Отчёт по лабораторной работе 1-C (НФИ-2)

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

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

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Отработка на практике методов обнаружения, анализа и нейтрализации многоэтапной компьютерной атаки, направленной на кражу научно-технической информации предприятия, с использованием учебного программного комплекса «Ampire».

# 2 Задание

1. Обнаружить подбор пароля к файловому серверу и последующую загрузку вредоносного файла.
2. Выявить бэкдор на рабочей станции через анализ планировщика задач и запущенных процессов.
3. Зафиксировать кражу учётных данных (например, с помощью утилиты LaZagne) и их использование для доступа к Redmine.
4. Проанализировать XSS-атаку в Redmine, которая привела к включению REST API и созданию привилегированного пользователя.
5. Обнаружить слепую SQL-инъекцию, используемую для извлечения конфиденциальных данных из базы данных.
6. Нейтрализовать последствия атаки: удалить бэкдор, несанкционированного пользователя и внедрённый вредоносный код.
7. Устранить уязвимости: пропатчить Redmine от XSS (CVE-2019-17427) и SQL-инъекции (CVE-2019-18890), усилить политику паролей.

# 3 Выполнение лабораторной работы

Активировали WireGuard и зашли на сайт платформы (рис. 1)

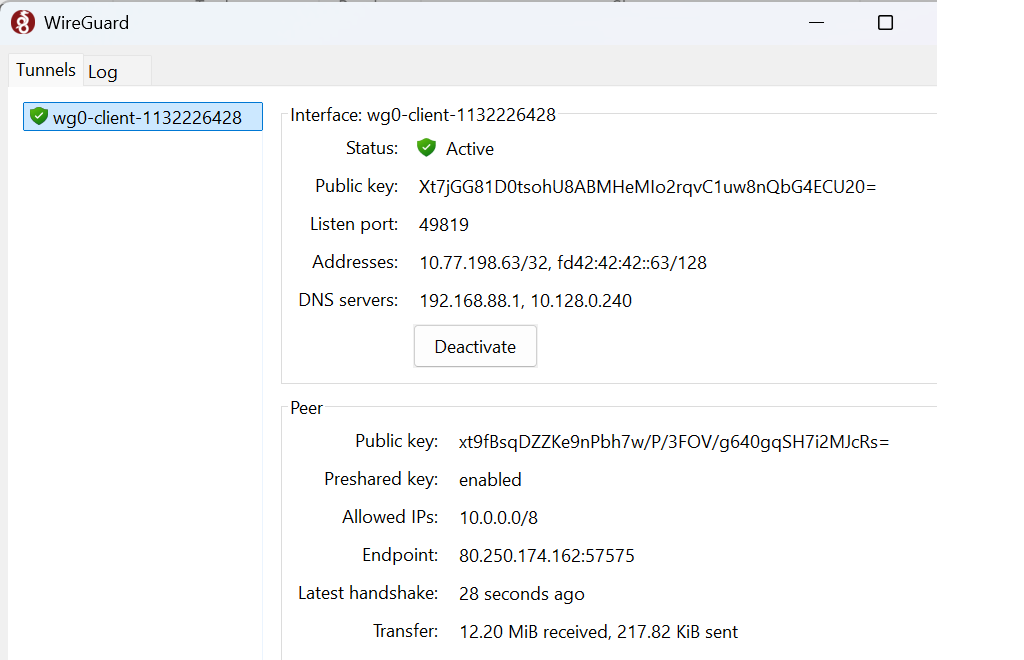


Рис. 1: Установка Chocolatey

На сайте ViPNet IDS NS просмотрели атакованные ip-адреса и суть атак (рис. 2)

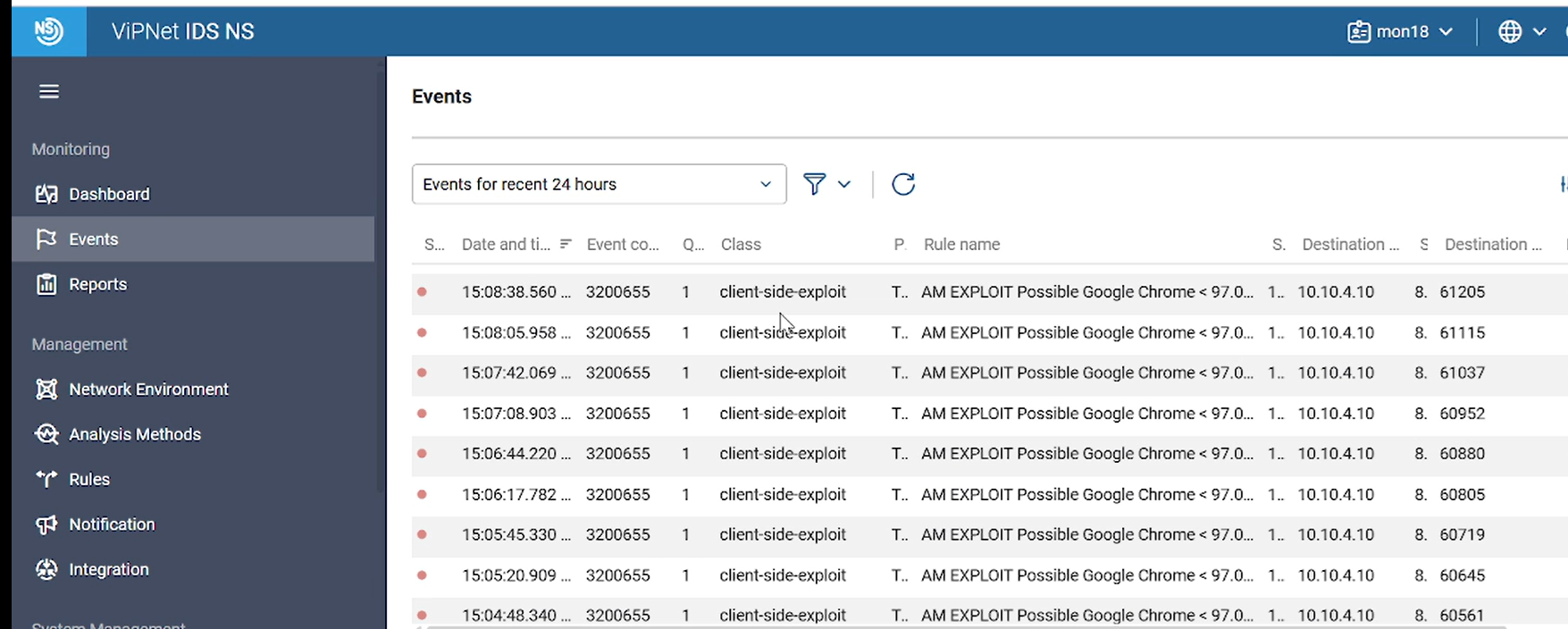


Рис. 2: Атакованные ip-адреса

Добавили карточку инцидента Weak Password (рис. 3)

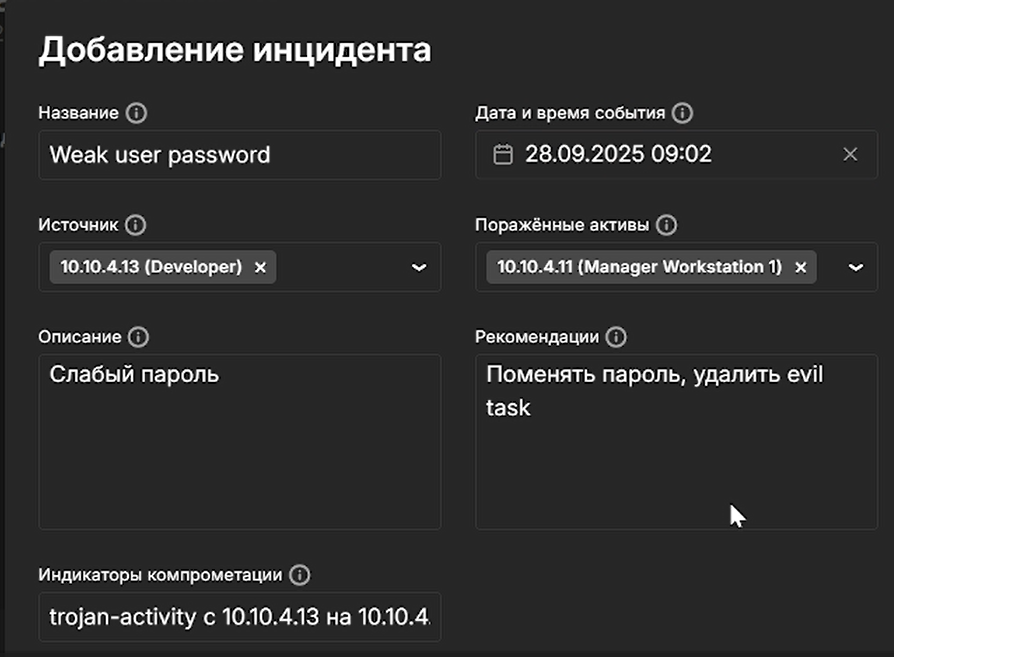


Рис. 3: Карточка инцидента Weak Password

Добавили карточку инцидента XSS (рис. 4)

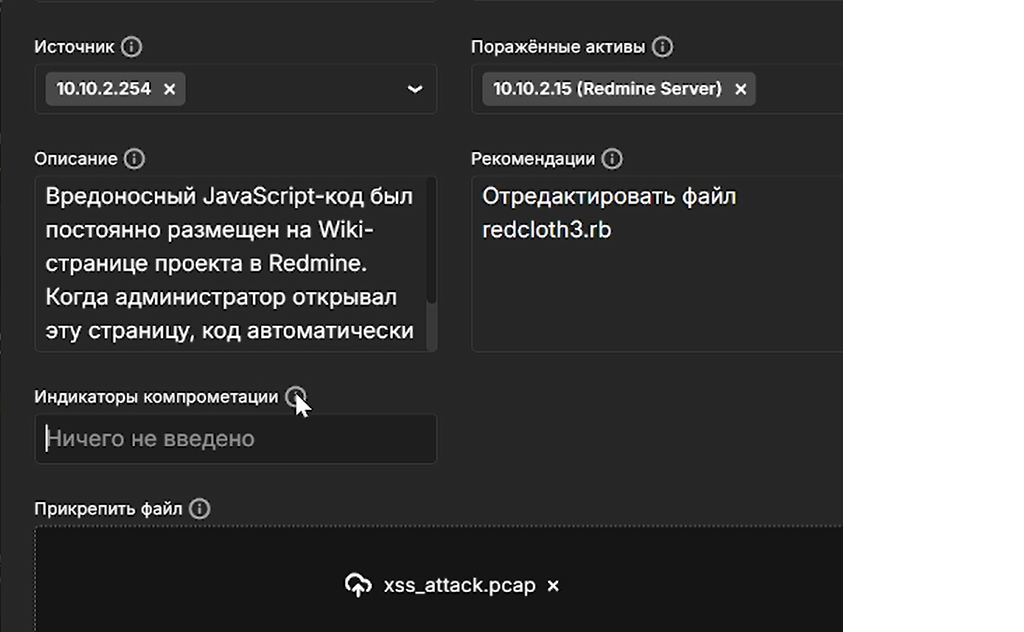


Рис. 4: Карточка инцидента XSS

Добавили карточку инцидента SQL-injection (рис. 5)

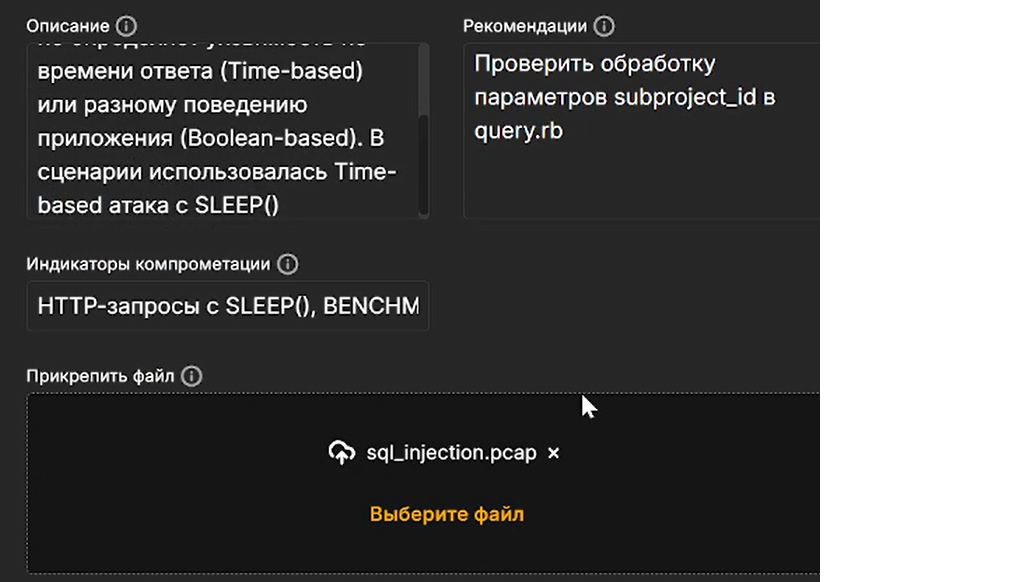


Рис. 5: Карточка инцидента SQL-injection

Атака XSS. Открыли на редактирование файл redcloth3.rb атакованного ip-адреса (рис. 6)

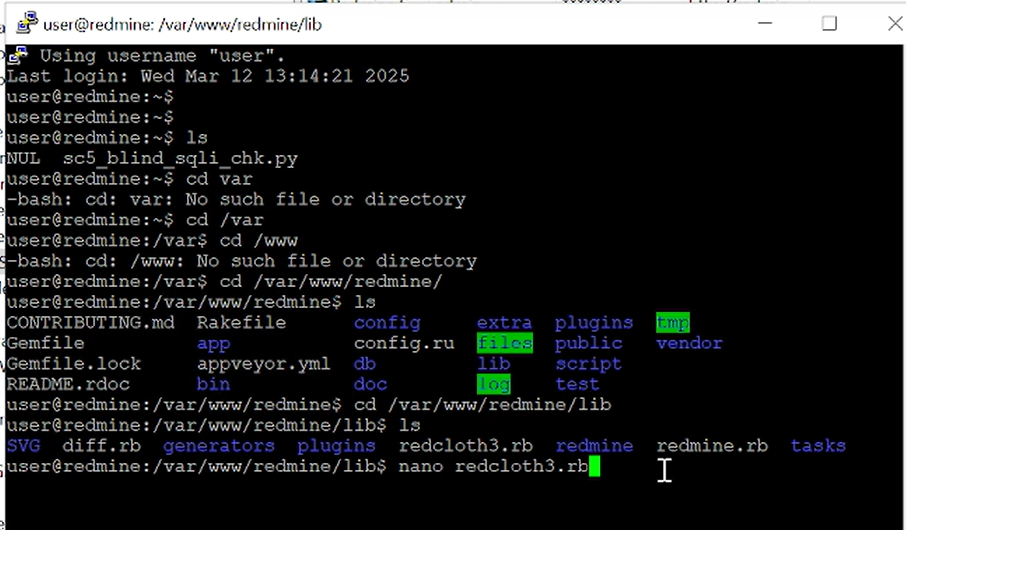


Рис. 6: Файл redcloth3.rb атакованного ip-адреса

Атака XSS. Удалили тег pre из разрешенных тегов, которые не будут экранированы (рис. 7)

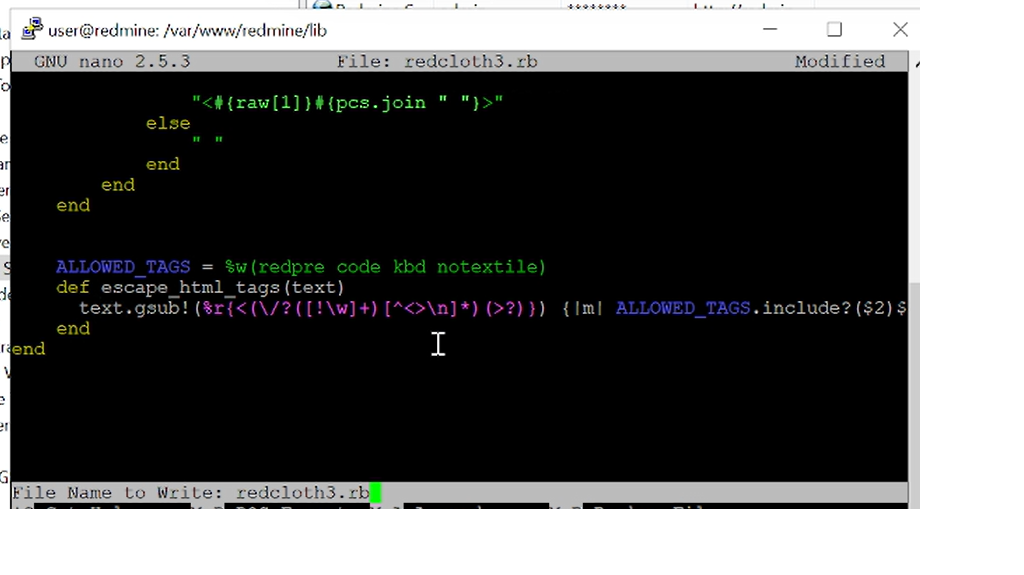


Рис. 7: Удаление тега

Атака XSS. Перезапустили службу веб-сервера: sudo systemctl restart nginx.service (рис. 8)

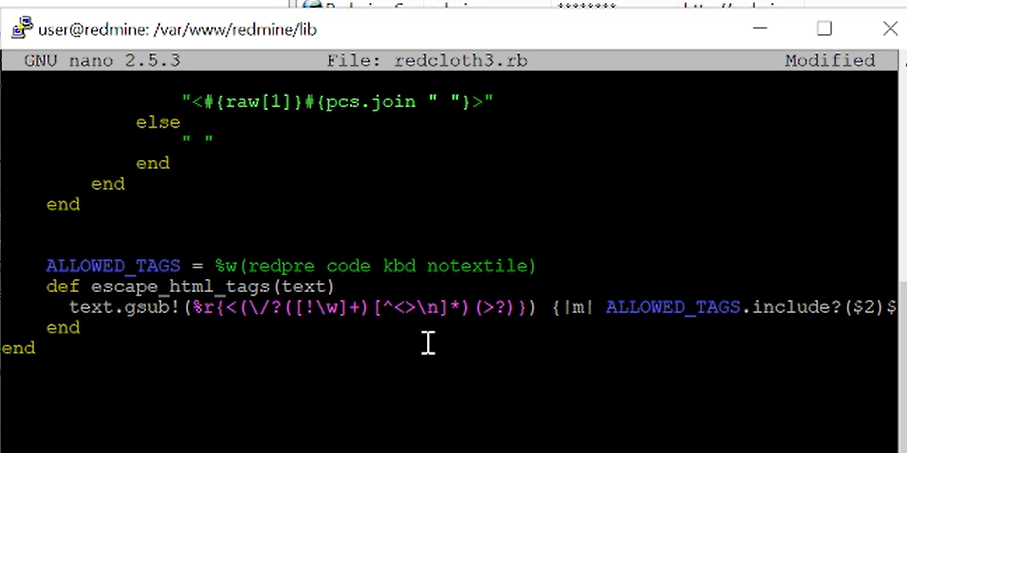


Рис. 8: Перезапуск службы веб-сервера

Последствия XSS. Удалили пользователя hacker (рис. 9)

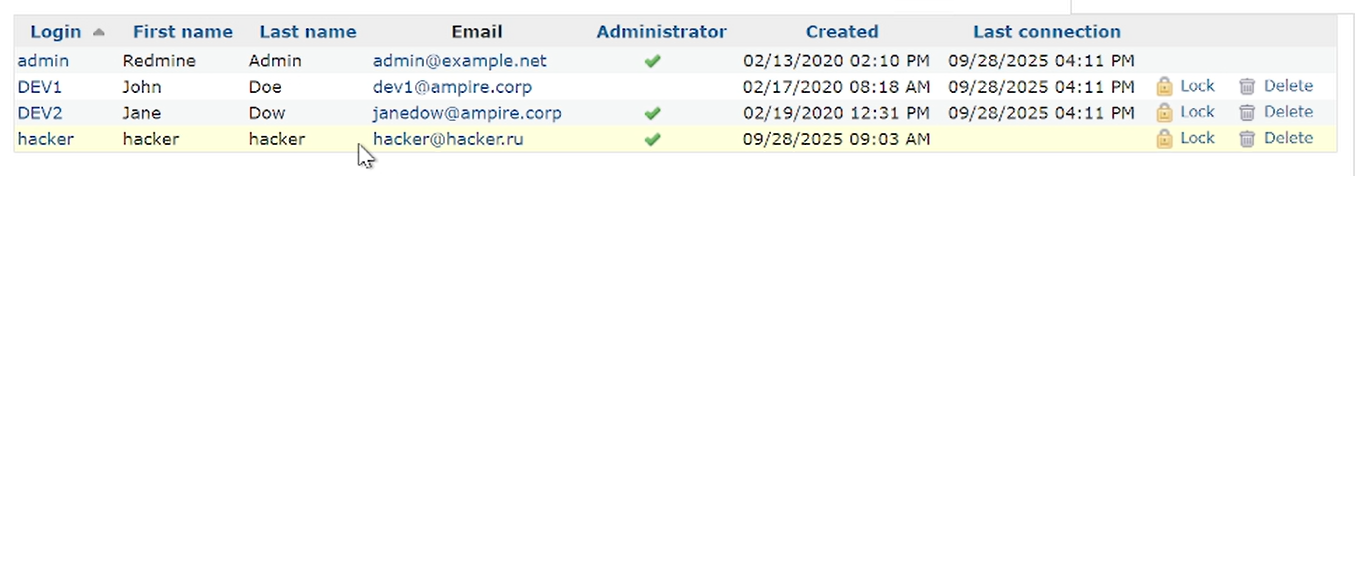


Рис. 9: Удалиление пользователя hacker

Атака SQL-инъекция. Открыли файл query.rb на редактирование на 10.10.2.15 (рис. 10)

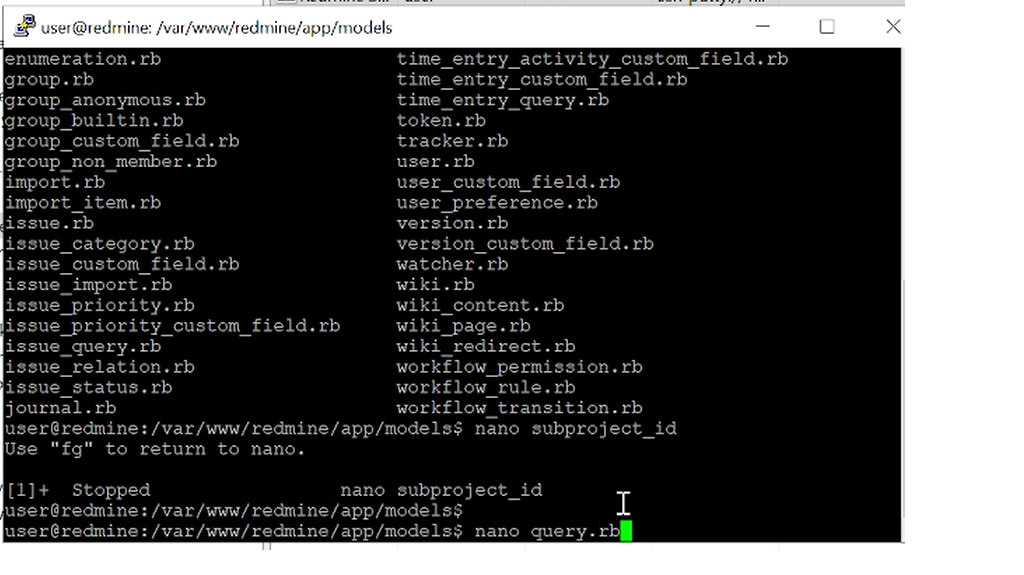


Рис. 10: Файл query.rb

Атака SQL-инъекция. Отредактировали query.rb, заменив each на map (рис. 11)

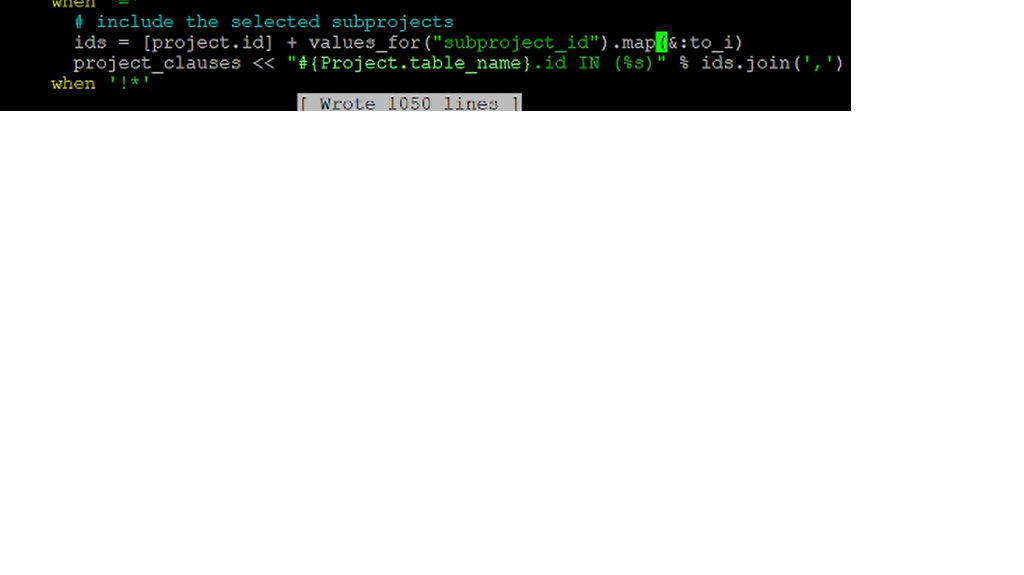


Рис. 11: Редактирование query.rb

Атака SQL-инъекция. Перезапустили nginx (рис. 12)

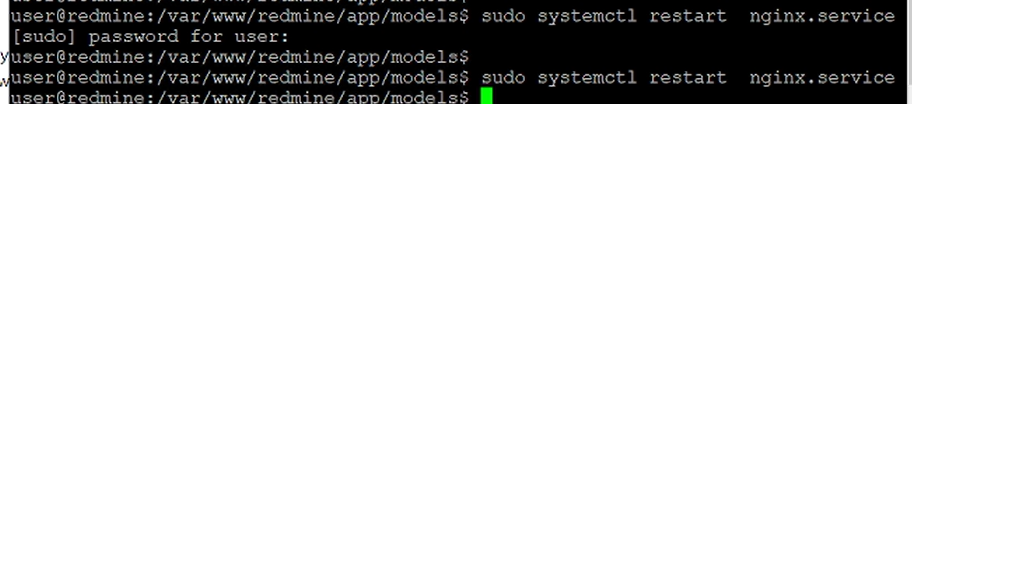


Рис. 12: Перезапуск nginx

Атака Weak Password. Зашли на MS Active Directory (рис. 13)

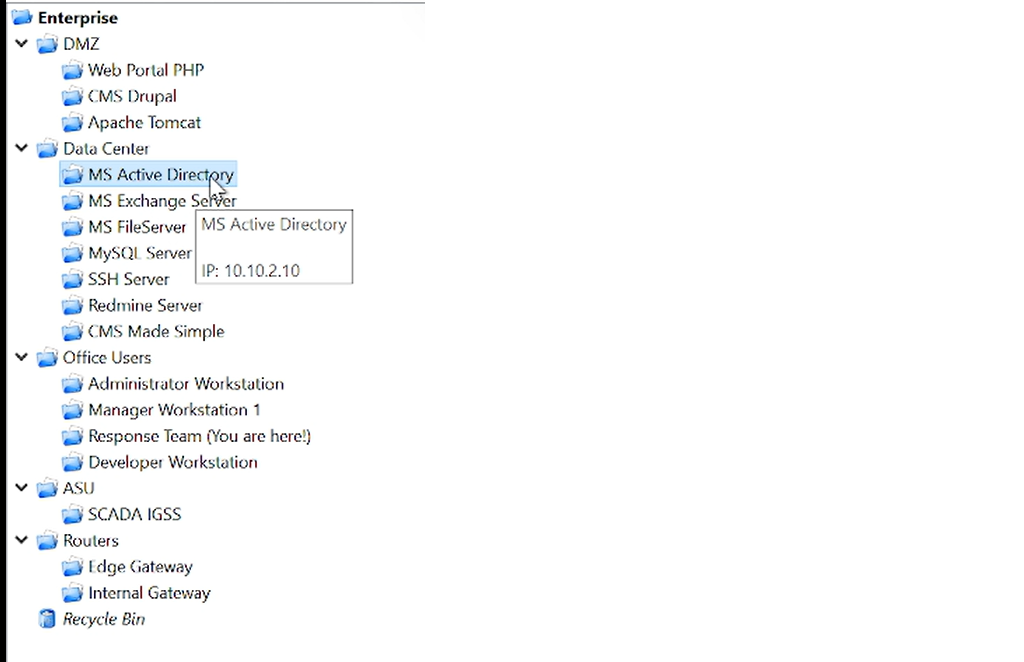


Рис. 13: MS Active Directory

Атака Weak Password. Сбросили пароль на dev1 (рис. 14)

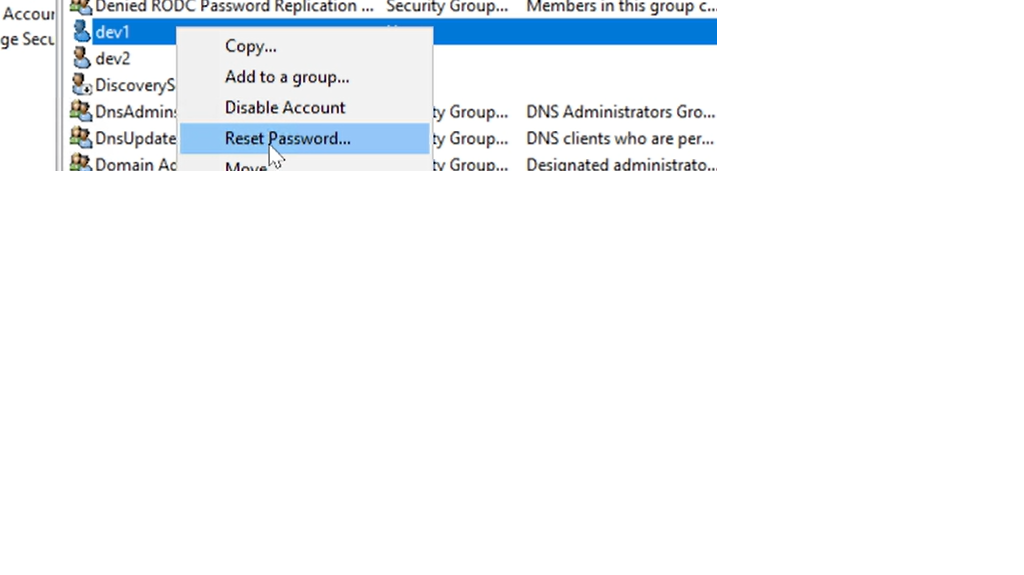


Рис. 14: Сброс пароля

Последствие Weak Password. Удалили Evil Task из планировщика задач (рис. 15)

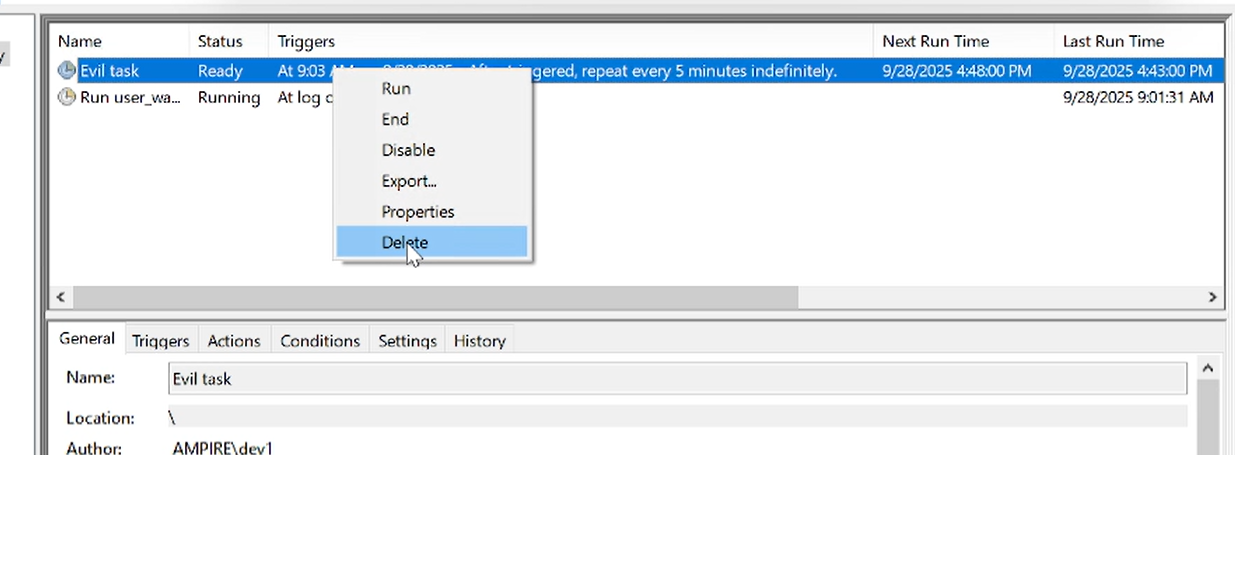


Рис. 15: Удаление Evil Task

Все атаки и их последствия успешно устранены

# 4 Выводы

Отработали на практике методы обнаружения, анализа и нейтрализации многоэтапной компьютерной атаки, направленной на кражу научно-технической информации предприятия, с использованием учебного программного комплекса «Ampire».

# 5 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