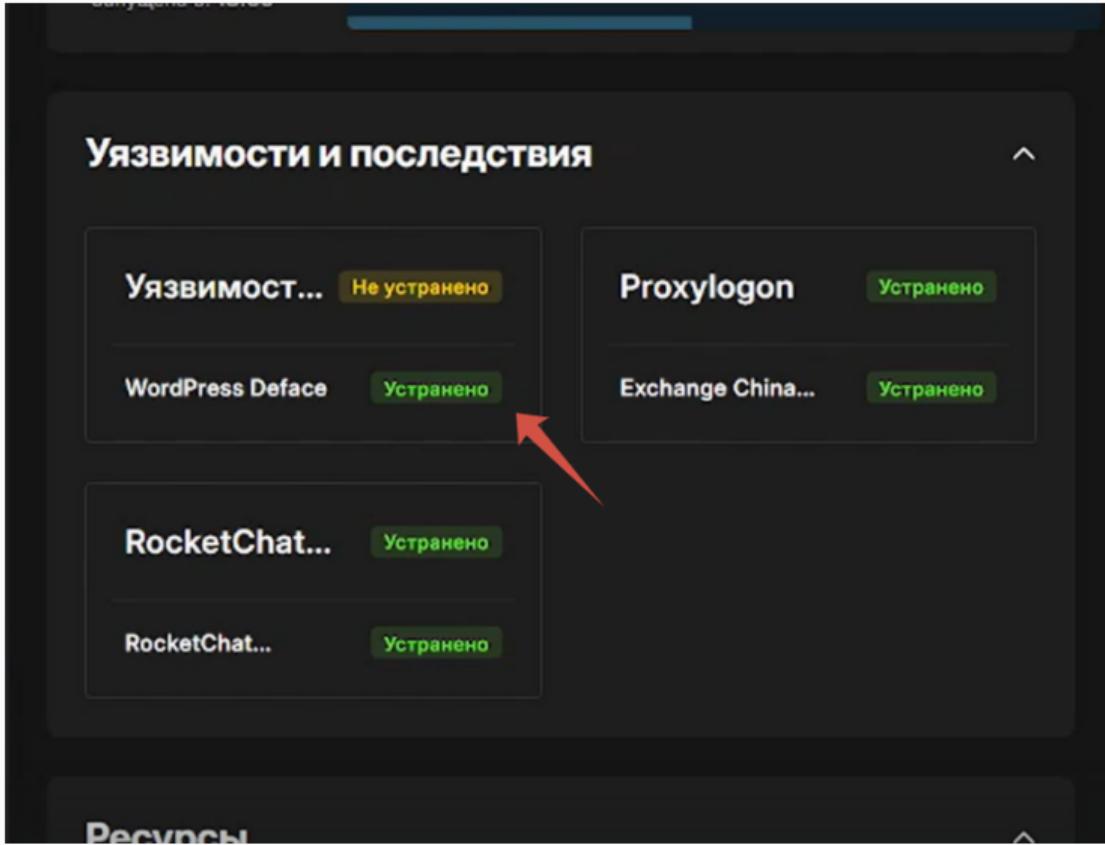
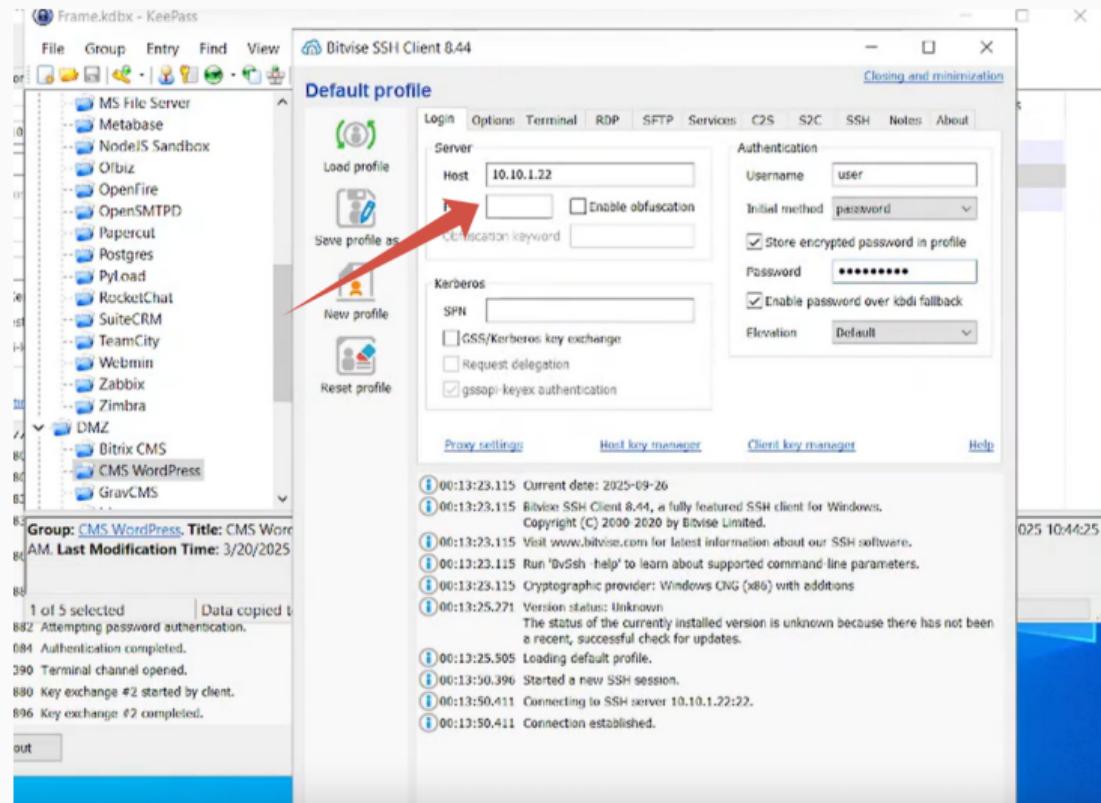


Figure 19: 21

Для того, чтобы уязвимость устранилась, нам потребовалось устранить последствие в виде вредоносного соединения. Через терминал мы вывели информацию об активных соединениях и, соответственно, закрыли ненужные, тем самым закрыли вредоносный сокет.



```
Last login: Mon Jul 21 09:48:28 2025
user@web-portal:~$ ss -tnp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB    0      0      10.10.1.22:46476        195.239.174.11:1085
ESTAB    0      0      10.10.1.22:22          10.10.1.253:57448
ESTAB    0      0      10.10.1.22:56672        195.239.174.11:5556
CLOSE-WAIT 0      0      10.10.1.22:58430        195.239.174.11:5557
FIN-WAIT-2 0      0      [::ffff:10.10.1.22]:80  [::ffff:10.10.1.253]:40154
user@web-portal:~$ sudo ss -tnp
[sudo] password for user:
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB    0      0      10.10.1.22:46476        195.239.174.11:1085 users:(("chisel.sh",pid=1953,fd=11))
ESTAB    0      36     10.10.1.22:22          10.10.1.253:57448 users:(("sshd",pid=12094,fd=3),("sshd",pid=11944,fd=3))
ESTAB    0      0      10.10.1.22:56672        195.239.174.11:5556 users:(("chisel.sh",pid=1953,fd=3),("sh",pid=1952,fd=3),("aDS2w",pid=1918,fd=3))
CLOSE-WAIT 0      0      10.10.1.22:58430        195.239.174.11:5557 users:(("chisel.sh",pid=1953,fd=12),("sh",pid=1952,fd=12),("aDS2w",pid=1918,fd=12))
FIN-WAIT-2 0      0      [::ffff:10.10.1.22]:80  [::ffff:10.10.1.253]:40154
user@web-portal:~$ kill 1953
-bash: Kill: (1953) - Operation not permitted
user@web-portal:~$ kill 1952
-bash: Kill: (1952) - Operation not permitted
user@web-portal:~$ sudo kill 1953
user@web-portal:~$ sudo kill 1952
kill: (1952): No such process
user@web-portal:~$ sudo ss -tnp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB    0      36     10.10.1.22:22          10.10.1.253:57448 users:(("sshd",pid=12094,fd=3),("sshd",pid=11944,fd=3))
ESTAB    0      0      10.10.1.22:56672        195.239.174.11:5556 users:(("aDS2w",pid=1918,fd=3))
CLOSE-WAIT 0      0      10.10.1.22:58430        195.239.174.11:5557 users:(("aDS2w",pid=1918,fd=12))
ESTAB    0      0      [::ffff:10.10.1.22]:80  [::ffff:10.10.1.253]:68234 users:(("apache2",pid=10750,fd=11))
```

4

→ CSIRT (26 сент. 00:10) Уязвимость WordPress wpDiscuz устранена

Запущена в: 18:59

1

Уязвимости и последствия

WordPress... Устранено

WordPress Deface Устранено

Proxylogon Устранено

Exchange China... Устранено

6

RocketChat... Устранено

RocketChat... Устранено

4

Ресурсы

The screenshot shows a mobile application interface with a dark theme. At the top, there's a header with the text '→ CSIRT (26 сент. 00:10) Уязвимость WordPress wpDiscuz устранена' and 'Запущена в: 18:59'. On the left side, there are two vertical columns with numbers '1' and '6' at the top, and '4' at the bottom. The main content area has a section title 'Уязвимости и последствия'. It contains several entries in a grid format. The first row has two entries: 'WordPress...' with a green button 'Устранено' and 'Proxylogon' with a green button 'Устранено'. The second row has two entries: 'WordPress Deface' with a green button 'Устранено' and 'Exchange China...' with a green button 'Устранено'. The third row has two entries: 'RocketChat...' with a green button 'Устранено' and 'RocketChat...' with a green button 'Устранено'. A red arrow points to the first 'WordPress...' entry. Below this section, there's another section titled 'Ресурсы'.

Figure 21: 24

Выводы

Выводы

В ходе выполнения лабораторной работы:

- Были выявлены и устранены уязвимости на различные узлы и их последствия.
- Система приведена в безопасное состояние.

:::