

Отчёт по выполнению лабораторной работы 1

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Уязвимость «PROXYLOGON»	7
3.2 Уязвимости «ROCKETCHAT»	9
3.3 Уязвимость «WPDISCUZ»	17
4 Выводы	22
Список литературы	23

Список иллюстраций

3.1	карточка	7
3.2	1.1	8
3.3	удаление файла веб-оболочки	8
3.4	карточка	9
3.5	8	11
3.6	13	16
3.7	16	17
3.8	17	18
3.9	18	18

Список таблиц

1 Цель работы

Закрепить практические навыки устранения уязвимостей и защиты корпоративных сервисов.

2 Задание

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

3 Выполнение лабораторной работы

3.1 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

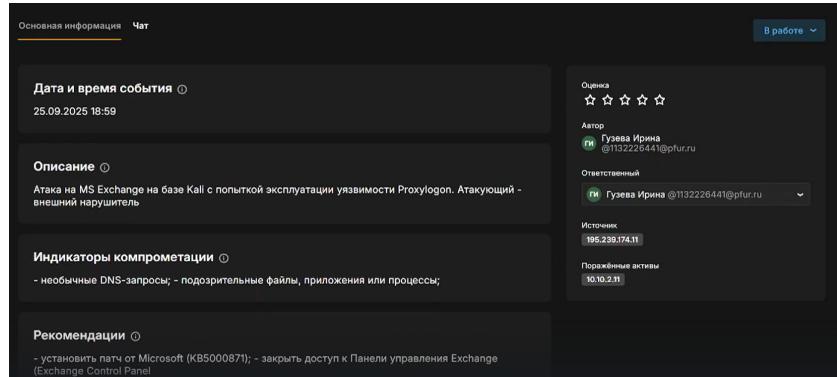


Рис. 3.1: карточка

Устранием уязвимость, ограничиваем доступ к панели управления

and Domain Restrictions

grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

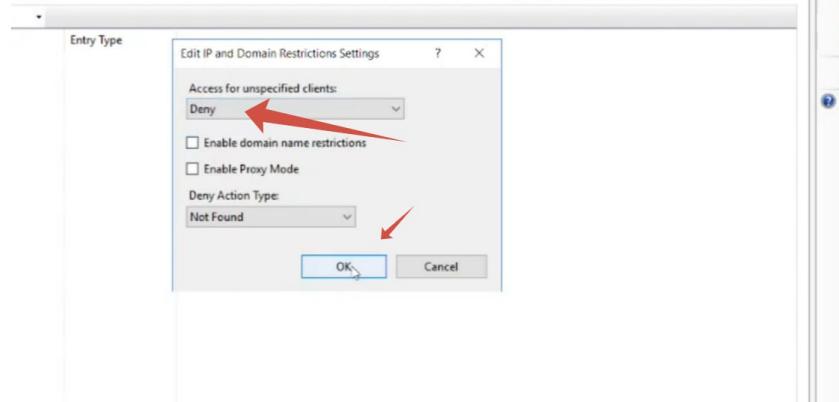


Рис. 3.2: 1.1

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

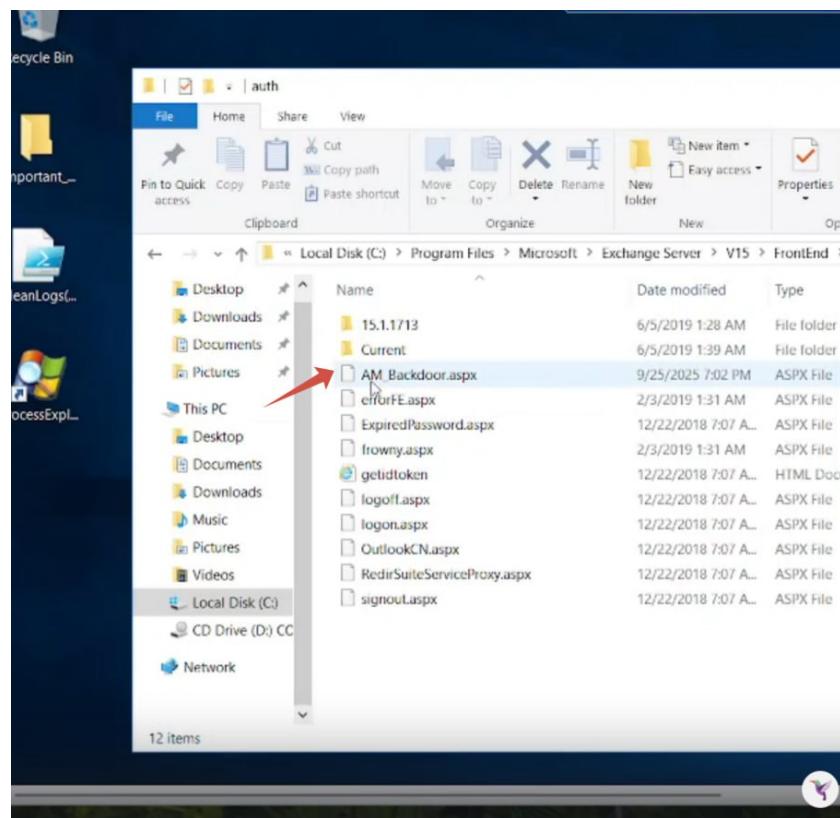


Рис. 3.3: удаление файла веб-оболочки

3.2 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 устранению

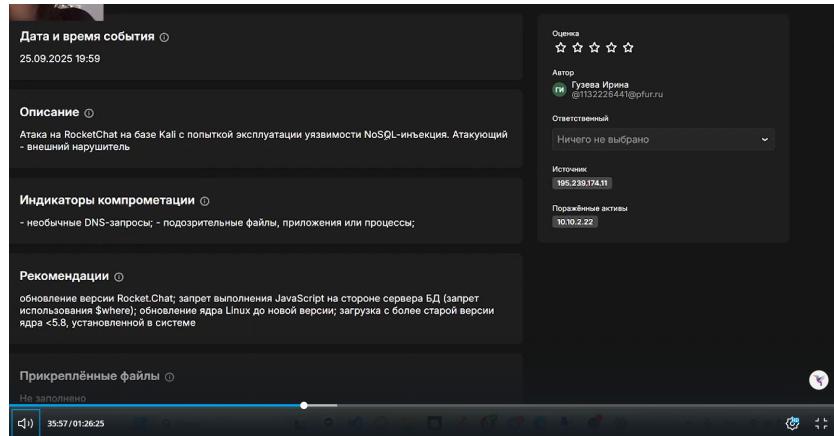
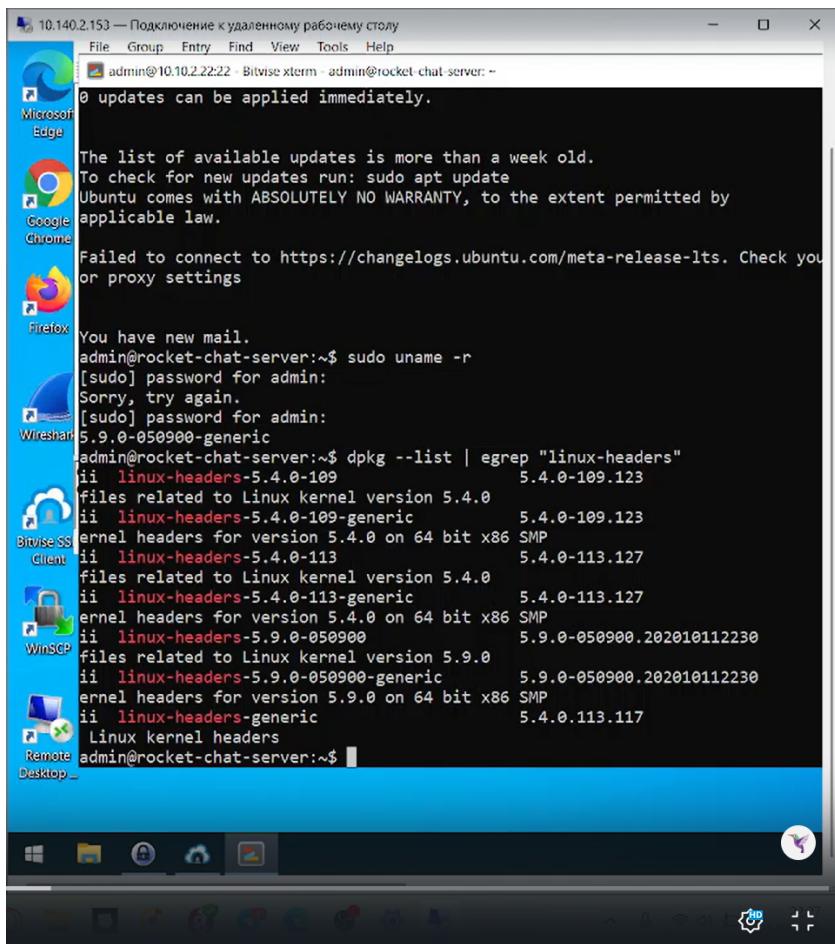


Рис. 3.4: карточка

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



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

The screenshot shows a Linux desktop environment with a terminal window titled "GNU nano 4.8" displaying the contents of the file "/etc/default/grub". The terminal window is part of a Bitvise xterm session, indicated by the title bar. The file contains configuration options for GRUB, such as GRUB_TIMEOUT_STYLE=hidden, GRUB_TIMEOUT=0, and GRUB_CMDLINE_LINUX_DEFAULT="maybe-ubiquity". The desktop background is blue, and various application icons are visible in the taskbar.

```
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_DISTRIBUTOR=`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="0x01234567,0xefefefef,0x89abcdef,0xfefefefef"

# Group: # Uncomment to disable graphical terminal (grub-pc only)
# Creation: #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

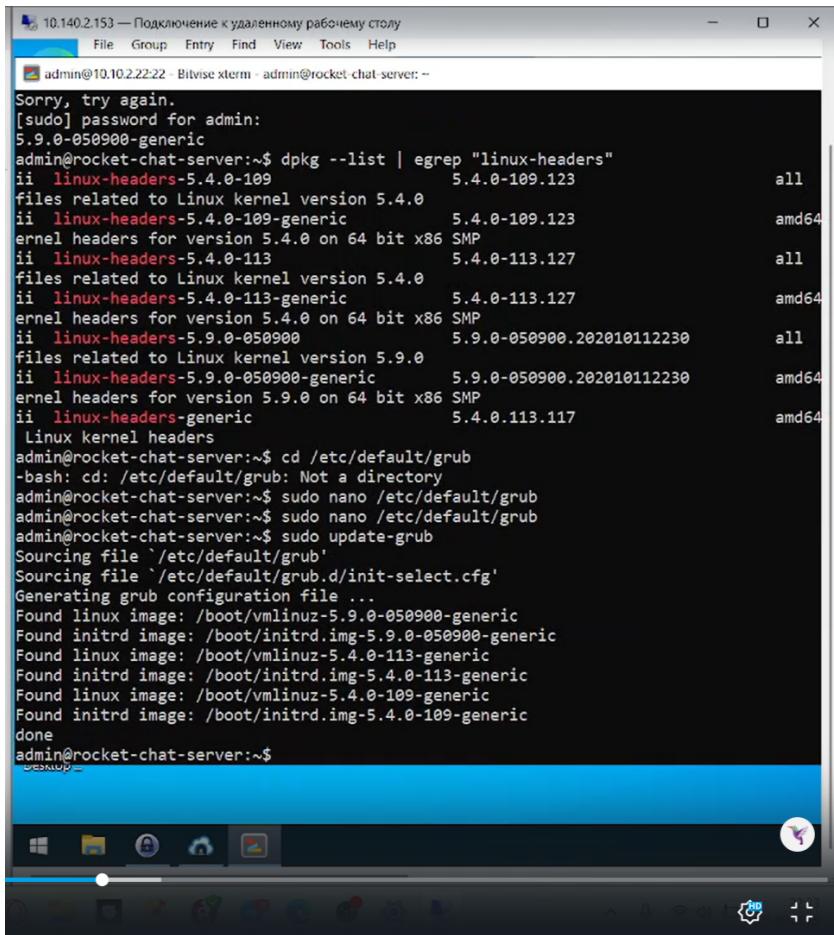
# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# 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 [^C]
[P] Exit [^R] Read File [^\\] Replace [^U] Paste Text [^T] To Spell [^_]
```

Рис. 3.5: 8

Перезагружаем систему и проверяем версию ядра



10.140.2.153 — Подключение к удаленному рабочему столу

File Group Entry Find View Tools Help

```
admin@10.2.22.22 - Bitvise xterm - admin@rocket-chat-server: ~
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@10.10.2.22.22 - 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

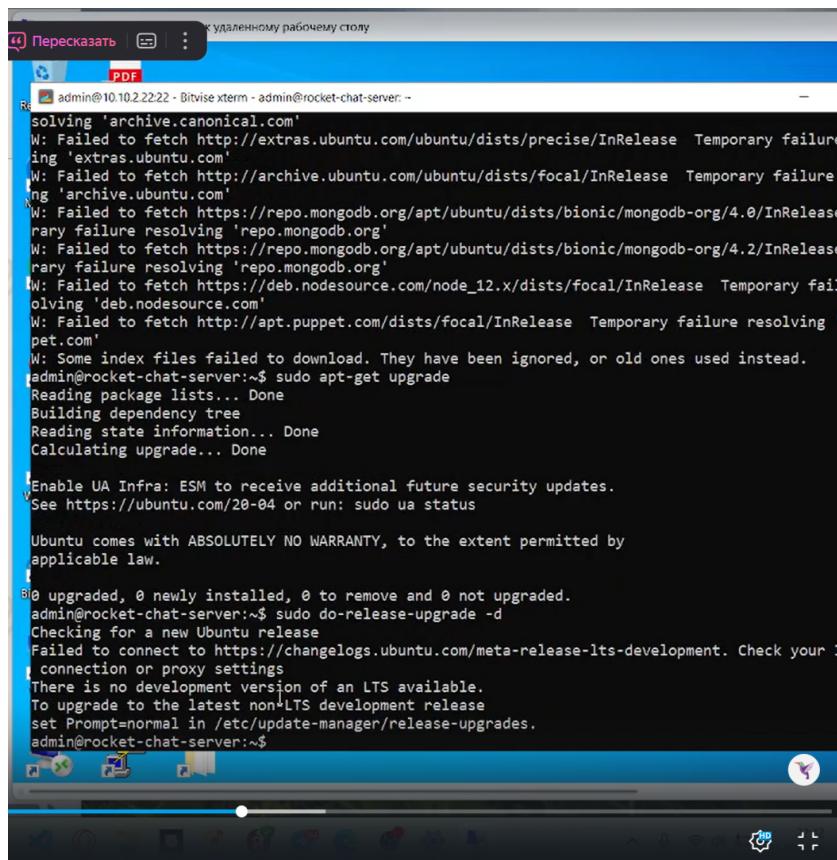
System load: 1.35      Processes: 138
Usage of /: 78.4% of 13.72GB  Users logged in: 0
Memory usage: 14%      IPv4 address for ens3: 10.10.2.22
Swap usage: 0%

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:~$
```



admin@10.10.2.22:22 - Bitvise xterm - admin@rocket-chat-server: ~

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done

[ Enable UA Infra: ESM to receive additional future security updates.
See https://ubuntu.com/20-04 or run: sudo ua status

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
admin@rocket-chat-server:~$ sudo do-release-upgrade -d
Checking for a new Ubuntu release
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts-development. Check your I
connection or proxy settings
There is no development version of an LTS available.
To upgrade to the latest non-LTS development release
set Prompt=normal in /etc/update-manager/release-upgrades.
admin@rocket-chat-server:~$
```

Также нам нужно было сбросить пароль, используя данную почту, мы сбросили пароль 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.

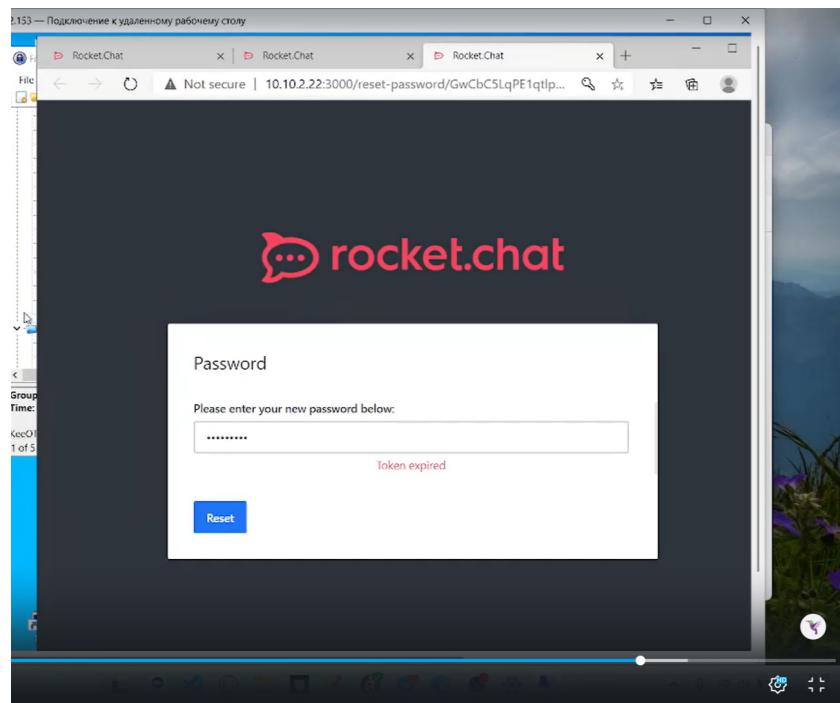


Рис. 3.6: 13

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	

```
2025-09-25T19:38:59.045+0000 I CONTROL [initandlisten]
2025-09-25T19:38:59.045+0000 I CONTROL [initandlisten] ** WARNING: Access control is disabled. Logon to the database at your own risk!
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, etc). 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
...
rs01:PRIMARY> db.users.update({username: "admin"}, {$set: {services: {password: "1234567890", ...}}})
...
admin@rocket-chat-server:~$ sudo nano /etc/mongod.conf
admin@rocket-chat-server:~$ sudo systemctl restart mongod
admin@rocket-chat-server:~$
```

Готово! Уязвимость и последствия на данный узел устраниены

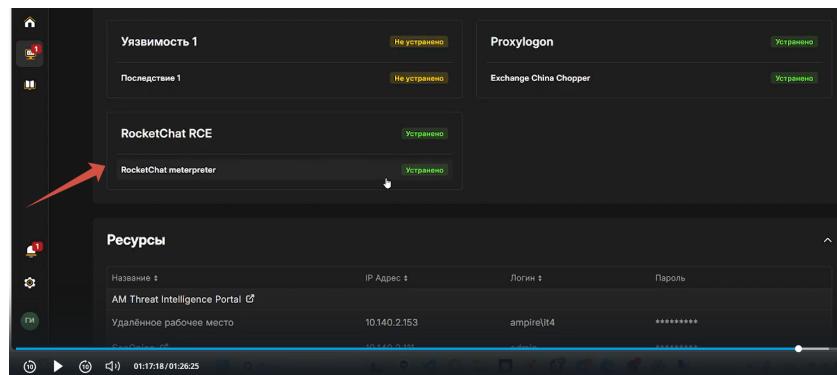


Рис. 3.7: 16

3.3 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.

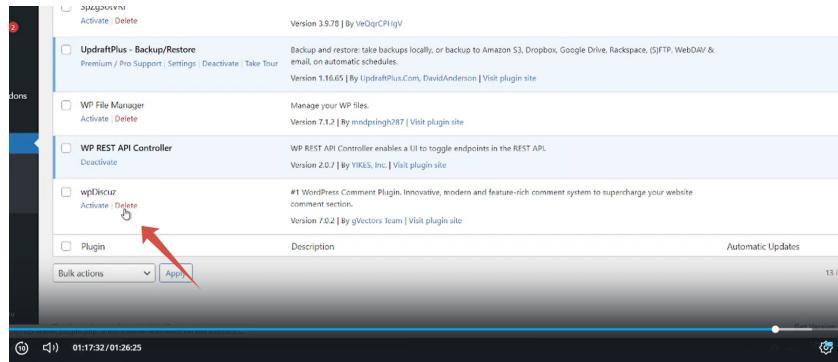


Рис. 3.8: 17

Далее нам нужно обновить плагин, мы обновили до версии 7.6.34

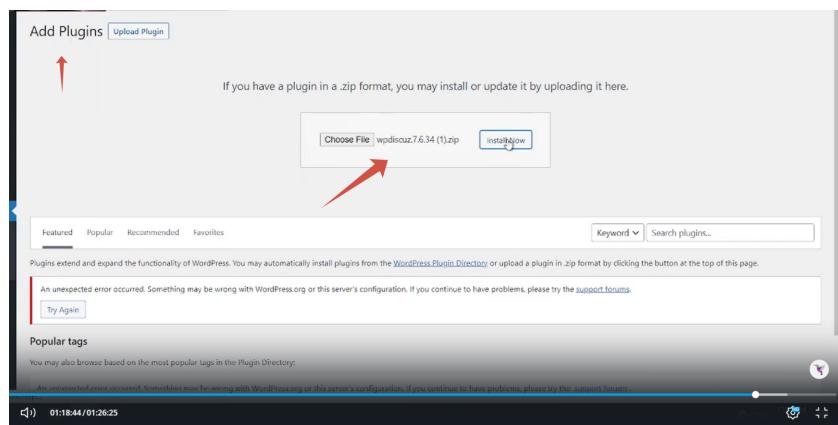
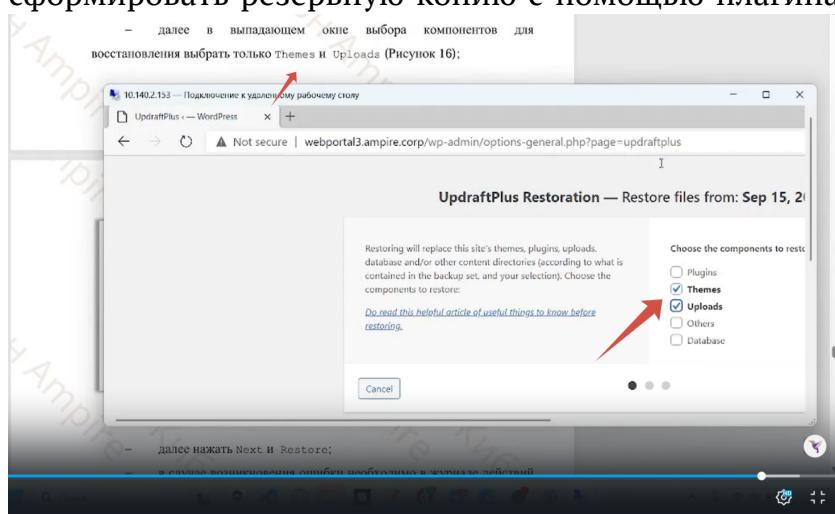


Рис. 3.9: 18

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

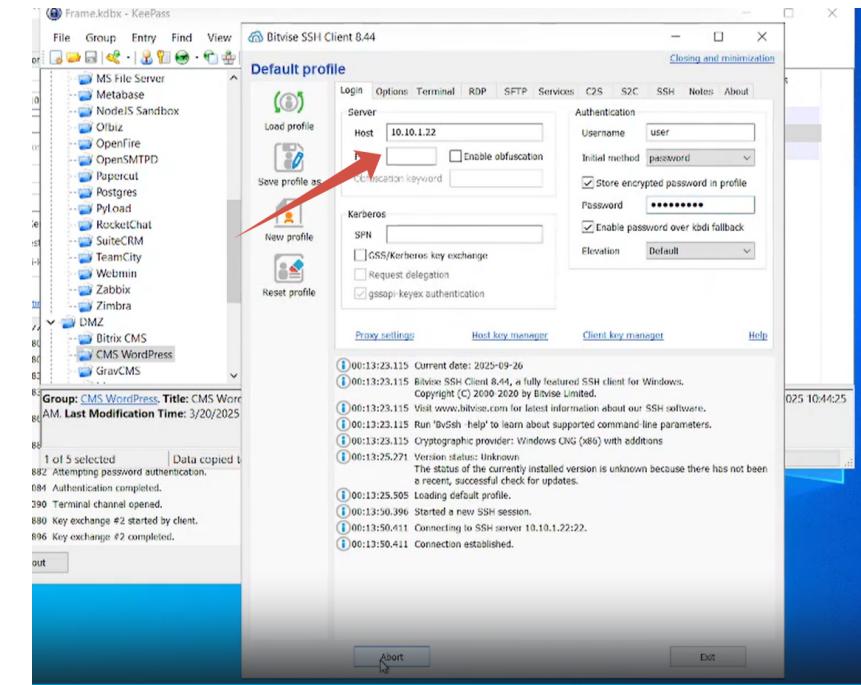


Бинго!

The top screenshot shows a successful restoration of a backup from Sep 15, 2023, at 8:49 AM. It includes an activity log detailing the process: moving old data, unpacking the backup, and cleaning up rubbish. A red arrow points to the 'Restore successful!' message.

The bottom screenshot shows a security audit report titled 'Уязвимости и последствия' (Vulnerabilities and Consequences). It lists several findings: 'Уязвимость' (Vulnerability) is marked as 'Не устранено' (Not fixed); 'Proxylogon' is marked as 'Устранено' (Fixed); 'WordPress Deface' is marked as 'Устранено' (Fixed); 'Exchange China...' is marked as 'Устранено' (Fixed); 'RocketChat...' is marked as 'Устранено' (Fixed); and another 'RocketChat...' entry is also marked as 'Устранено' (Fixed). A red arrow points to the 'WordPress Deface' entry.

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.

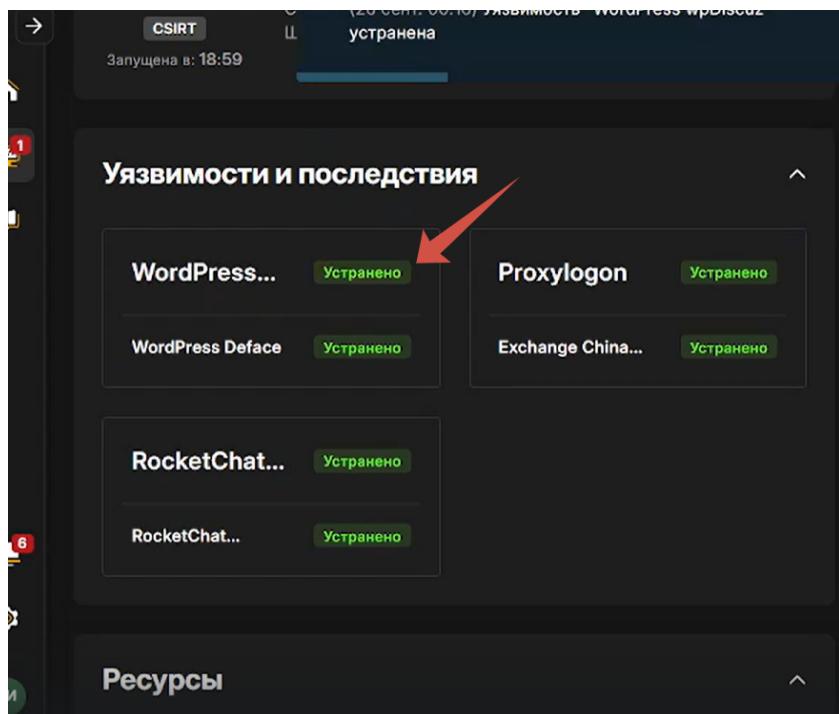


```

Last login: Mon Jul 21 09:48:28 2025
user@web-portal-3:~$ 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      36     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-3:~$ 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),("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=3),("aDS2w",pid=1918,fd=3))
FIN-WAIT-2 0   0      [:ffff:10.10.1.22]:80       [:ffff:10.10.1.253]:40154
user@web-portal-3:~$ kill ip[1953]
bash: kill: (1953) - Operation not permitted
user@web-portal-3:~$ kill 1952
-bash: kill: 1952: Operation not permitted
user@web-portal-3:~$ user@web-portal-3:~$ sudo kill 1953
user@web-portal-3:~$ sudo kill 1952
kill: (1952): No such process
user@web-portal-3:~$ sudo ss -tnp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB  0      0      10.10.1.22:22           10.10.1.253:57448 users:(("sshd",pid=12094,fd=3),("sshd",pid=11944,fd=3))
ESTAB  0      36     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=3))
ESTAB  0      0      [:ffff:10.10.1.22]:80       [:ffff:10.10.1.253]:60234 users:(("apache2",pid=19750,fd=13))

```

A red arrow points from the 'Peer Address:Port' column to the first entry (195.239.174.11:1085). Another red arrow points from the 'User' column to the same entry.



4 Выводы

В ходе выполнения лабораторной работы:

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

Список литературы