Отчёт по лабораторной работе 3-D (НФИ-2)

Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»

Козлов В.П., Гэинэ А., Шуваев С., Джахангиров И.З, Хватов М.Г. | НФИбд-02-22

Содержание

# Цель работы

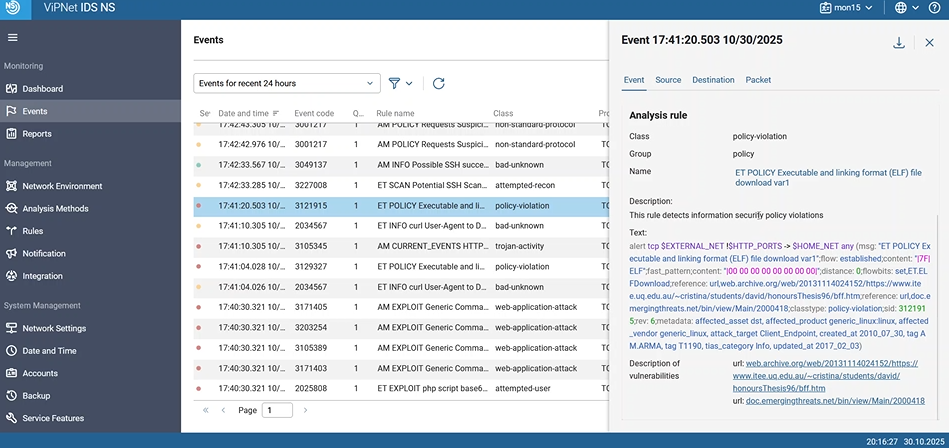
Отработать сценарий: Защита интеграционной платформы

# Задание

1. Обнаружить Bitrix vote RCE на Bitrix Server.
2. Устранить уязвимость путём отклонения всех запросов к директории vote.
3. Устранить последствие (Deface). Восстанавливаем бэкап сайта.
4. Обнаружить GitLab RCE на узле GitLab.
5. Зайти в панель администратора, ужесточить регистрацию. Удалить неизвестных пользователей.
6. Устранить последствие (Gitlab meterpreter). Убиваем сессию нарушителя.
7. Обнаружить WSO2 API-Manager RCE на узле MS API Manager.
8. Изменить параметр загрузки ресурсов в конфиг файле.
9. Устранить последствие (WSO Web User). Удалить нового привилегированного пользователя. Удалить бэкдор

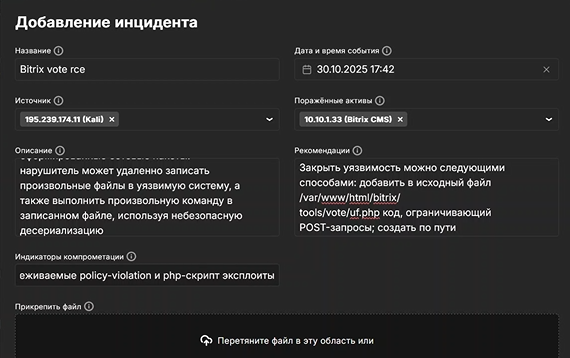
# Выполнение лабораторной работы

На сайте ViPNet IDS NS просмотрели атакованные активы и суть атак (рис. [-@fig:002])



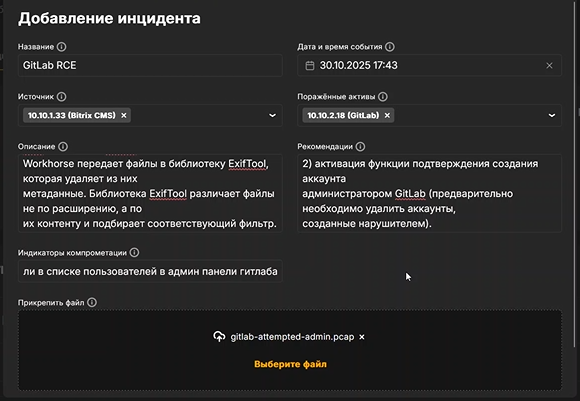
Атакованные ip-адреса

Добавили карточку инцидента “Bitrix vote RCE” (рис. [-@fig:100])



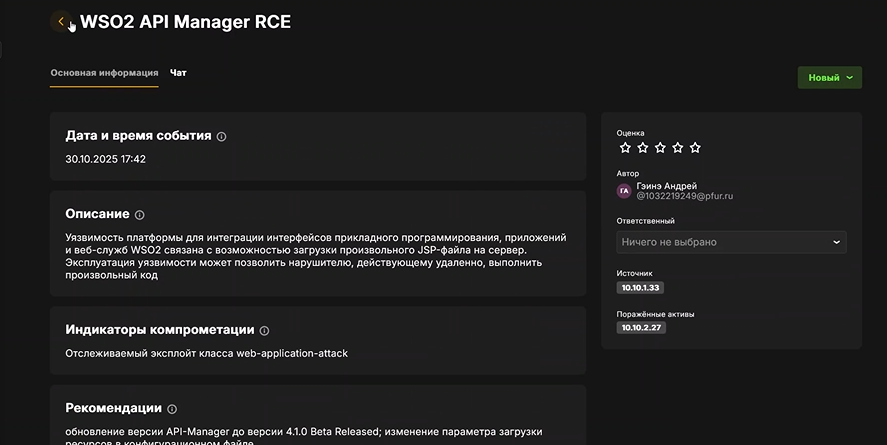
Карточка инцидента “Bitrix vote RCE”

Добавили карточку инцидента “GitLab RCE” (рис. [-@fig:200])



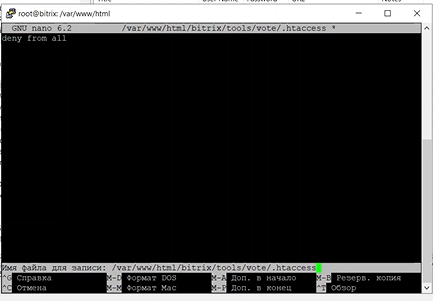
Карточка инцидента “GitLab RCE”

Добавили карточку инцидента “WSO2 API-Manager RCE” (рис. [-@fig:300])



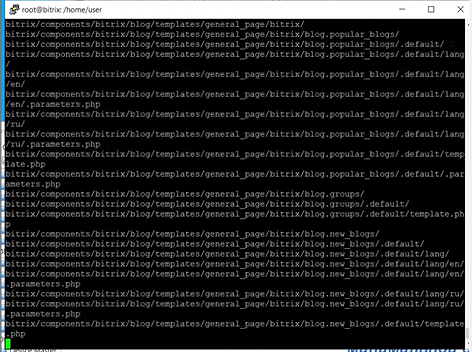
Добавили карточку инцидента “WSO2 API-Manager RCE”

Bitrix vote RCE. Устранили уязвимость путём отклонения всех запросов к директории vote (рис. [-@fig:003])



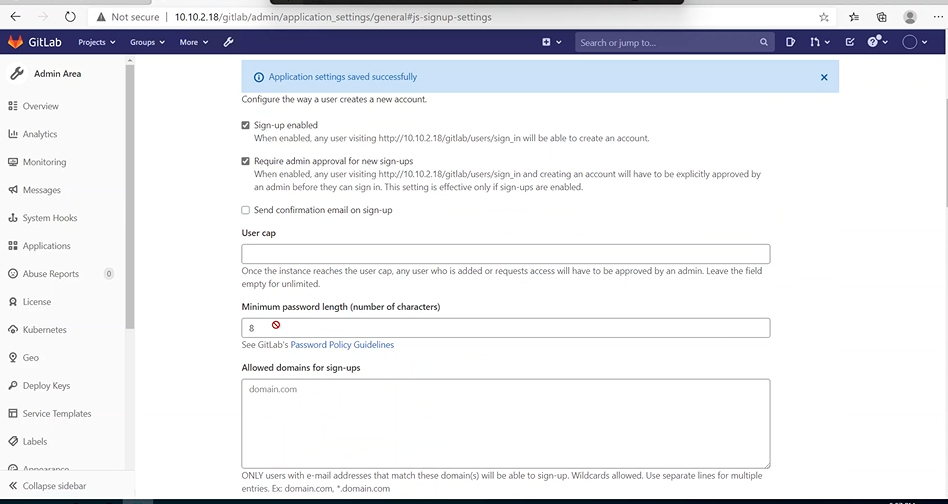
.htaccess

Bitrix vote RCE. Восстанавливаем бэкап сайта (рис. [-@fig:004])



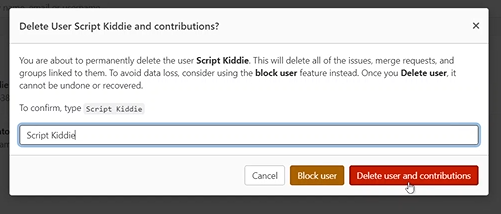
Процесс восстановления бэкапа

GitLab RCE. Заходим на панель администратора, ужесточаем регистрацию (рис. [-@fig:005])



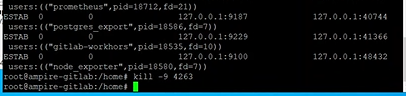
Настройки регистрации

GitLab RCE. Удаляем неизвестного нам пользователя (рис. [-@fig:006])



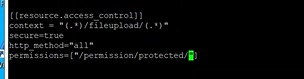
Удаляем неизвестного нам пользователя

GitLab RCE. Находим PID сессию с нарушителем, убиваем её (рис. [-@fig:007])



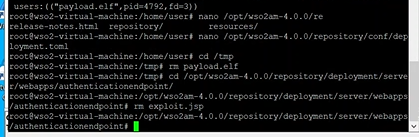
Сессия нарушителя устранена

WSO2 API-Manager RCE. Заходим на MS API Manager, изменяем паарметр загрузки ресурсов (рис. [-@fig:008])



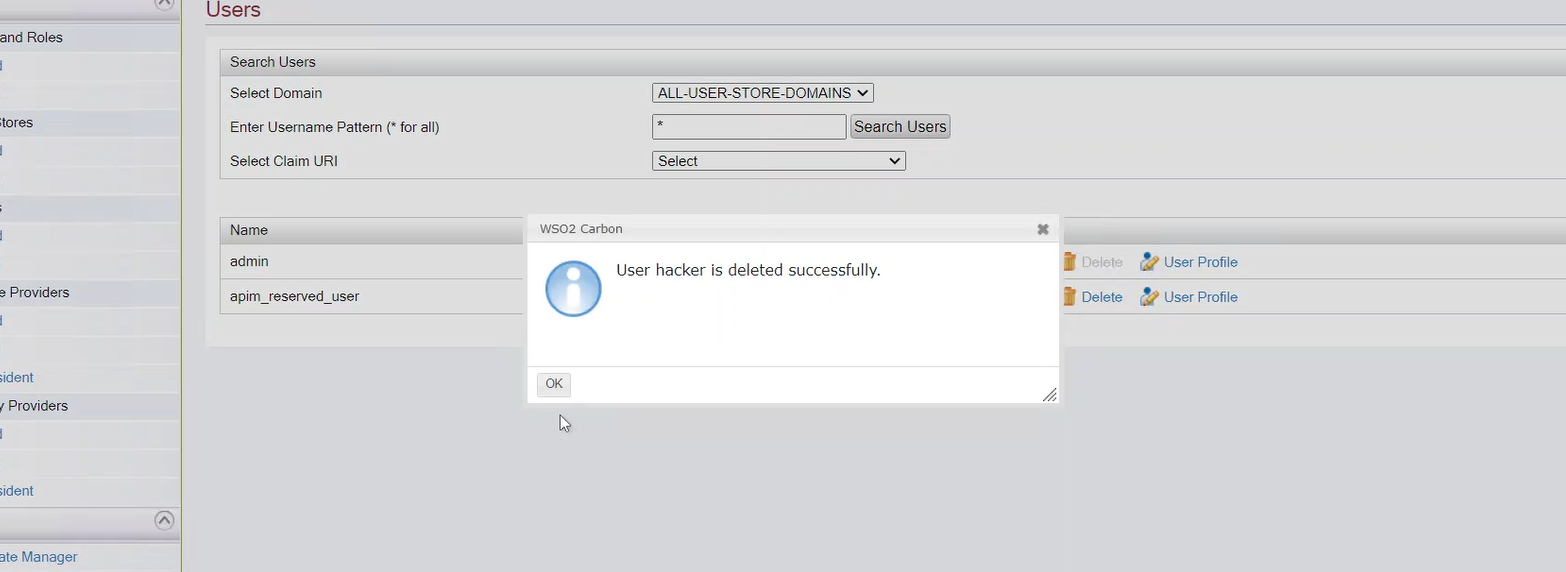
Меняем конф

WSO2 API-Manager RCE. Удаляем бэкдор (рис. [-@fig:009])



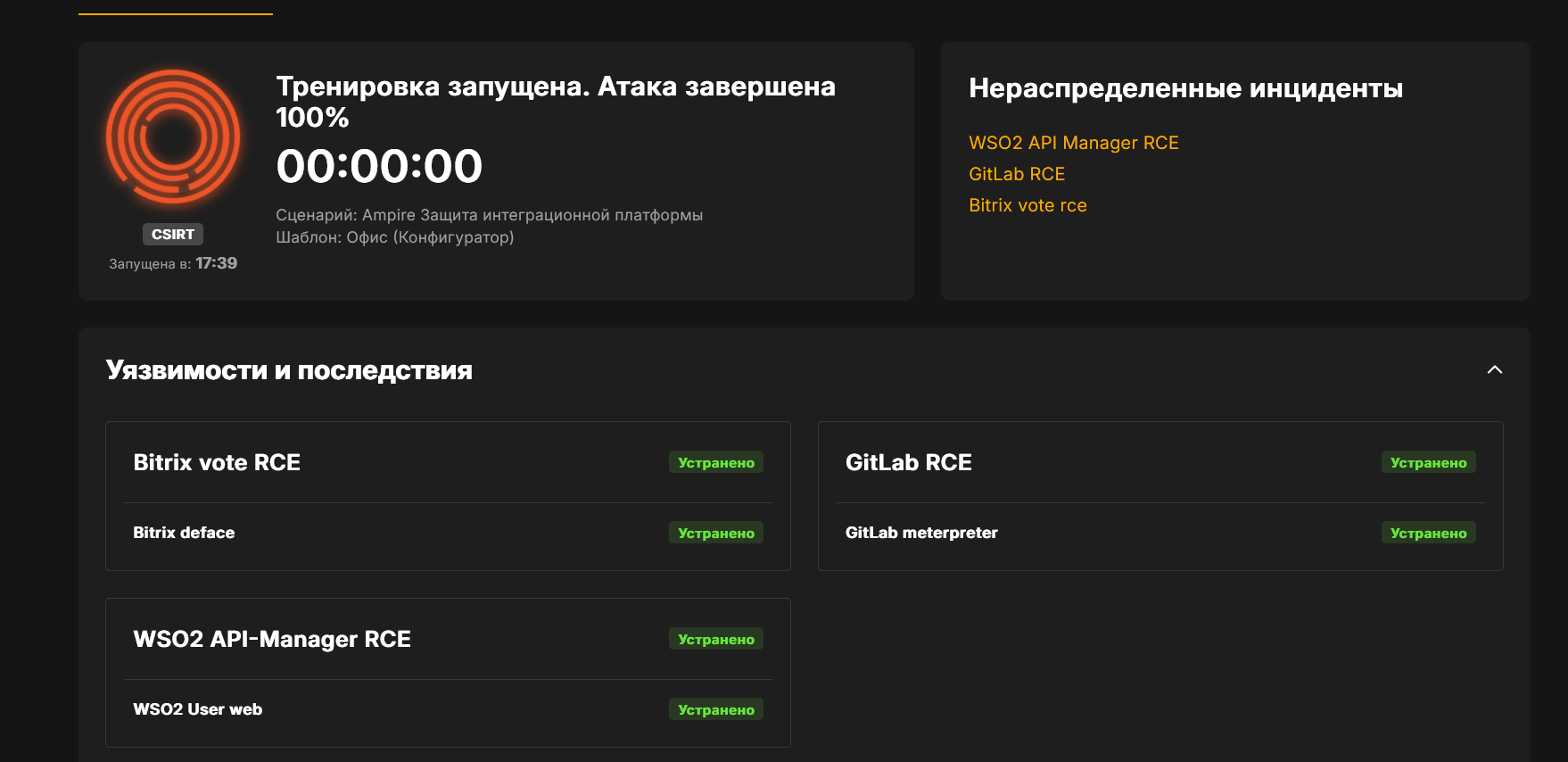
Удалили бэкдор

WSO2 API-Manager RCE. Удаляем нового пользователя (рис. [-@fig:009])



Удалили бэкдор

Все атаки и их последствия успешно устранены



Всё оки

# Выводы

Отработали сценарий: Защита интеграционной платформы.

# Список литературы

1. **CVE-2019-0630** — Common Vulnerabilities and Exposures.  
   URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0630
2. **CVE-2019-17427** — Уязвимость XSS в Redmine.  
   URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17427
3. **CVE-2019-18890** — Уязвимость Blind SQL-инъекции в Redmine.  
   URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18890