Отчёт о расследовании инцидента информационной безопасности

Лабораторная работа: Защита научно-технической информации предприятия

Содержание

Список иллюстраций

Список таблиц

# 1 Введение

## 1.1 Цель работы

Исследовать и задокументировать инцидент информационной безопасности в корпоративной инфраструктуре компании AMPIRE, выявить уязвимости и предложить меры по их устранению.

## 1.2 Описание инфраструктуры

Инфраструктура компании AMPIRE включает:

* Developer Workstation (10.10.4.13) - рабочее место разработчика dev1
* Manager Workstation (10.10.4.11) - рабочее место менеджера
* File Server (10.10.2.12) - файловый сервер
* Redmine Server (10.10.2.15) - сервер управления проектами
* Internal Router (10.10.2.254) - внутренний маршрутизатор

На (рис. 1) представлена схема сети компании.

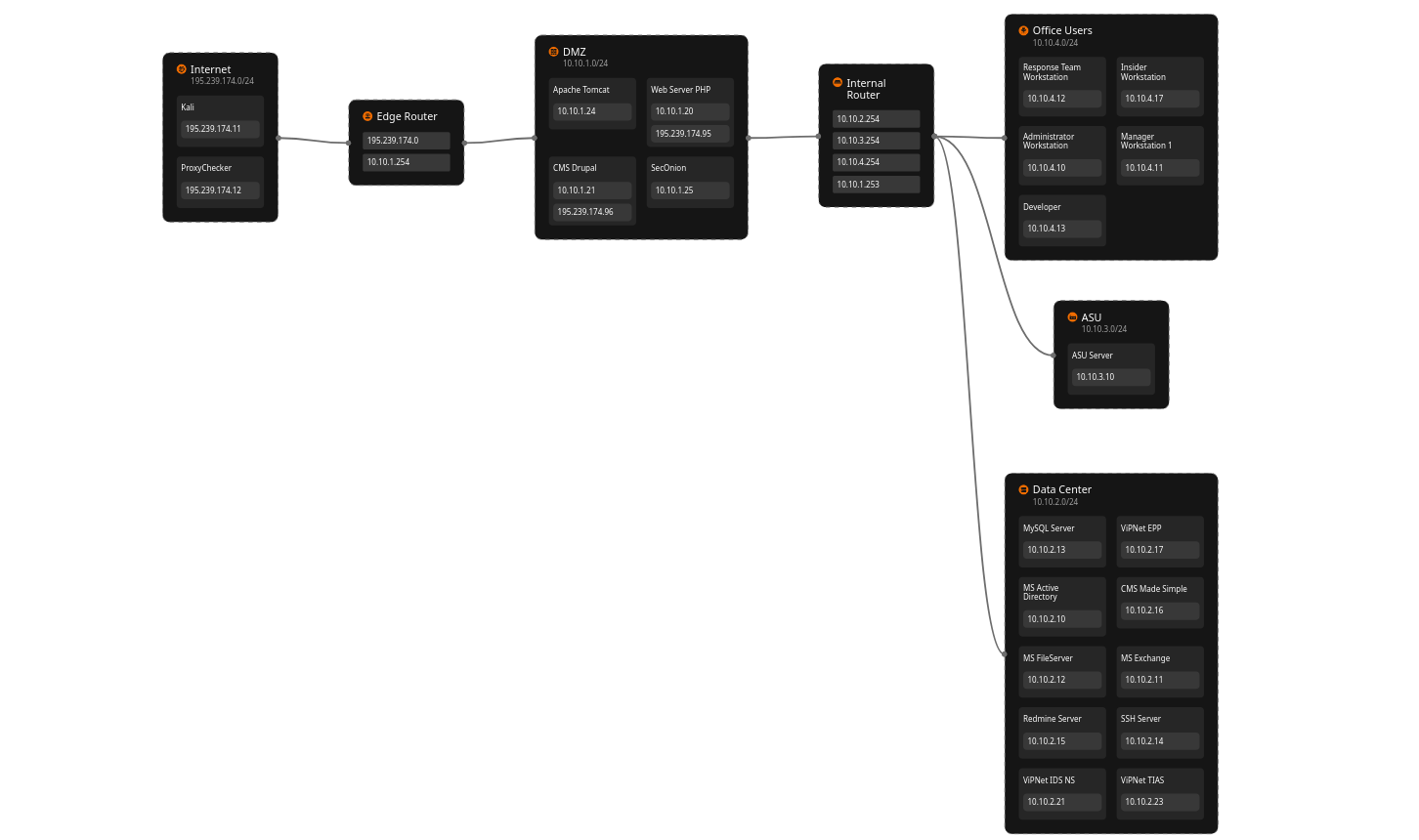


Рис. 1: Схема сети AMPIRE

# 2 Ход расследования

## 2.1 Этап 1: Начальная компрометация

### 2.1.1 Обнаружение подозрительной активности

При анализе событий ViPNet IDS были обнаружены подозрительные попытки подключения с узла 10.10.4.13 (Developer Workstation) к узлу 10.10.4.11 (Manager Workstation) (рис. 2).

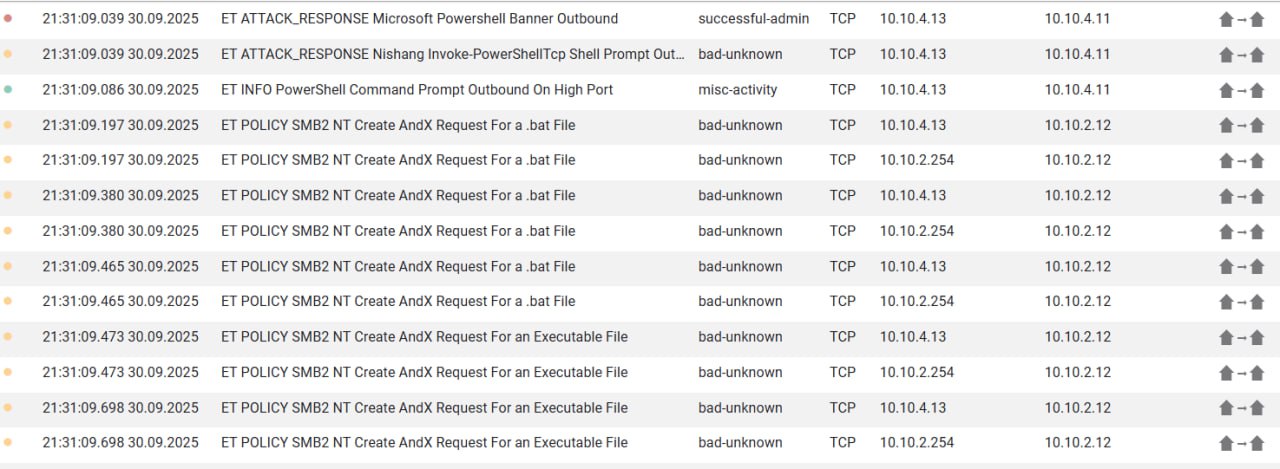


Рис. 2: События в ViPNet IDS - попытки подключения

### 2.1.2 Анализ логов аутентификации

Проверка журналов ViPNet IDS NS показала множественные попытки входа (рис. 3):

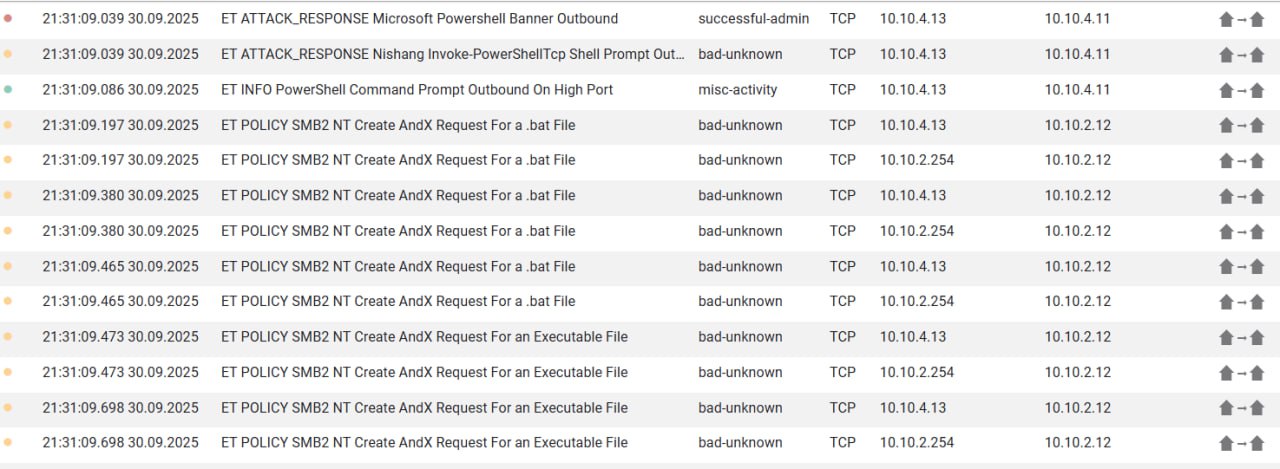


Рис. 3: ViPNet IDS NS

**Обнаружено:** - Множественные неудачные попытки входа - Успешный вход после серии неудачных попыток - Источник: 10.10.4.13 (Developer Workstation) - Цель: 10.10.4.11 (Manager Workstation)

## 2.2 Этап 2: Lateral Movement и установка backdoor

### 2.2.1 Загрузка вредоносных файлов

После успешной компрометации Manager Workstation, с неё были загружены файлы на File Server (рис. 4):



Рис. 4: Загрузка файлов на File Server через SMB

**Загруженные файлы:** - bcdoor.exe (backdoor) - legacy.exe (LaZagne - инструмент для кражи паролей) - Вредоносный .bat файл

### 2.2.2 Создание персистентности

На Developer Workstation была обнаружена задача в планировщике (рис. 5):

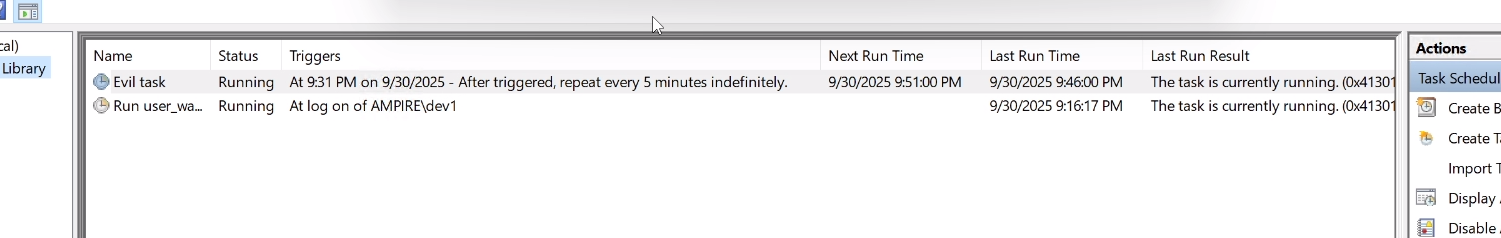


Рис. 5: Планировщик задач - Evil task

**Параметры задачи:** - Название: “Evil task” - Запуск: каждые 5 минут

### 2.2.3 Кража учетных данных

Запуск LaZagne для извлечения сохраненных паролей (рис. 6):

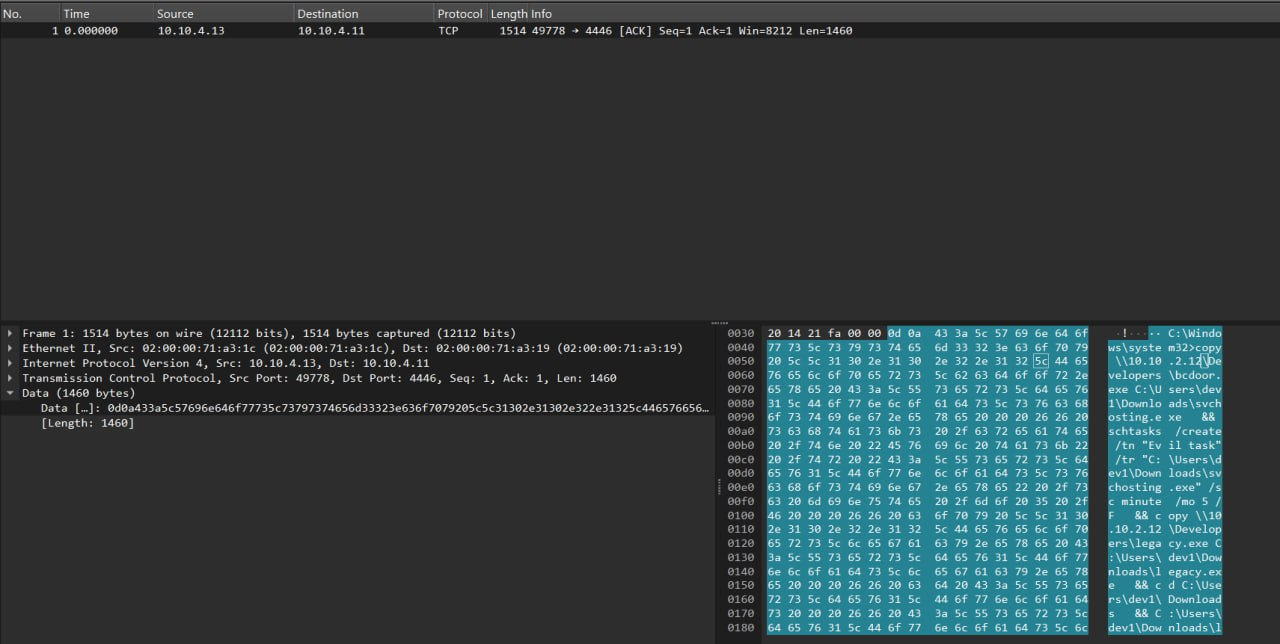


Рис. 6: Вывод LaZagne с паролями

**Извлеченные данные:**

URL: http://redmine.ampire.corp/  
Username: dev1  
Password: qwe123!@#

## 2.3 Этап 3: Атака XSS на Redmine (CVE-2019-17427)

### 2.3.1 Внедрение вредоносного кода

С Manager Workstation была проведена XSS атака на Redmine. На (рис. 7) показана wiki страница с внедренным payload:

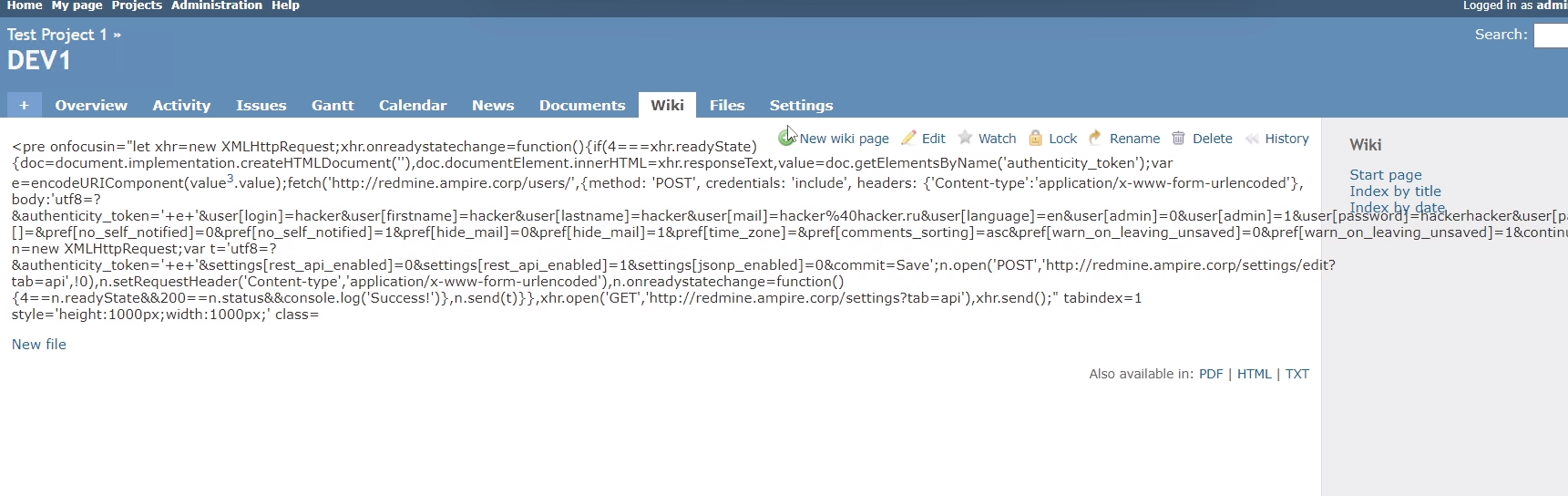


Рис. 7: Wiki страница с XSS payload

Исходный код страницы с вредоносным JavaScript представлен на (рис. 8):

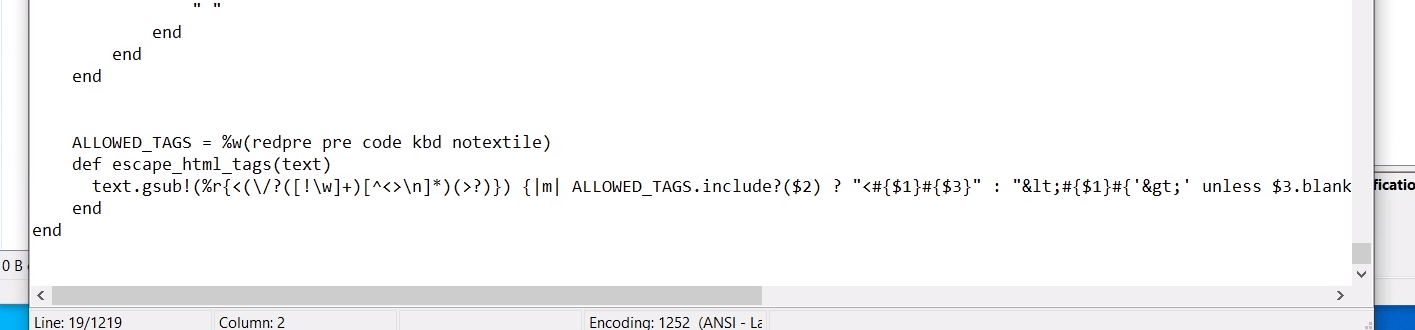


Рис. 8: Исходный код страницы с вредоносным JavaScript

**XSS Payload:**

<pre onfocusin="let xhr=new XMLHttpRequest;  
xhr.onreadystatechange=function(){  
 if(4===xhr.readyState){  
 // Извлечение CSRF токена  
 // Создание admin пользователя "hacker"  
 // Включение REST API  
 }  
},  
xhr.open('GET','http://redmine.ampire.corp/settings?tab=api'),  
xhr.send();" tabindex=1>

### 2.3.2 Результат XSS атаки

После срабатывания XSS при посещении страницы администратором были получены следующие результаты (рис. 9, 10):

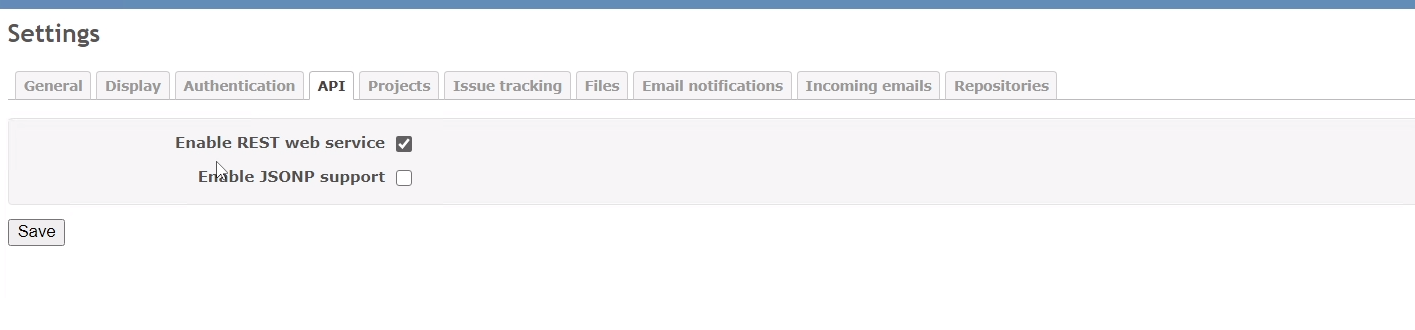


Рис. 9: Включенный REST API в настройках Redmine

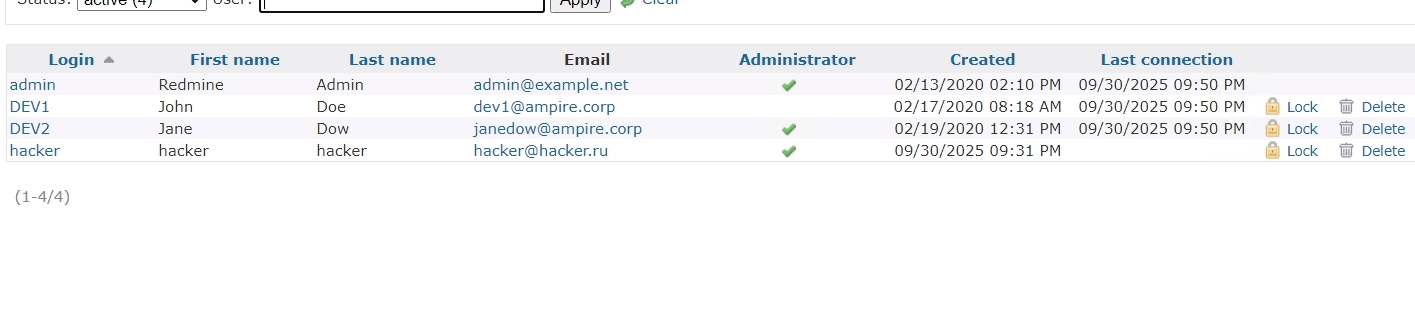


Рис. 10: Созданный пользователь hacker с правами администратора

**Созданный пользователь:** - Login: hacker - Email: hacker@hacker.ru - Права: Administrator - REST API: Enabled

## 2.4 Этап 4: SQL Injection (CVE-2019-18890)

### 2.4.1 Эксплуатация Blind SQL Injection

Используя REST API, была проведена Blind SQL инъекция. HTTP запрос с инъекцией показан на (рис. 11):



Рис. 11: HTTP запрос с SQL injection в параметре subproject\_id

**Техника атаки:**

GET /issues.xml?project\_id=1&subproject\_id=1;SELECT+SLEEP(2)  
  
Посимвольное извлечение данных:  
- Если символ верный → задержка 2 секунды  
- Если символ неверный → быстрый ответ

# 3 Анализ с помощью средств мониторинга

## 3.1 ViPNet IDS NS

### 3.1.1 Обнаруженные события

Общий список событий в ViPNet IDS представлен на (рис. 12):

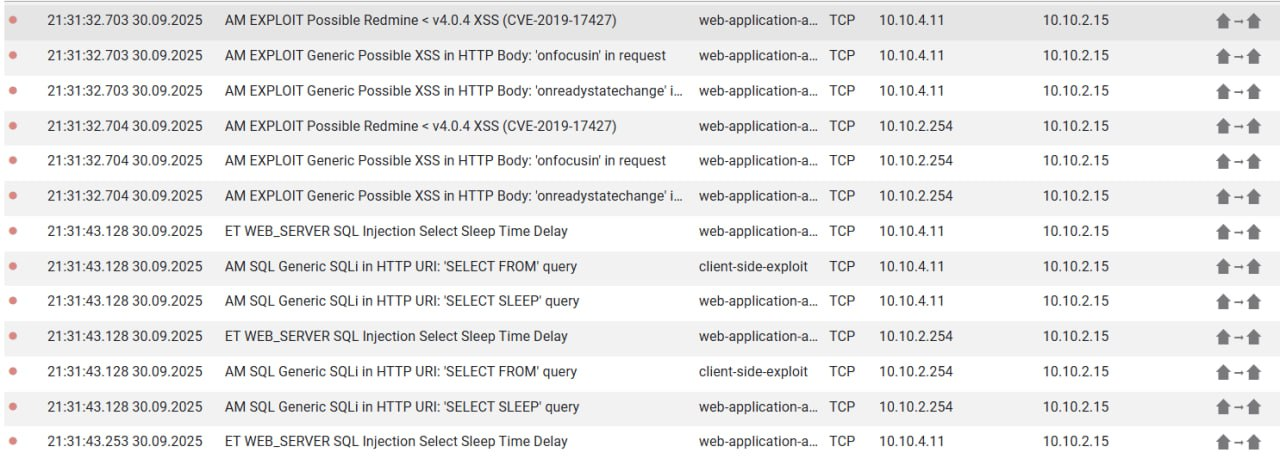


Рис. 12: Общий список событий в ViPNet IDS

**Критические события:** - ET ATTACK\_RESPONSE LaZagne Artifact Outbound - AM EXPLOIT Possible Redmine < v4.0.4 XSS (CVE-2019-17427) - ET WEB\_SERVER SQL Injection Select Sleep Time Delay

# 4 Устранение уязвимостей

## 4.1 Уязвимость 1: Слабый пароль

### 4.1.1 Изменение пароля в Active Directory

Процесс сброса пароля пользователя в Active Directory показан на (рис. 13):

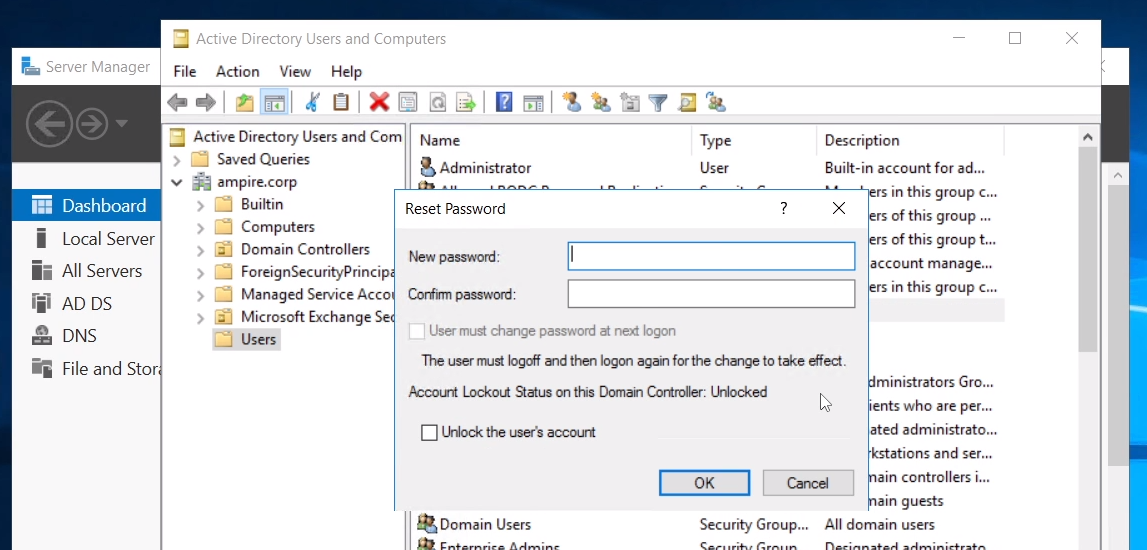


Рис. 13: Active Directory - сброс пароля пользователя

## 4.2 Уязвимость 2: XSS (CVE-2019-17427)

### 4.2.1 Исправление в коде Redmine

Файл redcloth3.rb до исправления показан на (рис. 14):

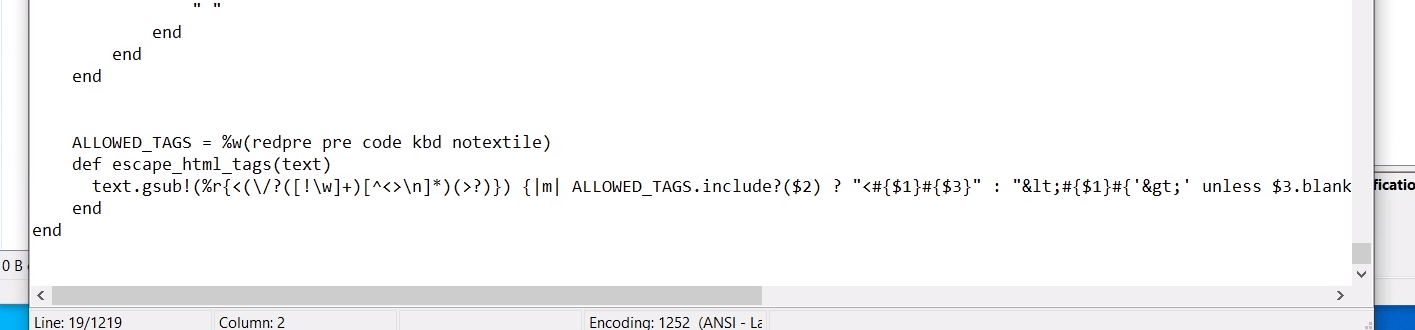


Рис. 14: Файл redcloth3.rb до исправления

Процесс внесения изменений в redcloth3.rb представлен на (рис. 15):

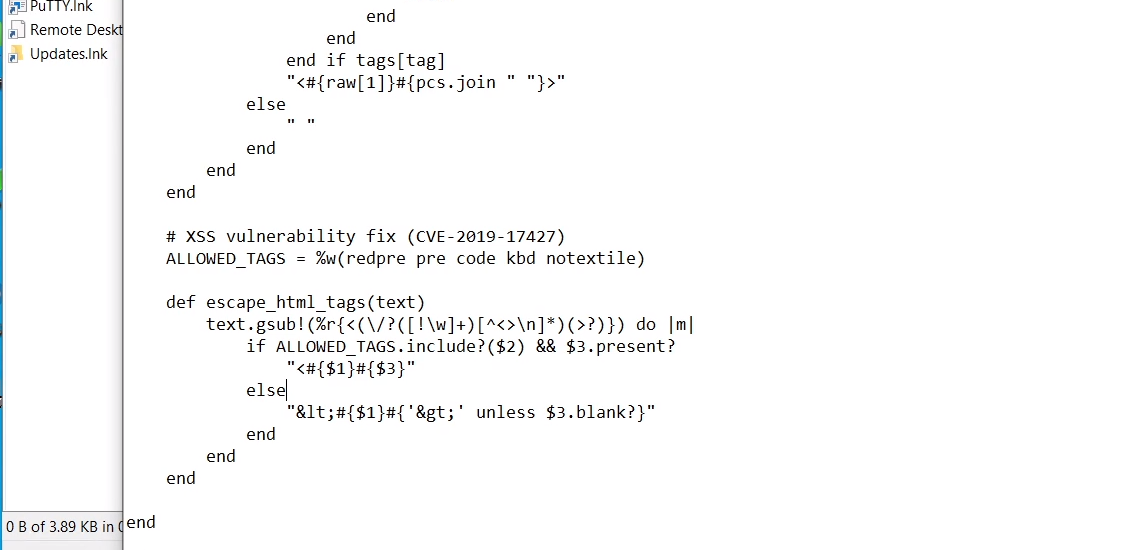


Рис. 15: Внесение изменений в redcloth3.rb

**Код исправления:**

ALLOWED\_TAGS = %w(redpre pre code kbd notextile)  
def escape\_html\_tags(text)  
 text.gsub!(%r{<(\/?([!\w]+)[^<>\n]\*)(>?)}) do |m|  
 if ALLOWED\_TAGS.include?($2) && $3.present?  
 "<#{$1}#{$3}"  
 else  
 "&lt;#{$1}#{'&gt;' unless $3.blank?}"  
 end  
 end  
end

### 4.2.2 Перезапуск сервера

* После внесения изменений необходимо было перезапустить службу веб сервера (рис. 16):

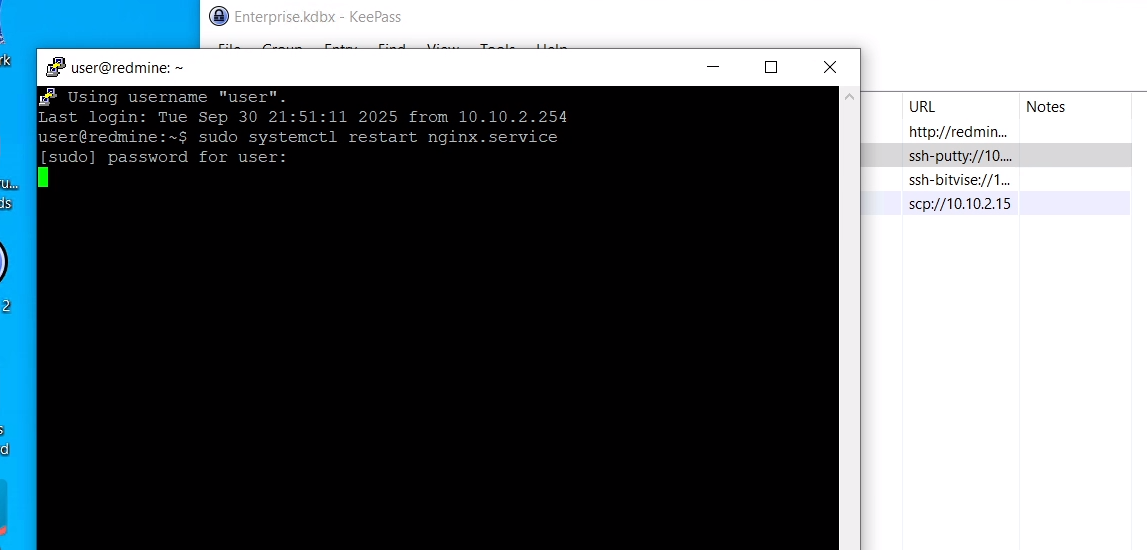


Рис. 16: Перезапуск сервера

## 4.3 Уязвимость 3: SQL Injection (CVE-2019-18890)

### 4.3.1 Исправление в query.rb

Файл query.rb с уязвимым кодом представлен на (рис. 17):

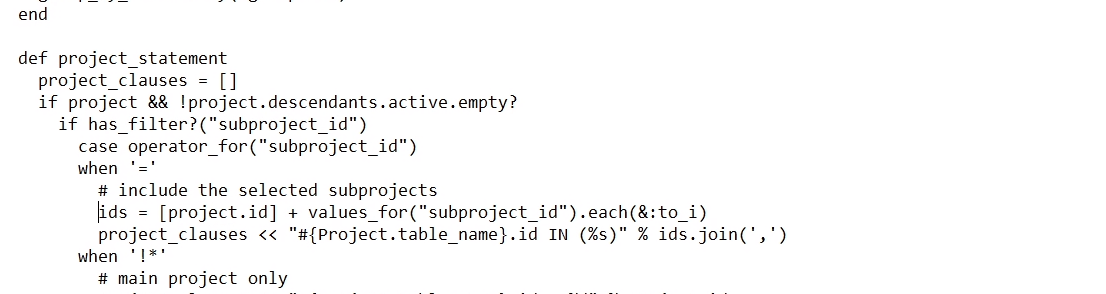


Рис. 17: Файл query.rb с уязвимым кодом

Исправленный код показан на (рис. 18):

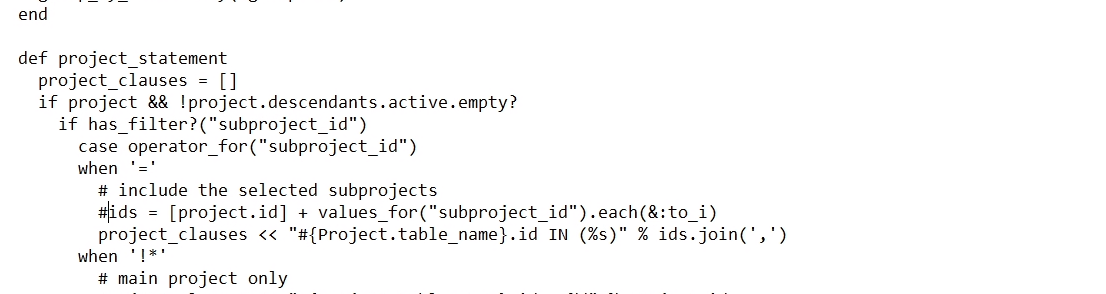


Рис. 18: Исправленный код

sudo nano /var/www/redmine/app/models/query.rb

* Нашли строку:

ids = [project.id] + values\_for(column.name).map(&:to\_i)

* Закомментировали ее:

# ids = [project.id] + values\_for(column.name).map(&:to\_i)

## 4.4 Удаление последствий

### 4.4.1 Удаление backdoor

Процесс удаления задачи из планировщика показан на (рис. 19):

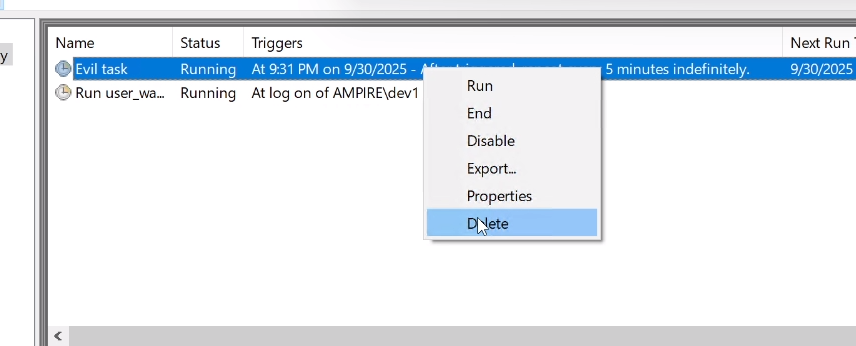


Рис. 19: Удаление задачи из планировщика

schtasks /delete /tn "Evil task" /F  
del C:\Users\dev1\Downloads\svchosting.exe /F  
del C:\Users\dev1\Downloads\legacy.exe /F

### 4.4.2 Удаление пользователя hacker

Удаление пользователя hacker из Redmine показано на (рис. 20):

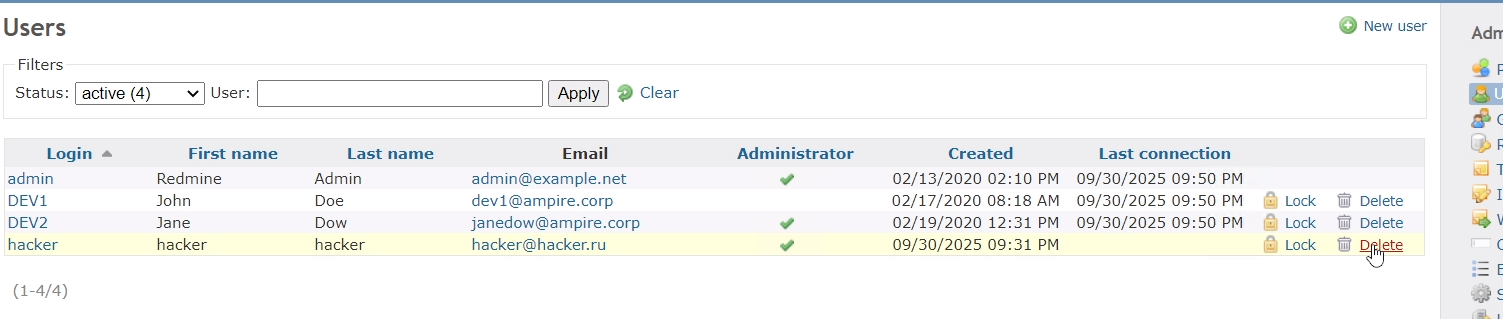


Рис. 20: Удаление пользователя hacker из Redmine

### 4.4.3 Отключение REST API

Процесс отключения REST API в настройках представлен на (рис. 21):

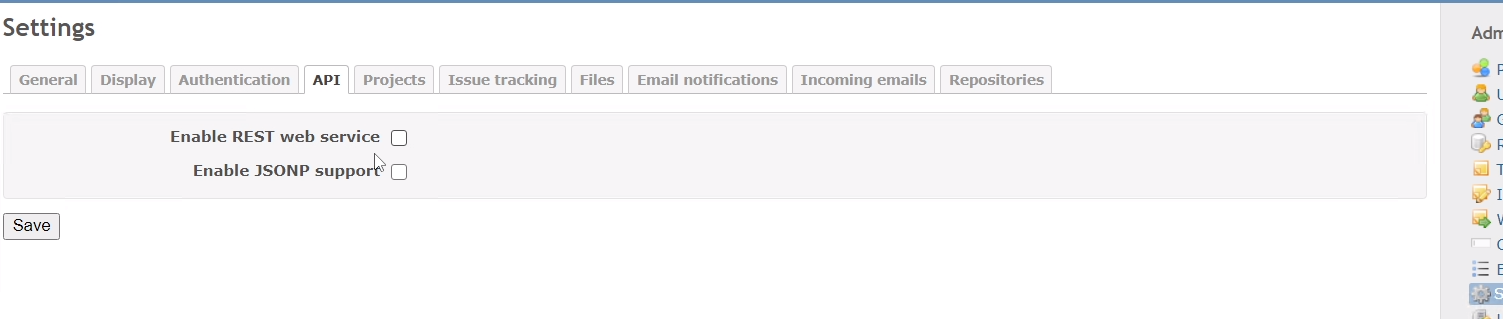


Рис. 21: Отключение REST API в настройках

# 5 Рекомендации

## 5.1 Немедленные меры

1. **Изоляция скомпрометированных узлов:**
   * 10.10.4.13 (Developer Workstation)
   * 10.10.4.11 (Manager Workstation)
   * 10.10.2.254 (Internal Router - требует проверки)
2. **Сброс всех паролей:**
   * Учетные записи Active Directory
   * Пароли приложений (Redmine, email, VPN)
   * Сервисные учетные записи
3. **Форензика:**
   * Создание образов дисков
   * Сбор логов для расследования
   * Анализ сетевого трафика

## 5.2 Долгосрочные меры

### 5.2.1 Организационные меры

1. **Усиление процедур найма:**
   * Тщательная проверка кандидатов
   * Background check
   * Проверка рекомендаций
2. **Security Awareness Training:**
   * Обучение персонала
   * Регулярные тренинги
   * Симуляции атак
3. **Incident Response Plan:**
   * Документированные процедуры
   * Назначенные роли
   * Регулярные учения

# 6 Заключение

В ходе лабораторной работы был успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE (рис. 22).

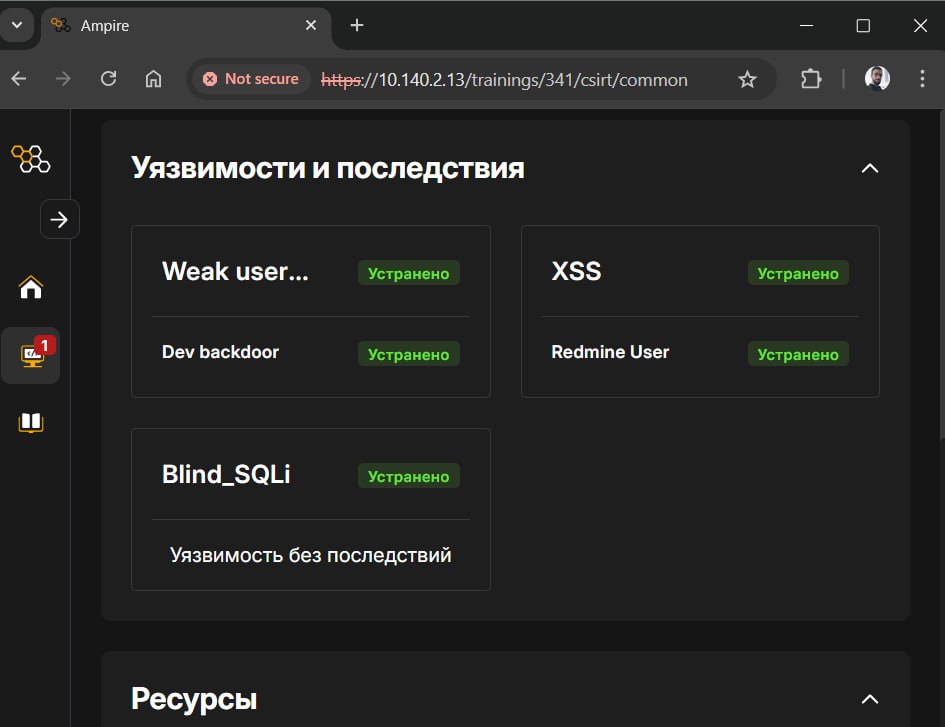


Рис. 22: успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE

Атака представляла собой сложную многоэтапную операцию, включающую:

1. **Insider threat** - инсайдер dev1 с рабочей станции 10.10.4.13
2. **Lateral movement** - компрометация Manager Workstation для использования как pivot point
3. **Dead drop механизм** - использование File Server для обмена данными

Все выявленные уязвимости были успешно устранены, вредоносное ПО удалено, несанкционированные учетные записи заблокированы. Предложенные рекомендации позволят предотвратить подобные инциденты в будущем.

## 6.1 Выводы

1. Критически важно внедрение многоуровневой защиты.
2. Необходим постоянный мониторинг insider threats
3. Своевременное обновление ПО предотвращает эксплуатацию известных уязвимостей
4. Корреляция событий из разных источников позволяет выявлять сложные атаки
5. Human factor остается слабым звеном в системе безопасности

# 7 Список использованных инструментов

* ViPNet IDS NS - обнаружение вторжений
* ViPNet TIAS - корреляция событий
* Security Onion (Kibana, Squert) - анализ сетевого трафика
* Wireshark - анализ пакетов
* Active Directory - управление учетными записями
* Планировщик задач Windows - поиск персистентности