Отчёт по лабораторной работе №1

Дисциплина: Кибербезопасность предприятия

Боровиков Даниил Александрович,
Хрусталев Влад Николаевич, Гисматуллин Артем,
Тщесноков Артёмий Pavlovich, Коннова Татьяна,
Нефедова Наталья, Уткина Алина,
Бансимба Клодели

Содержание

Список иллюстраций

Список таблиц

1 Задание

Сценарий №2

Защита контроллера домена предприятия

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам компании. Обнаружив несколько уязвимостей на внешнем периметре и закрепившись на одном из серверов, Злоумышленник проводит разведку корпоративной сети с целью захватить контроллер домена. Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации. Злоумышленник обладает опытом проведения почтовых фишинговых рассылок.

2 Выполнение лабораторной работы

2.1 Способы детектирования атаки

2.1.1 Детектирование с ViPNet IDS NS

- SQL-инъекция: Сканирование, Blind SQL-Injection, загрузка файла (рис. 2.1) (рис. 2.2). (рис. 2.3).
- Зафиксировали инцидент на платформе (рис. 2.4).
- RDP Brute-force: Множественные подключения (рис. 2.5).
- Зафиксировали инцидент на платформе (рис. 2.6).
- Зафиксировали инцидент на платформе (рис. 2.7)

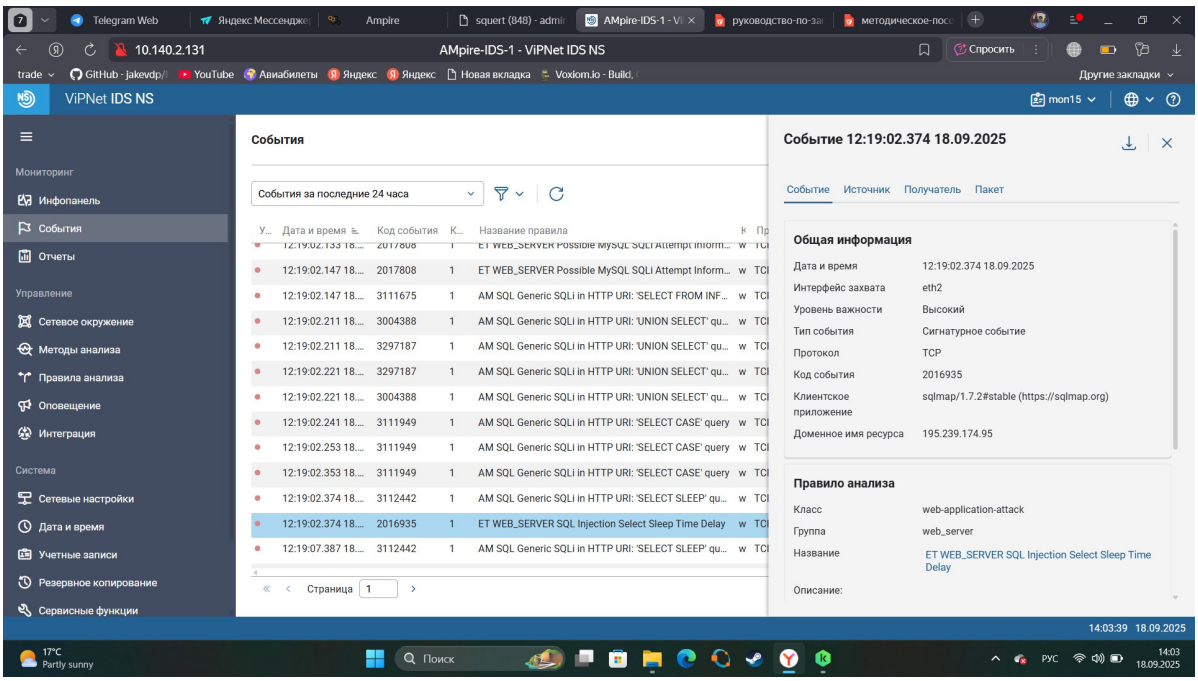

Рис. 2.1: Сканирование на SQL-инъекции

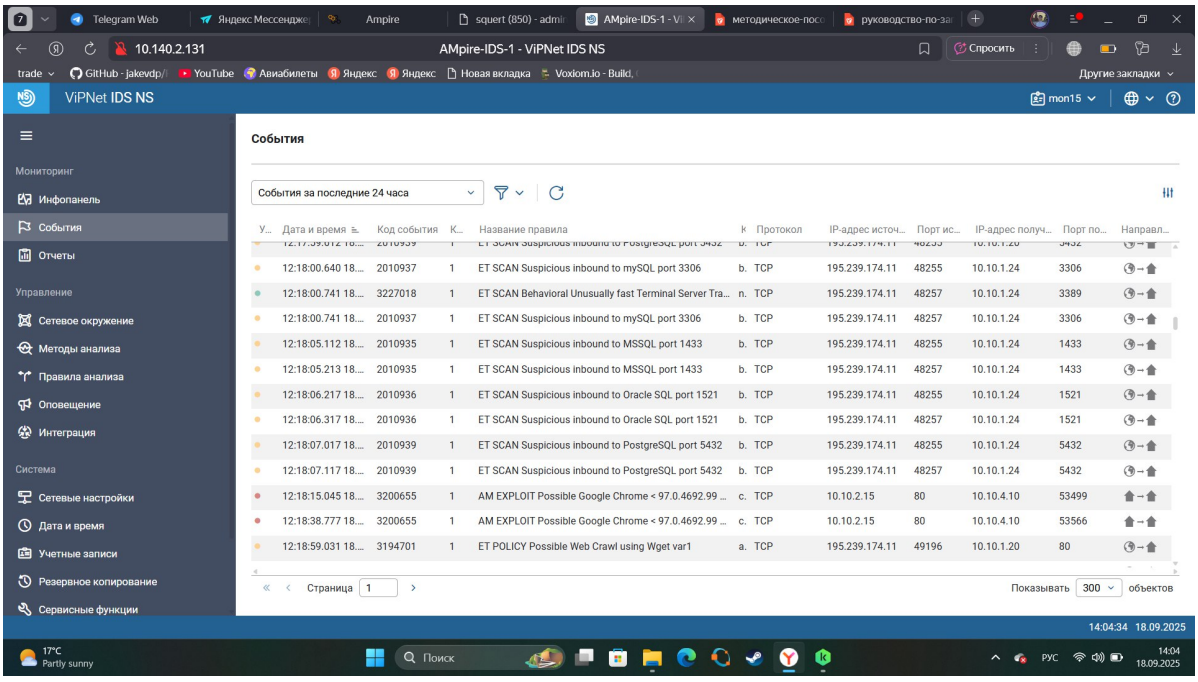

Рис. 2.2: Детектирование SQL-инъекции

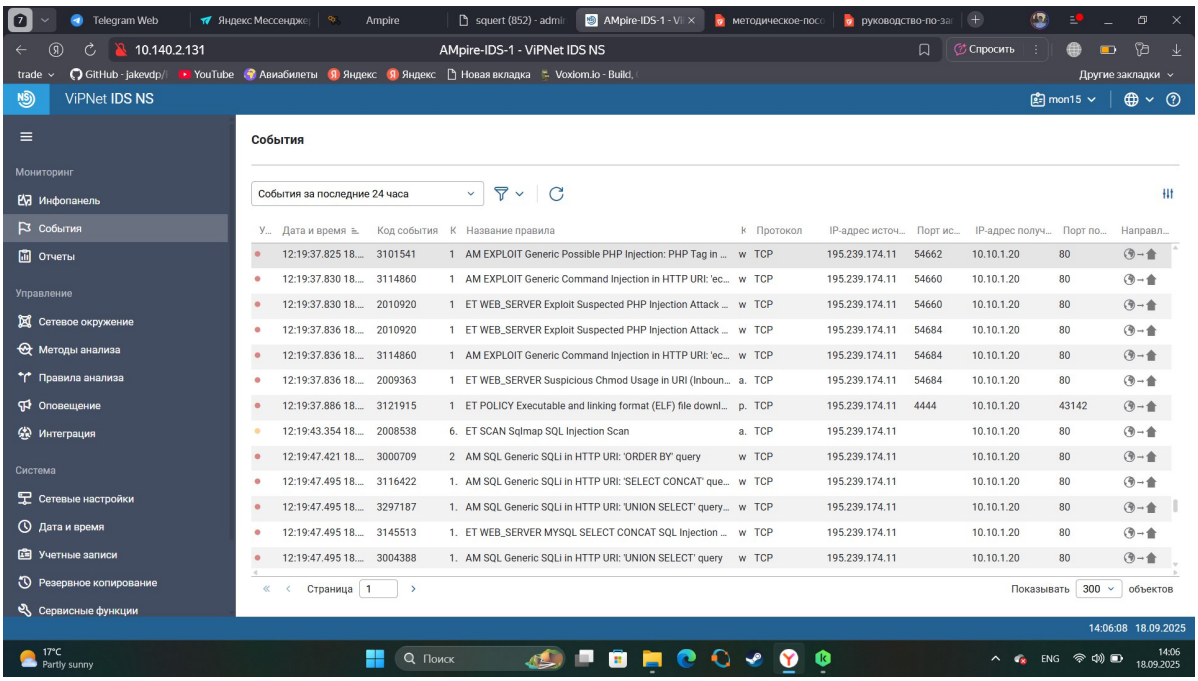

Рис. 2.3: Загрузка вредоносного файла

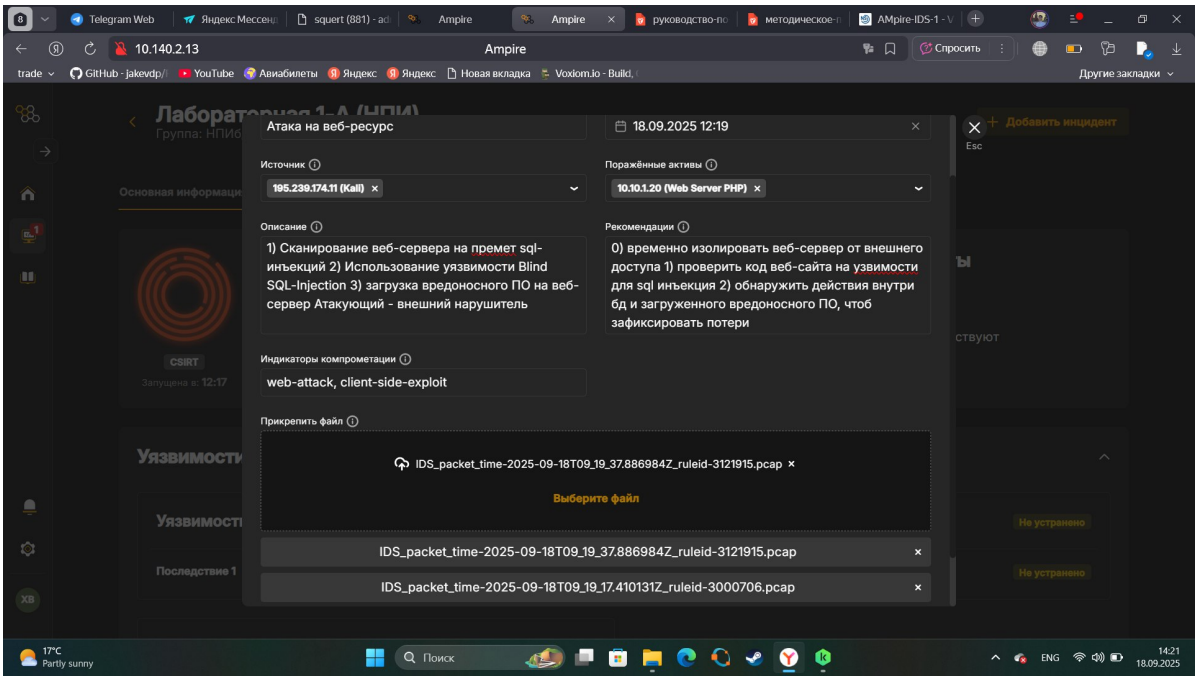

Рис. 2.4: Инцидент атака на веб сервер

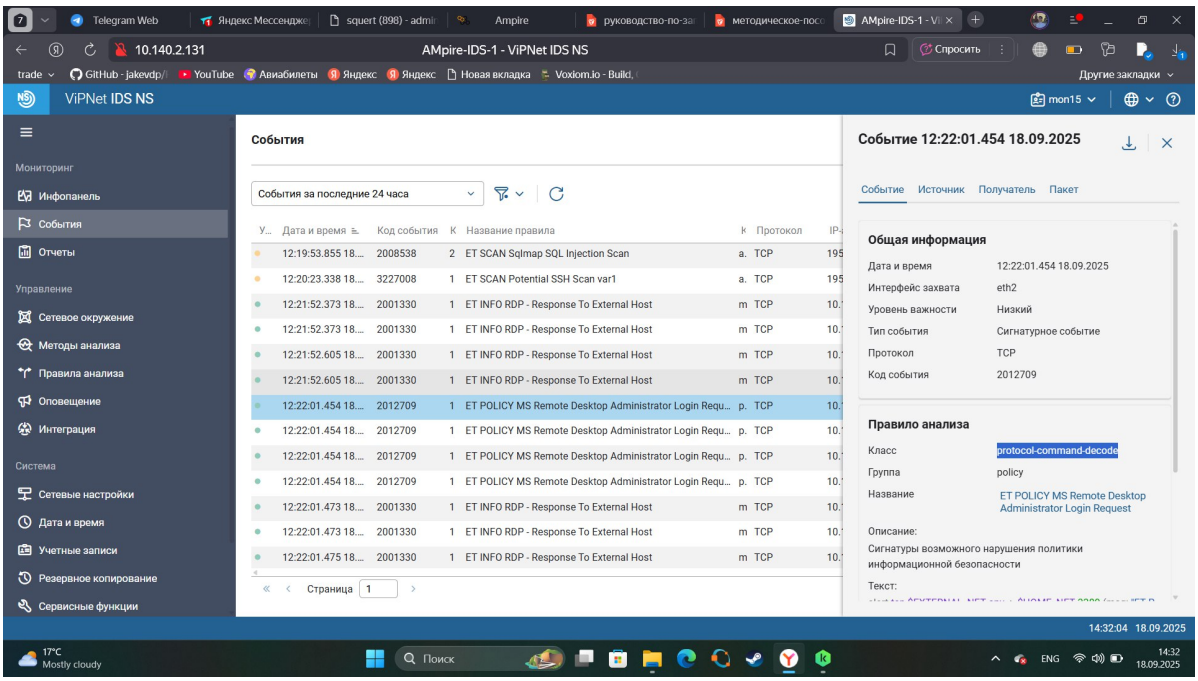

Рис. 2.5: RDP Brute-force

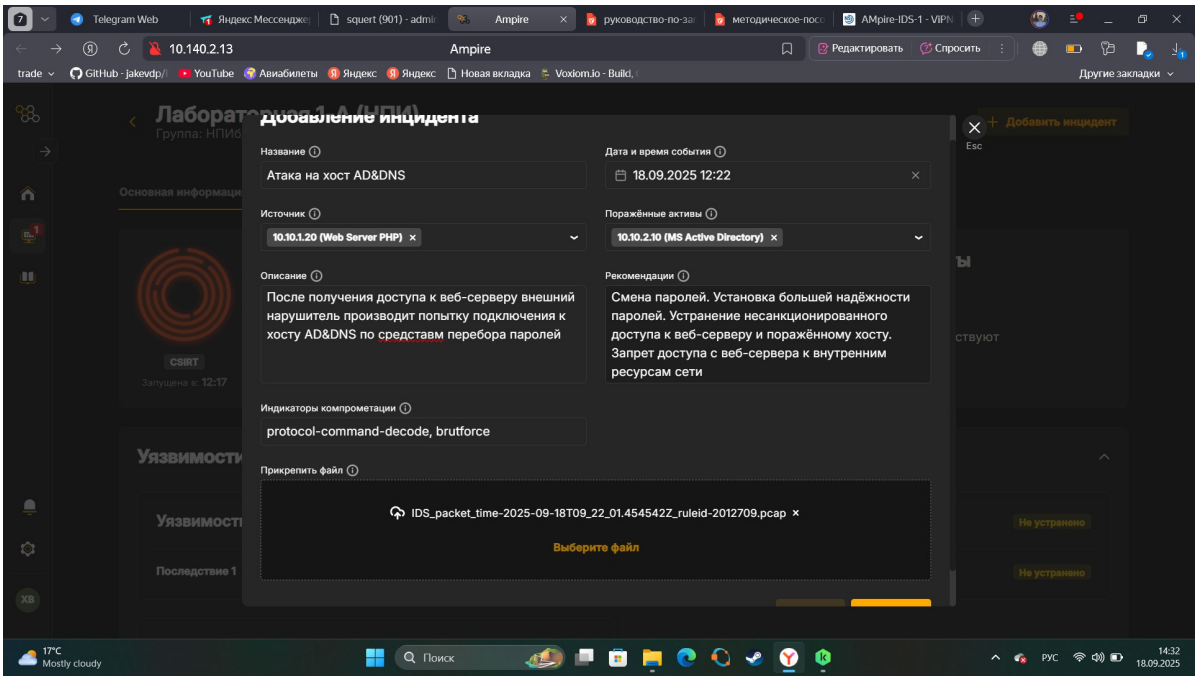

Рис. 2.6: Инцидент атака а хост, Brute-force

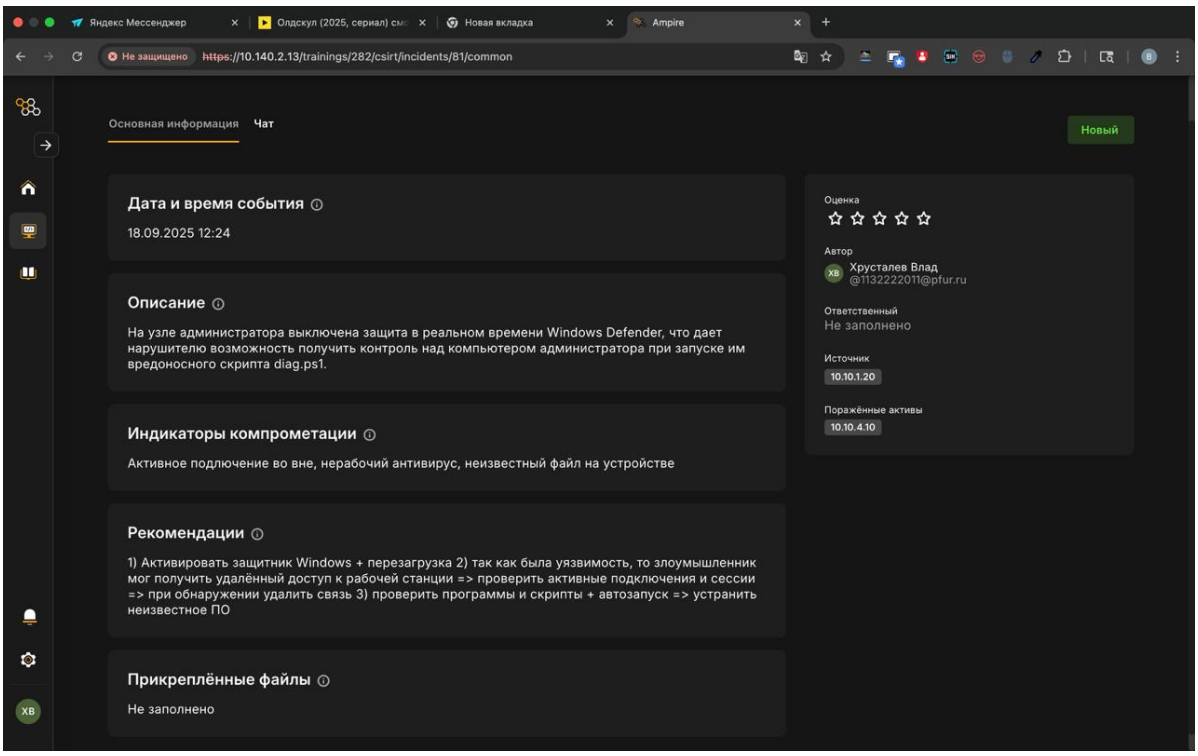

Рис. 2.7: Инцидент Атака на Administration WS

2.2 Перечень уязвимостей и последствий

Мы выявили и устранили три уязвимости и три последствия:

1. Уязвимость 1: SQL-инъекция.
2. Последствие: Web portal meterpreter.
3. Уязвимость 2: Отключенная защита антивируса.
4. Последствие: Admin meterpreter.
5. Уязвимость 3: Слабый пароль учетной записи.
6. Последствие: Добавление привилегированного пользователя.

2.2.1 SQL-инъекция

На узле Web Server PHP (порт 80) была уязвимость в веб-сервисе. Нарушитель использовал sqlmap для загрузки PHP reverse shell (рис. 2.8).

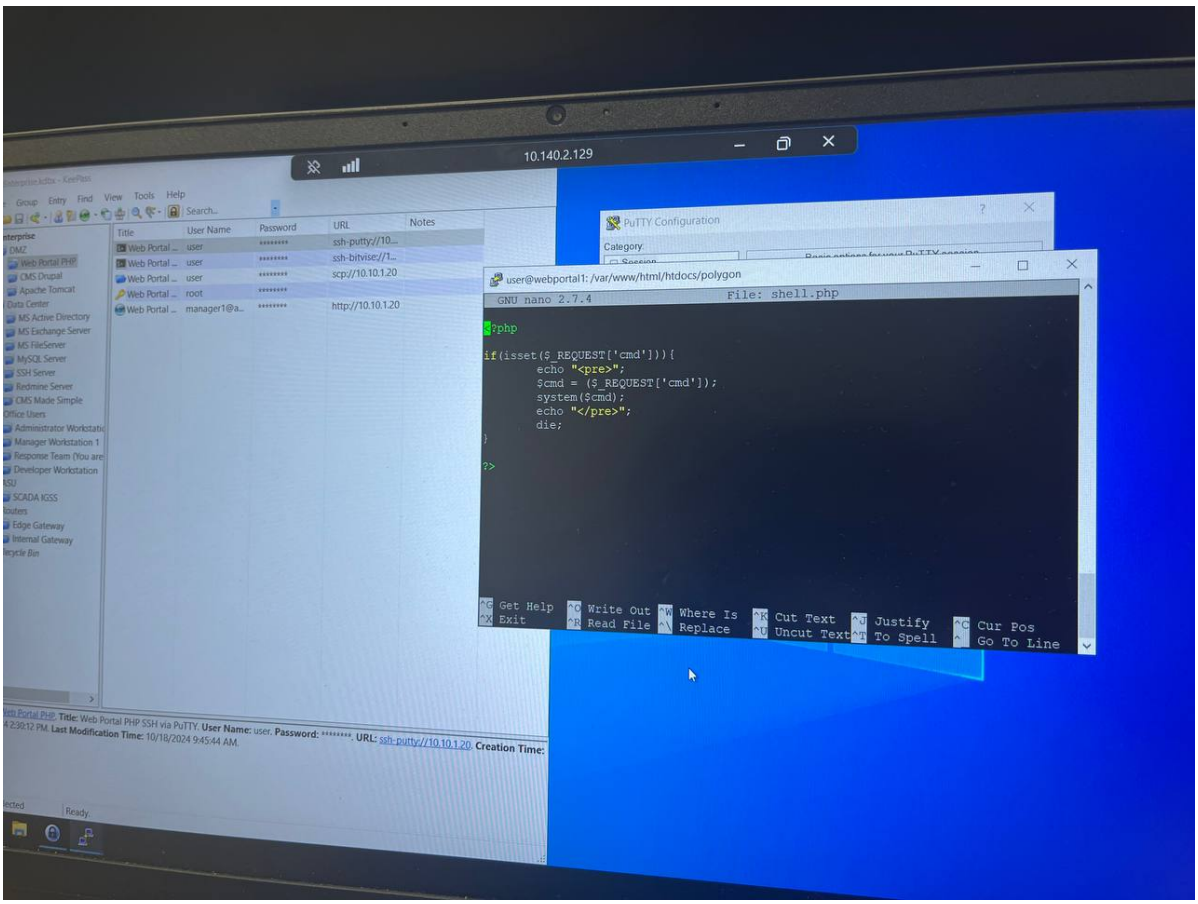

Рис. 2.8: PHP reverse shell

Устранение: Параметр $id в GET-запросе проверяли на тип с помощью is_numeric(). Изменили функцию actionView() в NewsController.php (рис. 2.9) (рис. 2.10) (рис. 2.11)

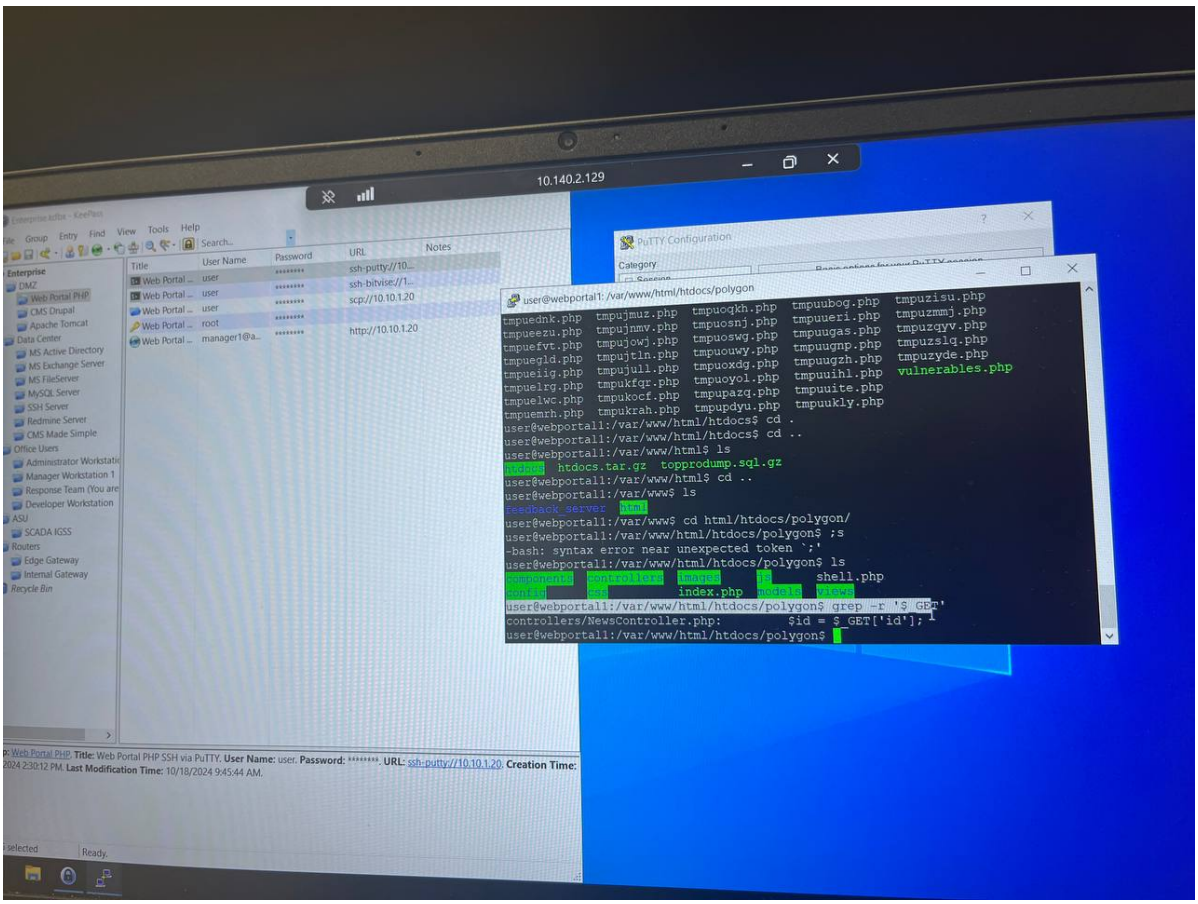

Рис. 2.9: Поиск места уязвимого параметра

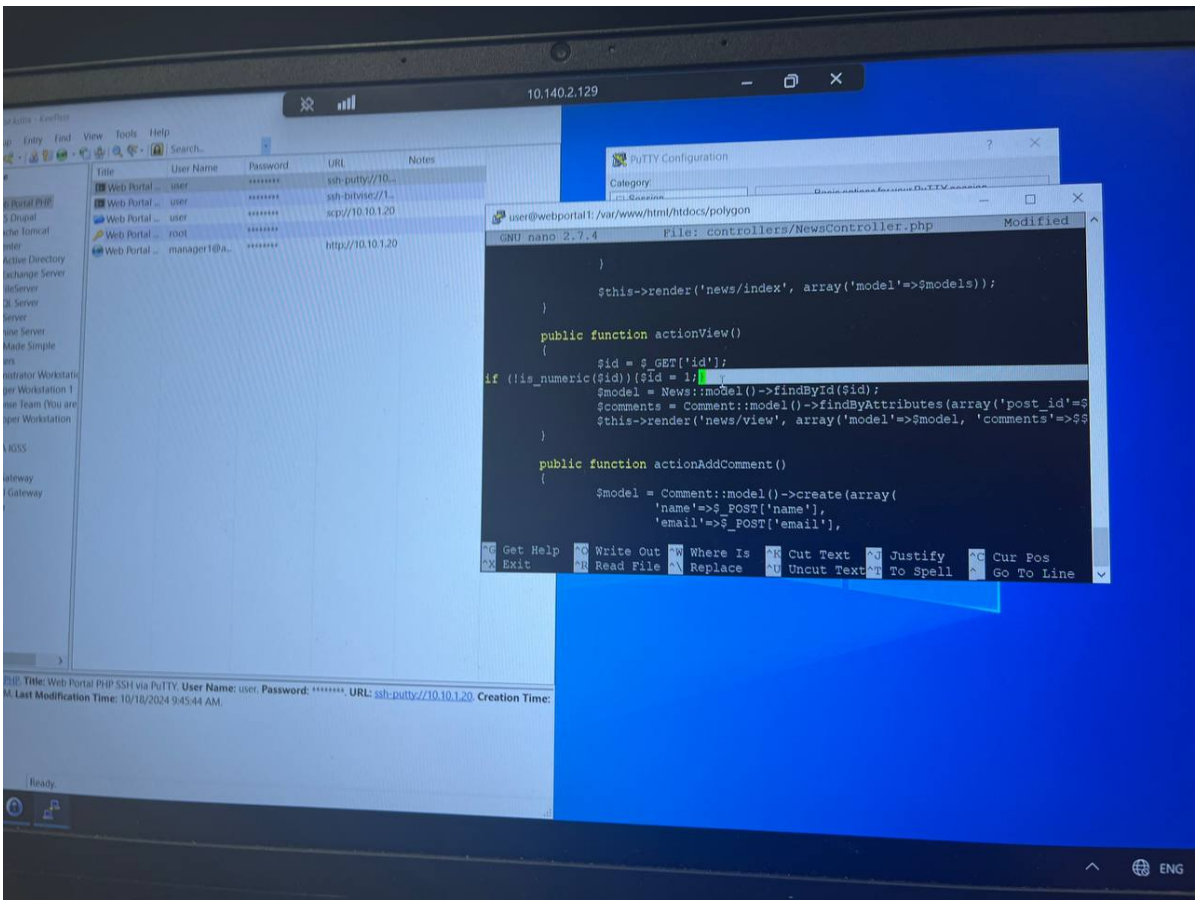

Рис. 2.10: Измененная функция actionView

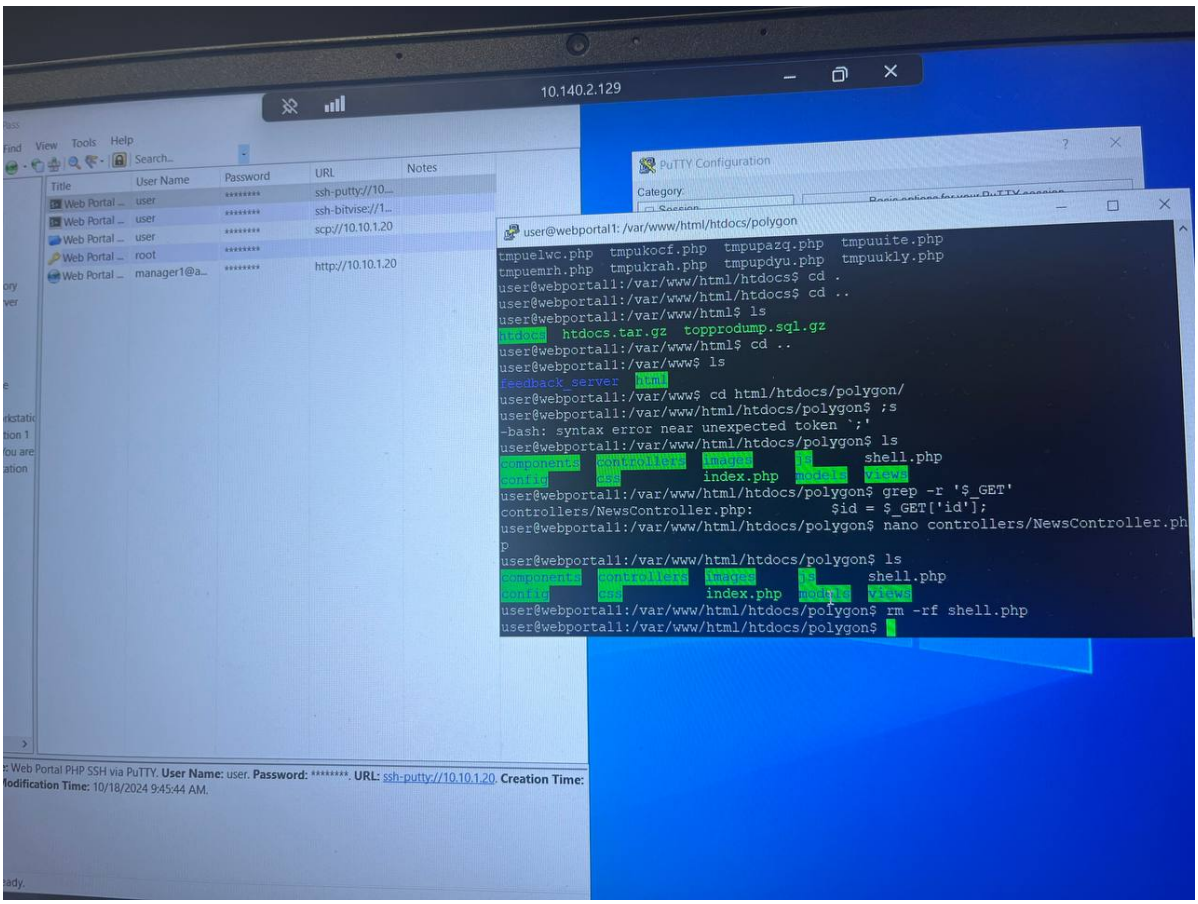

Рис. 2.11: Удаление вредоносного файла

После изменений уязвимость устранена.

2.2.2 Последствие: Web portal meterpreter

Нарушитель установил shell-сессию. Мы проверили сокеты командой ss -tp (рис. 2.12) и завершили сессию: sudo ss -K dst HACKER_IP dport=HACKER_PORT (рис. 2.13).

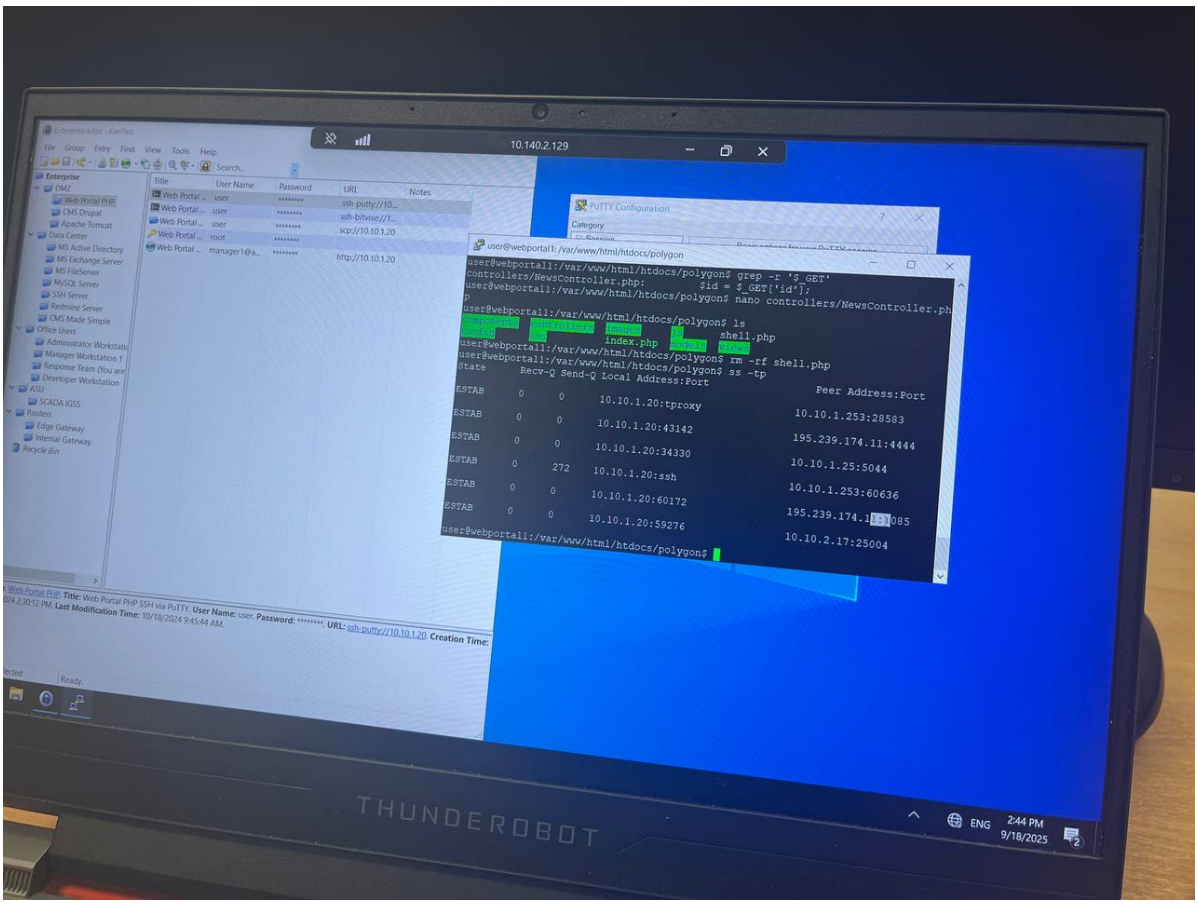

Рис. 2.12: Список установленных соединений

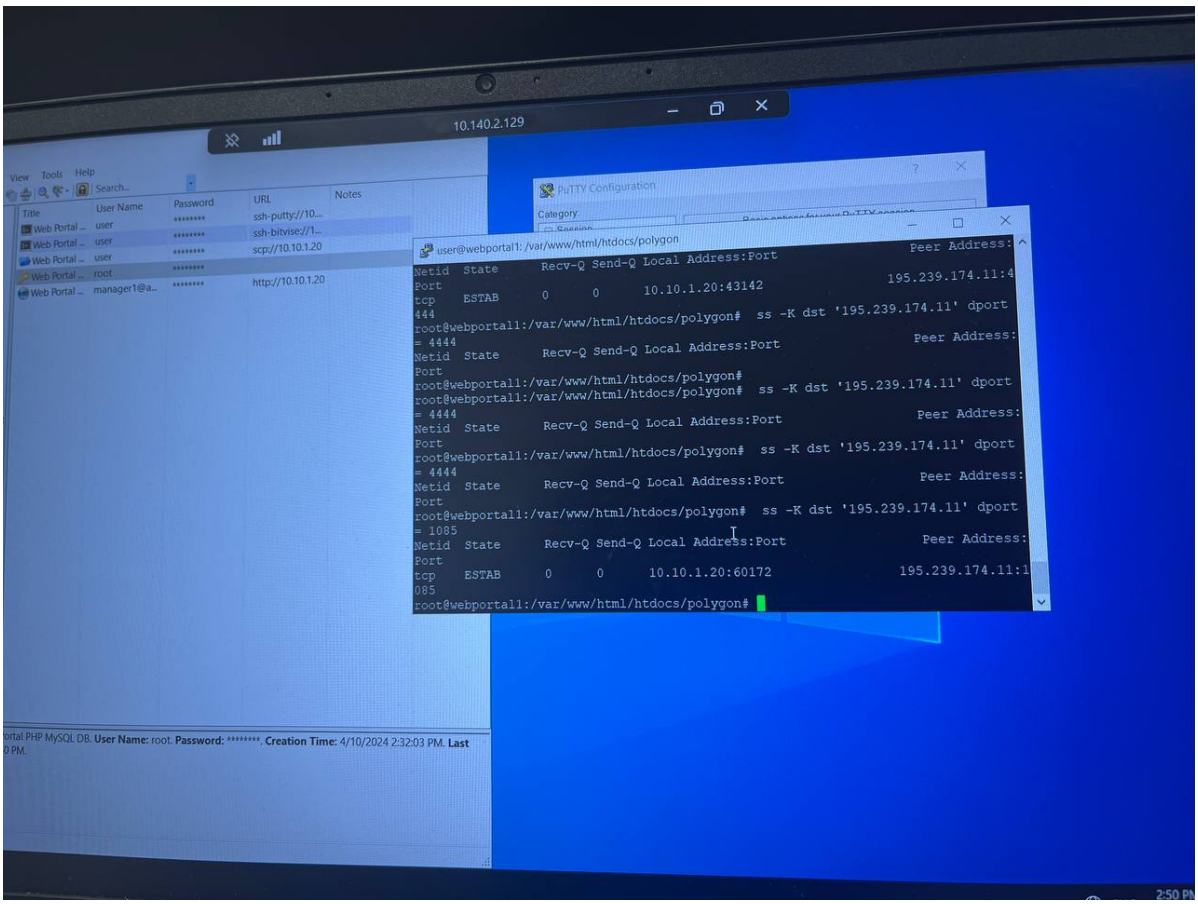

Рис. 2.13: Завершение сессий

Сессии завершены.

2.2.3 Отключенная защита антивируса

На Administrator Workstation отключена реал-тайм защита Windows Defender, что позволило запустить diag.ps1. Удалили запись в реестре: REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware (рис. 2.14) Перезапустили Virus & Threat Protection и включили Real-time Protection (рис. 2.15) Перезагрузили систему.

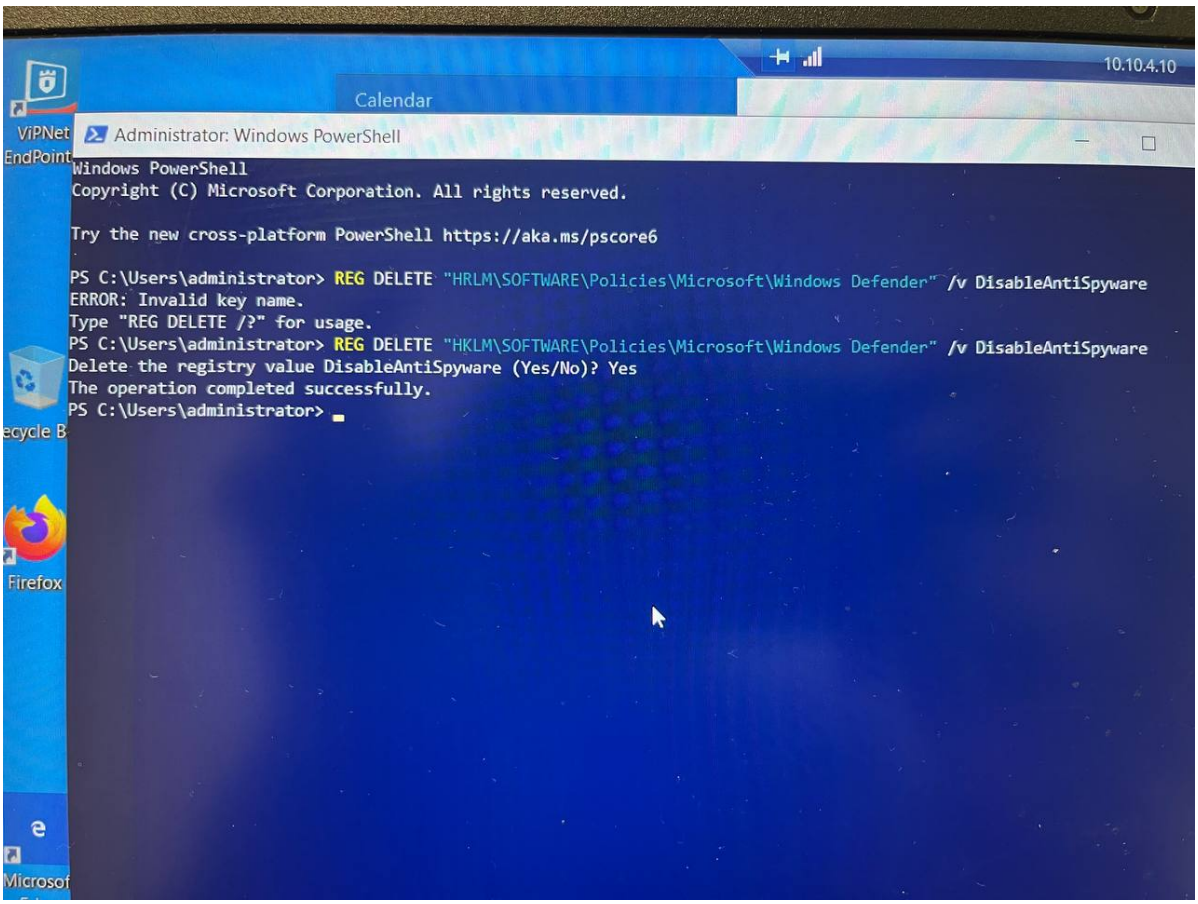

Рис. 2.14: Удаление записи DisableAntiSpyware

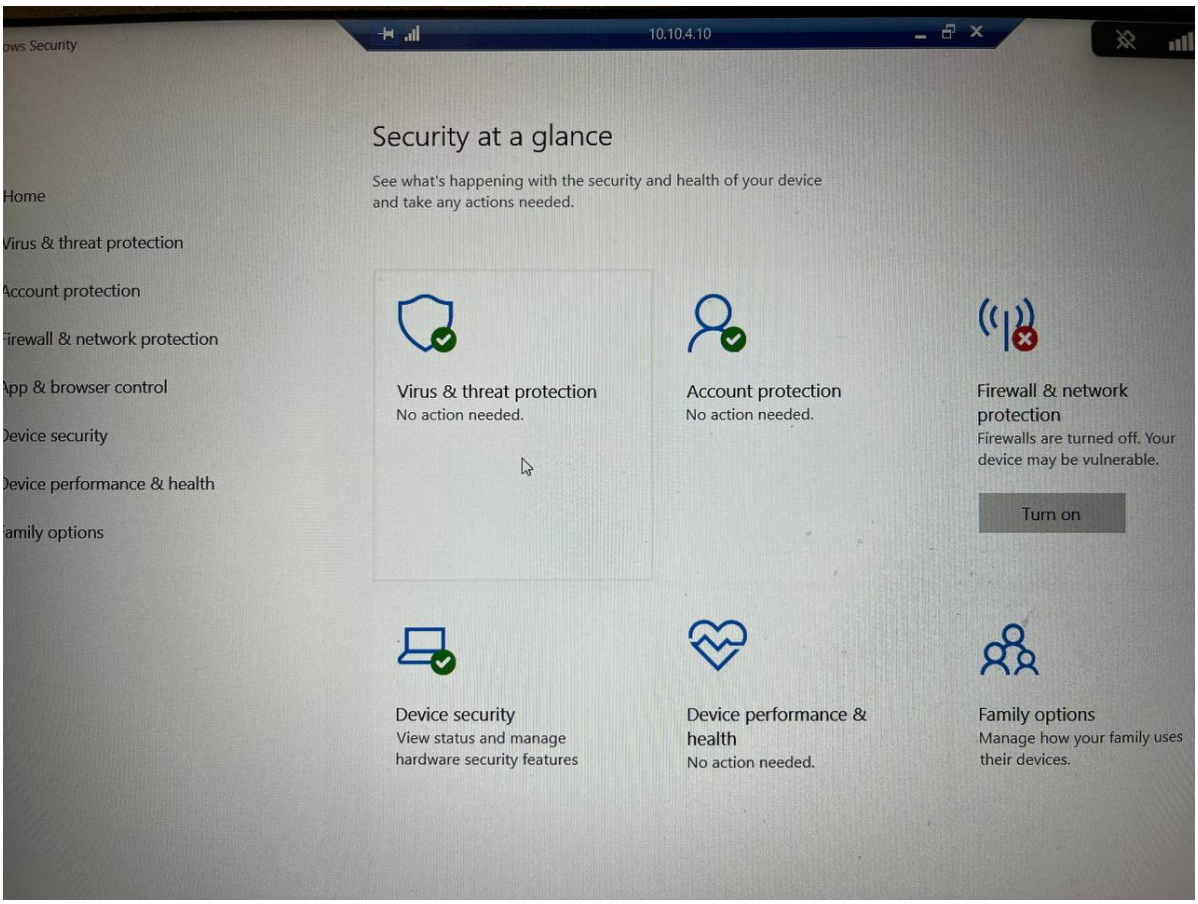

Рис. 2.15: Включение Real-time Protection

2.2.4 Последствие: Admin meterpreter

Сессия обнаружена netstat -ano (рис. 2.16) Завершили: taskkill /f /pid <PID> (рис. 2.17)

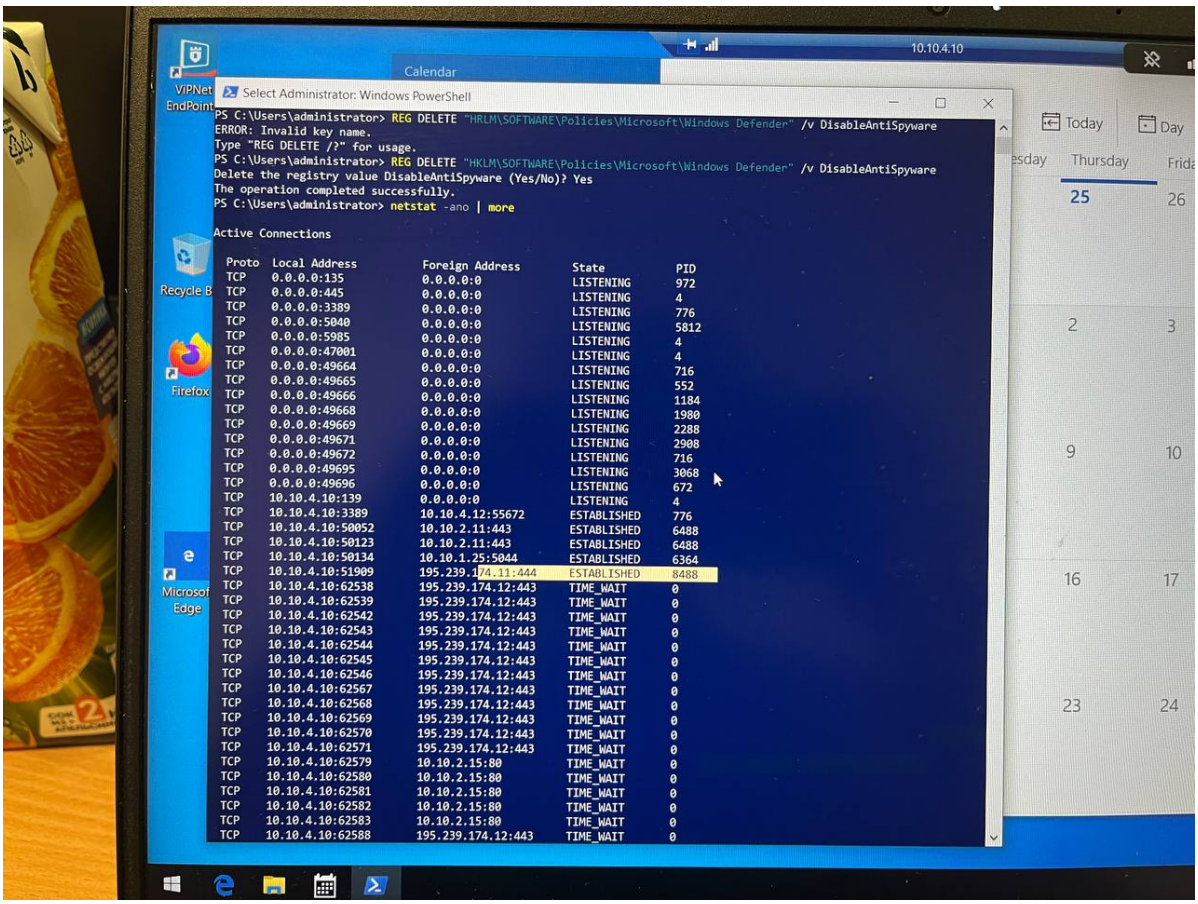

Рис. 2.16: Соединение с машиной нарушителя

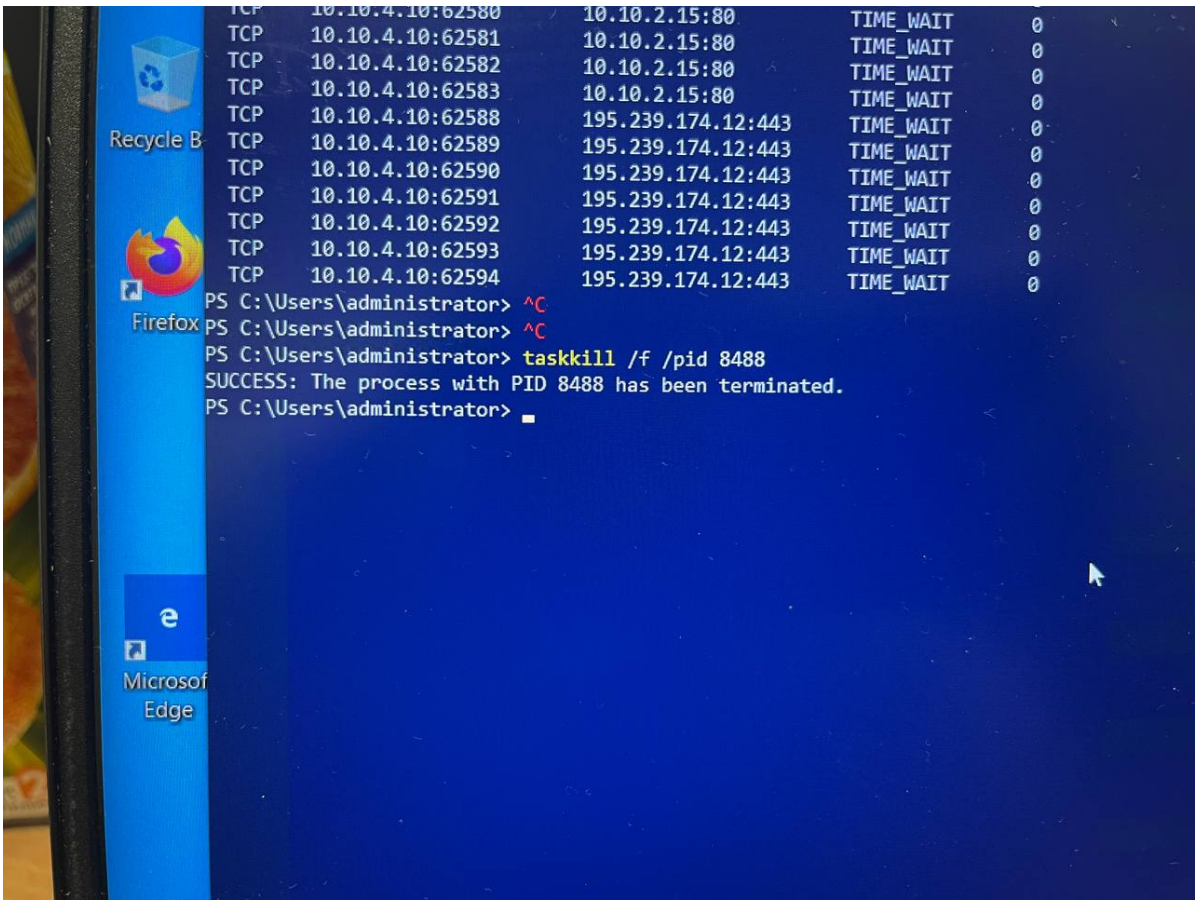

Рис. 2.17: Остановка процесса

Сессия завершена.

2.2.5 Слабый пароль учетной записи

На MS Active Directory слабый пароль администратора позволил brute-force по RDP (код события 1149). (рис. 2.18) Изменили пароль: net user Administrator * (рис. 2.19)

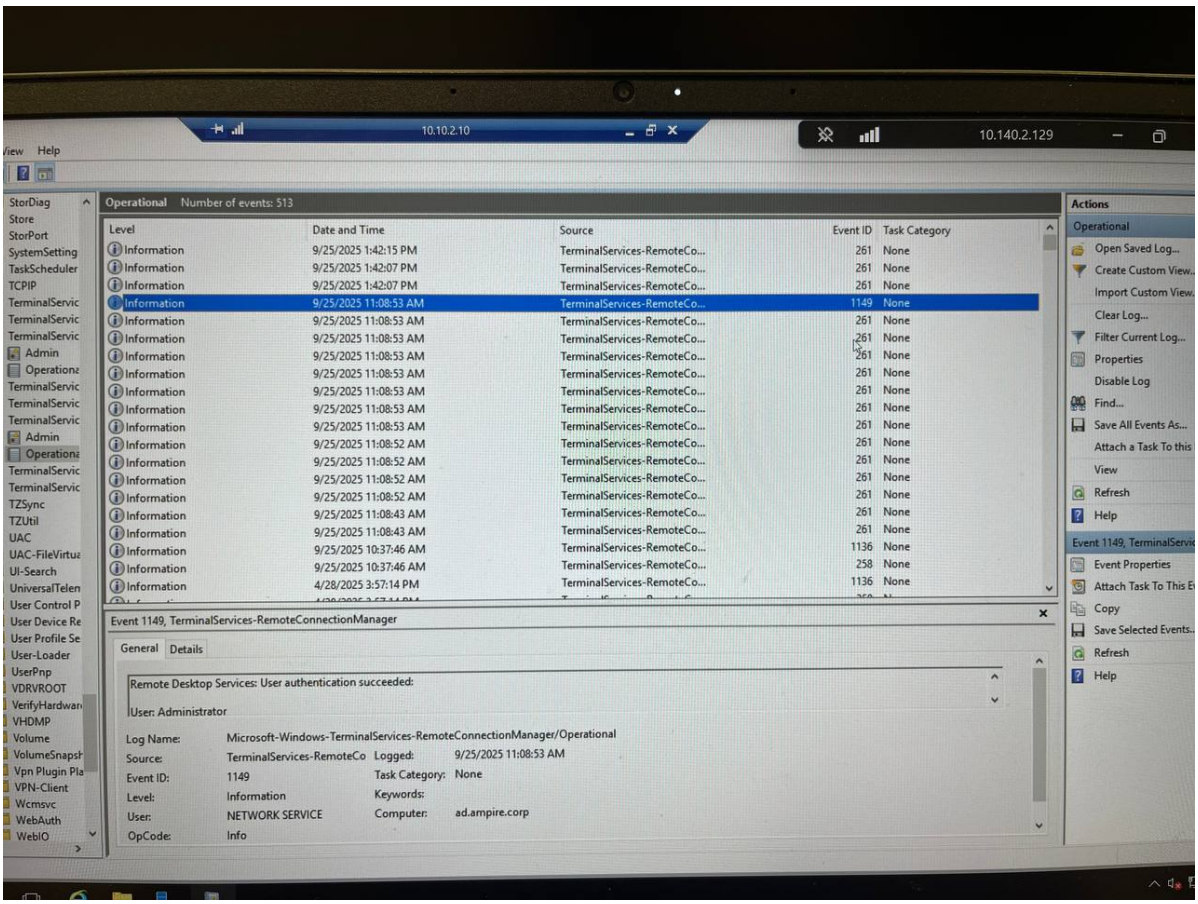

Рис. 2.18: Логи подключений по RDP

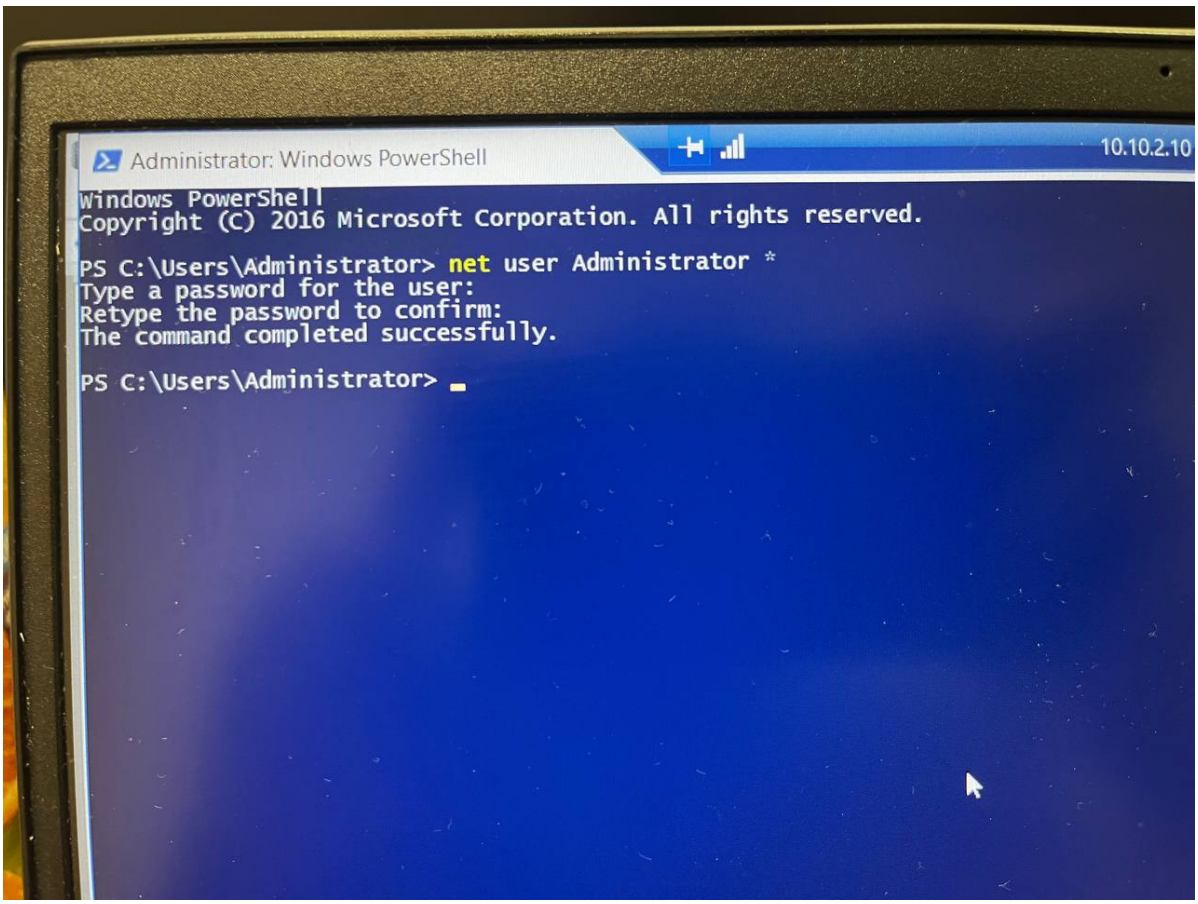

Рис. 2.19: Изменение пароля

Уязвимость устранена.

2.2.6 Последствие: AD User

Добавление пользователя “Hacked” отслежено в Event Viewer (ID 4720, Рисунок 16). Удалили в Active Directory Users and Computers (рис. 2.20) (рис. 2.21)

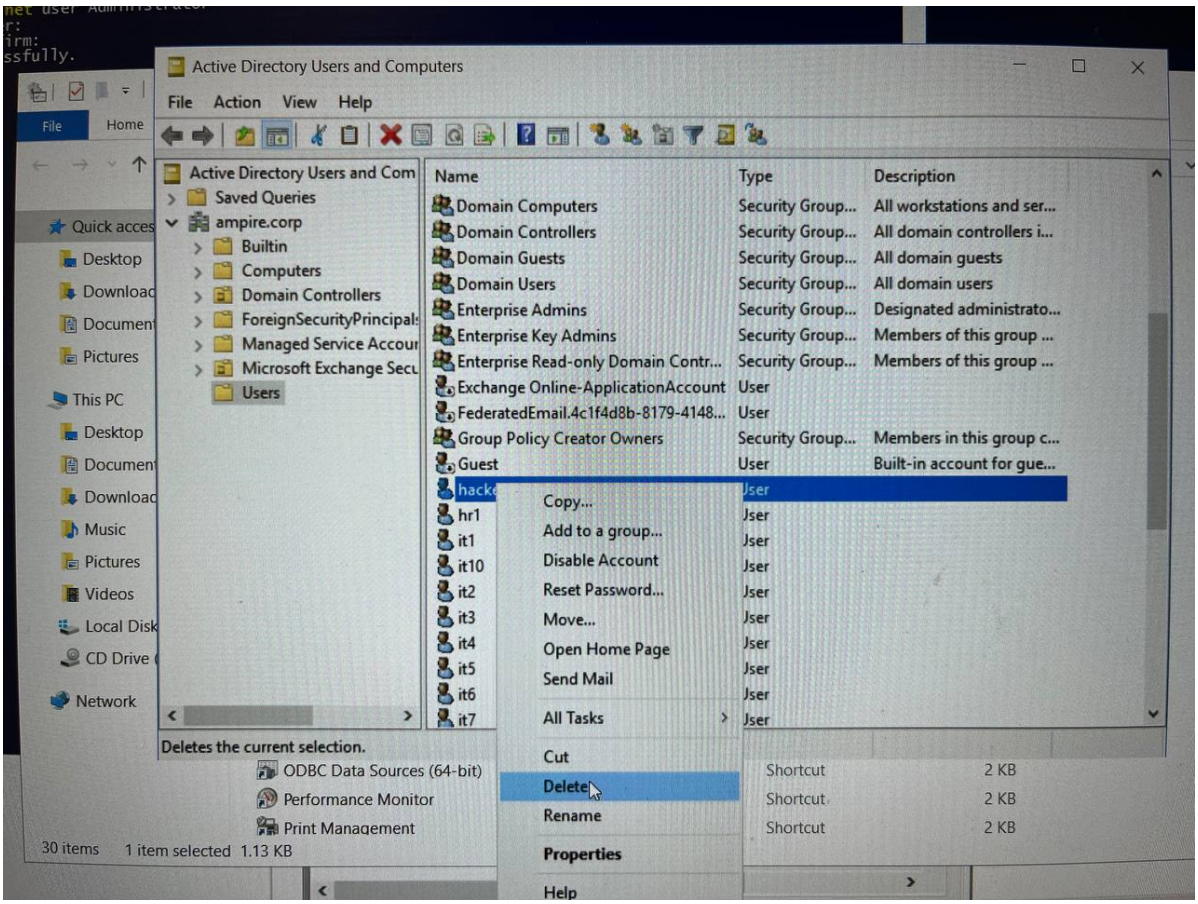

Рис. 2.20: Лог добавления нового пользователя

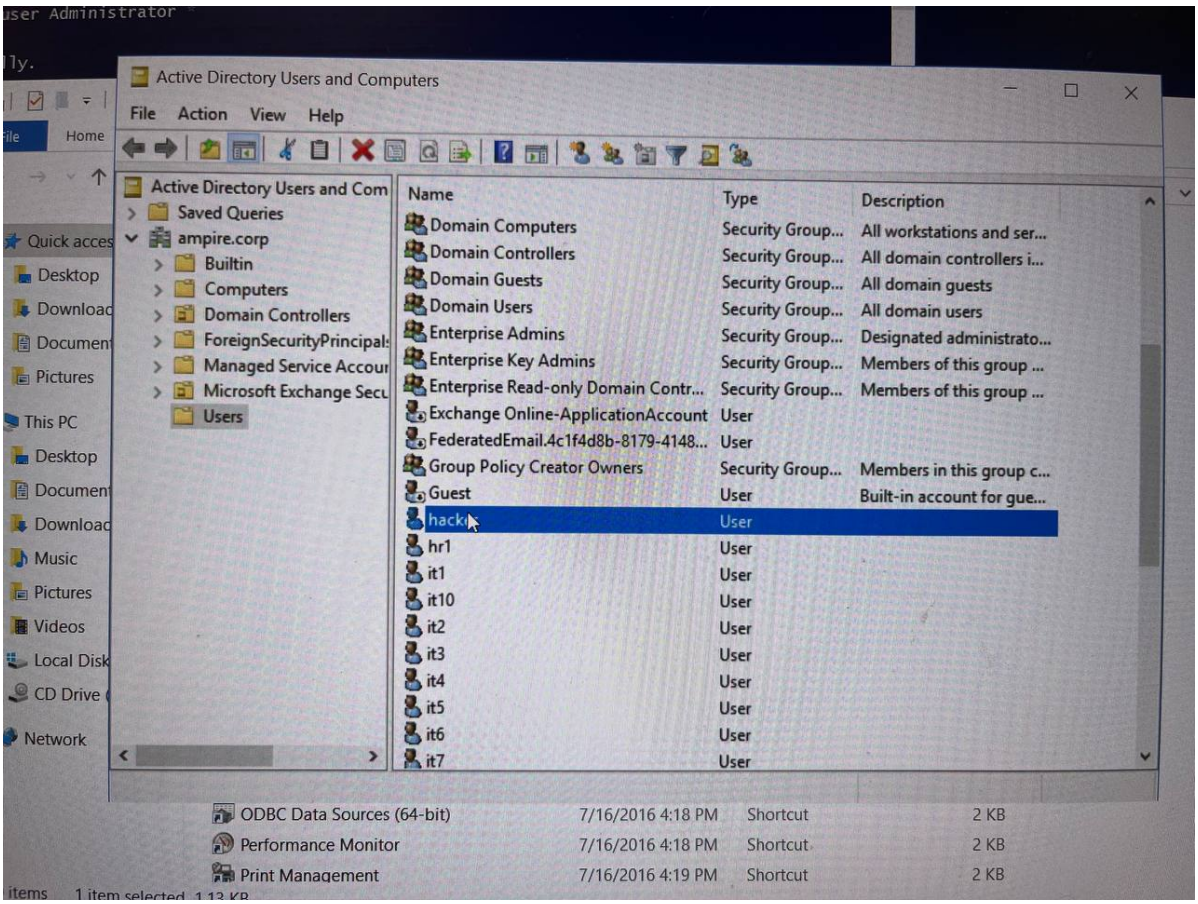

Рис. 2.21: Удаление пользователя

Пользователь удален.

Уязвимости устранены, мы научились находить инциденты несанкционированного доступа, находить последствия и исправлять уязвимости и их последствия на контролируемой системе(рис. 2.22)

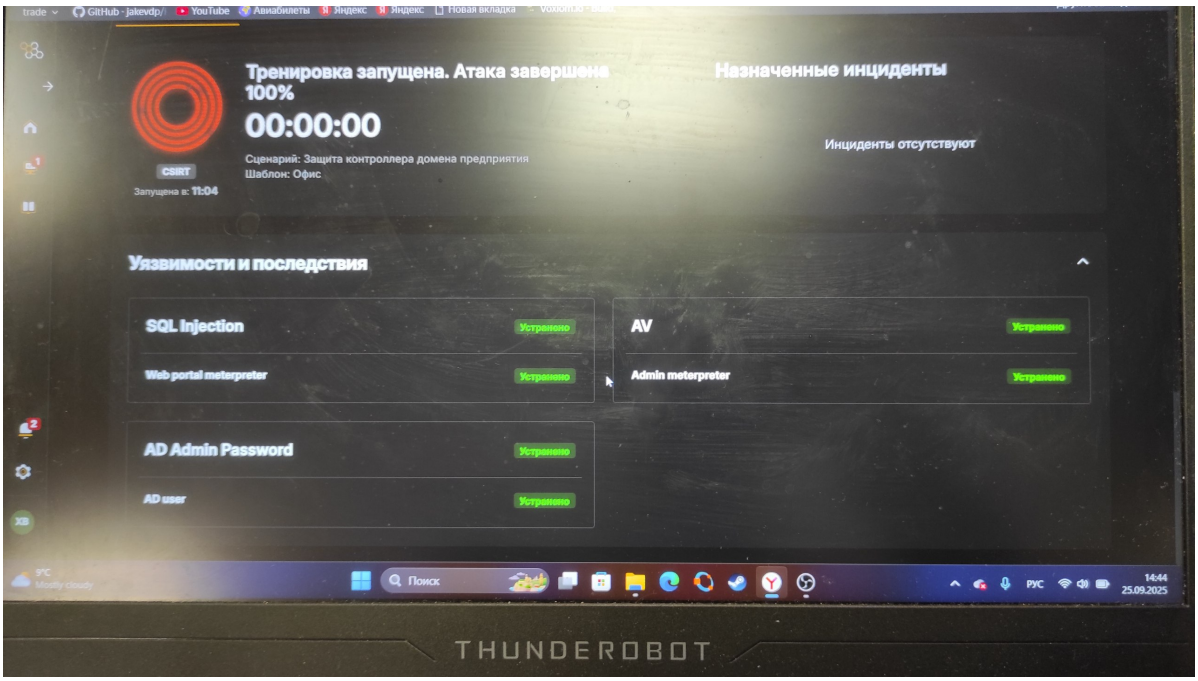

Рис. 2.22: Итоговый результат

3 Выводы

В рамках учебно-практического занятия на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» мы выполнили сценарий №2 «Защита контроллера домена предприятия».

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам компании. Обнаружив несколько уязвимостей на внешнем периметре и закрепившись на одном из серверов, злоумышленник проводит разведку корпоративной сети с целью захватить контроллер домена.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации. Злоумышленник обладает опытом проведения почтовых фишинговых рассылок.

Уровень сложности сценария — 7 (из 10). Мы успешно выявили уязвимости, проанализировали последствия атаки, устранили их и отработали методы детектирования с использованием инструментов ViPNet IDS NS, ViPNet TIAS и Security Onion.