

Лабораторная работа №1

Кибербезопасность предприятия

НКНбд-01-22; Аристид Жан, Акопян Сатеник, Кадров Виктор, Нве Манге Хосе Херсон
Мико, Эспиноса Висилита Кристина Микаела, НПИбд-01-22; Стариakov Данила, НФИбд-02-22;
Чемоданова Ангелина

Цель работы

Основная цель данной лабораторной работы заключается в выполнении тренировки “Защита корпоративного мессенджера” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы необходимо освоить практические навыки выявления, анализа и устранения уязвимостей в корпоративной инфраструктуре, а также освоить навыки отработки действий по нейтрализации последствий успешных атак.

Теоретическое введение. 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 использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Уязвимости:

- WordPress-wpDiscuz (CVE-2020-24186)
- Proxylogon (CVE 2020-26855, CVE 2021-27065)
- Rocket.Chat (CVE-2021-22911, CVE-2022-0847)

Теоретическое введение. Атака на CMS WordPress-wpDiscuz

WpDiscuz – один из плагинов CMS WordPress для создания комментариев на базе Ajax.

В версиях с 7.0.0 по 7.0.4 включительно существует уязвимость File Upload(CVE-2020-24186), которая позволяет получить RCE, если прикрепить любой файл(например, код на php) в поле для комментариев и загрузить на сервер. Данный процесс можно выполнить без аутентификации. После создания файла с полезной нагрузкой нарушитель будет производить POST-запрос с определенными параметрами по ссылке <http://webportal3.ampire.corp/index.php/wp-admin/admin-ajax.php> для загрузки файла.

Факт загрузки будет детектироваться в журнале активности в WordPress, в котором записывается хронологическая запись последовательности изменений и действий.

Теоретическое введение. Атака на почтовый сервер(ProxyLogon)

Уязвимость ProxyLogon (CVE 2020-26855 (Server-Side Request Forgery)) представляет собой SSRF в Exchange Server, позволяющую обойти аутентификацию и выдать себя за администратора. В сценарии данная уязвимость используется в связке с CVE2021-27065(запись файла в произвольную директорию).

SSRF - подделка запроса на стороне сервера – это атака, которая позволяет отправлять запросы от имени сервера к внешним или внутренним ресурсам.

При помощи ProxyLogon атакующий может выдать себя, например, за администратора и аутентифицироваться в панели управления Exchange(ECP), после чего перезаписать любой файл в системе при помощи CVE-2021-27065.

Уязвимости ProxyLogon подвержены все Exchange Server 2016 до версии 15.01.2106.013.

Уязвимость CVE-2021-22911 представляет собой сочетание из двух SQL инъекций:

- слепая NoSQL-инъекция (позволяет украсть токен сброса пароля пользователя);
- NoSQL-инъекция №2: повышение привилегий.

Уязвимость CVE-2022-0847 (Dirty Pipe) представляет собой уязвимость повышения привилегий, находящуюся в самом ядре Linux версии 5.8 и выше.

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

Для начала перейдем в ViPNet IDS NS, отфильтруем события и обнаружим анату на CMS WordPress.

Ampire-IDS-1 - VIPNet IDS NS - Zen Browser

предзентация - сценария - защита - корпоративного -

VIPNet IDS NS

Events

Events for recent 24 hours

Event 00:12:22:30

Event code	Rule name	Class	Protocol	Source IP.	Source	Description	Dest.	Direction
00:12:22:300... 201764	ET WEB SERVER PHP-L...	web-application-attack	TCP	195.239.174... 45015	10.10.1.22	80	④ → ②	
00:12:22:30... 3153064	AM EXPLOIT WordPress...	web-application-attack	TCP	195.239.174... 45015	10.10.1.22	80	④ → ②	
00:12:22:30... 3415451	AM EXPLOIT Generic Po...	web-application-attack	TCP	195.239.174... 45015	10.10.1.22	80	④ → ②	
00:12:22:30... 3590223	AM EXPLOIT Generic Co...	web-application-attack	TCP	195.239.174... 45015	10.10.1.22	80	④ → ②	
00:12:22:30... 9250504	AM EXPLOIT Generic Co...	web-application-attack	TCP	195.239.174... 45015	10.10.1.22	80	④ → ②	
00:12:22:30... 3121915	ET POLICY Executable...	policy-violation	TCP	195.239.174... 58515	10.10.1.22	90528	④ → ②	
00:12:22:30... 3298413	AM POLICY Suspicious...	policy-violation	TCP	18.12.3.11	7985	195.239.174... 8010	④ ← ③	
00:12:22:30... 2032162	ET INFO PFI Powershell...	bad-username	TCP	18.12.3.11	7983	195.239.174... 8010	④ ← ③	
00:12:22:30... 3298411	AM POLICY Suspicious...	policy-violation	TCP	18.10.1.253	58215	195.239.174... 8010	④ ← ③	
00:12:22:30... 2032161	ET INFO PFI Powershell...	bad-username	TCP	18.10.1.253	58215	195.239.174... 8010	④ ← ③	
00:12:22:30... 3089413	AM POLICY Suspicious...	policy-violation	TCP	18.12.3.11	7984	195.239.174... 8010	④ ← ③	
00:12:22:30... 2032163	ET INFO PFI Powershell...	bad-username	TCP	18.10.1.211	7984	195.239.174... 8010	④ ← ③	
00:12:22:30... 2032162	ET INFO PFI Powershell...	bad-username	TCP	18.10.1.253	54227	195.239.174... 8010	④ ← ③	
00:12:22:30... 3298414	AM POLICY Suspicious...	policy-violation	TCP	18.10.1.253	54227	195.239.174... 8010	④ ← ③	
00:12:22:30... 2025541	ET TIRGJAN Possible M...	trojan-activity	TCP	195.239.174... 5558	10.10.1.255	11767	④ → ②	
00:12:22:30... 2023944	ET TIRGJAN Possible M...	trojan-activity	TCP	195.239.174... 5559	10.10.2.11	7969	④ → ②	
00:12:22:30... 2025544	ET TIRGJAN Possible M...	trojan-activity	TCP	195.239.174... 5558	10.10.1.255	61793	④ → ②	
00:12:22:30... 2025541	ET TIRGJAN Possible M...	trojan-activity	TCP	195.239.174... 5558	10.10.2.11	7966	④ → ②	
00:12:22:30... 3122827	ET POLICY Executable...	policy-violation	TCP	195.239.174... 8910	10.10.1.253	26785	④ → ②	
00:12:22:30... 3122837	ET POLICY Executable...	policy-violation	TCP	195.239.174... 8910	10.10.2.22	90198	④ → ②	
00:12:22:30... 3121915	ET POLICY Executable...	policy-violation	TCP	195.239.174... 5559	10.10.1.255	49867	④ → ②	
00:12:22:30... 3121915	ET POLICY Executable...	policy-violation	TCP	195.239.174... 5559	10.10.2.22	90198	④ → ②	
00:12:22:30... 3121915	ET POLICY Executable...	policy-violation	TCP	195.239.174... 5559	10.10.2.22	90198	④ → ②	
00:12:19... 3039900	AM CURRENT_EVENTS...	bad-username	TCP	18.10.2.18	399	10.10.2.11	8652	④ ← ③
00:12:19... 3039900	AM CURRENT_EVENTS...	bad-username	TCP	18.10.2.18	399	10.10.2.11	8652	④ ← ③
10:34:55.325... 1000106...	AD HIGH SYNACK-F...	bad-username	undefined					
10:34:55.325... 1000106...	AD UNUSUALLY HIGH F...	bad-username	undefined					

General Information

Date and time: 09.12.22, 09:09:09 09/12/2022

Capture interface: eth2

Severity: High

Event type: Signature event

Protocol: TCP

Event code: 2011768

Client application: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.157.0 Safari/537.36 Edg/108.0.1462.46

Resource DNS name: 195.239.174.87

Analysis rule:

Description: This rule detects attacks against a web server

Test:

Alert top 1000LAYER_Net_ip ~show .NET HTTP_PORTS [req] ET WEB-SERV
OR HTTP tags in HTTP POST:Allow established_sessions,connect,POST?rescue:Http
-method=POST,allow=HTTP/1.1,allow=HTTP/1.0,allow=HTTP/2,allow=HTTP/2.1,allow=HTTP/3
-rule: 311768:alert,asset_id=1,asset_name=ET WEB-SERVER PHP tags in HTTP
-service: affected,asset_id=1,asset_name=ET WEB-SERVER PHP tags in HTTP,affected, vendor_id
0,interf=ether_Wlan0,interface_label=eth0,source_ip=195.239.174.87,signature_overview information
_id=1,signature_expansion_update_id=311.0.255

Description of vulnerabilities:

#1 no.sans.edu.th/dns/forShared9478

Рис. 1: События VipNet IDS NS

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

Проанализировав события, поймем, что перед нами уязвимость CVE-2020-24186. Получим дополнительную информацию об этой уязвимости.

Рис. 2: Событие CVE-2020-24186

Через ViPNet IDS NS выявим критические события на почтовом сервере MS Exchange, заметим загрузку подозрительных файлов с использованием фреймворка Metasploit.

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

Откроем Seclnoin, увидим подозрительный http-запрос и ответ сервера, изучим полученный пакет и найдем там использование WinAPI-функций, а также байтовый массив для инъектирования кода в память.

The screenshot shows the Seclnoin interface with the following details:

- Top bar: 2 (highlighted in red), 1, 1, 21:15:28, ET INFO PS1 Powershell File Request, 2032162, 6, 1.471%.
- Middle section: A log entry:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET INFO PS1 Powershell File Request"; flow:established,from_client; flowbits:set,ET.PS.Download; http_request_line; content:".ps1 HTTP/1."; nocase; fast_pattern; classtype:bad-unknown; sid:2032162; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2021_03_18, deployment Perimeter, former_category INFO, signature_severity Informational, updated_at 2021_03_18;)
```
- Below the log: file: [downloaded.rules:13127](#).
- Filter buttons: CATEGORIZE 0 EVENT(S), CREATE FILTER: [src](#) [dst](#) [both](#).
- Table headers: QUEUE, ACTIVITY, LAST EVENT, SOURCE, AGE, COUNTRY, DESTINATION, AGE, COUNTRY.
- Table rows:
 - Row 1: 2, ST, 2025-09-14 21:15:28, 10.10.2.11, 1, RFC1918 (.lo), 195.239.174.11, 1, RUSSIAN FEDERATION (.ru).
 - Row 2: RT, 2025-09-14 21:15:28, [3.25](#), 10.10.2.11, 7963, 195.239.174.11, 8010, ET INFO PS1 Powershell File Request.
 - Row 3: RT, 2025-09-14 21:15:28, [3.29](#), 10.10.2.11, 7964, 195.239.174.11, 8010, ET INFO PS1 Powershell File Request.
- Bottom bar: 2, 1, 1, 21:15:28, ET INFO Windows Powershell User-Agent Usage, 2033355, 6, 1.471%.

Рис. 3: Анализ Seclnoin

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

Мы можем прийти к выводам по технике атаки:

- Доставка: через http-запрос к скрипту;
- Выполнение: Инжектирование кода в память через VirtualAlloc + CreateThread;
- Цель: Обход антивируса(без записи на диск)

и по индикаторам компрометации(IoC):

- IP-адрес: 195.239.174.11;
- Порт: 8010/TCP; Хэш(SHA-256): Не вычислен(требуется анализ файла);
- Сигнатура кода: Использование VirtualAlloc + шелл-код

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

Атака оканчивается загрузкой бинарного файла в формате ELF, который, вероятно, содержит вредоносный код или эксплойт на узел 10.10.2.22.

```
user@web-portal-3:/var/log/apache2$ grep "195" access.log
195.239.174.11 - - [14/Sep/2025:21:12:17 +0000] "POST /wp-login.php HTTP/1.1" 302 1118 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:17 +0000] "GET /wp-admin/ HTTP/1.1" 302 450 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:18 +0000] "GET /wp-login.php?redirect_to=http%3A%2F%2Fwebportal3.ampire.corp%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 4391 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:18 +0000] "GET /wp-admin/plugins.php HTTP/1.1" 200 27192 "-" "python-requests/2.28.1"
195.239.174.11 - - [14/Sep/2025:21:12:21 +0000] "GET /wp-content/plugins/wp-discuz/readme.txt HTTP/1.1" 200 54253 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46"
195.239.174.11 - - [14/Sep/2025:21:12:21 +0000] "GET /index.php/2021/07/26/hello-world/ HTTP/1.1" 200 62591 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
```

Рис. 4: Логи посещения WordPress

Выполнение лабораторной работы. Атака на CMS WordPress-wpDiscuz

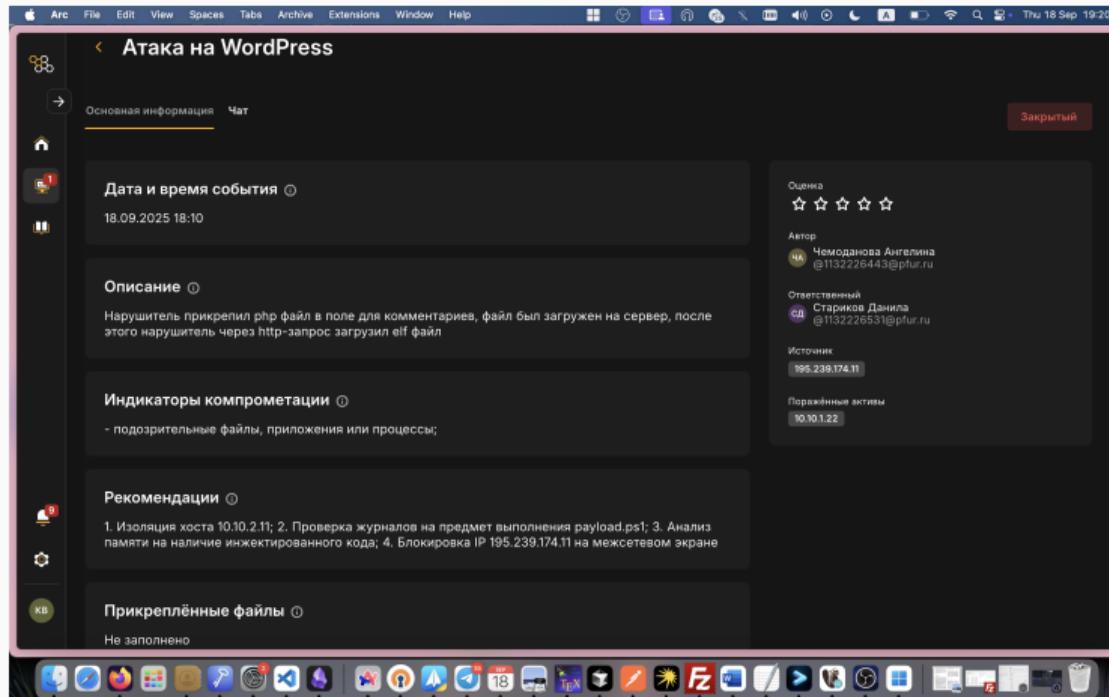


Рис. 5: Карточка первого инцидента

Если открыть страницу сайта компании, указать в строке браузера IP-адрес 10.10.1.22 (<http://webportal3.ampire.corp>), то можно заметить, что блог после атаки выглядит следующим образом: до использования полезной нагрузки на странице сайта красный крупнотоннажный грузовой автомобиль и после использования полезной нагрузки картинка “hacked”.

На веб-сервере работает ftp-сервер vsftpd, который дает возможность плагину Updraft сохранять и скачивать backup. Таким образом, можно выполнить backup-восстановление из последнего файла.

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

Этапы восстановления:

- в панели управления на странице Plugins найти плагин резервного восстановления UpdraftPlus, открыть настройки.
- для восстановления нажать Restore на последней резервной копии.

Выполнение лабораторной работы. Устранение последствия Deface веб-интерфейса

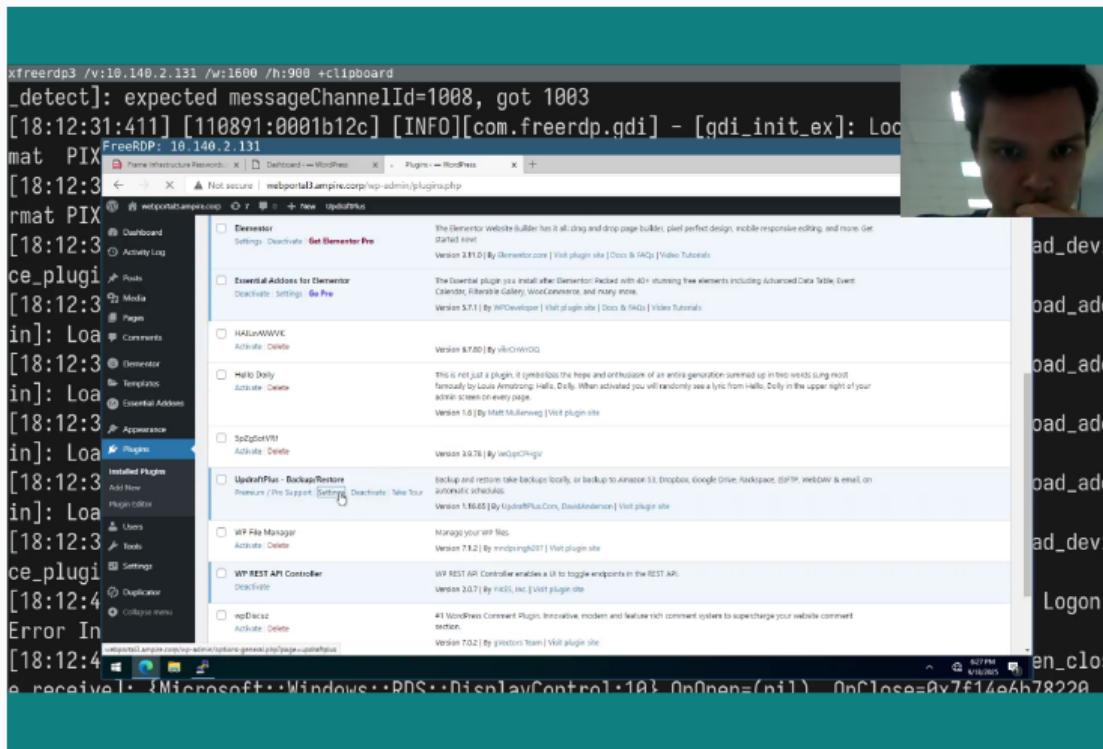


Рис. 6: Backup-восстановление

Выполнение лабораторной работы. Устранение последствия Deface веб-интерфейса

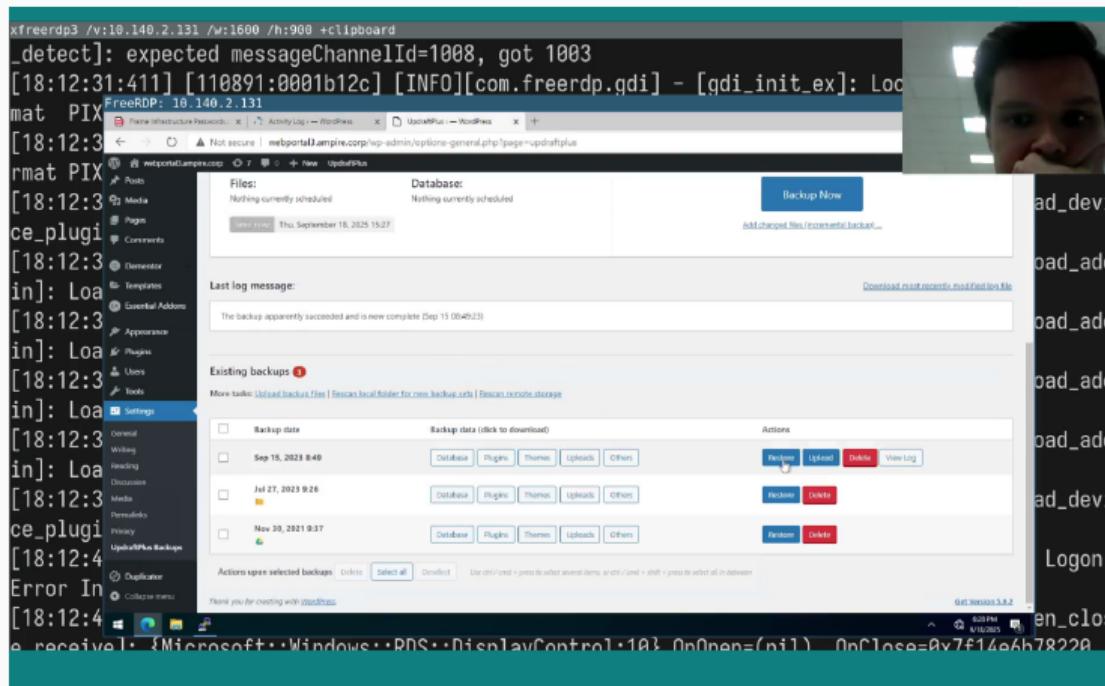


Рис. 7: Backup-восстановление

Выполнение лабораторной работы. Устранение последствия Deface веб-интерфейса

В выпадающем окне выбора компонентов для восстановления выбрать только “Themes” и “Uploads”.

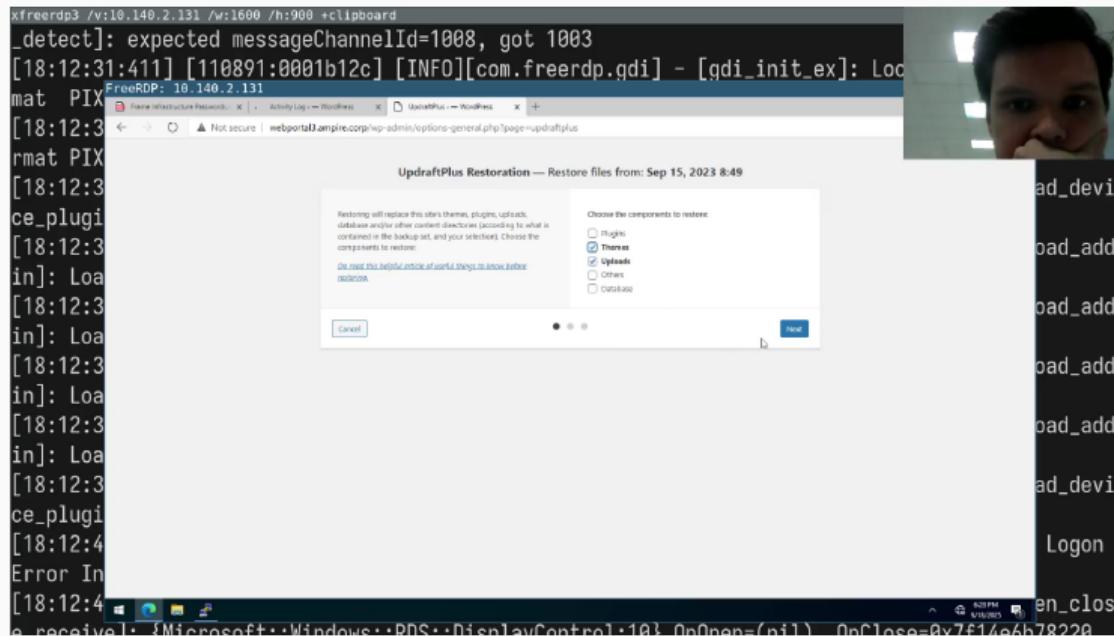


Рис. 8: Выбор компонент

Выполнение лабораторной работы. Устранение последствия Deface веб-интерфейса

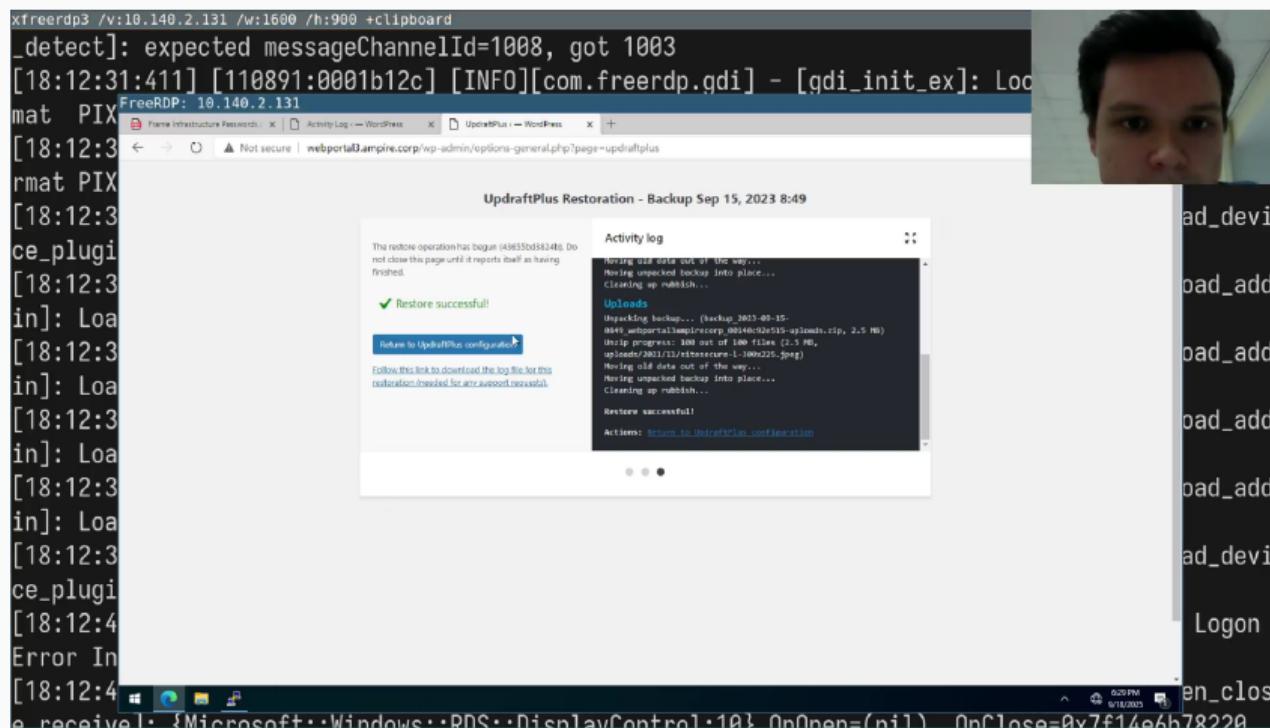


Рис. 9: Успешное восстановление

Выполнение лабораторной работы. Устранение уязвимости

Закрытие уязвимости можно осуществить несколькими способами:

- отключение плагина WpDiscuz;
- обновление версии WpDiscuz до версии 7.0.5 и выше(при наличии интернета).

Для отключения плагина в левой части панели инструментов необходимо открыть раздел Plugins, далее нажать на опцию Deactivate. Также можно полностью удалить плагин с сайта аналогичным образом с помощью опции Delete.

Выполнение лабораторной работы. Устранение уязвимости

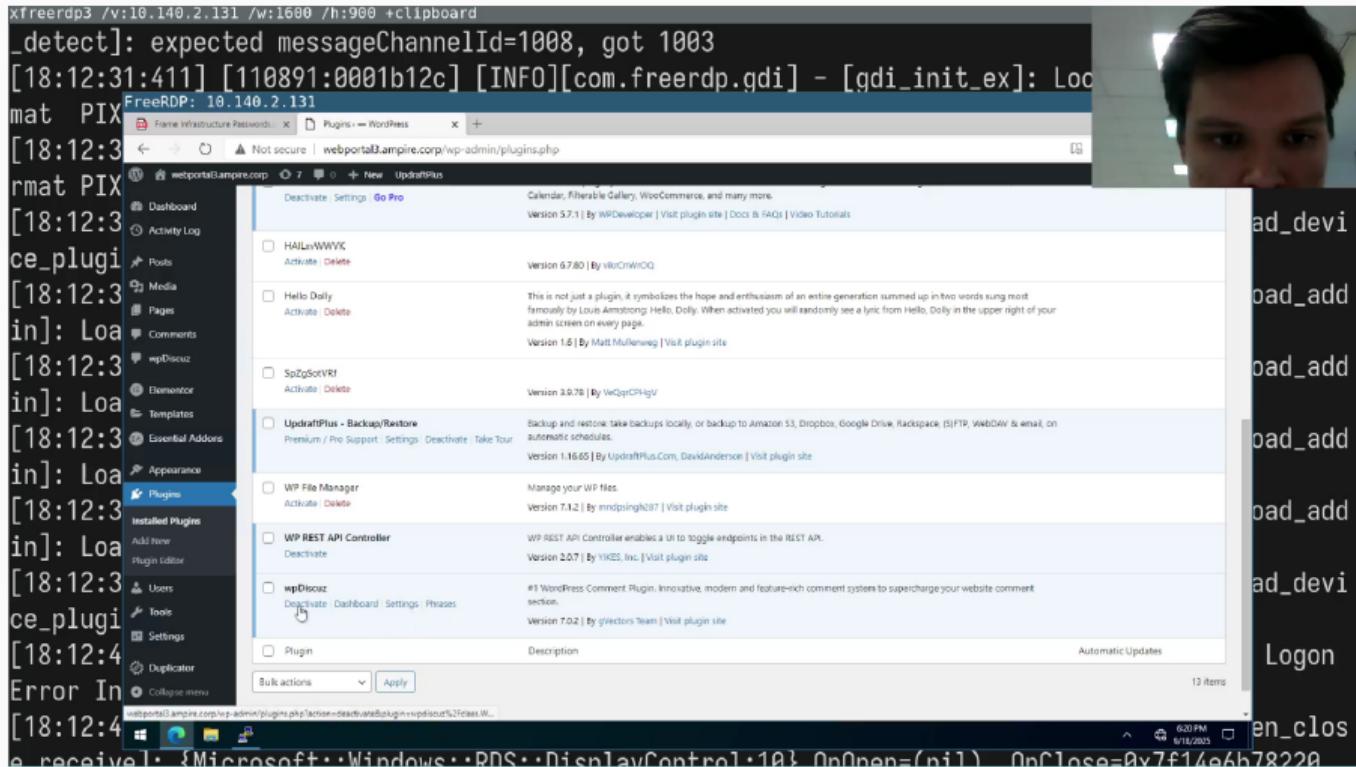


Рис. 10: Отклонение плагина WpDiscuz

Выполнение лабораторной работы. Устранение последствия Meterpreter-сессия

Также необходимо закрыть активные сессии с атакующим.

Для обнаружения meterpreter-сессии необходимо проверить сокеты уязвимой машины на подключение к определенному порту машины нарушителя с помощью утилиты ss.

Просмотреть сокеты только нужного протокола TCP и отфильтровать данные (например, вывести только активные TCP-соединения) можно с помощью команды: ss -tnp.

Выполнение лабораторной работы. Устранение последствия Meterpreter-сессия

Рис. 11: Все активные сети

Для закрытия вредоносного сокета необходимо завершить процесс, использующийся для поддержания соединения. При завершении процесса определить уникальный идентификатор процесса (PID) и прописать команду kill с соответствующими параметрами.

Выполнение лабораторной работы. Устранение последствия Meterpreter-сессия

```
xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
_detect]: expected messageChannelId=1008, got 1003
[18:12:31:411] [110891:0001b12c] [INFO][com.freerdp.gdi] - [gdi_init_ex]: Local mat PIX
FreeRDP: 10.140.2.131
admin@web-portal-3:~ % xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
_A, --query=QUERY, --socket=QUERY
    QUERY := {all|inet|tcp|udp|raw|unix|unix_dgram|unix_stream|unix_sepacket|packet|netlink|vsock_stream|vsock_dgram}{,?}
-D, --diag=FILE      Dump raw information about TCP sockets to FILE
-F, --filter=FILE   read filter information from FILE
    FILTER := { state STATE FILTER } { EXPRESSION }
    STATE_FILTER := {all|connected|synchronized|bucket|big|TCP-STATES}
    TCP-STATES := {established|syn-sent|syn-recv|fin-wait-{1,2}|time-wait|closed|close-wait|last-ack|listening|closing}
    connected := {established|syn-sent|syn-recv|fin-wait-{1,2}|time-wait|close-wait|last-ack|closing}
    synchronized := {established|syn-recv|fin-wait-{1,2}|time-wait|close-wait|last-ack|closing}
    bucket := {syn-recv|time-wait}
    big := {established|syn-sent|fin-wait-{1,2}|closed|close-wait|last-ack|listening|closing}
in]: Load module
SOCK_DESTROY answers: Operation not permitted
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31:411] admin@web-portal-3:~ % ss -K dst 195.239.174.11
admin@web-portal-3:~ % ss -K dst 195.239.174.
Error: an inet prefix is expected rather than "195.239.174.".
in]: Load module
Cannot parse dst/src address.
admin@web-portal-3:~ % ss -tp
state      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31:411] FIN-WAIT-2      0          0          10.10.1.22:58904      10.10.2.11:https
ESTAB      0          0          10.10.1.22:50720      195.239.174.11:005
in]: Load module
ESTAB      210         0          10.10.1.22:33136      195.239.174.12:https
ESTAB      0          64         10.10.1.22:sah      10.10.1.253:59827
ESTAB      0          0          10.10.1.22:39210      195.239.174.11:freciev
CLOSE-WAIT  0          0          10.10.1.22:38944      195.239.174.11:5557
admin@web-portal-3:~ % ss -K dst 195.239.174.11
Error: an inet prefix is expected rather than "195.239.174.".
in]: Load module
Cannot parse dst/src address.
admin@web-portal-3:~ % ss -K dst 195.239.174.11
SOCK_DESTROY answers: Operation not permitted
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
[18:12:31:411] admin@web-portal-3:~ % sudo ss -K dst 195.239.174.11
(sudo) password for admin:
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
tcp        ESTAB      0          0          10.10.1.22:50720      195.239.174.11:005
tcp        ESTAB      0          0          10.10.1.22:39210      195.239.174.11:freciev
tcp        CLOSE-WAIT  0          0          10.10.1.22:38944      195.239.174.11:5557
Error In Logon
```

Рис. 12: Закрытие активной сессии атакующего

Выполнение лабораторной работы. Устранение последствия Meterpreter-сессия

```
user@web-portal-3:~$ sudo ss --kill dst 195.239.174.11
[sudo] password for user:
Netid      State          Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
tcp        CLOSE-WAIT      1            0           10.10.1.22:51092      195.239.174.11:5557
tcp        ESTAB          0            0           10.10.1.22:48244      195.239.174.11:1085
tcp        ESTAB          0            0           10.10.1.22:60528      195.239.174.11:freeciv
```

Рис. 13: Закрытие активной сессии атакующего

Выполнение лабораторной работы. Атака на почтовый сервер(ProxyLogon). Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS

Proxylogon представляет собой SSRF в Exchange Server, позволяющую обойти аутентификацию и выдать себя за администратора. В сценарии данная уязвимость используется в связке с CVE 2021-27065 (запись файла в произвольную директорию). Уязвимости Proxylogon подвержены все Exchange Server 2016, до версии 15.01.2106.013.

Сетевой сенсор ViPNet IDS NS во время атаки детектирует несколько событий, которые потенциально могут быть связаны с эксплуатацией уязвимости на уязвимом хосте. В списке событий присутствуют признаки загрузки на уязвимый хост подозрительных файлов в формате .exe.

Также зафиксирована активность вредоносного программного обеспечения Metasploit.

Выполнение лабораторной работы. Атака на почтовый сервер(ProxyLogon). Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS

The screenshot shows the ViPNet IDS NS software interface. On the left is a sidebar with navigation links like Monitoring, Dashboard, Events, Reports, Network Environment, Analysis Methods, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, and Audit. The main area has a title "Events" and a sub-section "Events for recent 24 hours". A table lists events with columns: S., Date and time, ID, Event code, Q..., Rule name, and Class. Most events are "ET INFO Windows Power..." or "ET INFO PE EXE Download..." with "not-suspicious" class. One event is highlighted in blue: "00:15:28.477 0... 2033355 1 ET TROJAN Possible Met... trojan-activity". To the right of this table is a detailed view of the selected event:

Event 00:15:30.281 0... 2025644 1 ET TROJAN Possible Met... trojan-activity

Event	Source	Description
Capture interface		
Severity		Signature event
Event type		TCP
Protocol		
Event code		2025644

Analysis rule

Class	trojan-activity
Group	trojan
Name	ET TROJAN Possible Metasploit Payload Common Construct Bind_API (from server)

Description:
This rule detects a malware activity

Text:
alert tcp \$EXTERNAL_NET any -> \$HOME_NET any (msg: "ET TROJAN Possible Metasploit Payload Common Construct Bind_API (from server)"; flow: from_server; stable; shed_content: "60 89 45 31"; content: "64 84 B4"; distance: 2;within: 2;content: "00 8b 7f";distance: 1;within: 2;content: "0c 8b 82 14 8b 72 28 01 b7 4a 26 31 ff";distance: 1;within: 13;content: "1c 3c 61 7c 02 2c 20 c1 cf 0d 01 c7 e2";within: 15;content: "192 57 89 52 10";distance: 1;within: 1;signature_type: trojan-activity;id: 2025644;rev: 2;meta data: affected_asset_id, affected_product_id, affected_vendor_id, attack_target, Client_Endpoint, confidence_Medium, created_at 2016_05_16, deployment_Dataset, er_deployment_Internal, deployment_Internet, deployment_Perimeter, signature_sever

20:27:47 15.09.2023

Рис. 14: Список событий, направленных на уязвимый сервер

Выполнение лабораторной работы. Атака на почтовый сервер(ProxyLogon). Обнаружение средствами Security Onion

Для обнаружения последствий эксплуатации в Security Onion следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. Для просмотра данных о событиях нужно открыть ссылку на веб-приложение Squert на главной странице Security Onion.

На скриншоте представлены события, зафиксированные веб-приложением Squert. Данные события аналогичны событиям, зафиксированным сетевым сенсором ViPNet IDS NS.

Выполнение лабораторной работы. Атака на почтовый сервер(ProxyLogon). Обнаружение средствами Security Onion

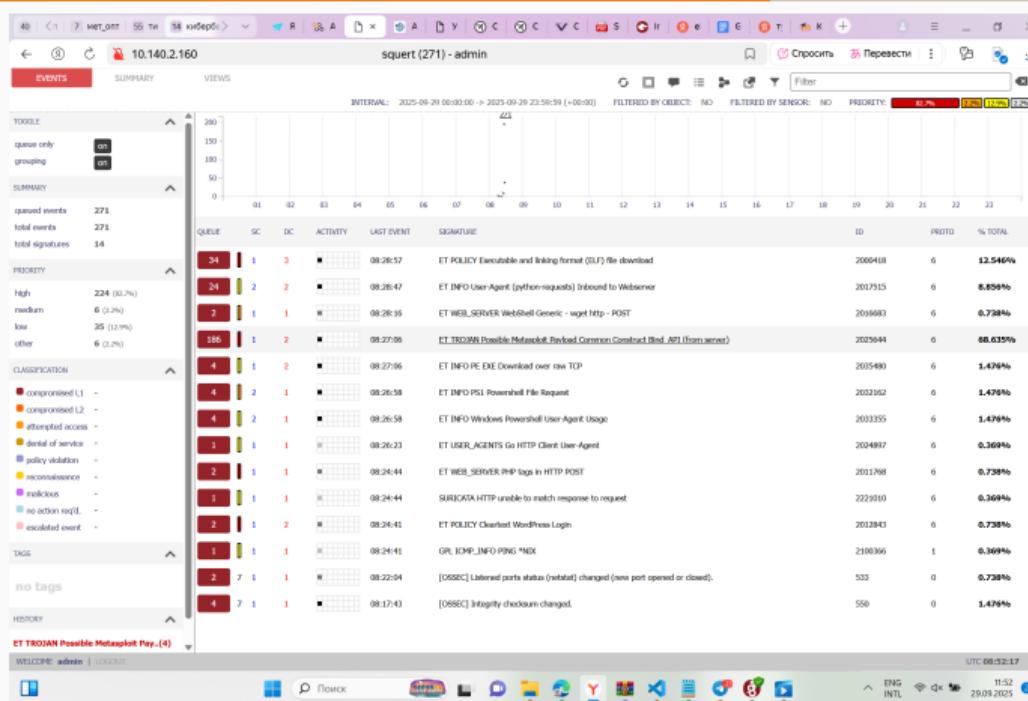


Рис. 15: События, зафиксированные Squert

Выполнение лабораторной работы. Атака на почтовый сервер(ProxyLogon). Обнаружение средствами Security Onion

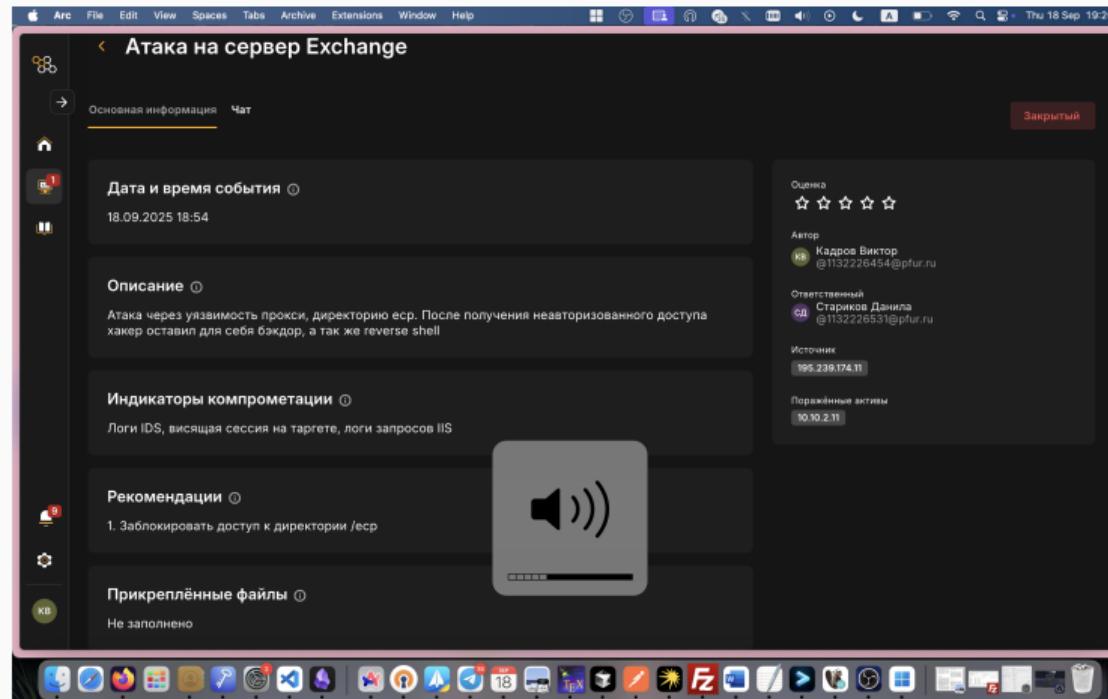


Рис. 16: Карточка второго инцидента

Выполнение лабораторной работы. Устранение уязвимости ProxyLogon

Во время эксплуатации уязвимости Proxylogon нарушитель совершает GET и POST запросы к /ecp. Достаточно ограничить доступ к вышеуказанной директории чтобы уязвимость не эксплуатировалась.

Открыть Internet Information Services (IIS) Manager. Для этого необходимо нажать сочетание клавиш «Win+R», ввести «inetmgr» и нажать «Enter». В открывшемся окне перейти во вкладку MAIL/Sites/Default Web Site/ecp и нажать на IP Address and Domain Restrictions. Далее в «Edit Feature Settings» – «Access for unspecified clients» выбрать пункт «Deny» и нажать «OK».

Выполнение лабораторной работы. Устранение уязвимости ProxyLogon

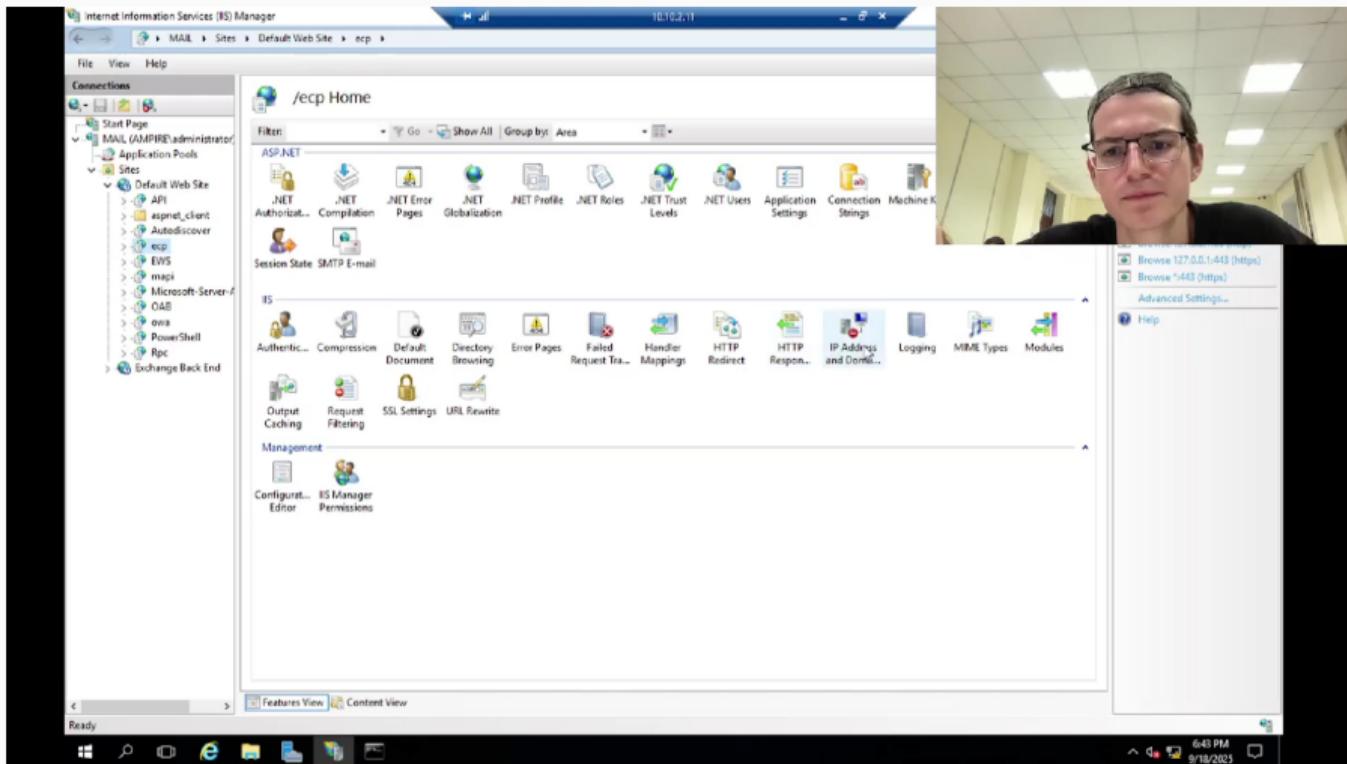


Рис. 17: MAIL/Sites/Default Web Site/ecp

Выполнение лабораторной работы. Устранение уязвимости ProxyLogon

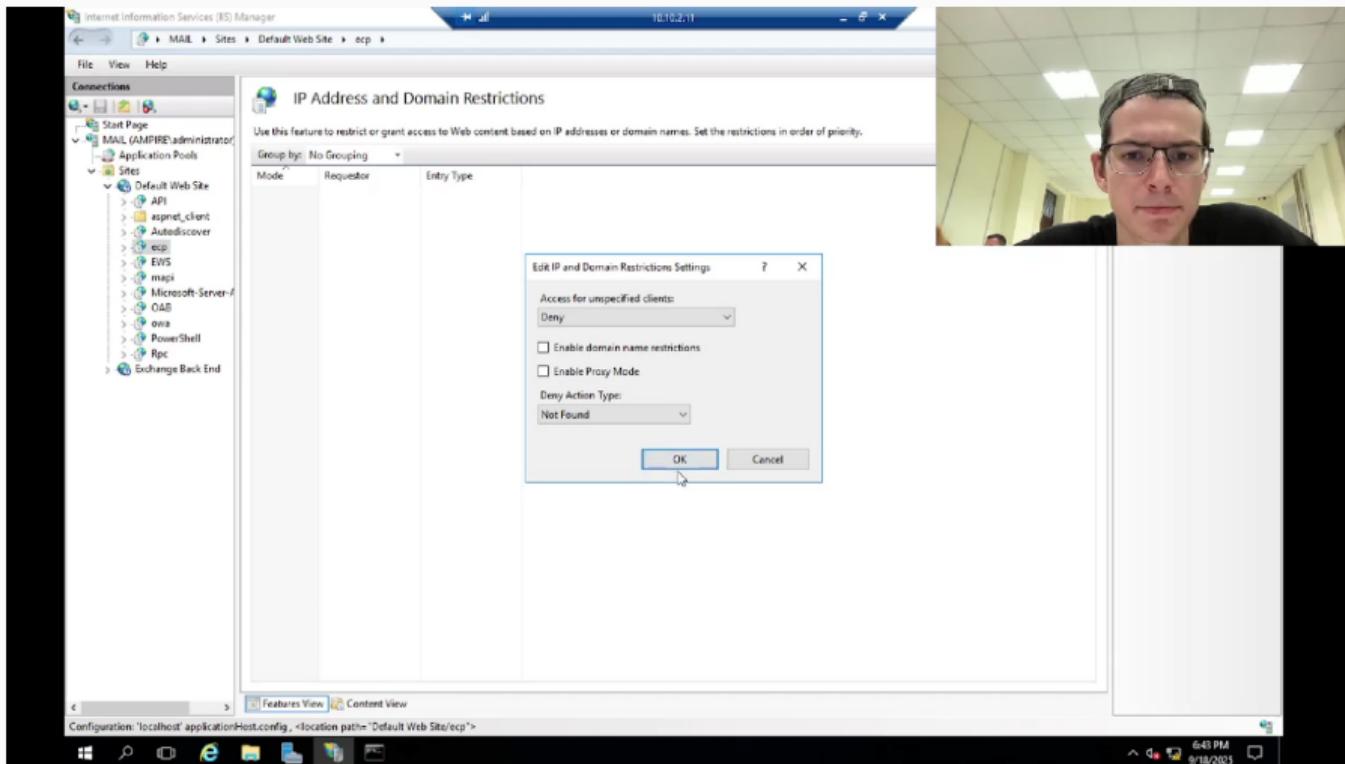


Рис. 18: MAIL/Sites/Default Web Site/ecp/IP Address and Domain Restrictions

Выполнение лабораторной работы. Устранение последствия China Chopper

Backdoor “China Chopper” можно найти в очевидной для таких атак директории C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/owa/auth/AM_backdoor.aspx.

Большинство РОС (проверок концепций) эксплуатации уязвимости Proxylogon записывают файл именно по данному адресу, что выполняется для доступа backdoor(backdoor — «чёрный ход», дословно «задняя дверь» — уязвимость, которая даёт несанкционированный доступ к компьютеру, смартфону и т. п.) без авторизации из веб-директории owa/auth. При необходимости последствие можно записать в другую директорию.

Для устранения последствия необходимо: - удалить файл веб-оболочки по пути C:/ProgramFiles/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/..auth/;

Выполнение лабораторной работы. Устранение последствия China Chopper

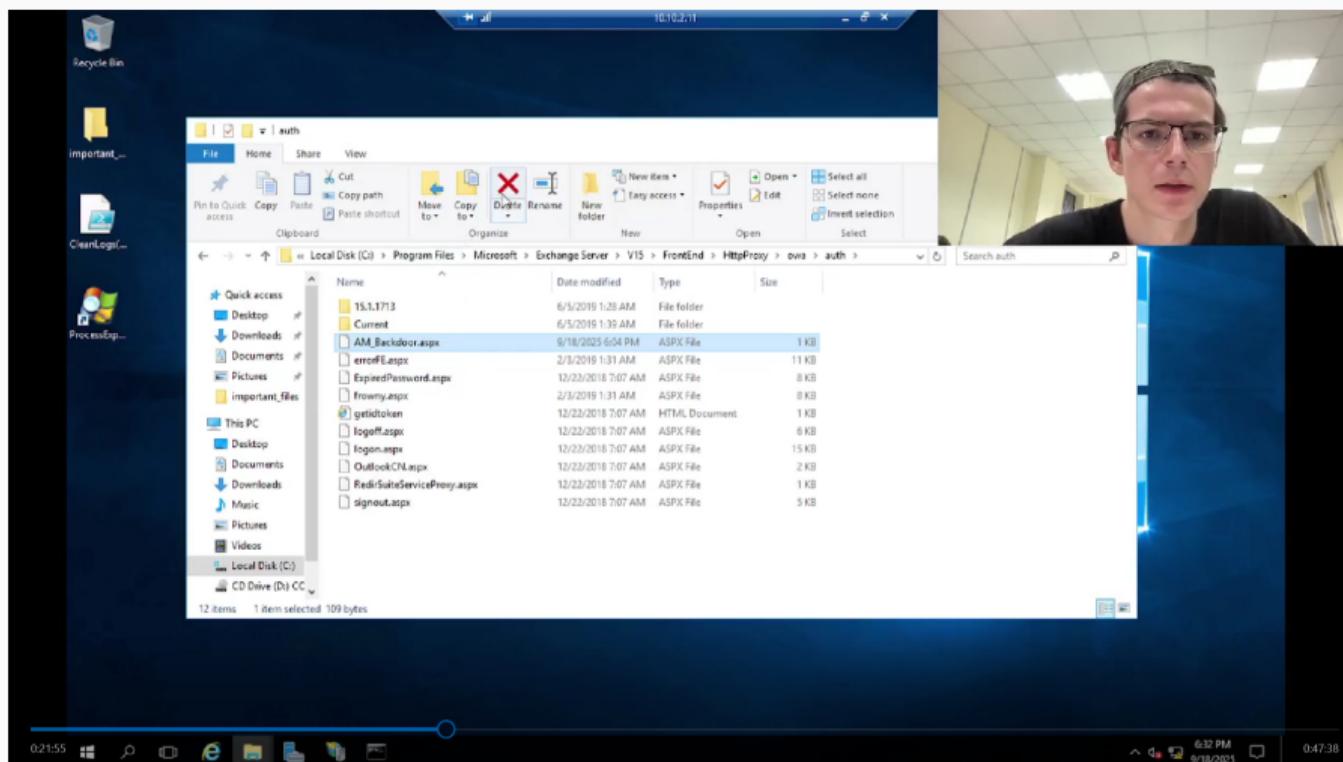


Рис. 19: Удаление файла AM_backdoor

Признак эксплуатации NoSQL-инъекции - это невозможность осуществления входа на веб-интерфейс под учетными данными администратора (логин: admin@rocket-local.com, пароль: qwe123!@#). В syslog пишутся следующие строчки:

- ошибка отправки приветственного сообщения при регистрации нового аккаунта;
- письмо для сброса пароля админа;
- ошибки при выполнении сценариев WebHook.

Выполнение лабораторной работы. Атака на RocketChat (CVE-2021-22911)

```
root@rocket-chat-server:~# less /var/log/syslog | grep smtpd
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: NOQUEUE: reject: RCPT from localhost[127.0.0.1]: 550 5.1.1 <hacker.com>: Recipient address rejected: hacker.com; from=<rocketchat@rocket-local.com> to=<hacker@hacker.com> proto=ESMTP helo=<127.0.0.1>
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: lost connection after RCPT from localhost[127.0.0.1]
Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=0/1 commands=2/3
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: ECAC1748BD: client=localhost[127.0.0.1]
Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 commands=4
root@rocket-chat-server:~#
```

Рис. 20: Ошибка подтверждения e-mail

Выполнение лабораторной работы. Атака на RocketChat (CVE-2021-22911)

```
root@rocket-chat-server:/var/log# less /var/log/syslog | grep -n postfix
29:Sep 29 08:17:34 rocket-chat-server postfix/postfix-script[1279]: warning: symlink leaves directory: /etc/postfix./.makefiles.out
32:Sep 29 08:17:34 rocket-chat-server postfix/postfix-script[1463]: starting the Postfix mail system
33:Sep 29 08:17:34 rocket-chat-server postfix/master[1465]: daemon started -- version 3.4.13, configuration /etc/postfix
254:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
255:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: NOQUEUE: reject: RCPT from localhost[127.0.0.1]: 550 5.1.1 <hacker@hacker.com>; Recipient address rejected: hacker.com; from=<rocketchat@rocket-local.com> to=<hacker@hacker.com> proto=ESMTP helo=<[127.0.0.1]>
256:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: lost connection after RCPT from localhost[127.0.0.1]
257:Sep 29 08:27:44 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=0/1 commands=2/3
260:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: connect from localhost[127.0.0.1]
261:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: ECAC1748BD: client=localhost[127.0.0.1]
262:Sep 29 08:27:55 rocket-chat-server postfix/cleanup[1882]: ECAC1748BD: message-id=<83dc9a2b-d7a7-39de-e94b-58eb84dcd884@rocket-local.com>
263:Sep 29 08:27:55 rocket-chat-server postfix/qmgr[1468]: ECAC1748BD: from=<rocketchat@rocket-local.com>, size=5870, nrcpt=1 (queue active)
264:Sep 29 08:27:55 rocket-chat-server postfix/smtpd[1872]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 commands=4
265:Sep 29 08:27:56 rocket-chat-server postfix/local[1883]: ECAC1748BD: to=<admin@rocket-local.com>, relay=local, delay=0.06, delays=0.03/0.02/0/0, dsn=2.0.0, status=sent (delivered to mailbox)
266:Sep 29 08:27:56 rocket-chat-server postfix/qmgr[1468]: ECAC1748BD: removed
root@rocket-chat-server:/var/log#
```

Рис. 21: Письмо со сбросом пароля

Выполнение лабораторной работы. Атака на RocketChat (CVE-2021-22911)

```
Sep 29 08:28:22 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" n  
ot in Trigger rce ]  
Sep 29 08:28:34 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" n  
ot in Trigger rce ]  
Sep 29 08:28:48 rocket-chat-server rocketchat[682]: server.js:204 Integrations → Incoming WebHook.error [Class "Script" n  
ot in Trigger rce ]
```

Рис. 22: Ошибки при выполнении сценариев WebHook

Выполнение лабораторной работы. Атака на RocketChat (CVE-2021-22911)

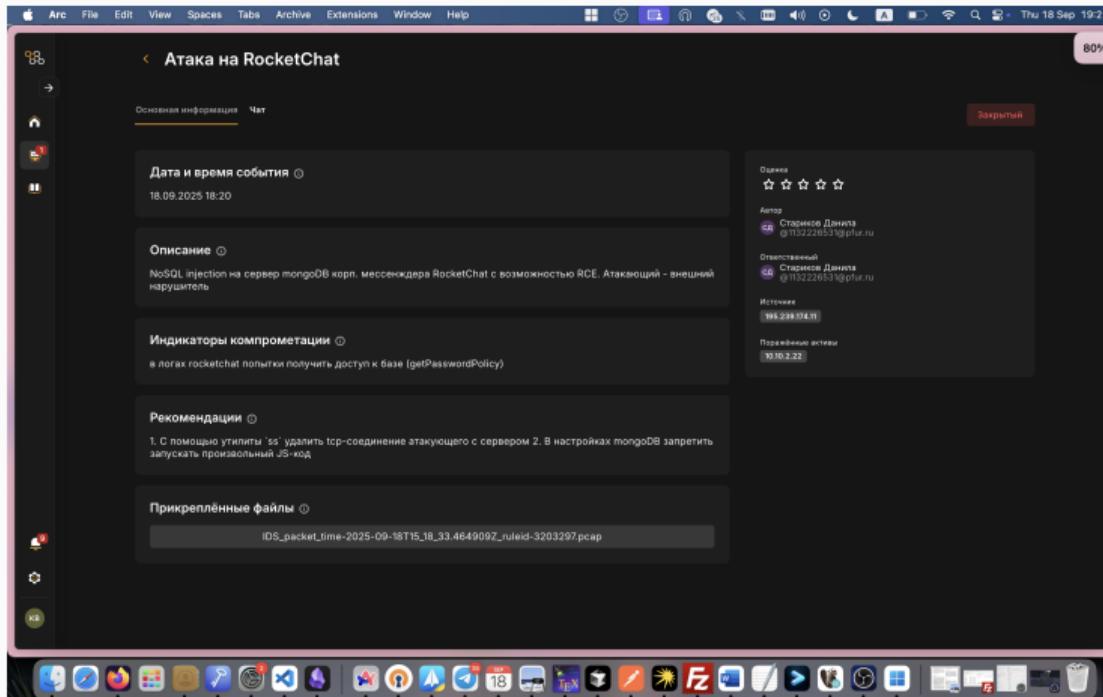
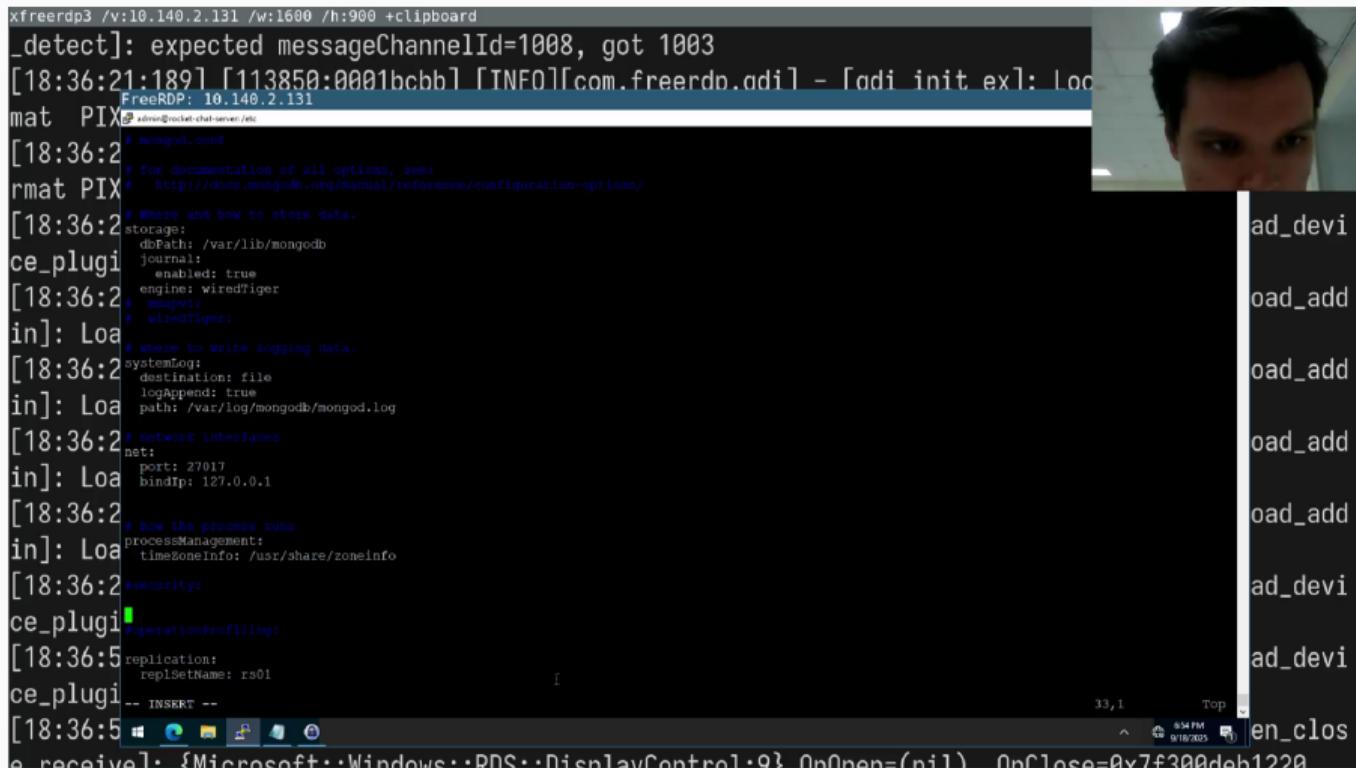


Рис. 23: Карточка третьего инцидента

Так как NoSQL-инъекция для повышения привилегий использует высокоуровневый оператор БД `$where`, временной, смягчающей мерой, может стать отключение выполнения JavaScript на стороне сервера базы данных.

Для этого необходимо отредактировать файл конфигурации БД `/etc/mongod.conf`, добавив строчку `javascriptEnabled: false`.

Выполнение лабораторной работы. Закрытие уязвимости RocketChat



The screenshot shows a terminal window with the command `xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard` running. The terminal displays the contents of the `/etc/mongod.conf` file. The configuration includes settings for storage, network interfaces, process management, and security. A portion of the configuration is highlighted with a yellow selection bar.

```
xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
_detect]: expected messageChannelId=1008, got 1003
[18:36:21:189] [113850:0:001bcbb] [INFO][com.freerdp.adil - adi_init_ex]: Loc
FreeRDP: 10.140.2.131
mat PIX
# mongod.conf
[18:36:2
# for documentation of all options, see:
rmat PIX
[18:36:2
# Where and how to store data.
ce_plugi
[18:36:2
# snappy:
in]: Loa
[18:36:2
# where to write logging data.
[18:36:2
systemLog:
destination: file
logAppend: true
path: /var/log/mongodb/mongod.log
[18:36:2
# network interfaces
net:
in]: Loa
[18:36:2
# how the process runs
in]: Loa
processManagement:
timeZoneInfo: /usr/share/zoneinfo
[18:36:2
#security:
ce_plugi
[18:36:5
#operationProfiling:
[18:36:5
replication:
replicaSetName: rs01
ce_plugi
-- INSERT --
[18:36:5

```

On the right side of the terminal window, there is a vertical stack of text snippets, likely from a previous slide or context, including:

- ad_devi
- oad_add
- oad_add
- oad_add
- oad_add
- oad_add
- ad_devi
- ad_devi
- en_clos

Рис. 24: Изначальный файл конфигурации БД /etc/mongod.conf

Выполнение лабораторной работы. Закрытие уязвимости RocketChat

```
xfreerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard  
_detect]: expected messageChannelId=1008, got 1003  
[18:36:21:189] [113850:0001bcbb1] [INFO][com.freerdp.adil] - [adi init ex]: Loc  
mat PIX  
[18:36:2  
rmat PIX  
[18:36:2  
ce_plugi  
[18:36:2  
in]: Loa  
[18:36:2  
ce_plugi  
[18:36:5  
ce_plugi  
[18:36:5  
ce_plugi  
[18:36:5  
e receive: {Microsoft::Windows::PDS::DisplayControl1::OnOpen=(nil)} OnClose=0x7f300deb1220  
FreeRDP: 10.140.2.131  
# /etc/mongod.conf  
# mongod.conf  
# for documentation of all options, see:  
#   http://docs.mongodb.org/manual/reference/configuration-options/  
# Where and how to store data.  
storage:  
  dbPath: /var/lib/mongodb  
  journal:  
    enabled: true  
    engine: wiredTiger  
#   snapsh:  
#   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  
-- INSERT --  
33, 25 Top en_clos
```

Рис. 25: Измененный файл конфигурации БД /etc/mongod.conf

Выполнение лабораторной работы. Закрытие уязвимости и последствия

Для применения настроек необходимо перезапустить службу: sudo systemctl restart mongod.service.

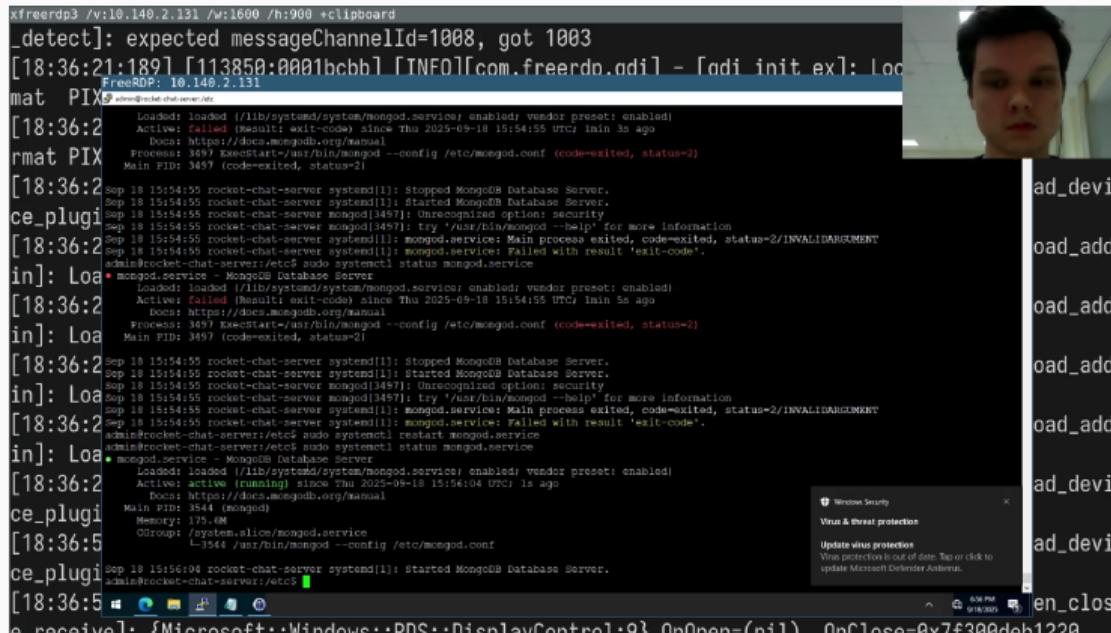


Рис. 26: Перезапуск службы: sudo systemctl restart mongod.service

Данное последствие можно обнаружить при выводе сетевой статистики с помощью утилиты ss и параметрами -tp (позволяет просматривать сведения по TCP-соединениям, список процессов в данный момент). В случае установления соединения, на уязвимой машине появится сокет с машиной нарушителя.

Нейтрализовать meterpreter-сессию также можно при помощи утилиты ss с ключом -K, чтобы завершить все сессии с машиной нарушителя необходимо ввести: sudo ss -K dst HACKER_IP dport = HACKER_PORT.

Выполнение лабораторной работы. Закрытие уязвимости и последствия

```
freerdp3 /v:10.140.2.131 /w:1600 /h:900 +clipboard
_detect]: expected messageChannelId=1008, got 1003
[18:36:21:189] [113850:0:001bcbb] [INFO][com.freerdp.adil] - [adi init ex]: Local
FreeRDP: 10.140.2.131
mat PIX] admin@rocket-chat-server:~/mail$ 
[18:36:2 ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59544
rmat PIX] ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59556
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59584
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59554
ESTAB 0 0 127.0.0.1:59570 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59520
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59578
ce_plugin] ESTAB 0 0 10.10.2.22:40506 195.239.174.11:5553
ESTAB 0 0 127.0.0.1:59572 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:595616 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59588
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59580
in]: Loa ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59518
ESTAB 0 0 127.0.0.1:59562 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59560
ce_plugin] ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59576
ESTAB 0 0 127.0.0.1:59560 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59564 127.0.0.1:27017
in]: Loa ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59566
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59562
[18:36:2 ESTAB 0 0 127.0.0.1:59556 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59580 127.0.0.1:27017
in]: Loa ESTAB 0 0 10.10.2.22:3000 10.10.2.254:26597
ESTAB 0 0 127.0.0.1:59558 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59584 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:59570
ESTAB 0 0 127.0.0.1:59546 127.0.0.1:27017
ESTAB 0 0 10.10.2.22:ssh 10.10.2.254:52899
ESTAB 0 0 127.0.0.1:59544 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59520 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59580 127.0.0.1:27017
ESTAB 0 0 127.0.0.1:59516 127.0.0.1:27017
ce_plugin] admin@rocket-chat-server:~/var/mail$ ss -K dst 195.239.174.11
SOCK_DESTROY answers: Operation not permitted
[18:36:5 admin@rocket-chat-server:~/var-mails sudo ss -K dst 195.239.174.11
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp ESTAB 0 0 10.10.2.22:40506 195.239.174.11:5559
ce_plugin] admin@rocket-chat-server:~/var/mail$ 
[18:36:5 e_receive: {Microsoft::Windows::RDS::DisplayControl1:9} OnOpen=(nil) OnClose=0x7f300deb1220
```

Рис. 27: Закрытие сессии с нарушителем

Вывод

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Защита корпоративного мессенджера” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы освоили практические навыки выявления, анализа и устранения уязвимостей в корпоративной инфраструктуре, а также освоили навыки отработки действий по нейтрализации последствий успешных атак.