Отчёт по лабораторной работе №1

Кибербезопасность предприятия

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Устранить уязвимости и последствия информационных систем Компании.

# 2 Выполнение лабораторной работы

## 2.1 Уязвимость 1.SQL-инъекция.

Начнём выполнение лабораторной, сразу зайдём в список событий и найдём информацию о произошедшем (рис. 1):

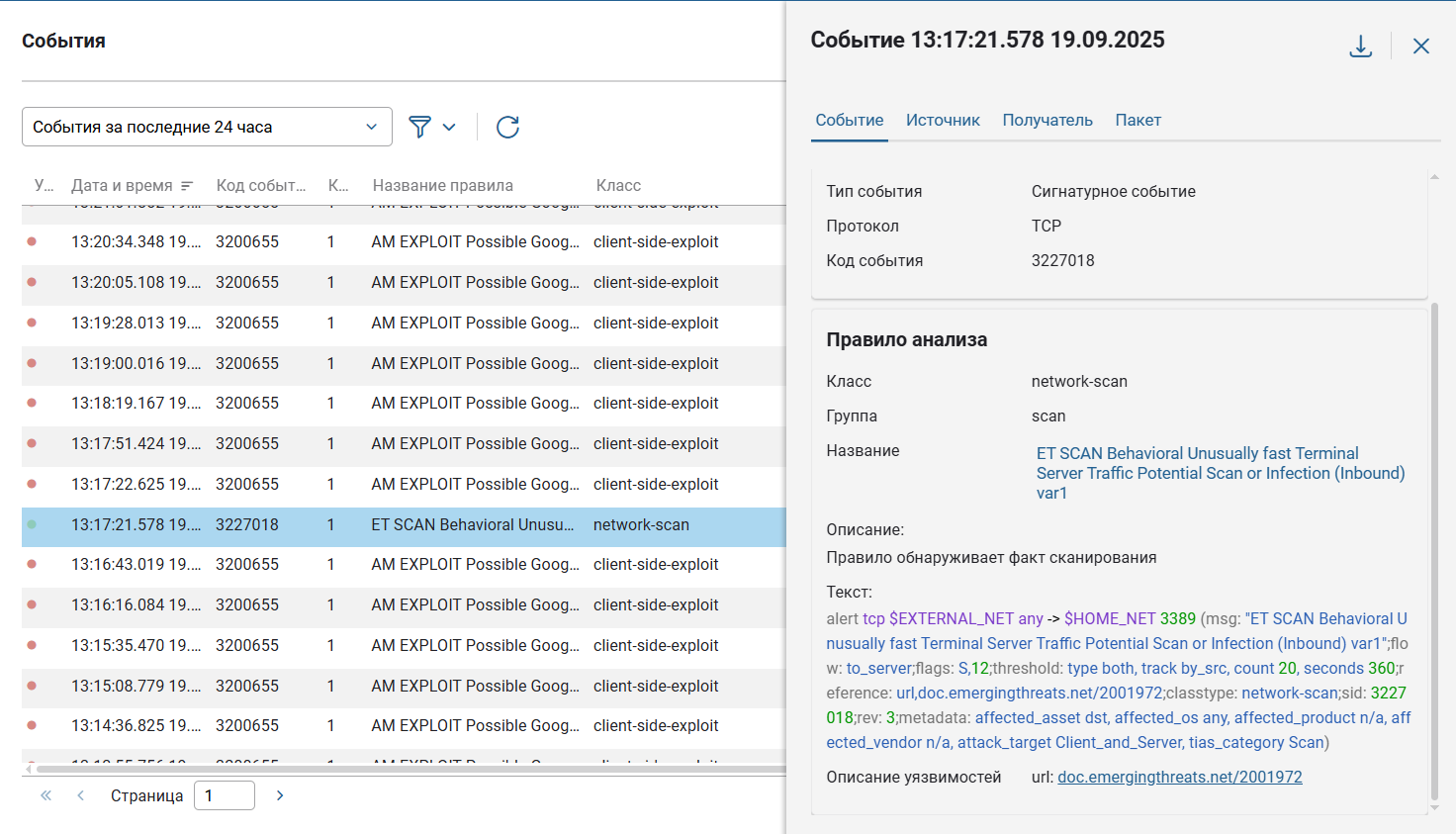


Рис. 1: Найдено сканирование.

Посмотрели описание на CVE (рис. 2):

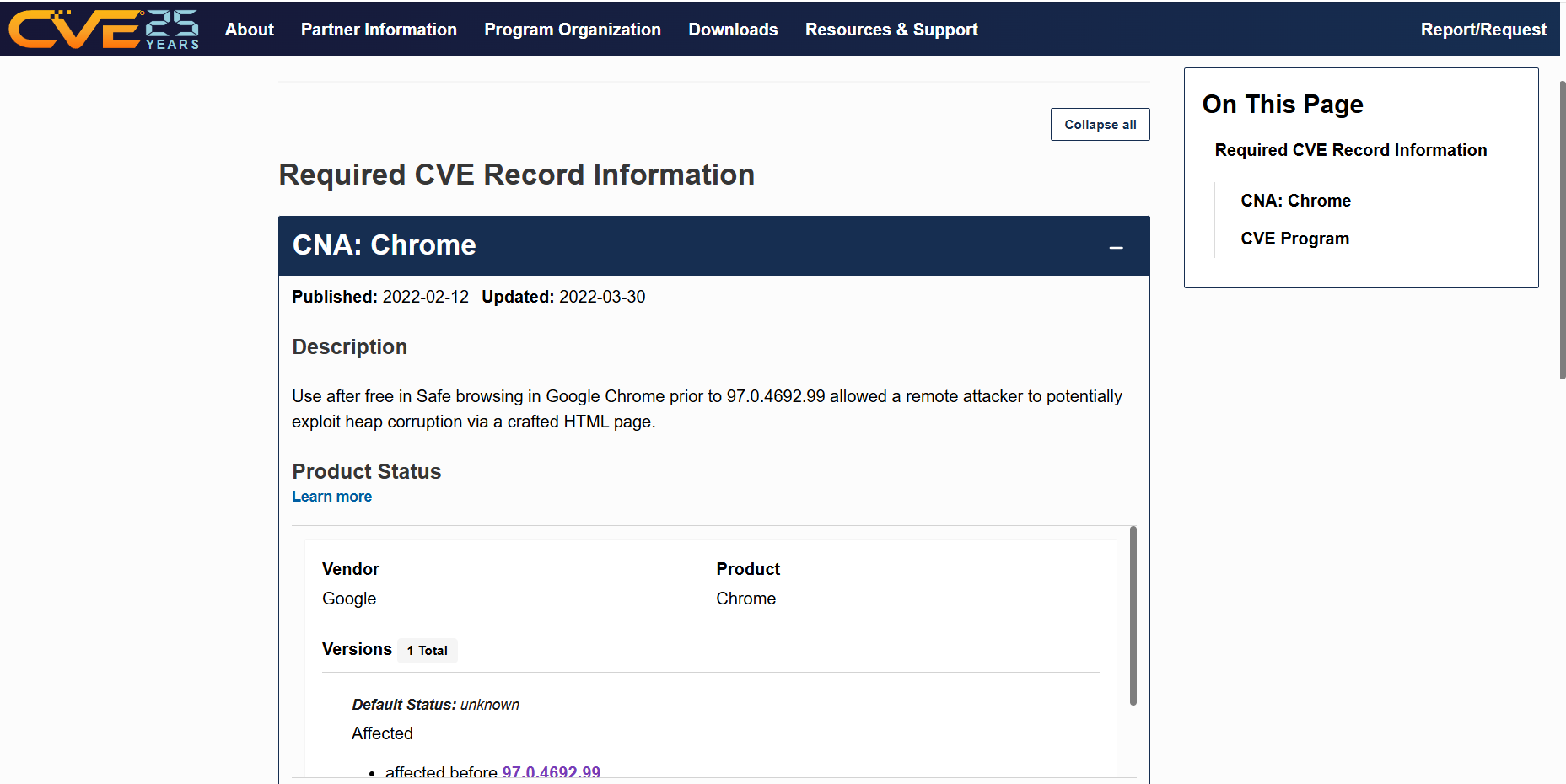


Рис. 2: Описание

Делаем вывод. Нарушитель проводит сканирование сети 195.239.174. Пока его мотивы неясны.

Здесь мы можем наблюдать, что в сетевом трафике найден программный код(рис. 3):

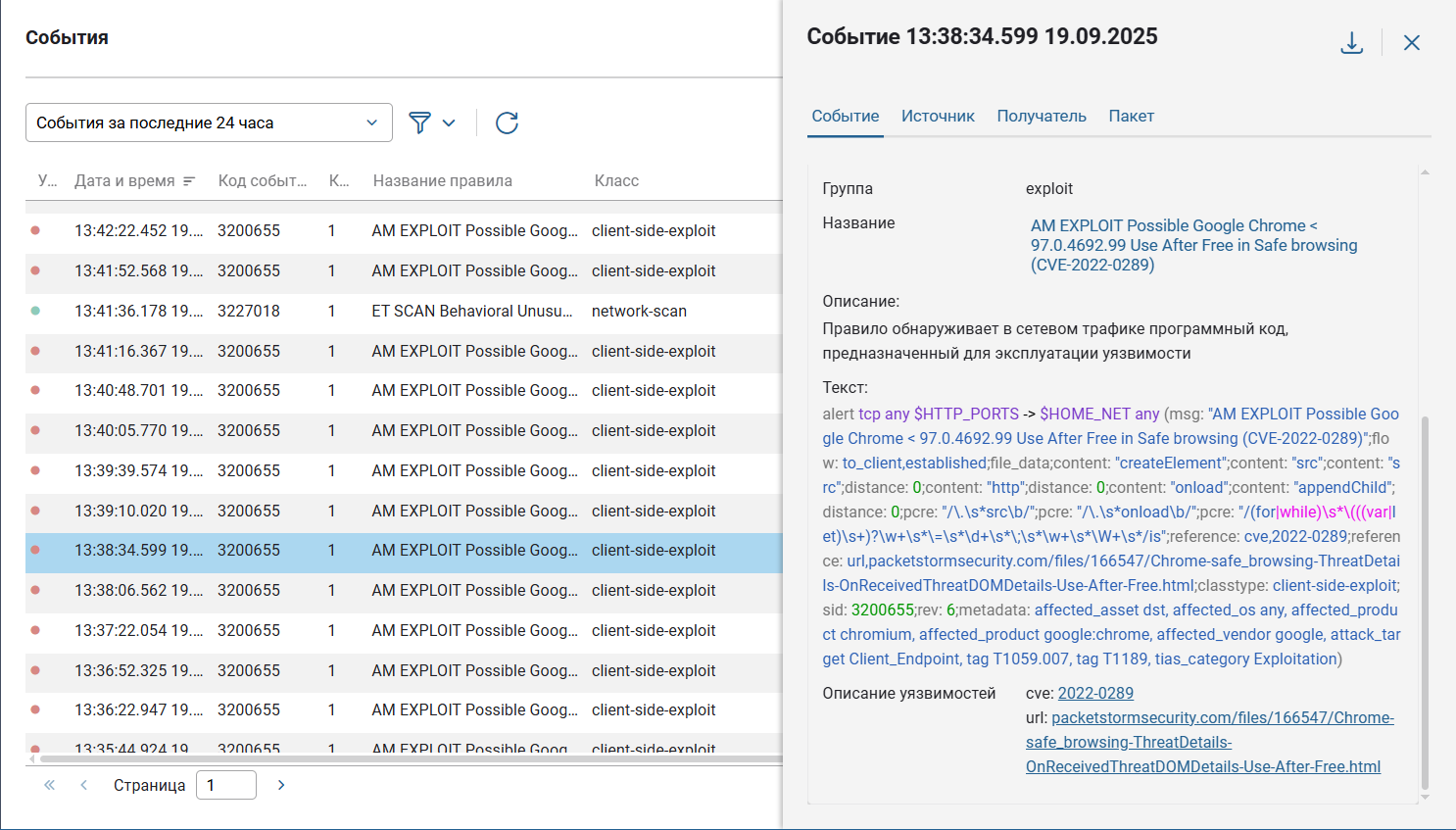


Рис. 3: Найден exploit

Найденные улики дают нам понять, что нарушитель сканирует веб-сервер на предмет SQL-инъекций утилитой sqlmap. Нарушитель генерирует php reverse shell, используя найденную SQL-инъекцию, загружает вредоносный файл на веб-сервер. Нарушитель генерирует письмо с вредоносным вложением и отправляет администратору.Администратор в свою же очередь открывает письмо и тогда запускает вредоносный скрипт. Об этом как раз таки свидетельствует наличие программного кода в сетевом трафике.Как итог, нарушитель получает контроль над компьютером администратора и meterpreter-сессию.

Изучили уязвимость, добавили инцидент (рис. 4):

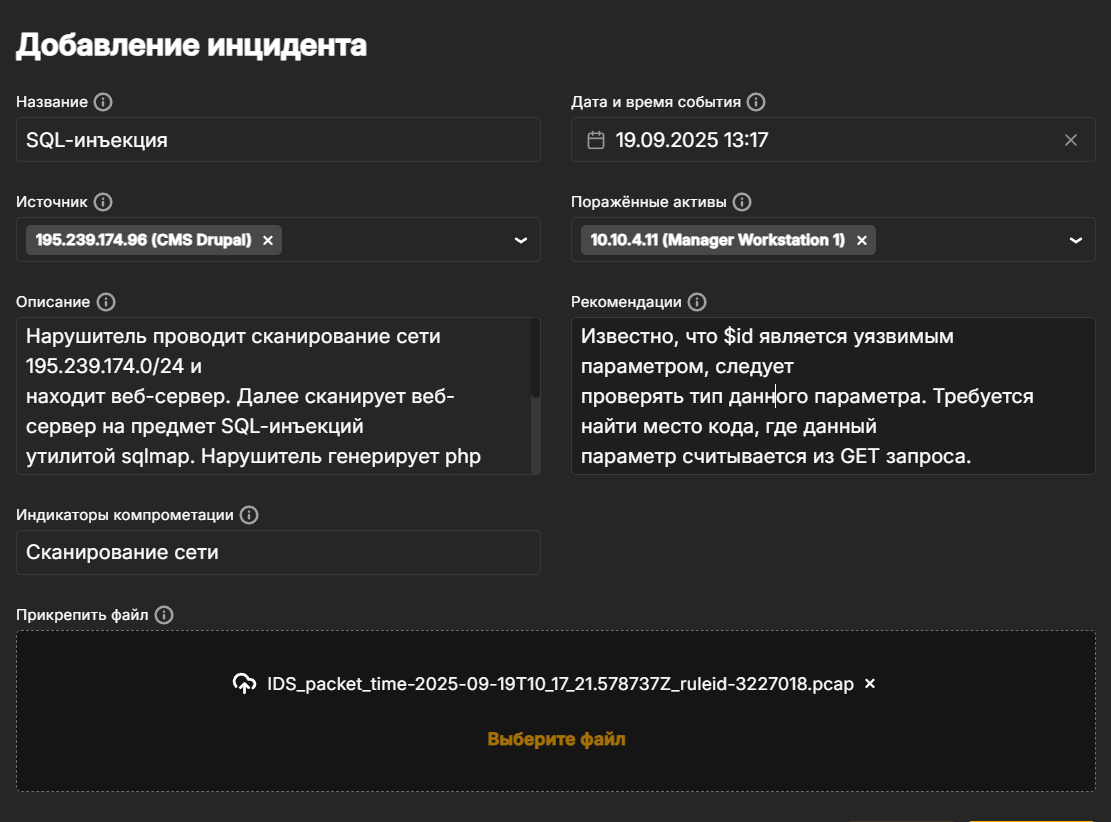


Рис. 4: Добавление инцидента по уязвимости 1.

На узле Web Server PHP находится уязвимый веб-сервер на 80 порту. Нарушитель использует данную уязвимость для загрузки и для выполнения php reverse shell. Для этого мы подключаемся к удаленному рабочему столу (рис. 5):

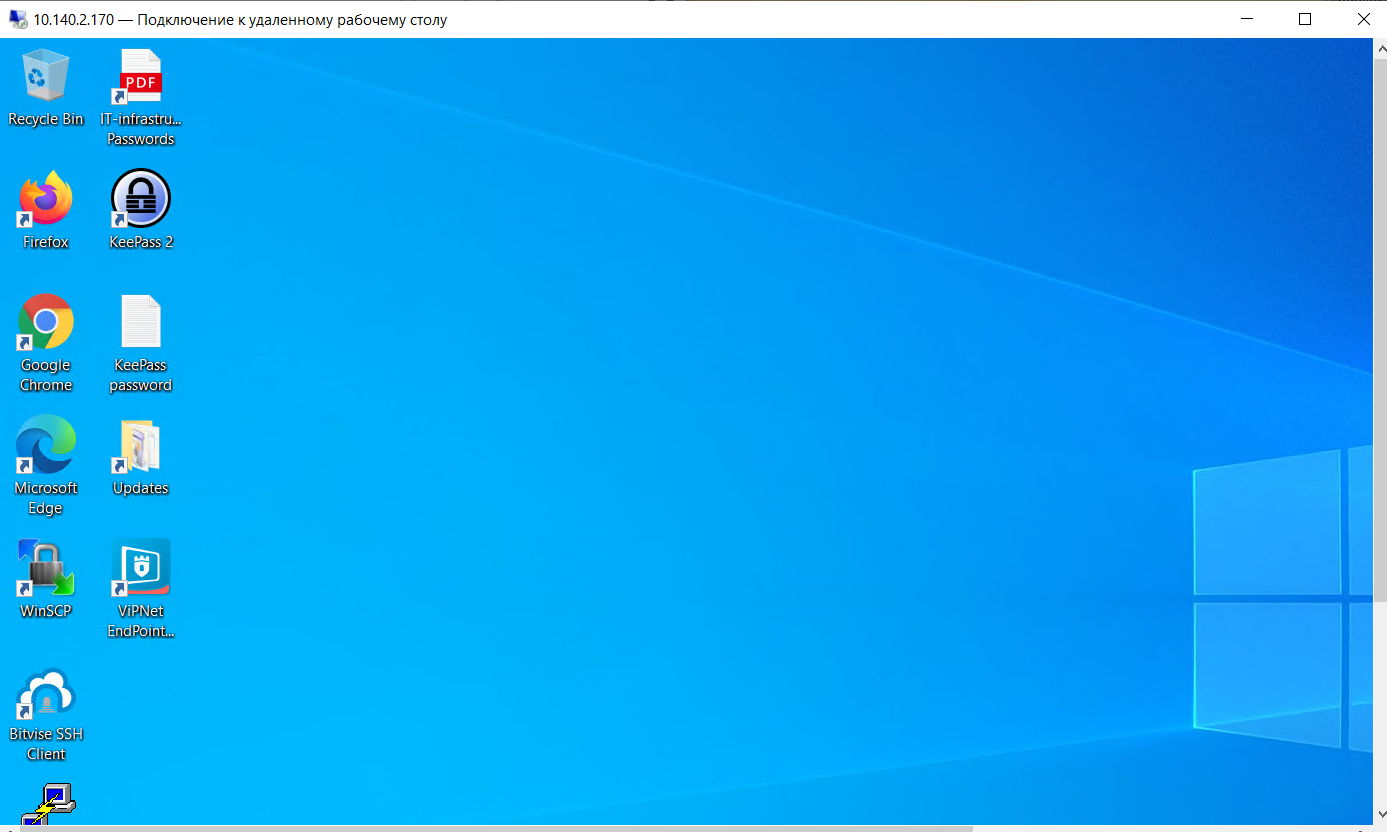


Рис. 5: Подключение к удалённому ПК.

С удалённого ПК зашли на веб-портал (рис. 6):

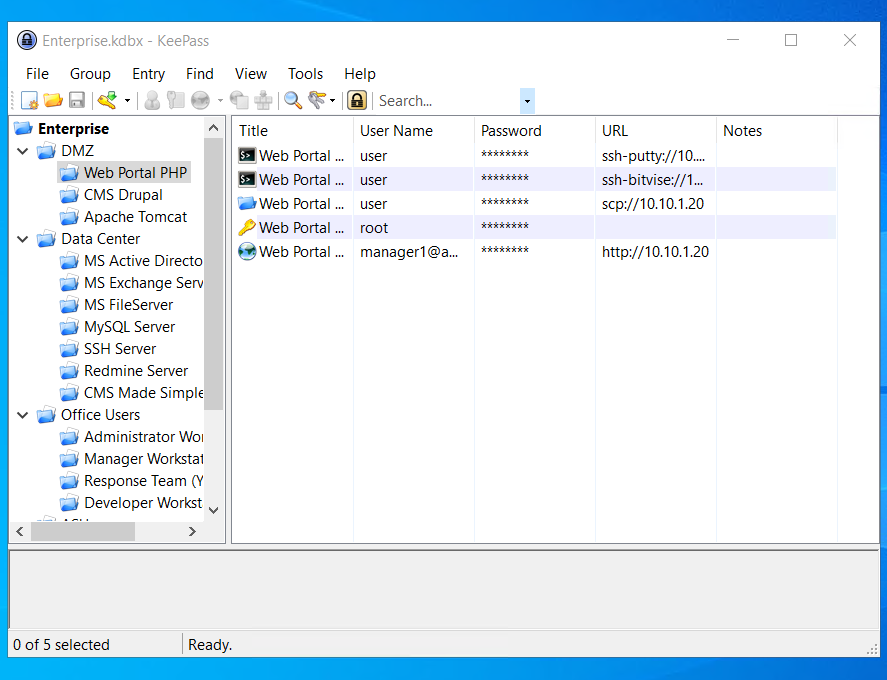


Рис. 6: Заходим на веб-портал.

Далее для устранения уязвимости зашли в командную строку (рис. 7):

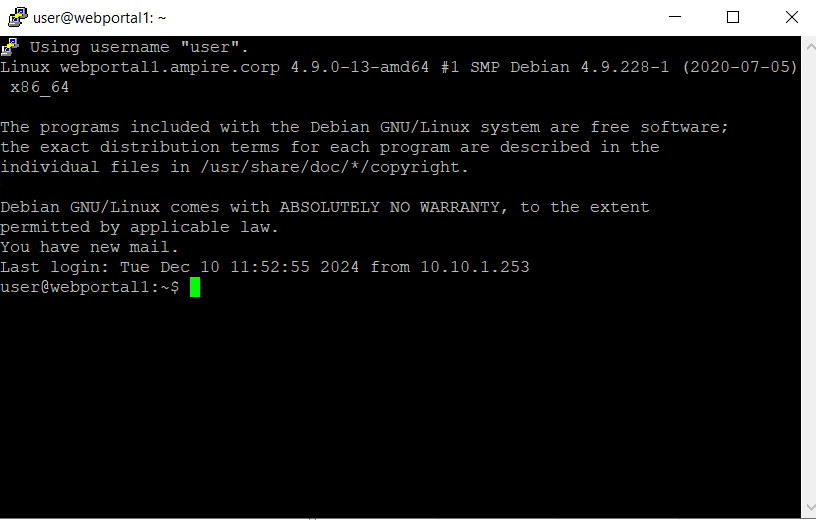


Рис. 7: Командная строка.

Известно, что 4id$ является уязвимым параметром, следует проверять тип данного параметра. Требуется найти место кода, где данный параметр считывается из GET запроса (рис. 8):

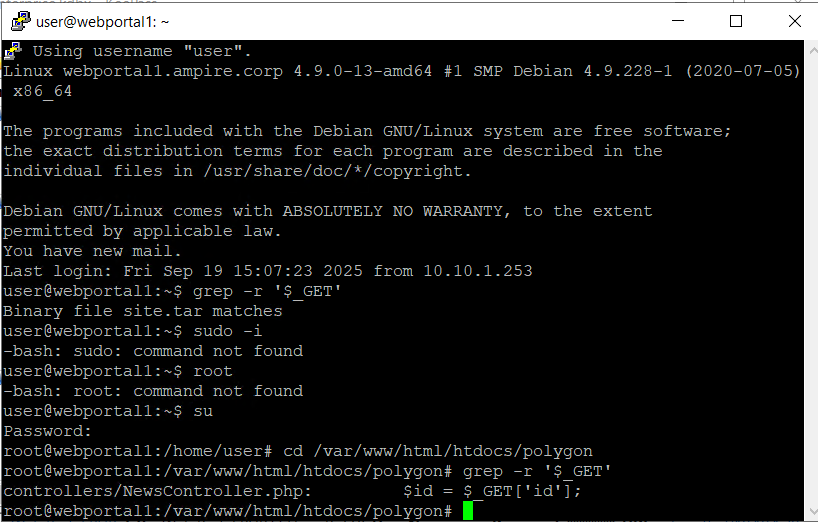


Рис. 8: Поиск уязвимости.

Нашли место с уязвимостью - она в функции actionView (рис. 9):

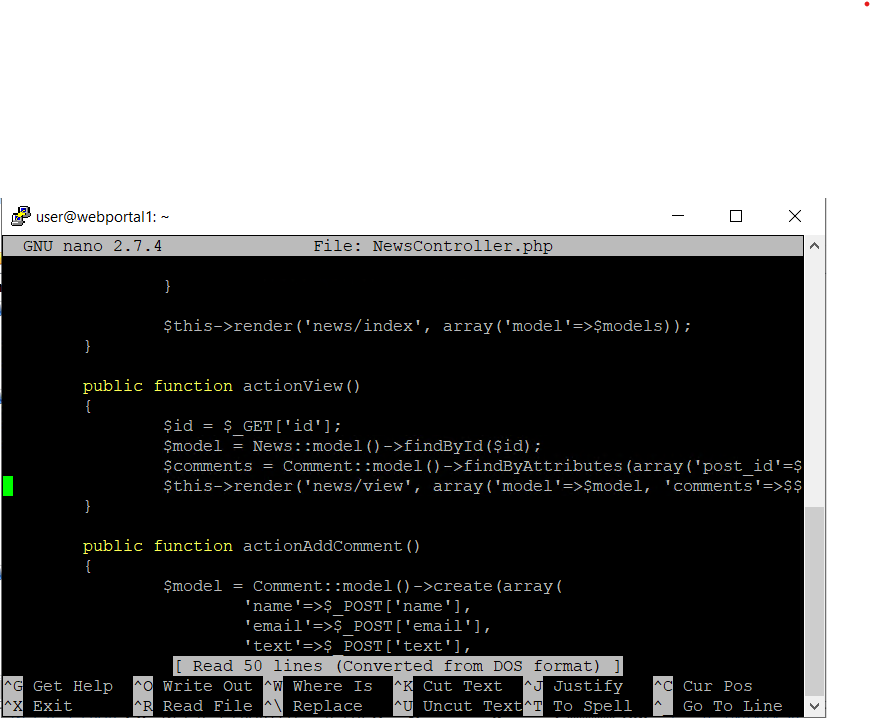


Рис. 9: Параметры уязвимой функции.

Устраним уязвимость, добавляя проверку типа параметра $id (рис. 10):

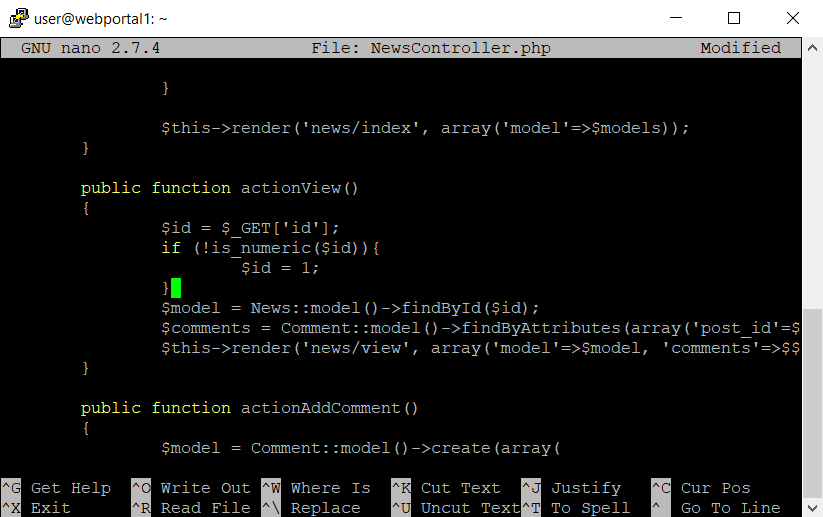


Рис. 10: Исправляем уязвимость.

Проверили, что инцидент устранён (рис. 11), теперь будем устранять последствие:

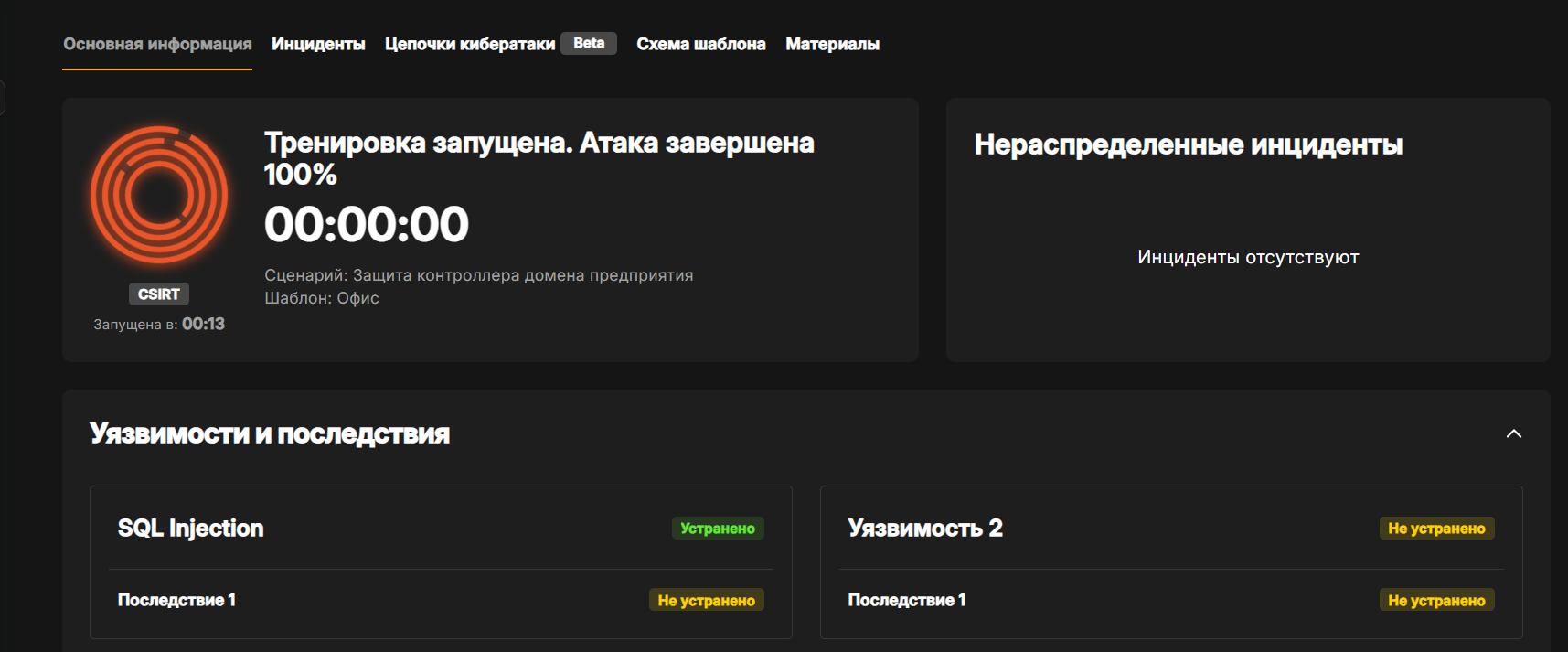


Рис. 11: Устранили уязвимость 1.

## 2.2 Последствие уязвимости 1

Нарушитель устанавливает shell сессию с веб-порталом PHP. Для обнаружения последствия необходимо проверить сокеты уязвимой машины при помощи утилиты ss с ключами -tp (рис. 12):

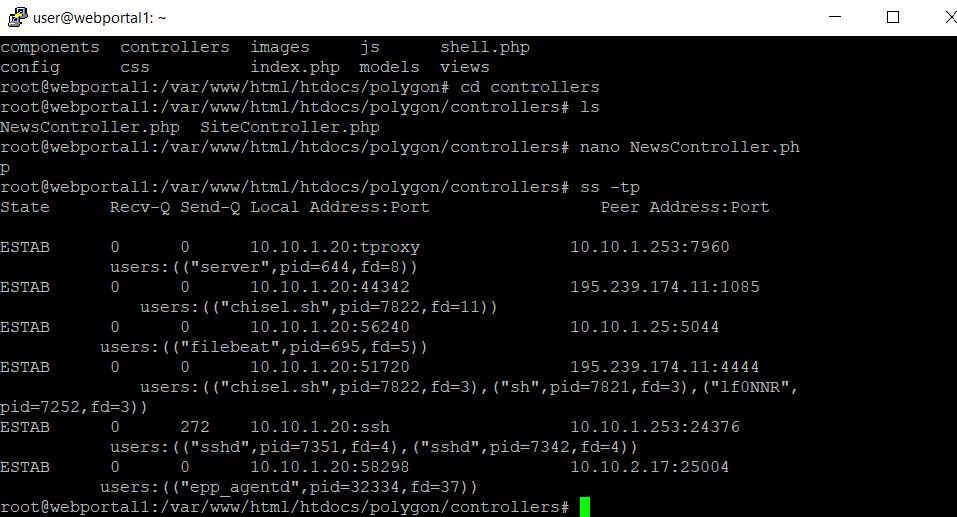


Рис. 12: Список установленных соединений.

Завершаем сессию нарушителя с помощью команды ss и параметром -K (рис. 13):

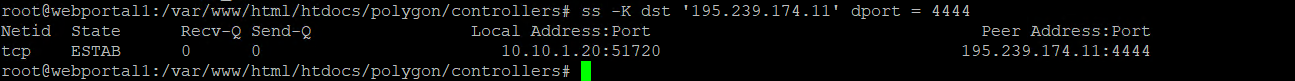


Рис. 13: Разрыв соединения с нарушителем.

Таким образом, устранили последствия первой уязвимости и закрыли инцидент (рис. 14):

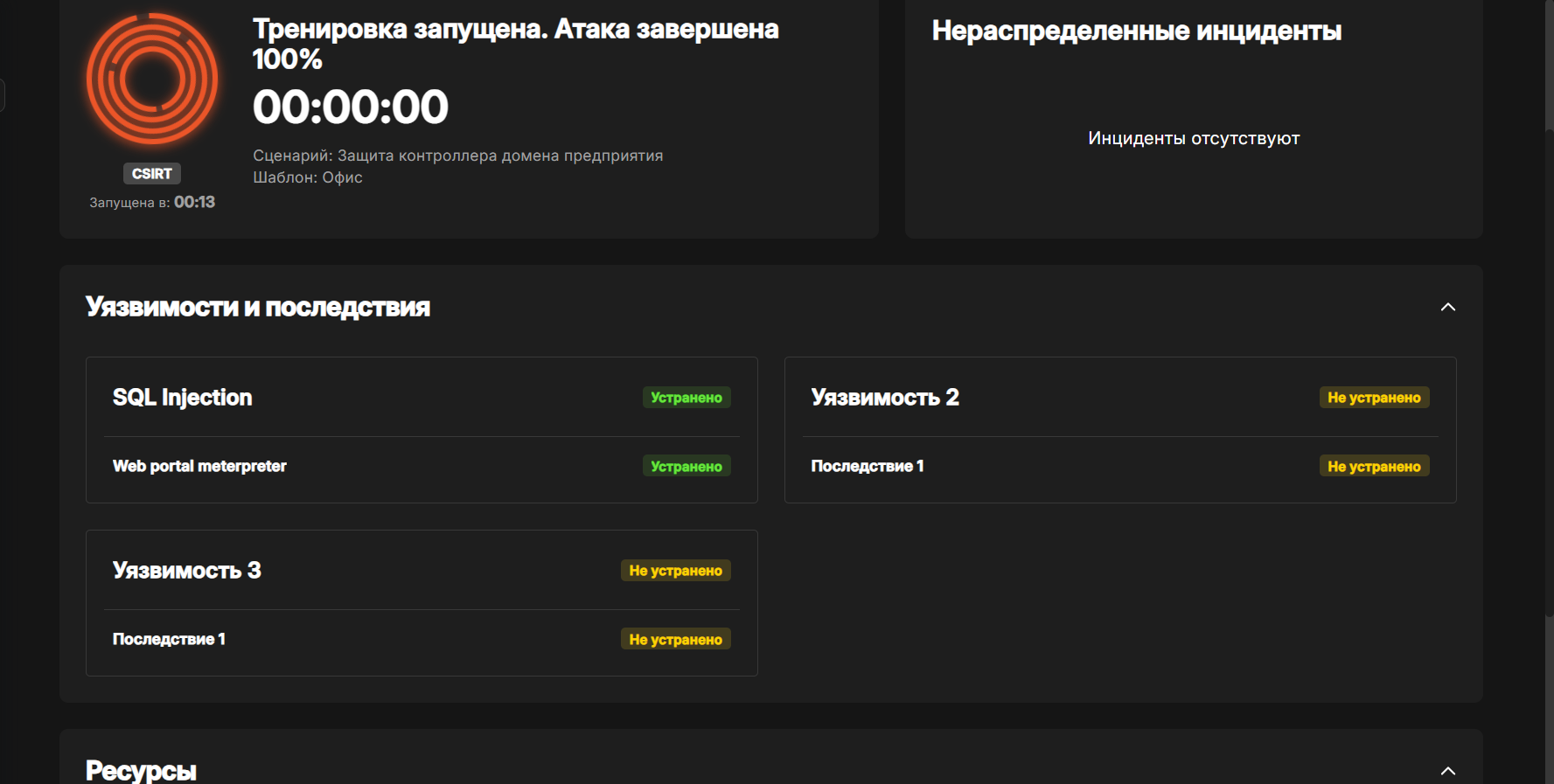


Рис. 14: Последствия первой уязвимости устранены.

## 2.3 Уязвимость 2. Отключенная защита антивируса.

На узле администратора выключена защита в реальном времени Windows Defender, что дает нарушителю возможность получить контроль над компьютером администратора при запуске им вредоносного скрипта diag.psl.

Создаём запись об инциденте (рис. 15):

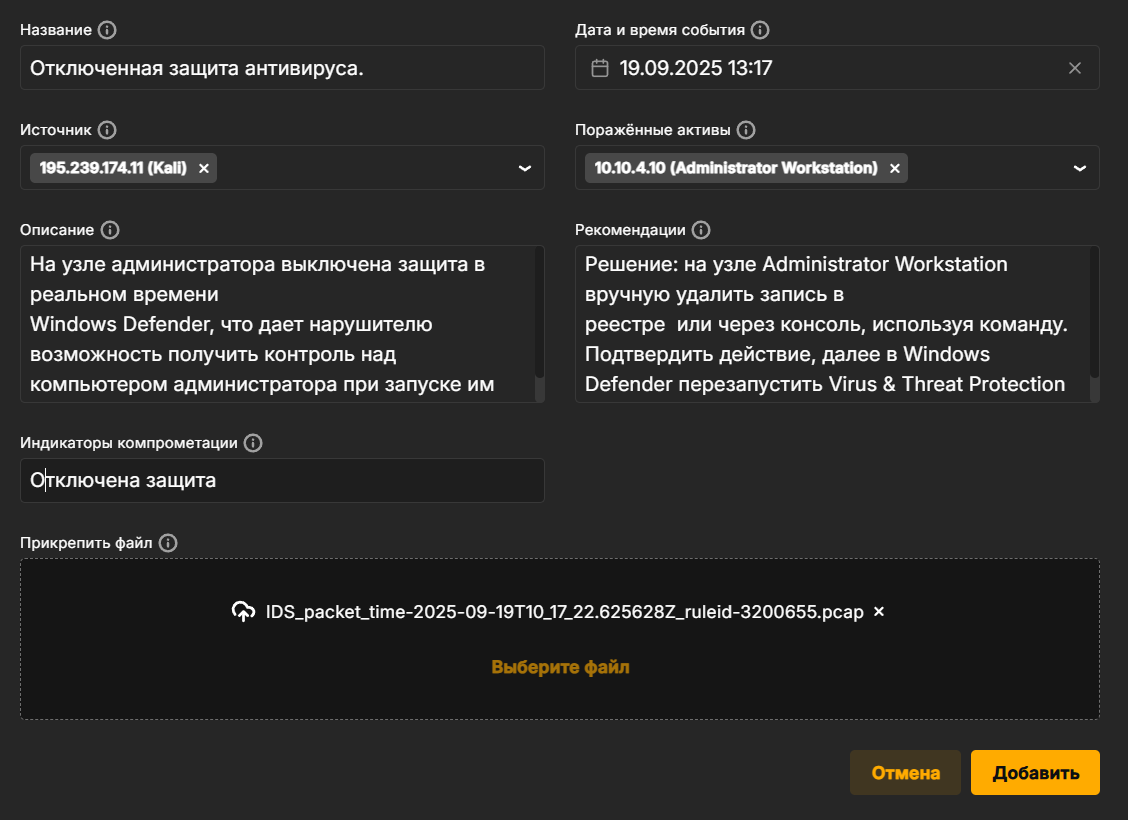


Рис. 15: Создали запись об инциденте.

Далее, поскольку на узле Administrator Defender антивирус был отключен, вручную удаляем запись (рис. 16), подтверждаем действие, в Windows Defender перезапускаем Virus & Threat Protection (рис. 17), включаем Real-time Protection (рис. 18), проверяем, что всё работает (рис. 19):

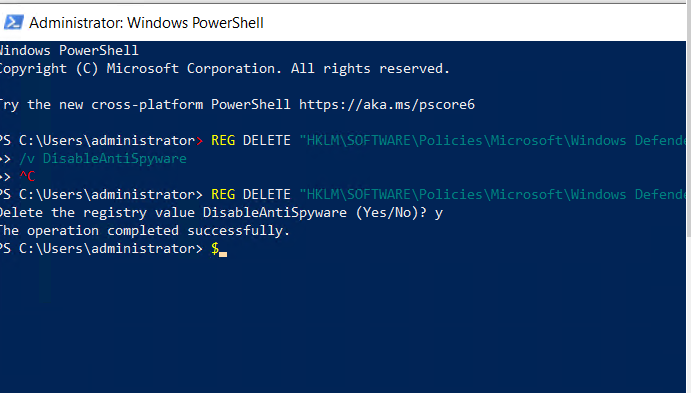


Рис. 16: Удаление записи DisableAntiSpyware в реестре.

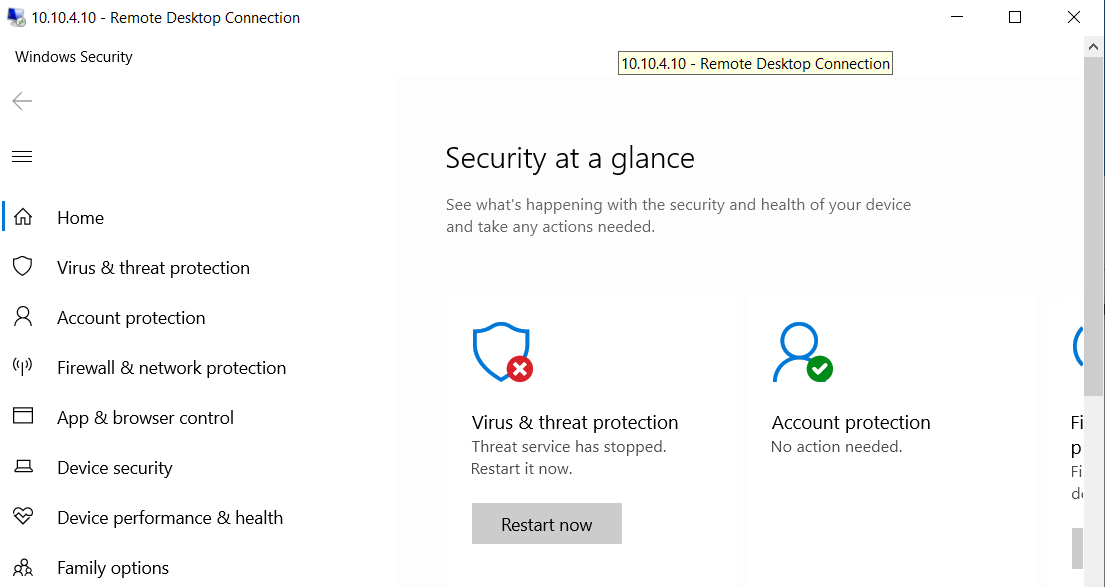


Рис. 17: Интерфейс Windows Defender.

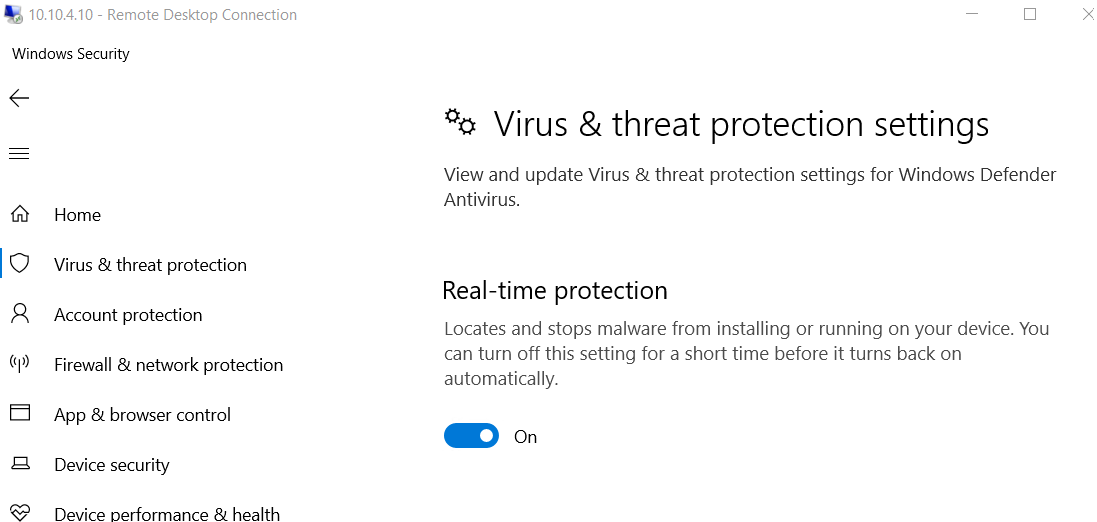


Рис. 18: Включение Real-time Protection.

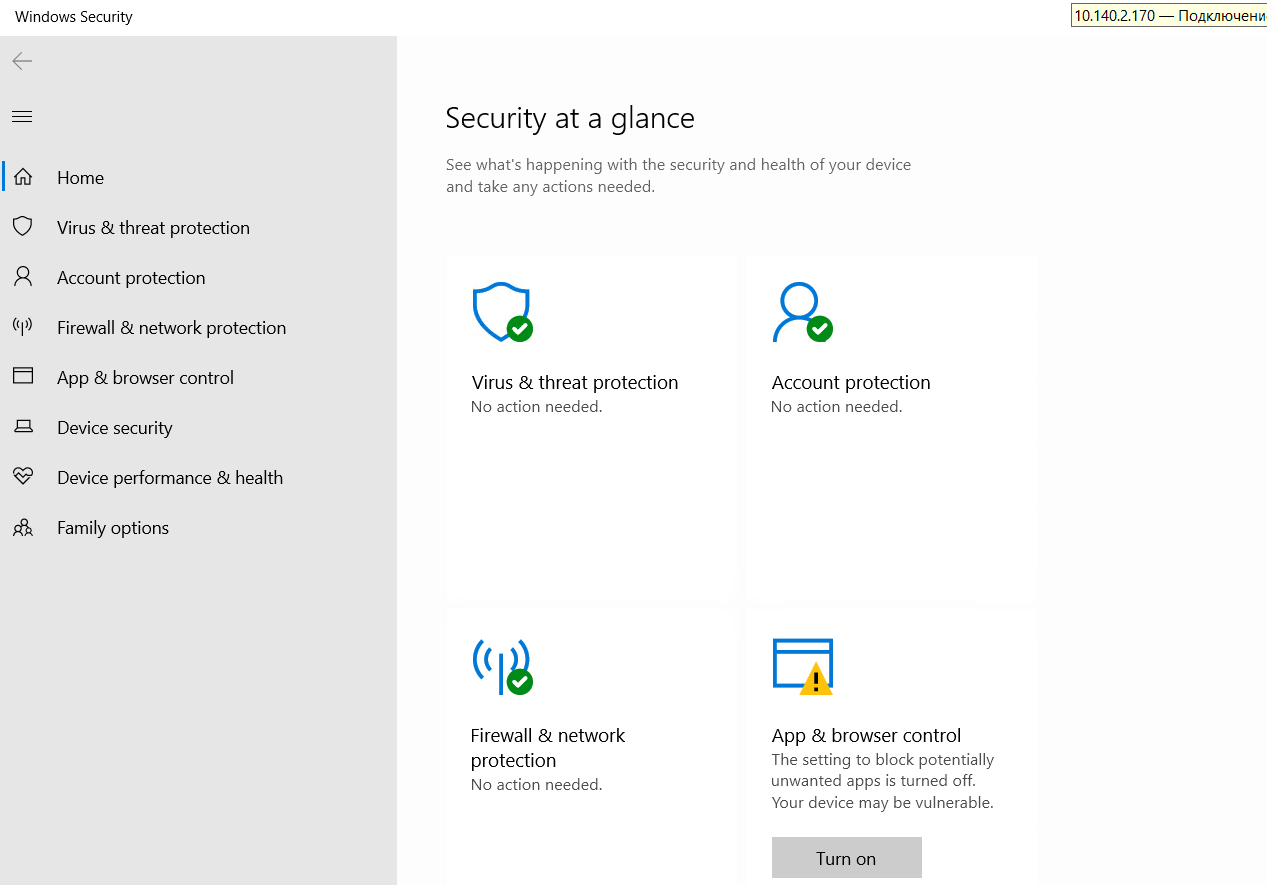


Рис. 19: Антивирус работает.

После выполненных действий необходимо перезагрузить Windows.

## 2.4 Последствие уязвимости 2. Admin meterpreter.

Далее устраняем последствия. Проверяем, что сейчас соединение нарушителя есть (рис. 20):

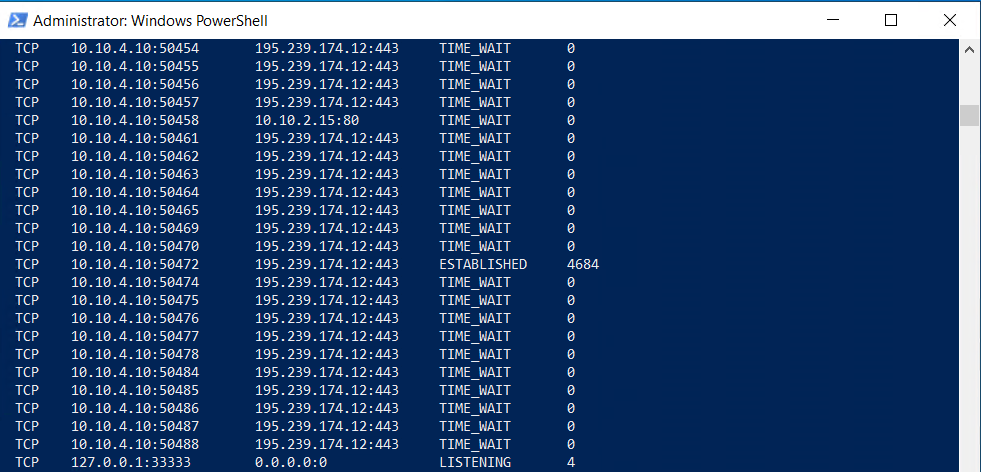


Рис. 20: Соединение с машиной нарушителя.

Разрываем соединение с помощью команды taskkill (рис. 21):



Рис. 21: Остановка процесса.

Далее устраняем проблему, связанную со слабым паролем. На узле MS Active Directory установлен слабый пароль к учётной записи администратора, что позволяет нарушителю подобрать пароль, смотрим логи подключений по RDP (рис. 22):

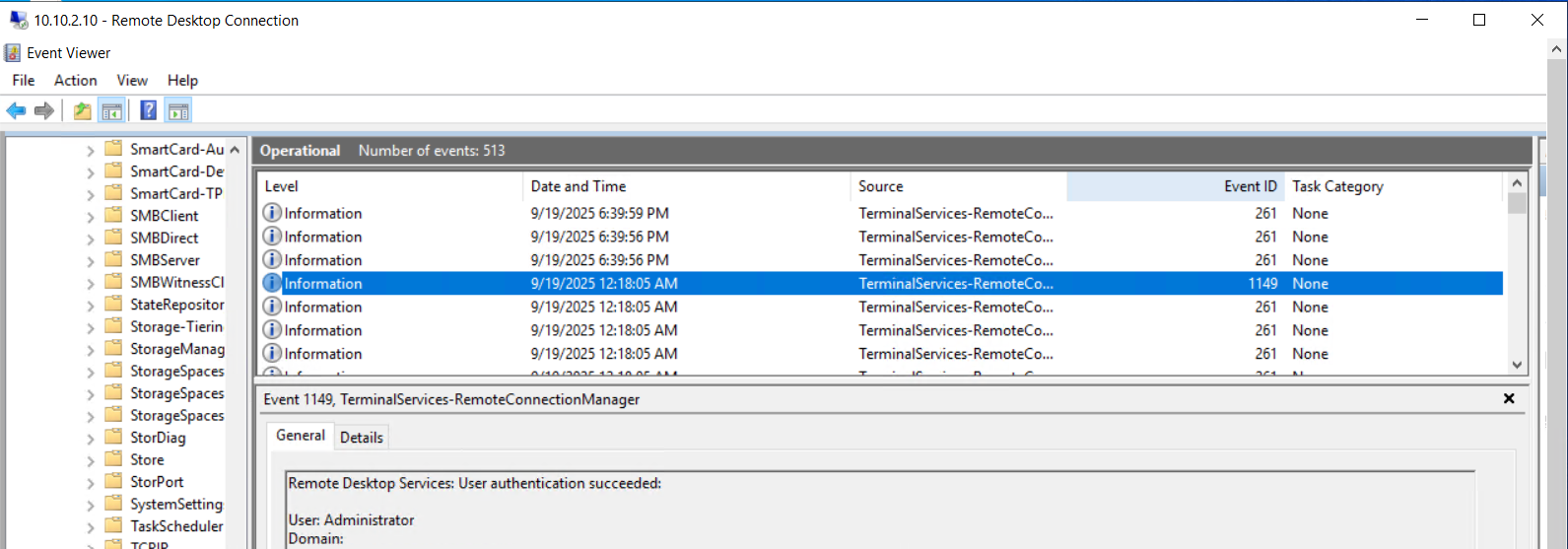


Рис. 22: Логи подключений по RDP и успешная аутентификация.

Устраним уязвимость, сменив пароль администратора (рис. 23):

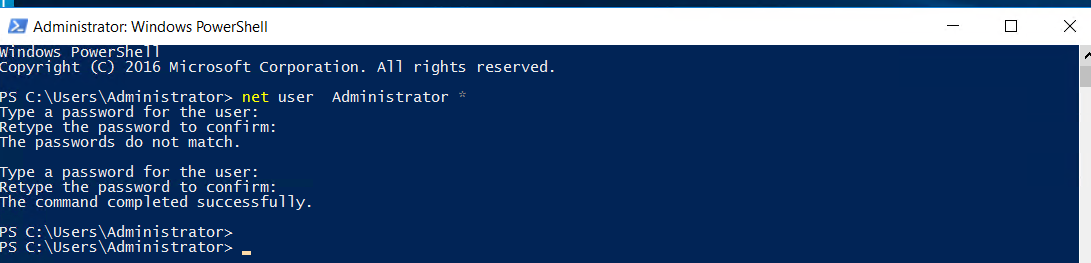


Рис. 23: Изменение пароля администратора.

Переходим к устранению последствий. Был создан новый привелигированный пользователь, находим его в Administrative Tools - Active Directory Users and computers, во вкладке Users и удаляем (рис. 24):

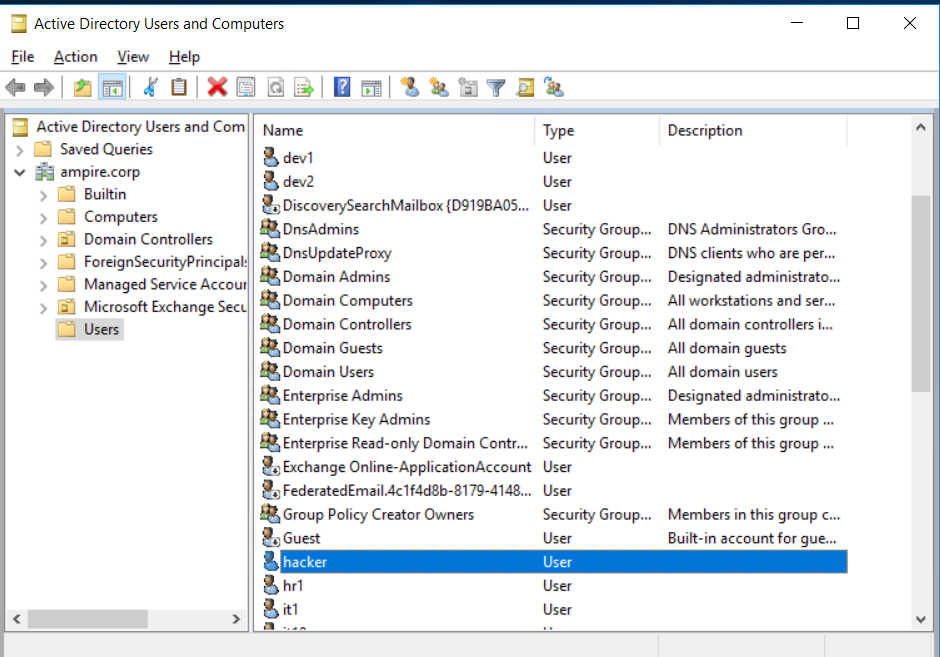


Рис. 24: Удаление привилегированного пользователя.

Проверяем, что все уязвимости и их последствия устранены (рис. 25):

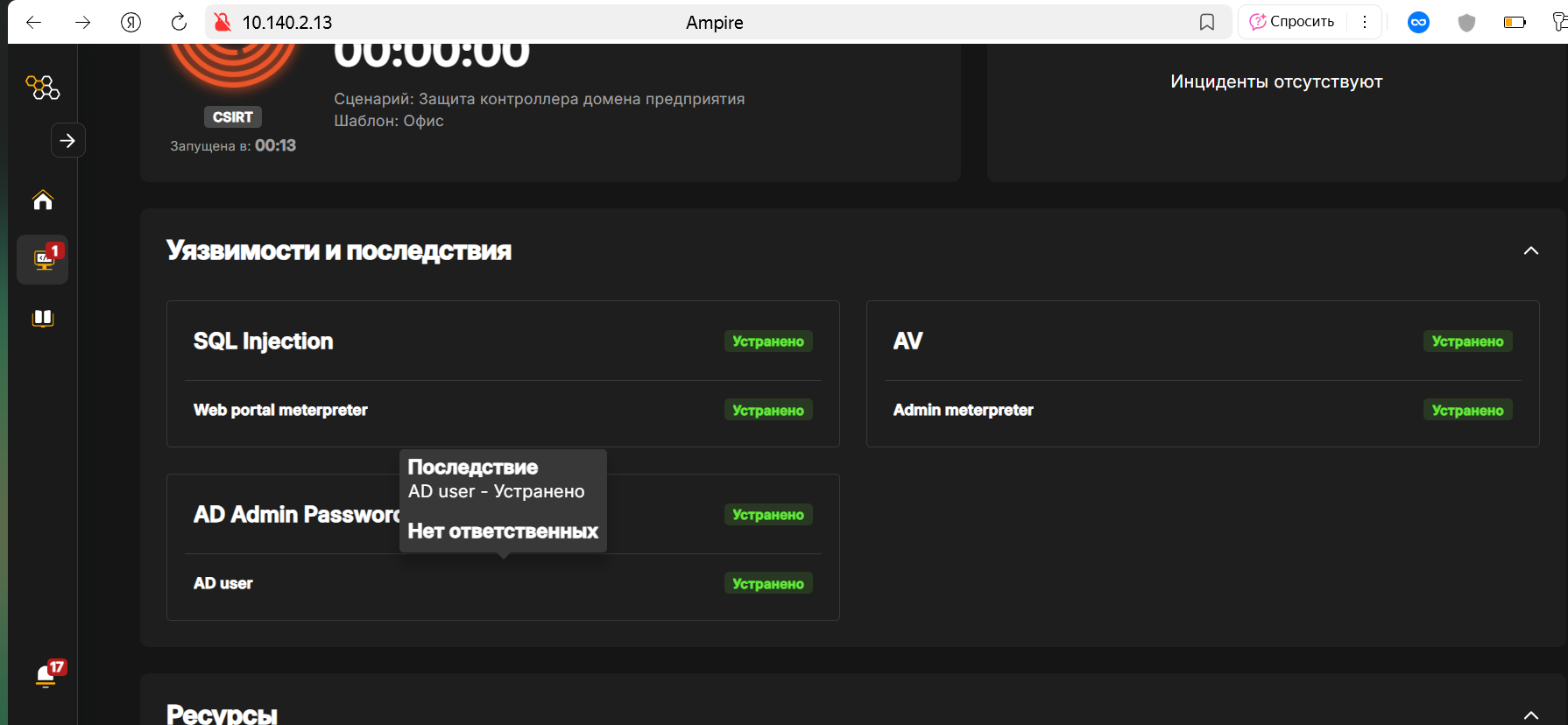


Рис. 25: Все уязвимости устранены.

# 3 Выводы

Устранили уязвимости сайта Компании.