Лабораторная работа 2-А (09\_10)

Кибербезопасность предприятия

Ищенко Ирина

Мишина Анастасия

Дикач Анна

Галацан Николай

Амуничников Антон

Барсегян Вардан

Дудырев Глеб

Дымченко Дмитрий

Содержание

Список иллюстраций

Список таблиц

# 1 Цель тренировки

Разобраться с сценарием действий нарушителя “Защита контроллера домена предприятия”. Выявить и устранить уязвимости и их последствия.

# 2 Выявленные уязвимости и последствия

По ходу выполнения тренировки были выявлены следующие уязвимости:

**Уязвимость 1.** SQL-инъекция

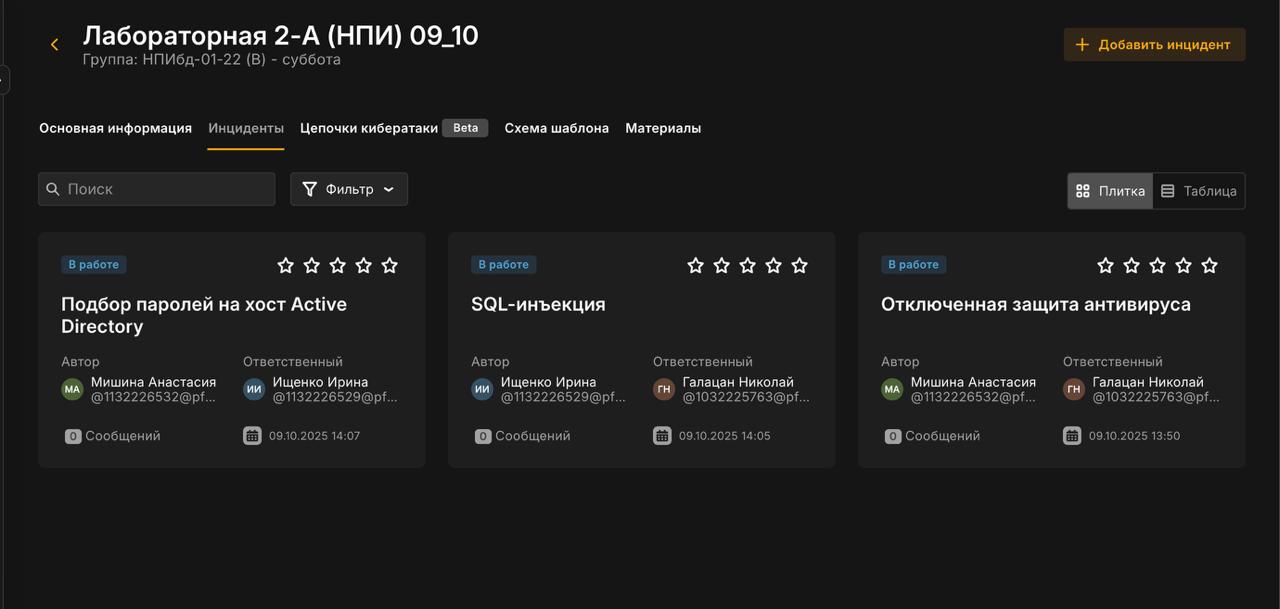
**Последствие.** Web portal meterpreter

**Уязвимость 2.** Отключённая защита антивируса

**Последствие.** Admin meterpreter

**Уязвимость 3.** Слабый пароль учётной записи

**Последствие.** Добавление привилегированного пользователя

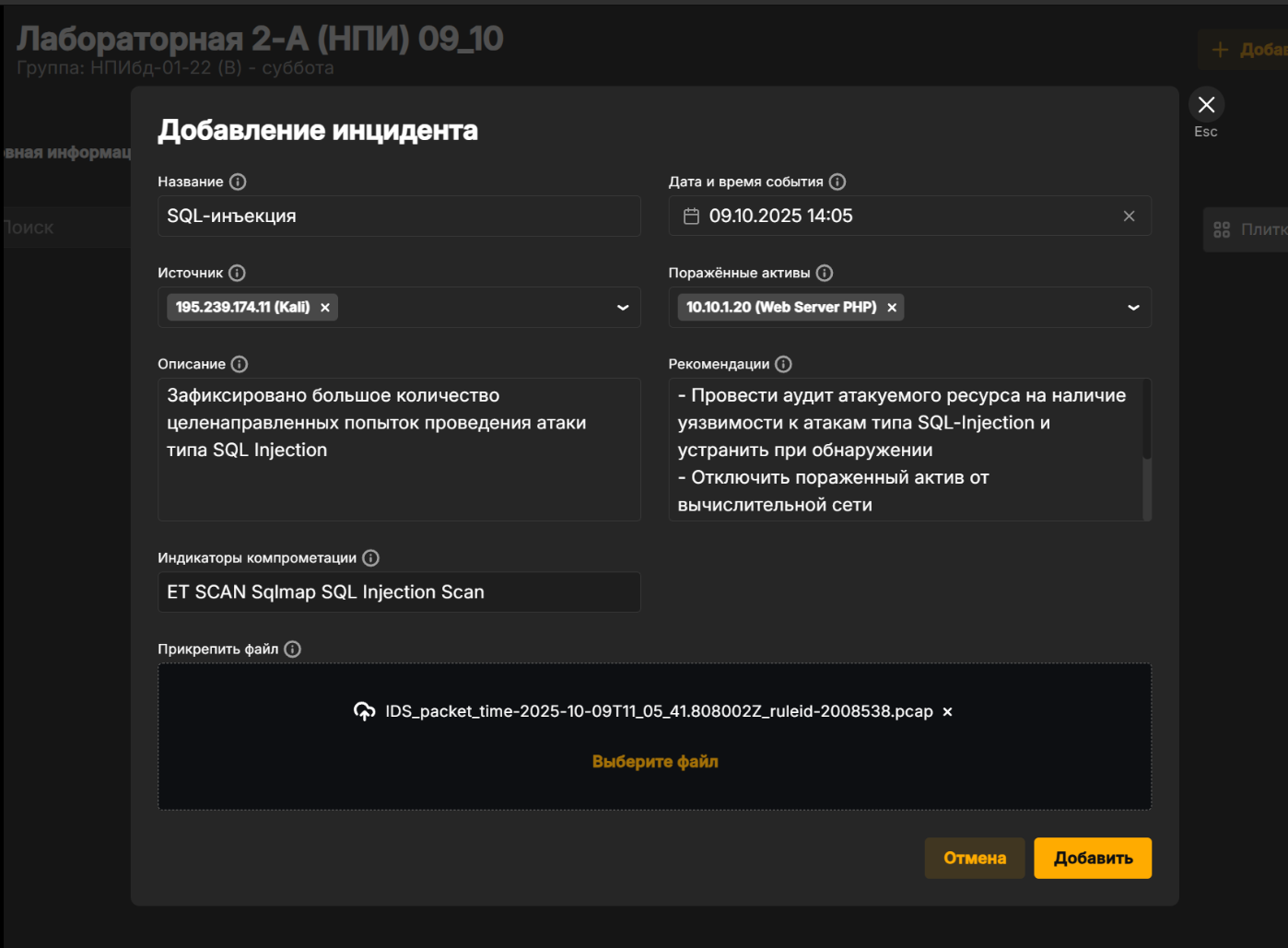


Выявленные уязвимости

## 2.1 SQL-инъекция

На узле Web Server PHP находится уязвимый веб-сервис на порту 80. Нарушитель использует уязвимый параметр id в GET-запросе для загрузки и выполнения php reverse shell.

### 2.1.1 Описание инцидента



Описание инцидента

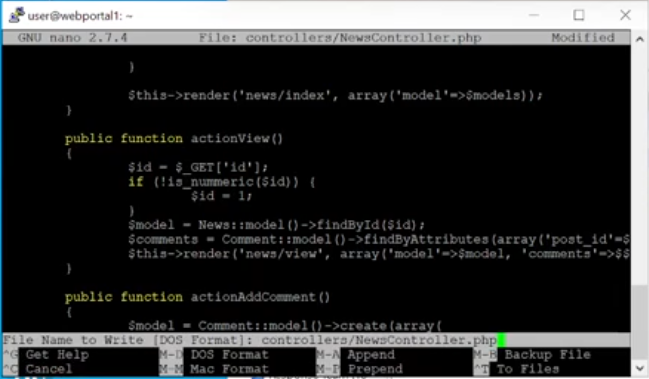
### 2.1.2 Решение

Находим место кода, где $id считывается из GET запроса

Считываем параметр сайта в функции actionView() в файле NewsController.php

Используем функцию is\_numeric для проверки типа $id. Она возвращает True в случае, если $id - число, иначе - False. В случае успешной проверки параметр будет передаваться в запрос, иначе - запрос будет статичным и независимым от $id.

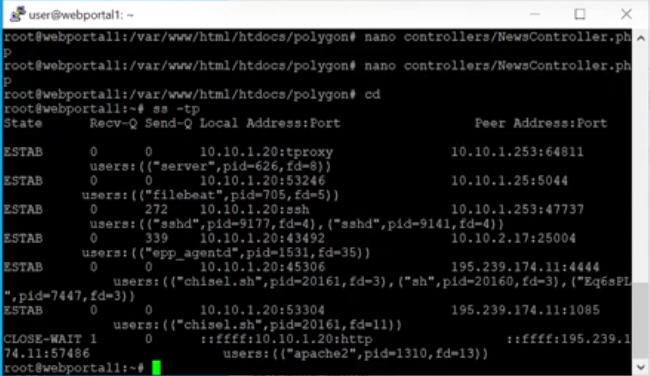
После внесения изменений в файл конфигурации и проверки значения параметра $id уязвимость SQL-инъекции успешно устранена.



Устранение уязвимости

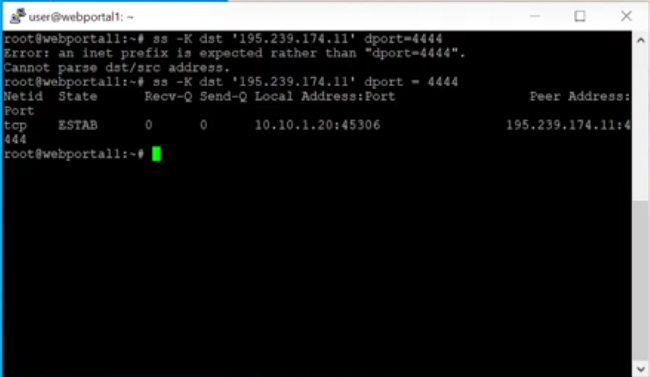
### 2.1.3 Последствие Web portal meterpreter

Нарушитель устанавливает shell сессию с веб-порталом PHP. Для обнаружения последствия проверяем сокеты уязвимой машины при помощи утилиты ss с ключами -tp.



Проверка сокетов

Обнаруживаем то что етсь активное соединение веб-портала с IP-адресом нарушителя. Для устранения пользуемся командой ss с правами привилегированного пользователя, используя ключ -K и соответствующий адрес, порт для завершения сессии с нарушителем: sudo ss -K dst **HACKER\_IP** dport=**HACKER\_PORT**. В результате выполнения команды сессия с нарушителем завершена.

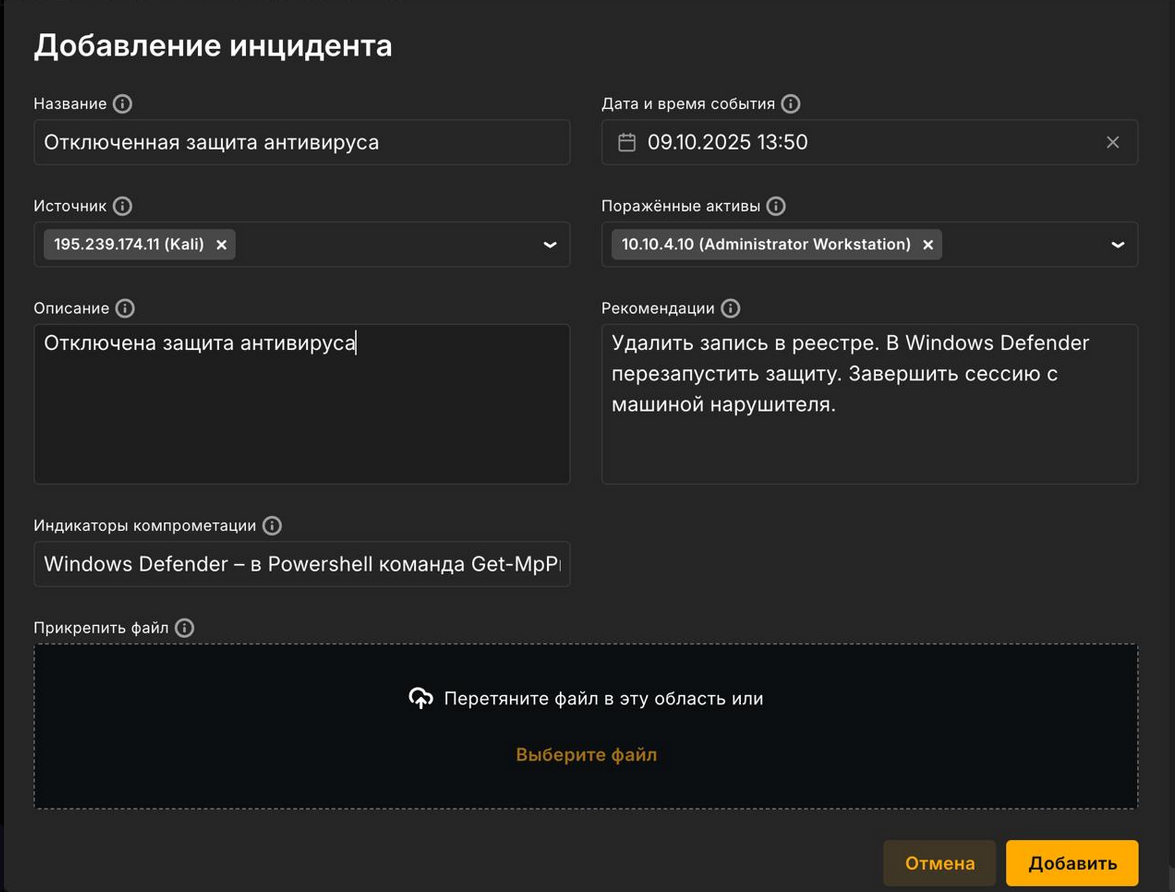


Завершение сессии с нарушителем

## 2.2 Отключённая защита антивируса

На рабочей станции администратора отключена защита в реальном времени Windows Defender (параметр DisableAntiSpyware в реестре), что позволяет запустить вредоносный скрипт.

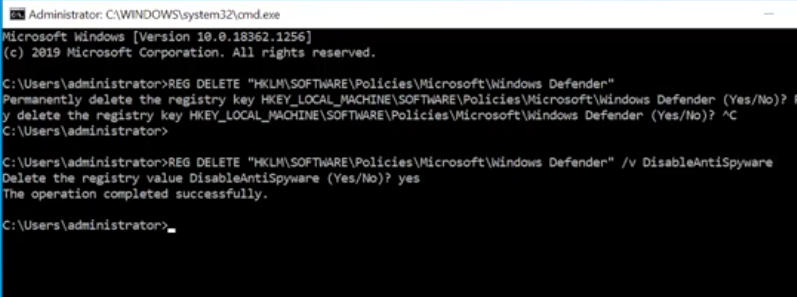
### 2.2.1 Описание инцидента



Описание инцидента

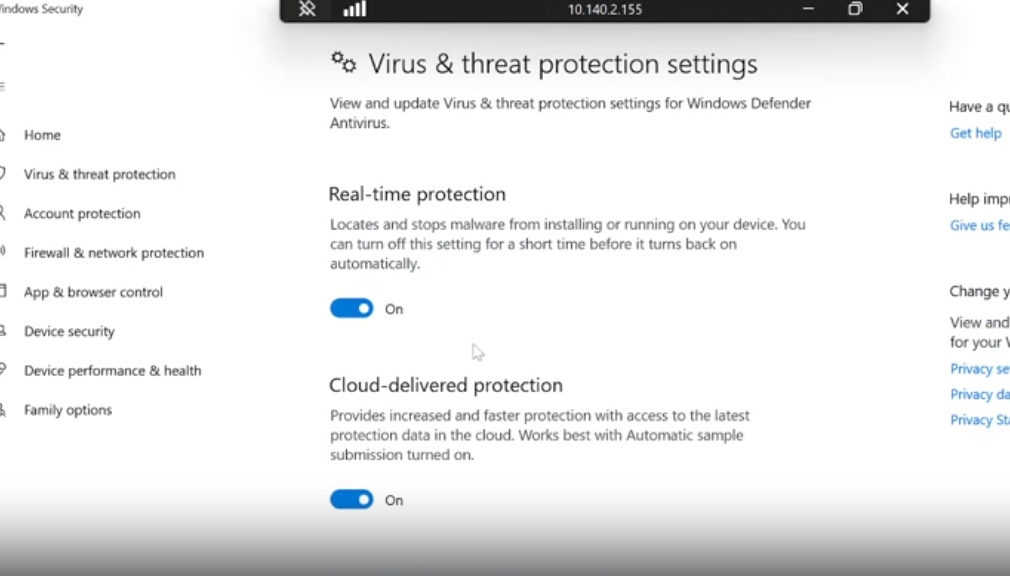
### 2.2.2 Решение

На узле Administrator Workstation вручную удаляем запись в реестре или через консоль с помощью команды.



Удаление записи в реестре

Подтверждаем действие, далее в Windows Defender перезапускаем Virus & Threat Protection и включаем Real-time Protecton.



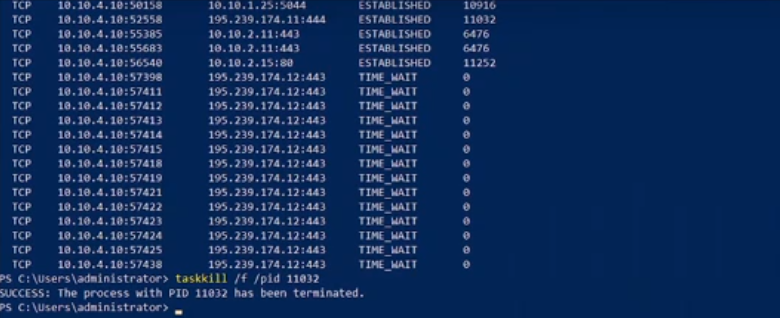
Virus & Threat Protection и Real-time Protecton

После Удаления записи реестра и включения защиты антивирусной программы перезапускаем Windows.

### 2.2.3 Последствия Admin meterpreter

Установленную сессию с нарушителем находим при помощи утилиты netstat с ключами -ano

Для устранения завершаем сессию с машиной нарушителя.

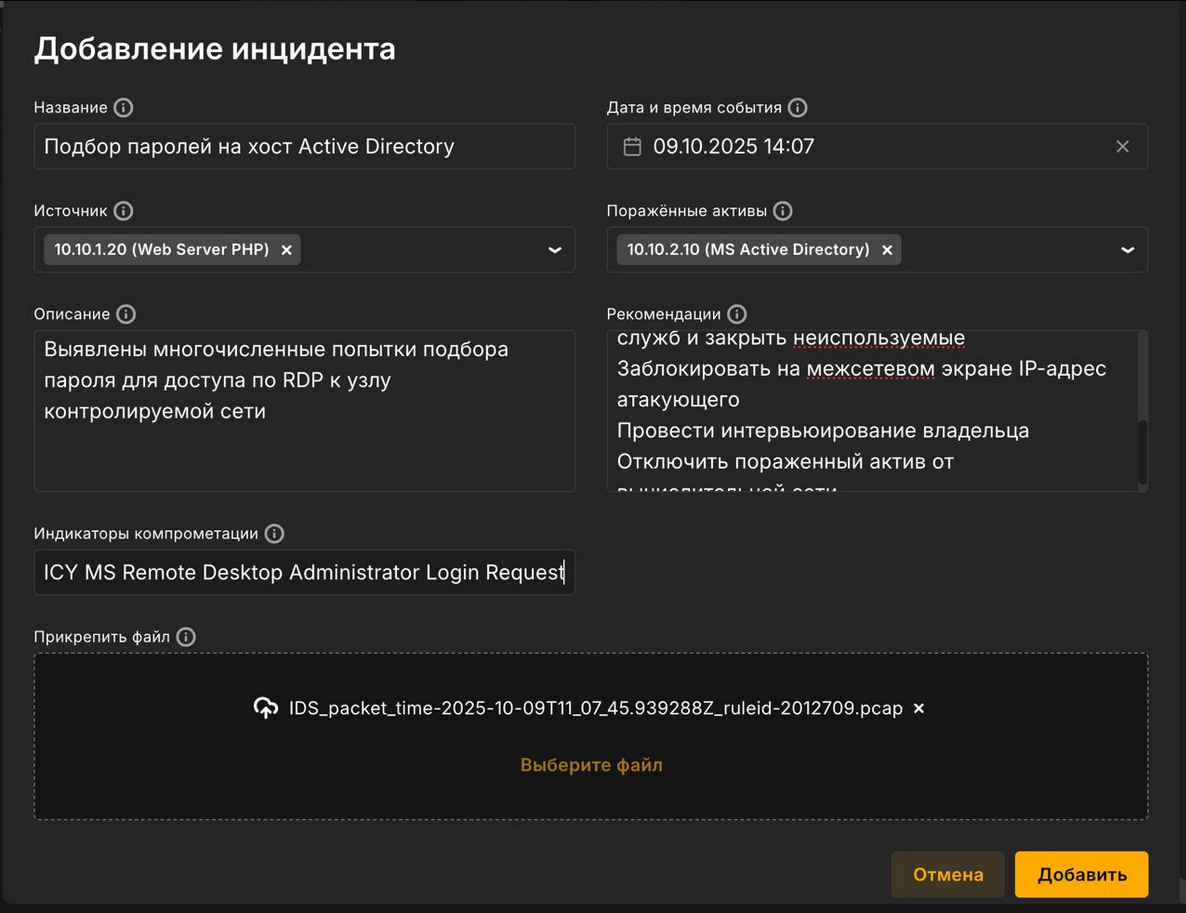


Завершаем сессию с машиной нарушителя

## 2.3 Слабый пароль учётной записи

На узле MS Active Directory установлен слабый пароль учетной записи администратора, что позволяет нарушителю успешно подобрать его брутфорс-атакой (RDP Bruteforce). В журнале безопасности Windows событие с ID 1149 указывает на успешную аутентификацию.

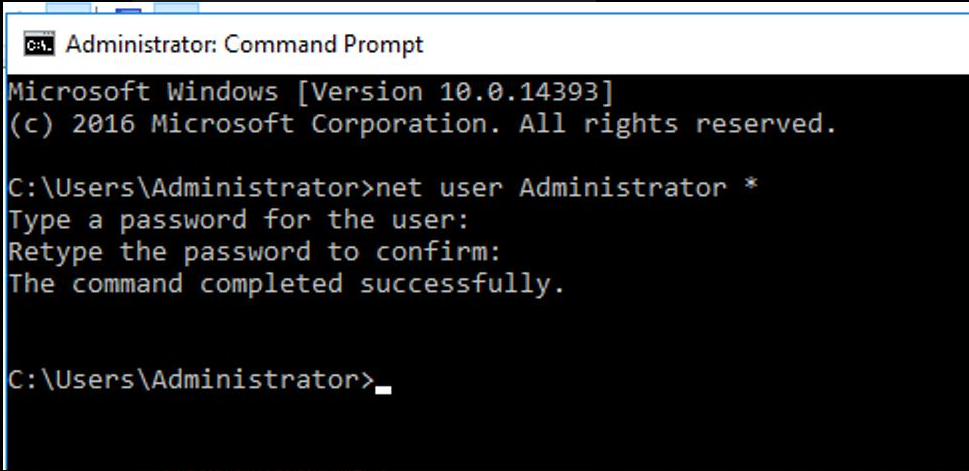
### 2.3.1 Описание инцидента



Описание инцидента

### 2.3.2 Решение

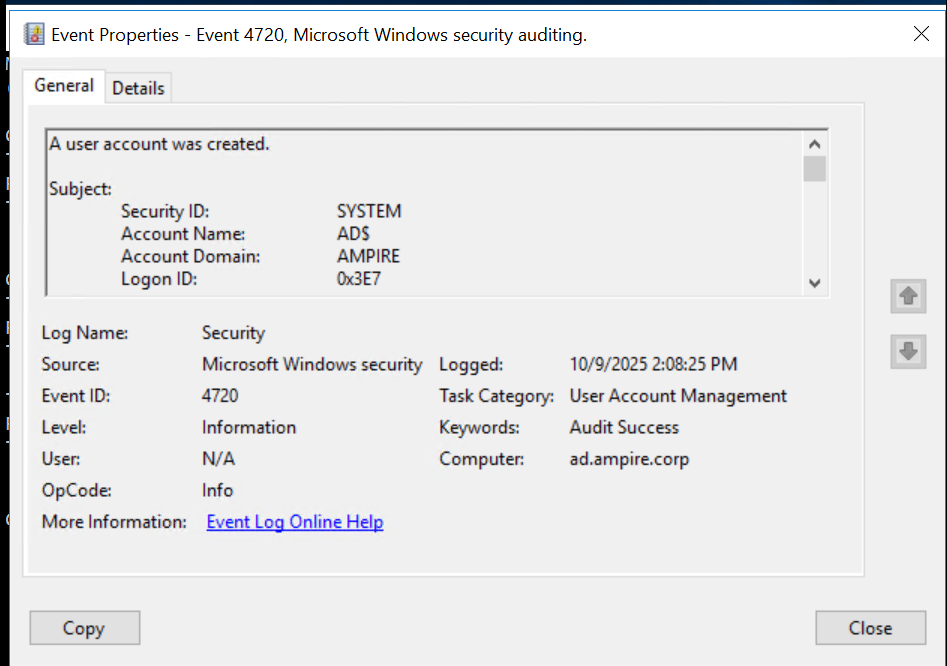
Изменяем пароль к учётной записи администратора на более сложный, не содержащийся в словарях.



Изменение пароля

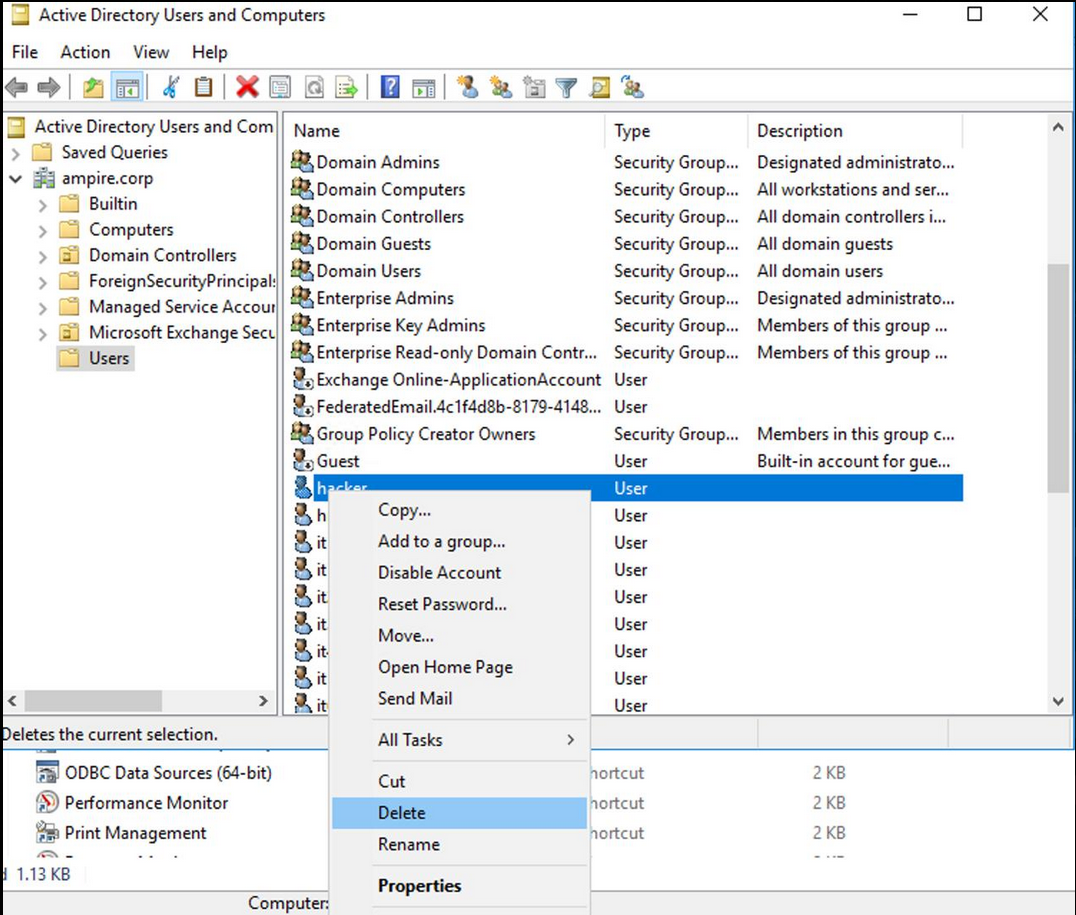
### 2.3.3 Последствие AD User

Находим нового привилегированного пользователя с помощью аудита событий входа в учётную запись Windows security, где появилось событие с ID 4720. Переходим в Evevnt Viewer и в Windows Logs - Secuirity, затем применяем фильтр на логи.



Аудит событий

Чтобы удалить пользователя заходим в Administrative Tools - Active Directory Users and computers. Затем во вкладке Users находим и удаояем нового привилегированного пользователя с именем “Hackes”.

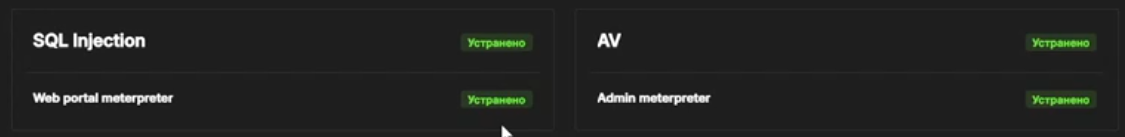
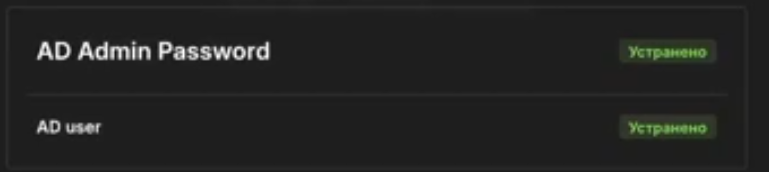


Удаление пользователя

В результате выполенения вышеупомянутых действий привилегированный пользователь удалён и последствие успешно устранено.

# 3 Вывод

Разобрались с сценарием действий нарушителя “Защита контроллера домена предприятия”. Выявили и устранили уязвимости и их последствия

# Список литературы