

## Лабораторная работа №2

### Кибербезопасность предприятия

---

НКНбд-01-22; Аристид Жан, Акопян Сатеник, Кадров Виктор, Нве Манге Хосе Херсон  
Мико, Эспиноса Висилита Кристина Микаела, НПИбд-01-22; Стариakov Данила, НФИбд-02-22;  
Чемоданова Ангелина

## Цель работы

---

Основная цель данной лабораторной работы заключается в выполнении тренировки “Защита контроллера домена предприятия” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы необходимо освоить практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоить навыки отработки действий по нейтрализации последствий успешных атак.

## Легенда “Защита интеграционной платформы”

---

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.

Последовательность действий нарушителя следующая:

1. Нарушитель проводит сканирование сети 195.239.174.0/24 и находит веб-сервер. Далее сканирует веб-сервер на предмет SQL-инъекций утилитой sqlmap. Нарушитель генерирует php reverse shell, используя найденную SQL-инъекцию, загружает вредоносный файл на веб-сервер. Для закрепления на хосте нарушитель устанавливает meterpreter-соединение.
2. Нарушитель определяет маршрут к сети 10.10.2.0/24, сканирует сеть и находит почтовый сервер. Нарушитель генерирует письмо с вредоносным вложением и отправляет администратору.

3. Администратор открывает письмо, запускается вредоносный скрипт.
4. Нарушитель получает контроль над компьютером администратора и meterpreter-сессию.
5. Нарушитель находит AD&DNS сервер, проверяет, открыт ли порт 3389 (стандартный порт RDP). В случае открытого порта 3389 пытается с помощью инструмента hydra получить доступ к AD&DNS серверу, перебирая пароль по словарю. Для закрепления на контроллере домена нарушитель добавляет нового привилегированного пользователя.

Уязвимости и последствия:

- SQL-инъекция -> Web portal meterpreter
- Отключенная защита антивируса -> Admin meterpreter
- Слабый пароль учетной записи -> Добавление привилегированного пользователя

## Первый инцидент

---

Сетевой сенсор ViPNet IDS NS детектирует события сканирования веб-сервера на предмет SQL-инъекций, использование определенного типа инъекции (Blind SQL-Injection), а также загрузку вредоносного файла с php скриптом и выставление права доступа на выполнение.

# Первый инцидент

ViNet IDS NS

События

События за последние 24 часа

У...	Дата и время	Название правила	Класс	Про...	IP-адрес исто...	Порт ...	IP-адрес получа...	Порт пол...
●	17:38:33.601 23.10....	AM EXPLOIT Generic Possible XSS in URI: 'script' in request var 2	web-ap...	TCP	195.239.174.11	57858	10.10.1.20	80
●	17:38:33.601 23.10....	AM EXPLOIT Generic URL XSS attempt	web-ap...	TCP	195.239.174.11	57858	10.10.1.20	80
●	17:38:33.601 23.10....	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT in HTTP URI	web-ap...	TCP	195.239.174.11	57858	10.10.1.20	80
●	17:38:33.601 23.10....	AM EXPLOIT Generic Path Traversal in HTTP URI var 3	web-ap...	TCP	195.239.174.11	57858	10.10.1.20	80
●	17:38:28.370 23.10....	AM SQL Generic SQLi in HTTP URI: 'SELECT CASE' query	web-ap...	TCP	195.239.174.11	54026	10.10.1.20	80
●	17:38:28.370 23.10....	AM SQL [ET] Generic SQLi in HTTP URI: 'SELECT VERSION' query	web-ap...	TCP	195.239.174.11	54026	10.10.1.20	80
●	17:38:28.337 23.10....	AM SQL Generic SQLi in HTTP URI: 'SELECT CASE' query	web-ap...	TCP	195.239.174.11	54010	10.10.1.20	80
●	17:38:28.209 23.10....	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query	web-ap...	TCP	195.239.174.11	53934	10.10.1.20	80
●	17:38:28.209 23.10....	AM SQL Generic SQLi in HTTP URI: 'SELECT CONCAT' query	web-ap...	TCP	195.239.174.11	53934	10.10.1.20	80
●	17:38:28.209 23.10....	ET WEB_SERVER MySQL SELECT CONCAT SQL Injection Attempt	web-ap...	TCP	195.239.174.11	53934	10.10.1.20	80
●	17:38:28.209 23.10....	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query var2	web-ap...	TCP	195.239.174.11	53934	10.10.1.20	80
●	17:38:28.197 23.10....	AM SQL Generic SQLi in HTTP URI: 'SELECT CONCAT' query	web-ap...	TCP	195.239.174.11	53926	10.10.1.20	80
●	17:38:28.197 23.10....	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query	web-ap...	TCP	195.239.174.11	53926	10.10.1.20	80
●	17:38:28.197 23.10....	ET WEB_SERVER MySQL SELECT CONCAT SQL Injection Attempt	web-ap...	TCP	195.239.174.11	53926	10.10.1.20	80
●	17:38:28.197 23.10....	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query var2	web-ap...	TCP	195.239.174.11	53926	10.10.1.20	80
●	17:38:28.178 23.10....	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query	web-ap...	TCP	195.239.174.11	53898	10.10.1.20	80

Страница 1 из 1

Показывать 300 объектов

Рис. 1: Сканирование на предмет SQL-инъекций

# Первый инцидент

VIPNet IDS NS

События

События за последние 24 часа

У...	Дата и время	Название правила	Класс	Про...	IP-адрес источ...	Порт ...	IP-адрес получа...	Порт полу...
●	17:38:45.015	23.10.... AM SQL Generic SQLi in HTTP URI: 'ORDER BY' query	web-ap...	TCP	195.239.174.11	52800	10.10.1.20	80
●	17:38:44.998	23.10.... AM SQL Generic SQLi in HTTP URI: 'ORDER BY' query	web-ap...	TCP	195.239.174.11	52786	10.10.1.20	80
●	17:38:44.987	23.10.... AM SQL Generic SQLi in HTTP URI: 'ORDER BY' query	web-ap...	TCP	195.239.174.11	52774	10.10.1.20	80
●	17:38:44.970	23.10.... AM SQL Generic SQLi in HTTP URI: 'ORDER BY' query	web-ap...	TCP	195.239.174.11	58170	10.10.1.20	80
●	17:38:39.950	23.10.... ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-ap...	TCP	195.239.174.11	58186	10.10.1.20	80
●	17:38:39.950	23.10.... AM SQL SLEEP function in GET - Possible Blind SQL Injection Attempt	client-si...	TCP	195.239.174.11	58186	10.10.1.20	80
●	17:38:39.950	23.10.... AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	client-si...	TCP	195.239.174.11	58186	10.10.1.20	80
●	17:38:39.950	23.10.... AM SQL Generic SQLi in HTTP URI: 'SELECT SLEEP' query	web-ap...	TCP	195.239.174.11	58186	10.10.1.20	80
●	17:38:39.940	23.10.... ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-ap...	TCP	195.239.174.11	58164	10.10.1.20	80
●	17:38:39.940	23.10.... AM SQL SLEEP function in GET - Possible Blind SQL Injection Attempt	client-si...	TCP	195.239.174.11	58164	10.10.1.20	80
●	17:38:39.940	23.10.... AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	client-si...	TCP	195.239.174.11	58164	10.10.1.20	80
●	17:38:39.940	23.10.... AM SQL Generic SQLi in HTTP URI: 'SELECT SLEEP' query	web-ap...	TCP	195.239.174.11	58164	10.10.1.20	80
●	17:38:38.233	23.10.... AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query	web-ap...	TCP	195.239.174.11		10.10.1.20	80
●	17:38:38.233	23.10.... AM SQL Generic SQLi in HTTP URI: 'SELECT CONCAT' query	web-ap...	TCP	195.239.174.11		10.10.1.20	80
●	17:38:38.233	23.10.... ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	web-ap...	TCP	195.239.174.11		10.10.1.20	80
●	17:38:38.233	23.10.... AM SQL Generic SQLi in HTTP URI: UNION SELECT query var2	web-ap...	TCP	195.239.174.11		10.10.1.20	80

Страница 1 из 1

Показывать 300 объектов

Рис. 2: Детектирование SQL-инъекции

# Первый инцидент

The screenshot shows the ViPNet IDS NS web interface. On the left, a list of events is displayed for the last 24 hours. One specific event is highlighted in blue. On the right, a detailed view of this event is shown.

**События**

События за последние 24 часа

У...	Дата и время	Название правила	Класс
●	17:38:45.540 23.10...	AM SQL Generic SQLi in HTTP URI: 'SELECT LOAD_FILE' query	web-application
●	17:38:45.540 23.10...	ET WEB_SERVER Possible SQL Injection SELECT CAST in HTTP URI	attempted-admin
●	17:38:45.513 23.10...	AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt	web-application
●	17:38:45.513 23.10...	AM SQL Generic SQLi in HTTP URI: 'SELECT DUMPFILE' query	web-application
●	17:38:45.513 23.10...	AM EXPLOIT Generic Possible PHP Injection: hex encoded PHP Tag in HTTP request	web-application
●	17:38:45.455 23.10...	AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt	web-application
●	17:38:45.455 23.10...	AM SQL Generic SQLi in HTTP URI: 'SELECT DUMPFILE' query	web-application
●	17:38:45.455 23.10...	AM EXPLOIT Generic Possible PHP Injection: hex encoded PHP Tag in HTTP request	web-application
●	17:38:45.404 23.10...	AM SQL Generic SQLi in HTTP URI (double encoded) var 1	web-application
●	17:38:45.404 23.10...	AM SQL Generic SQLi in HTTP URI: 'INTO OUTFILE' query	web-application
●	17:38:45.404 23.10...	ET WEB_SERVER Possible SQL Injection INTO OUTFILE Arbitrary File Write Attempt	web-application
●	17:38:45.404 23.10...	AM EXPLOIT Generic Possible PHP Injection: hex encoded PHP Tag in HTTP request	web-application
●	17:38:45.360 23.10...	AM SQL Generic SQLi in HTTP URI: 'SELECT CASE' query	web-application
●	17:38:45.360 23.10...	ET WEB_SERVER Possible attempt to enumerate MS SQL Server version	attempted-admin
●	17:38:45.347 23.10...	AM SQL Generic SQLi in HTTP URI: 'SELECT CASE' query	web-application
●	17:38:45.347 23.10...	AM SQL [ET] Generic SQLi in HTTP URI: 'SELECT VERSION' query	web-application

Событие 17:38:45.455 23.10.2025

Событие Источник Получатель Пакет

**Общая информация**

Дата и время	17:38:45.455 23.10.2025
Интерфейс захвата	eth2
Уровень важности	Высокий
Тип события	Сигнатурное событие
Протокол	TCP
Код события	3000708
Клиентское приложение	sqlmap/1.7.2#stable (https://sqlmap.org)
Доменное имя ресурса	195.239.174.95

**Правило анализа**

Класс	web-application-attack
Группа	sql
Название	AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt
Описание:	Правило обнаруживает атаки на реляционную базу данных SQL.
Текст:	alert top \$EXTERNAL_NET any > \$HOME_NET \$HTTP_PORTS (msg: "AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt";flow: to_server,establish;

Рис. 3: Загрузка вредоносного файла и выставление права доступа на выполнение

# Первый инцидент

SQL-инъекция

Основная информация Чат

Закрытый

Дата и время события ①  
20.10.2025 19:30

Описание ①  
На узле Web Server PHP находится уязвимый веб-сервис на 80 порту. Нарушитель использует данную уязвимость для загрузки и для выполнения php reverse shell. Используя уязвимый параметр id, нарушитель успешно загружает вредоносный файл на веб-сервер.

Индикаторы компрометации ①  
- подозрительные файлы, приложения или процессы; - аномально высокое количество обращений к одному файлу;

Рекомендации ①  
Внесение изменений в конфигурационный файл

Прикреплённые файлы ①

Оценка  
☆ ☆ ☆ ☆ ☆

Автор  
Чемоданова Ангелина  
@1132226443@pfur.ru

Ответственный  
Кадров Виктор  
@1132226454@pfur.ru

Источник  
195.239.174.11

Поражённые активы  
10.10.1.20

Рис. 4: Карточка первого инцидента

## Устранение уязвимости “SQL-инъекция”

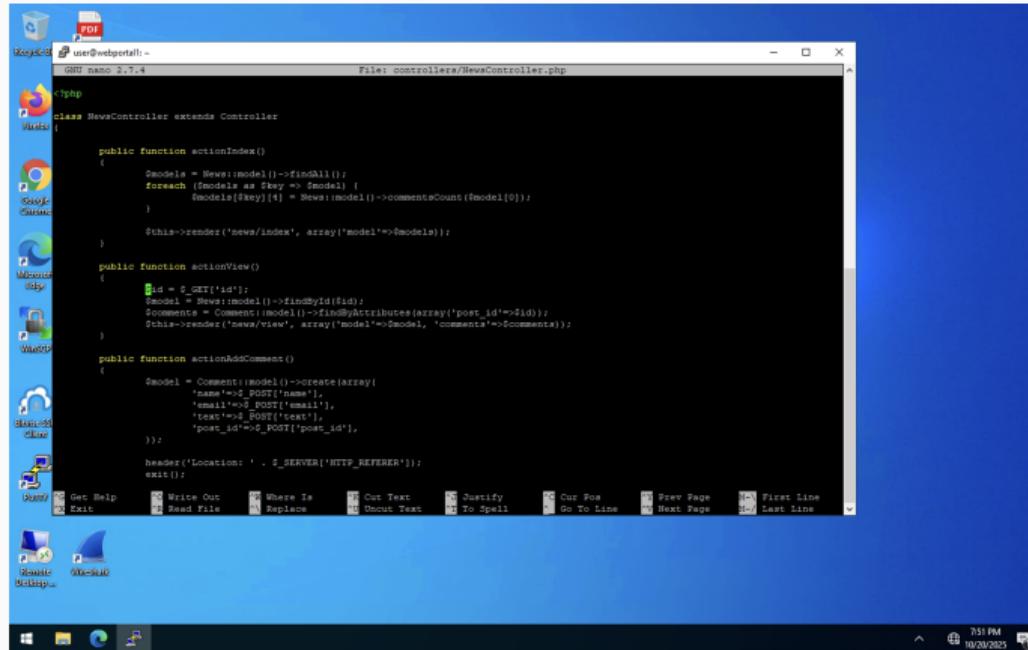
Решение: известно, что \$id является уязвимым параметром, следует проверять тип данного параметра. Требуется найти место кода, где данный параметр считывается из GET запроса.

```
user@webportal1:~$ su root
Password:
root@webportal1:/home/user# cd /var/html/
bash: cd: /var/html/: No such file or directory
root@webportal1:/home/user# cd /var/www/html/htdocs/polygon/
root@webportal1:/var/www/html/htdocs/polygon# ls
components controllers images js shell.php
config css index.php models views
root@webportal1:/var/www/html/htdocs/polygon# nano config/
config/controllers/
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/
NewsController.php SiteController.php
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/NewsController.ph
■
```

Рис. 5: Поиск места уязвимого параметра

# Устранение уязвимости “SQL-инъекция”

Считывание параметра сайта происходит в функции actionView() в файле NewsController.php.



```
user@webportal: ~
File: controllers/NewsController.php
nano 2.7.4
cryptp
class NewsController extends Controller
{
    public function actionIndex()
    {
        $models = News::model()->findAll();
        foreach ($models as $key => $model) {
            $models[$key]['commentsCount'] = News::model()->commentsCount($model[0]);
        }
        $this->render('news/index', array('model'=>$models));
    }

    public function actionView()
    {
        $id = $_GET['id'];
        $model = News::model()->findById($id);
        $comments = Comment::model()->findByNameAttributes(array('post_id'=>$id));
        $this->render('news/view', array('model'=>$model, 'comments'=>$comments));
    }

    public function actionAddComment()
    {
        $model = Comment::model()->create(array(
            'name'=>$_POST['name'],
            'email'=>$_POST['email'],
            'text'=>$_POST['text'],
            'post_id'=>$_POST['post_id'],
        ));
        header('Location: ' . $_SERVER['HTTP_REFERER']);
        exit();
    }
}
```

Рис. 6: Параметры уязвимой функции

## Устранение уязвимости “SQL-инъекция”

---

Для проверки типа \$id используется функция `is_numeric`, которая возвращает `True` в случае, если `$id` – число, иначе – `False`. В случае успешной проверки параметр `$id` будет передаваться в запрос, иначе – запрос будет статичным и независимым от `$id`.

## Устранение уязвимости “SQL-инъекция”

The screenshot shows a terminal window with the nano 2.7.4 editor open. The file is named controllers/NewsController.php. The code is a PHP class NewsController extending Controller. It contains three methods: actionIndex, actionView, and actionAddComment. The actionView method is highlighted with a red box around the line where \$id is checked for numericity. The terminal window includes standard nano navigation and search keys at the bottom.

```
GNU nano 2.7.4                               File: controllers/NewsController.php                                Modified ^

<?php

class NewsController extends Controller
{
    public function actionIndex()
    {
        $models = News::model()->findAll();
        foreach ($models as $key => $model) {
            $models[$key][4] = News::model()->commentsCount($model[0]);
        }
        $this->render('news/index', array('model'=>$models));
    }

    public function actionView()
    {
        $id = $_GET['id'];
        if (!is_numeric($id)){
            $id = 1;
        }
        $model = News::model()->findById($id);
        $comments = Comment::model()->findByAttributes(array('post_id'=>$id));
        $this->render('news/view', array('model'=>$model, 'comments'=>$comments));
    }

    public function actionAddComment()
    {
        $model = Comment::model()->create(array(
            'name'=>$_POST['name'],
            'email'=>$_POST['email'],
            'text'=>$_POST['text'],
            'post_id'=>$_POST['post_id'],
        ));
    }
}

Get Help      C Write Out      M Where Is      K Cut Text      J Justify      C Cur Pos      N Prev Page      F First Line
Exit         R Read File      R\ Replace      U Uncut Text      I To Spell      G Go To Line      N Next Page      L Last Line
```

Рис. 7: Измененная функция actionView с проверкой типа параметра \$id

## Последствие Web portal meterpreter

Нарушитель устанавливает shell сессию с веб- порталом PHP. Для обнаружения последствия необходимо проверить сокеты уязвимой машины при помощи утилиты ss с ключами -tp. На скриншоте ниже изображено активное соединение веб-портала с IP-адресом нарушителя (195.239.174.11). Необходимо устранить соединение, воспользовавшись командой kill.

```
root@webportall:~# ss -tp
State      Recv-Q Send-Q          Local Address:Port          Peer Address:Port
ESTAB      0      0              10.10.1.20:43908          195.239.174.11:4444
users:(("x2E2a3",pid=1678,fd=3))
ESTAB      0      0              10.10.1.20:48842          10.10.1.25:5044
users:(("filebeat",pid=698,fd=5))
ESTAB      0      0              10.10.1.20:42954          10.10.2.17:25004
users:(("epp_agentd",pid=1533,fd=35))
SYN-SENT   0      1              10.10.1.20:50236          195.239.174.125:puppet
users:(("puppet",pid=28142,fd=6))
ESTAB      0      0              10.10.1.20:tproxy          10.10.1.253:61576
users:(("sezver",pid=620,fd=8))
ESTAB      0      352             10.10.1.20:ssh            10.10.1.253:46696
users:(("sshd",pid=21936,fd=4),("sshd",pid=21907,fd=4))
CLOSE-WAIT  1      0              ::ffff:10.10.1.20:http        ::ffff:195.239.174.11:37466
users:(("apache2",pid=19699,fd=13))
root@webportall:~# ss -tp
root@webportall:~# kill 1678
root@webportall:~#
```

Рис. 8: Завершение сессии с нарушителем

В результате выполнения команды сессия с нарушителем завершена, последствие Web portal meterpreter успешно устранено.

## Второй инцидент

---

Один из способов проверки состояния защиты в реальном времени Windows Defender – в Powershell ввести команду Get-MpPreference и проверить значение параметра DisableRealtimeMonitoring. Если значение – True, то защита в реальном времени выключена.

## Второй инцидент

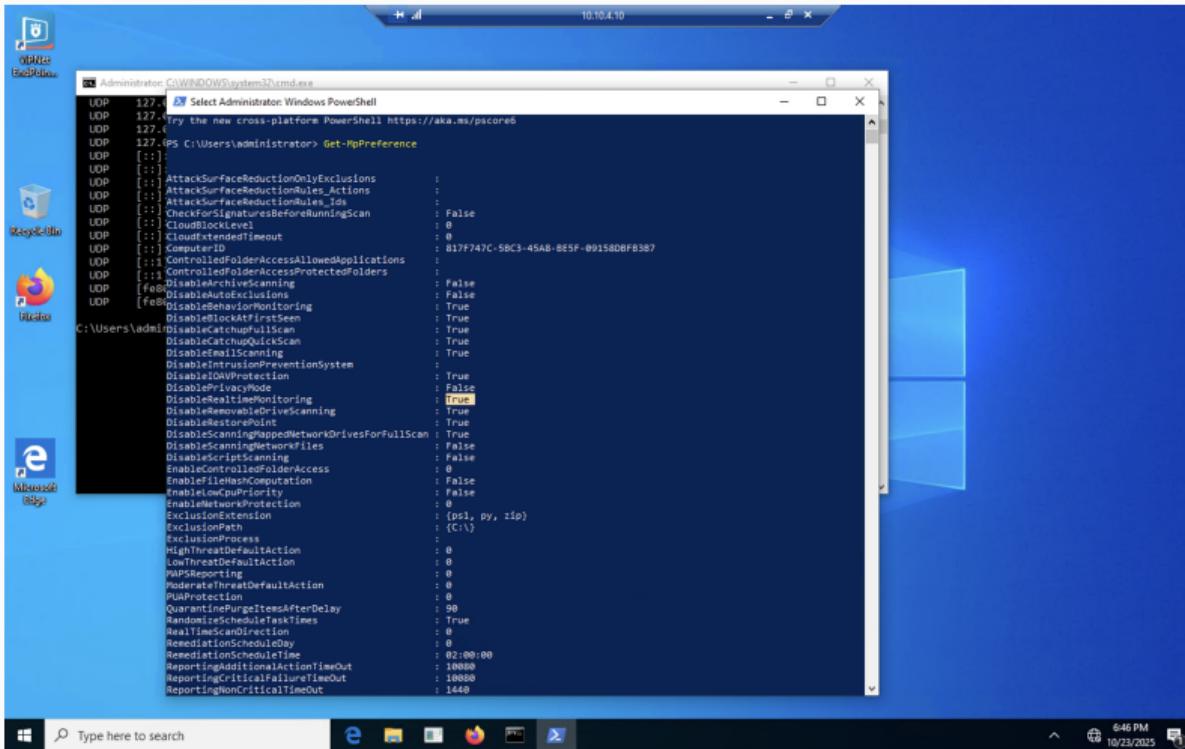


Рис. 9: Настройки Windows Defender

## Второй инцидент

### Доступ к компьютеру админа

Основная информация Чат Закрытый

**Дата и время события** ①  
20.10.2025 19:28

**Описание** ①  
Нарушитель генерирует письмо с вредоносным вложением, а администратор его открывает. Защита MS Defender Antispyware отключена, поэтому хакер получает доступ

**Индикаторы компрометации** ①  
Сессия meterpreter на компьютере админа

**Рекомендации** ①  
Включить политику в реестре, перезагрузить MS Defender и разорвать сессию нарушителя

**Оценка**  
☆ ☆ ☆ ☆ ☆

**Автор**  
KB Кадров Виктор  
@1132226454@pfur.ru

**Ответственный**  
СД Стариков Данила  
@1132226531@pfur.ru

**Источник**  
195.239.174.11

**Поражённые активы**  
10.10.4.10

Рис. 10: Карточка второго инцидента

## Устранение уязвимости “Отключенная защита антивируса”

Решение: на узле Administrator Workstation вручную удалить запись в реестре или через консоль, используя команду: REG DELETE «HKLM/SOFTWARE/Policies/Microsoft/Windows Defender» /v DisableAntiSpyware. Подтвердить действие, далее в Windows Defender перезапустить Virus & Threat Protection и включить Real-time Protection.

# Устранение уязвимости “Отключенная защита антивируса”

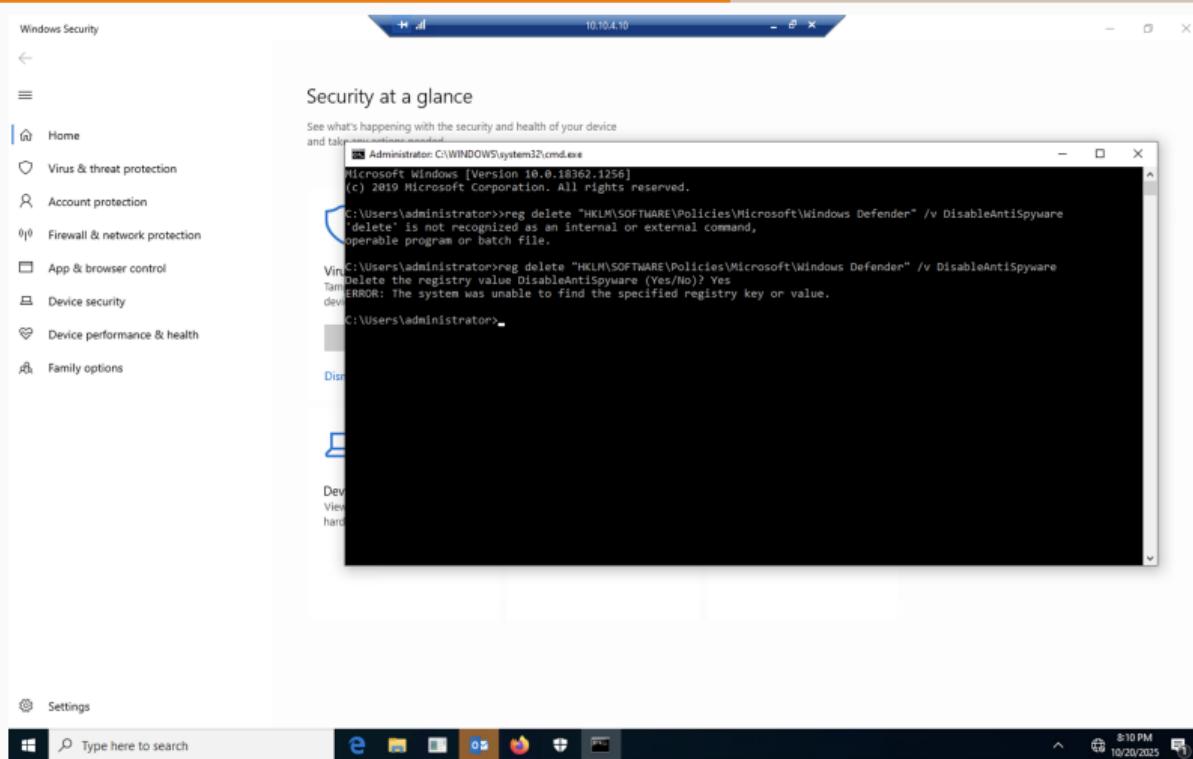


Рис. 11: Удаление записи DisableAntiSpyware в реестре

# Устранение уязвимости “Отключенная защита антивируса”

Security at a glance

See what's happening with the security and health of your device and take any actions needed.

The screenshot shows the Windows Defender Security Center. It displays seven sections: Virus & threat protection (warning, service stopped, button 'Restart now' highlighted with a red box), Account protection (green checkmark), Firewall & network protection (red exclamation mark, button 'Turn on'), App & browser control (green checkmark), Device security (green checkmark), Device performance & health (green checkmark), and Family options (green checkmark). Each section includes a brief description and a status icon.

Category	Status	Action
Virus & threat protection	Threat service has stopped. Restart it now.	Restart now
Account protection	No action needed.	
Firewall & network protection	Firewalls are turned off. Your device may be vulnerable.	Turn on
App & browser control	No action needed.	
Device security	View status and manage hardware security features	
Device performance & health	No action needed.	
Family options	Manage how your family uses their devices.	

Рис. 12: Интерфейс Windows Defender

### • Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

#### Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.



Рис. 13: Включение Real-time Protection

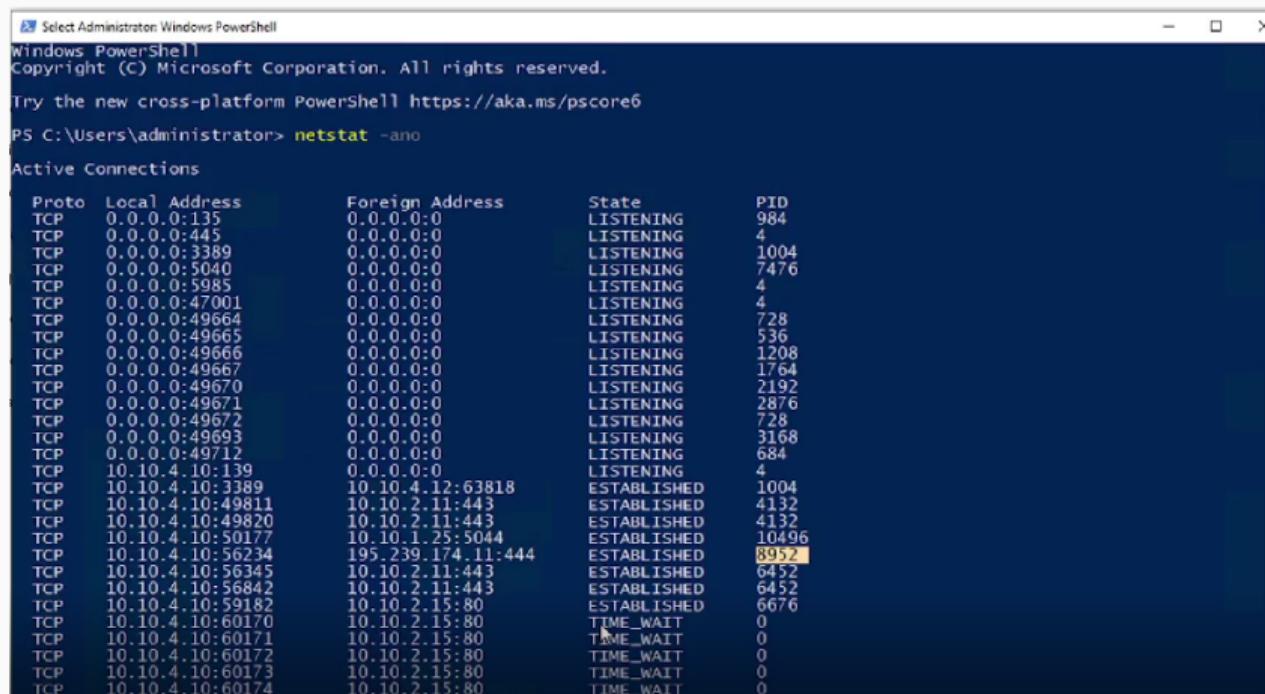
После удаления записи реестра и включения защиты антивирусной программы Microsoft Defender необходимо перезагрузить Windows.

## Последствие Admin meterpreter

---

Установленную сессию с нарушителем можно обнаружить при помощи утилиты netstat с ключами -апо. Для устранения необходимо завершить сессию с машиной нарушителя. Например, при помощи команды taskkill /f /pid . В результате выполнения команды сессия с машиной нарушителя завершена, последствие Admin meterpreter успешно устранено.

## Последствие Admin meterpreter



```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\administrator> netstat -ano

Active Connections

  Proto  Local Address        Foreign Address      State       PID
  TCP    0.0.0.0:135          0.0.0.0:0          LISTENING   984
  TCP    0.0.0.0:445          0.0.0.0:0          LISTENING   4
  TCP    0.0.0.0:3389         0.0.0.0:0          LISTENING   1004
  TCP    0.0.0.0:5040         0.0.0.0:0          LISTENING   7476
  TCP    0.0.0.0:5985         0.0.0.0:0          LISTENING   4
  TCP    0.0.0.0:47001        0.0.0.0:0          LISTENING   4
  TCP    0.0.0.0:49664        0.0.0.0:0          LISTENING   728
  TCP    0.0.0.0:49665        0.0.0.0:0          LISTENING   536
  TCP    0.0.0.0:49666        0.0.0.0:0          LISTENING   1208
  TCP    0.0.0.0:49667        0.0.0.0:0          LISTENING   1764
  TCP    0.0.0.0:49670        0.0.0.0:0          LISTENING   2192
  TCP    0.0.0.0:49671        0.0.0.0:0          LISTENING   2876
  TCP    0.0.0.0:49672        0.0.0.0:0          LISTENING   728
  TCP    0.0.0.0:49693        0.0.0.0:0          LISTENING   3168
  TCP    0.0.0.0:49712        0.0.0.0:0          LISTENING   684
  TCP    10.10.4.10:139       0.0.0.0:0          LISTENING   4
  TCP    10.10.4.10:3389      10.10.4.12:63818  ESTABLISHED 1004
  TCP    10.10.4.10:49811     10.10.2.11:443    ESTABLISHED 4132
  TCP    10.10.4.10:49820     10.10.2.11:443    ESTABLISHED 4132
  TCP    10.10.4.10:50177     10.10.1.25:5044   ESTABLISHED 10496
  TCP    10.10.4.10:56234     195.239.174.11:444 ESTABLISHED 8952
  TCP    10.10.4.10:56345     10.10.2.11:443    ESTABLISHED 6452
  TCP    10.10.4.10:56842     10.10.2.11:443    ESTABLISHED 6452
  TCP    10.10.4.10:59182     10.10.2.15:80     ESTABLISHED 6676
  TCP    10.10.4.10:60170     10.10.2.15:80     TIME_WAIT   0
  TCP    10.10.4.10:60171     10.10.2.15:80     TIME_WAIT   0
  TCP    10.10.4.10:60172     10.10.2.15:80     TIME_WAIT   0
  TCP    10.10.4.10:60173     10.10.2.15:80     TIME_WAIT   0
  TCP    10.10.4.10:60174     10.10.2.15:80     TIME_WAIT   0
```

Рис. 14: Соединение с машиной нарушителя

## Последствие Admin meterpreter

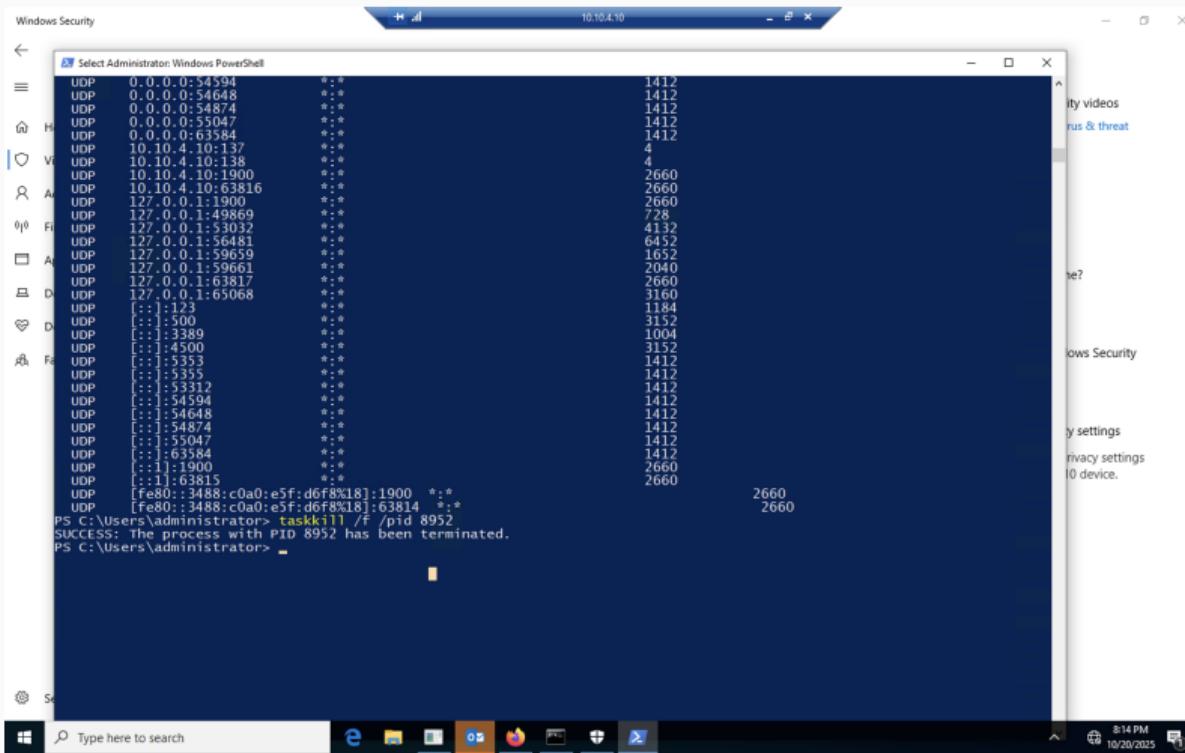


Рис. 15: Остановка процесса

## Третий инцидент

---

С помощью ViPNet IDS NS в сетевом трафике обнаруживаются множественные попытки подключения к хосту AD&DNS с портом 3389, сканирование системы, что может говорить о попытках подбора пароля. Также если мы зайдем на сам узел MS Active Directory, откроем Viewer Properties, перейдем в необходимую директорию с событиями (TerminalServices...), то сможем увидеть событие с кодом 1149, которое говорит о том, что пользователю удалось подключиться по RDP.

## Третий инцидент

The screenshot shows the ViPNet IDS NS application running on a Mac OS X desktop. The main window displays a list of network events for the past 24 hours. One specific event is highlighted in blue, indicating it is currently being analyzed. The detailed view on the right side of the interface provides information about this event, including its date and time (18:06:26.862 10/20/2025), source (eth2), destination (TCP), and event code (2001330). The event is identified as an 'ET INFO RDP - Response To External Host' with a 'misc-activity' class. The analysis rule for this event is described as detecting uncommon network requests for information, such as requests for service status that never run normally or run extremely rarely. The rule's text is as follows:

```
Text:  
alert tcp $HOME_NET 3389 -> $EXTERNAL_NET any (msg:"ET INFO RDP - Response To External Host";flow: established,to_client,content:"[0D]";offset: 0;depth: 1;content:"[0D]";offset: 5;depth: 1;reference: url/doc.emergingthreats.net/2001330;classtype: misc-activity;sid: 2001330;rev: 1;metadata: affected_asset sn: affected_product
```

Рис. 16: Детектирование Remote Desktop Protocol

## Третий инцидент

Слабый пароль учетной записи на узле MS Active Directory

Основная информация Чат В работе

Дата и время события ①  
20.10.2025 19:30

Описание ①  
На узле MS Active Directory установлен слабый пароль к учетной записи администратора, что позволяет нарушителю перебирать пароль.

Индикаторы компрометации ①  
Журнал безопасности Windows и логи подключений нарушителя на узел Active Directory по RDP

Рекомендации ①  
Изменить пароль к учетной записи администратора на более сложный

Прикрепленные файлы ①  
Не заполнено

Оценка  
☆ ☆ ☆ ☆ ☆

Автор  
Чемоданова Ангелина  
@1132226443@pfur.ru

С ответственным  
Кадров Виктор @1132226454@pfur.ru

Источник  
10.10.4.10

Поражённые активы  
10.10.2.10

Рис. 17: Карточка третьего инцидента

## Устранение уязвимости “Слабый пароль учетной записи”

Решение: изменить пароль к учетной записи администратора на более сложный, не содержащийся в словарях.

```
C:\Users\Administrator>net user Administrator *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
```

```
C:\Users\Administrator>_
```

Рис. 18: Изменение пароля администратора

На вышеупомянутом рисунке изображена смена пароля администратора на узле MS Active Directory командой «`net user Administrator *`». В результате изменения ненадежного пароля уязвимость успешно устранена.

Добавление нового привилегированного пользователя можно отследить с помощью аудита событий входа в учетную запись Windows security, где появится событие с ID 4720.

Необходимо перейти в Event Viewer и в Windows Logs – Security, затем применить фильтр на логи. Ниже показан лог, генерируемый при добавлении нового пользователя.

## Последствие AD User

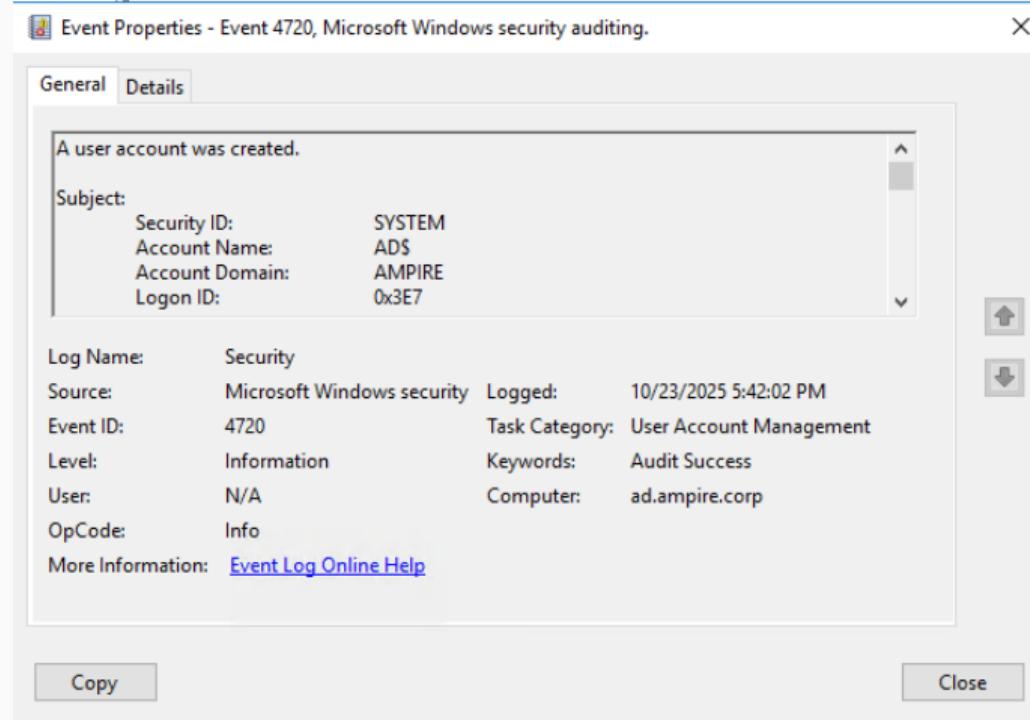


Рис. 19: Лог добавления нового пользователя

Для удаления пользователя необходимо зайти в Administrative Tools – Active Directory Users and computers. Затем во вкладке Users найти и удалить нового привилегированного пользователя с именем «Hacked».

# Последствие AD User

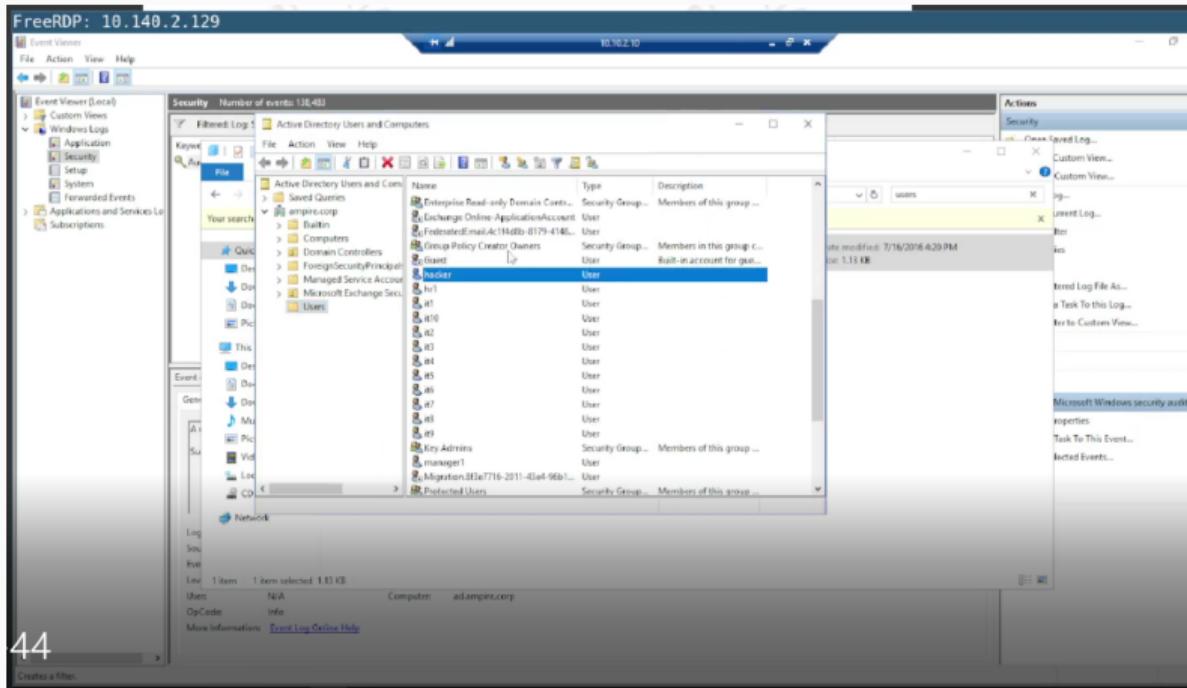


Рис. 20: Удаление пользователя hacker в AD User & Computers

## Последствие AD User

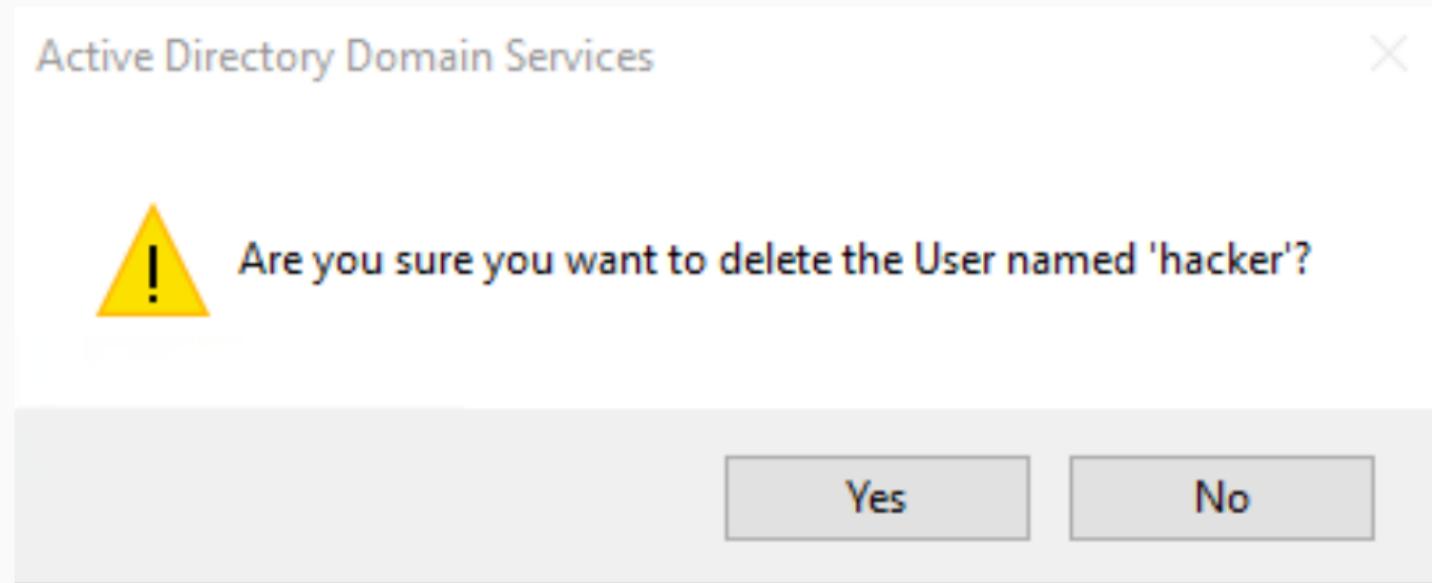


Рис. 21: Удаление пользователя hacker в AD User & Computers

В результате выполнения вышеупомянутых действий привилегированный пользователь удален, последствие AD User успешно устранено.

# Результат проделанной работы

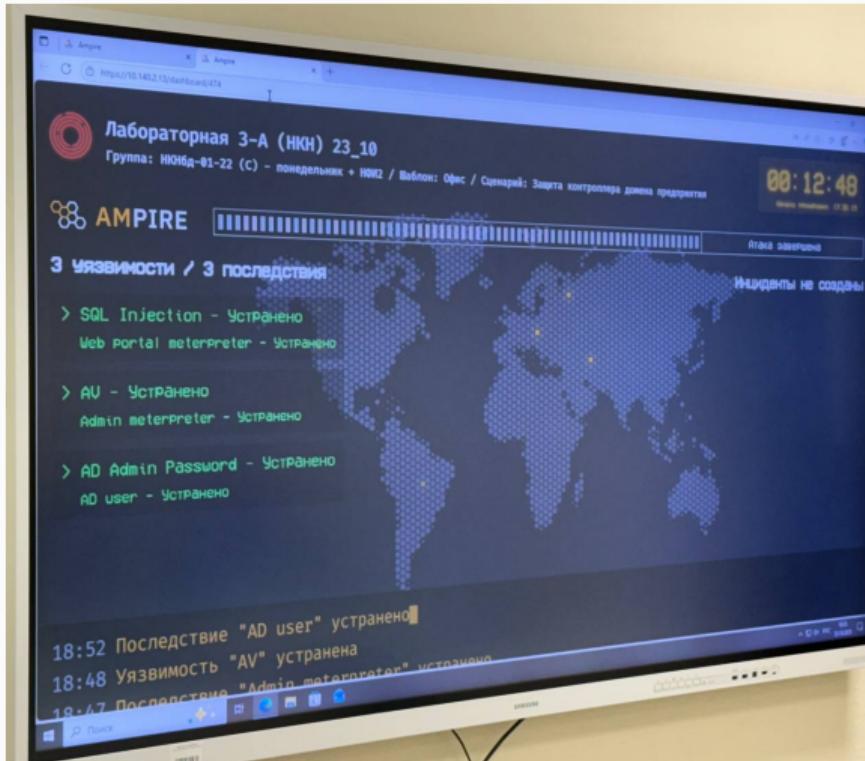


Рис. 22: Результат проделанной работы

## Вывод

---

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Защита контроллера домена предприятия” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы освоили практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоили навыки отработки действий по нейтрализации последствий успешных атак.