

# **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

<b>1</b>	<b>Цель тренировки</b>	<b>5</b>
<b>2</b>	<b>Выявленные уязвимости и последствия</b>	<b>6</b>
2.1	SQL-инъекция . . . . .	7
2.1.1	Описание инцидента . . . . .	7
2.1.2	Решение . . . . .	7
2.1.3	Последствие Web portal meterpreter . . . . .	8
2.2	Отключённая защита антивируса . . . . .	10
2.2.1	Описание инцидента . . . . .	11
2.2.2	Решение . . . . .	11
2.2.3	Последствия Admin meterpreter . . . . .	13
2.3	Слабый пароль учётной записи . . . . .	13
2.3.1	Описание инцидента . . . . .	14
2.3.2	Решение . . . . .	14
2.3.3	Последствие AD User . . . . .	15
<b>3</b>	<b>Вывод</b>	<b>18</b>
	<b>Список литературы</b>	<b>19</b>

# Список иллюстраций

2.1	Выявленные уязвимости . . . . .	6
2.2	Описание инцидента . . . . .	7
2.3	Устранение уязвимости . . . . .	8
2.4	Проверка сокетов . . . . .	9
2.5	Завершение сессии с нарушителем . . . . .	10
2.6	Описание инцидента . . . . .	11
2.7	Удаление записи в реестре . . . . .	12
2.8	Virus & Threat Protection и Real-time Protection . . . . .	12
2.9	Завершаем сессию с машиной нарушителя . . . . .	13
2.10	Описание инцидента . . . . .	14
2.11	Изменение пароля . . . . .	15
2.12	Аудит событий . . . . .	16
2.13	Удаление пользователя . . . . .	17

## **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

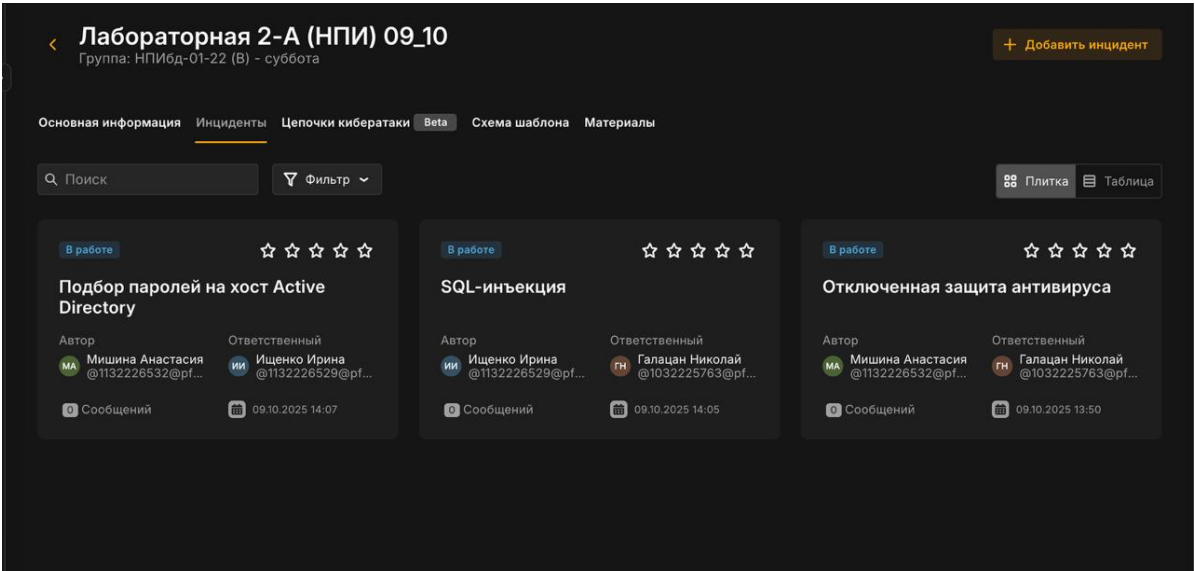


Рис. 2.1: Выявленные уязвимости

## 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

**Лабораторная 2-А (НПИ) 09\_10**  
Группа: НПИбд-01-22 (В) - суббота

**Добавление инцидента**

Название ⓘ: SQL-инъекция

Дата и время события ⓘ: 09.10.2025 14:05

Источник ⓘ: 195.239.174.11 (Kali) x

Поражённые активы ⓘ: 10.10.1.20 (Web Server PHP) x

Описание ⓘ: Зафиксировано большое количество целенаправленных попыток проведения атаки типа SQL Injection

Рекомендации ⓘ:  
- Провести аудит атакуемого ресурса на наличие уязвимости к атакам типа SQL-Injection и устранить при обнаружении  
- Отключить пораженный актив от вычислительной сети

Индикаторы компрометации ⓘ: ET SCAN Sqlmap SQL Injection Scan

Прикрепить файл ⓘ:  
IDS\_packet\_time-2025-10-09T11\_05\_41.808002Z\_ruleid-2008538.pcap x  
Выберите файл

Отмена Добавить

Рис. 2.2: Описание инцидента

### 2.1.2 Решение

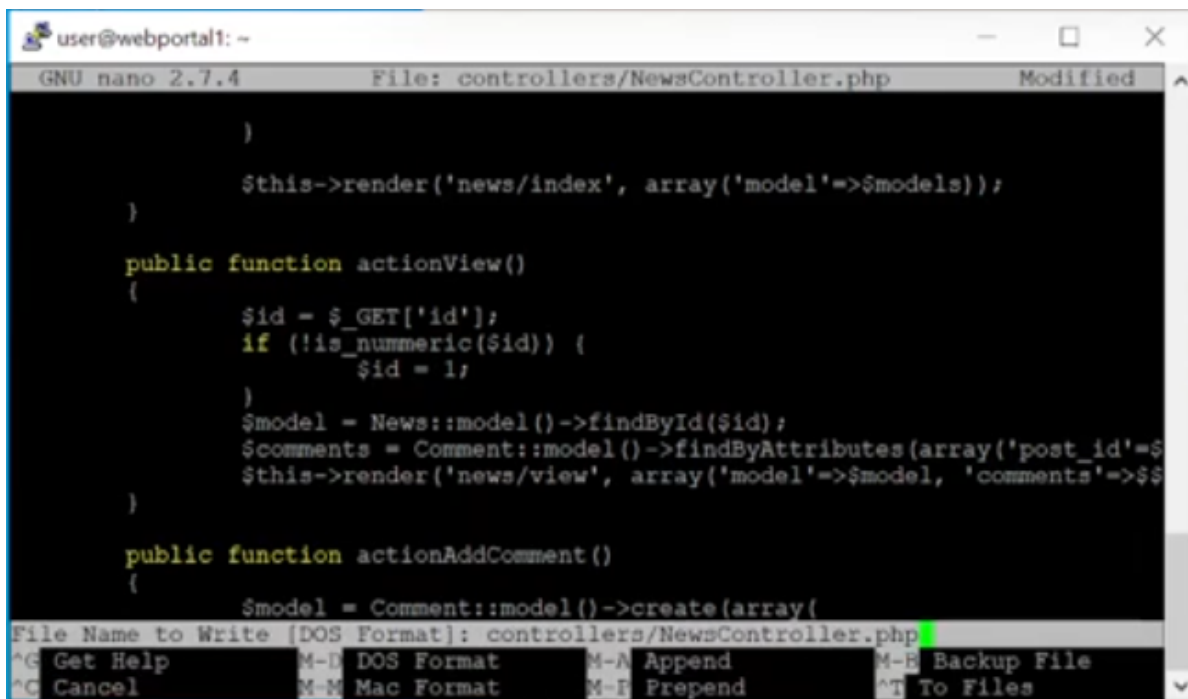
Находим место кода, где `$id` считывается из GET запроса

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.



```
user@webportal1: ~  
GNU nano 2.7.4 File: controllers/NewsController.php Modified  
  
    )  
    $this->render('news/index', array('model'=>$models));  
}  
  
public function actionView()  
{  
    $id = $_GET['id'];  
    if (!is_numeric($id)) {  
        $id = 1;  
    }  
    $model = News::model()->findById($id);  
    $comments = Comment::model()->findByAttributes(array('post_id'=$  
    $this->render('news/view', array('model'=>$model, 'comments'=>$$  
}  
  
public function actionAddComment()  
{  
    $model = Comment::model()->create(array(  
File Name to Write [DOS Format]: controllers/NewsController.php  
^G Get Help      M-B DOS Format  M-A Append      M-B Backup File  
^C Cancel        M-M Mac Format  M-E Prepend     ^T To Files
```

Рис. 2.3: Устранение уязвимости

### 2.1.3 Последствие Web portal meterpreter

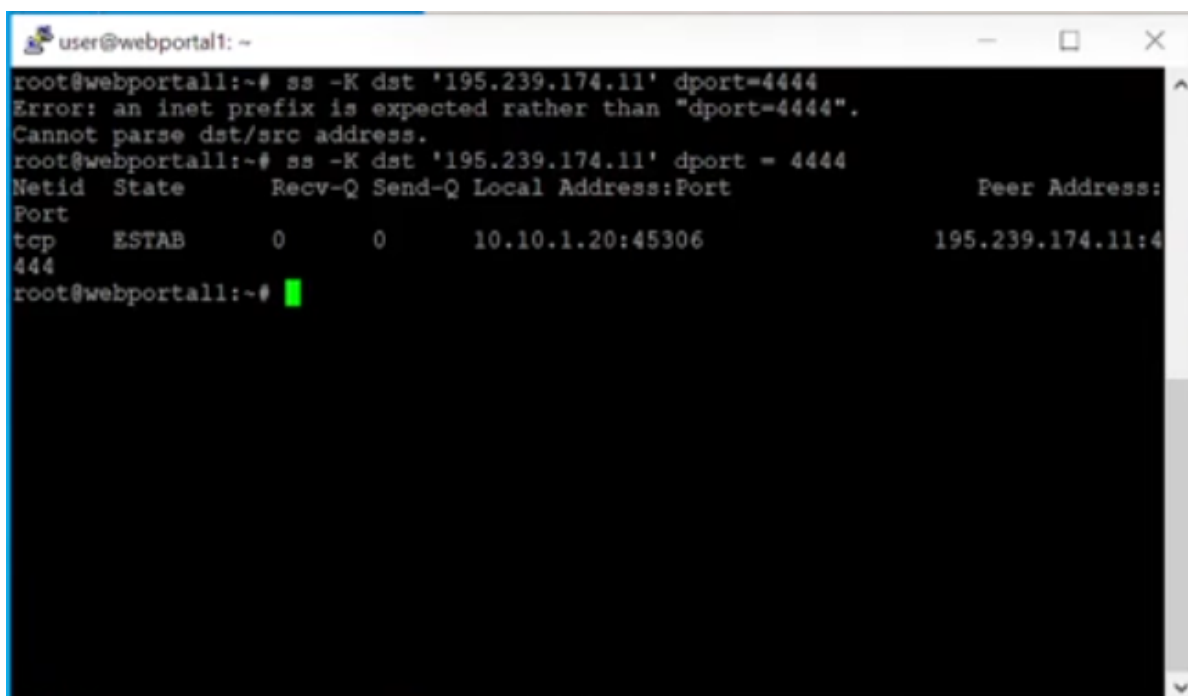
Нарушитель устанавливает shell сессию с веб-порталом PHP. Для обнаружения последствия проверяем сокет уязвимой машины при помощи утилиты ss с ключами -tr.



```
user@webportal1: ~  
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/NewsController.php  
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/NewsController.php  
root@webportal1:/var/www/html/htdocs/polygon# cd  
root@webportal1:~# ss -tp  
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port  
ESTAB      0      0      10.10.1.20:tpoxy        10.10.1.253:64811  
            users: ({"server",pid=626,fd=8})  
ESTAB      0      0      10.10.1.20:53246        10.10.1.25:5044  
            users: ({"filebeat",pid=705,fd=5})  
ESTAB      0      272     10.10.1.20:ssh          10.10.1.253:47737  
            users: ({"sshd",pid=9177,fd=4}, {"sshd",pid=9141,fd=4})  
ESTAB      0      339     10.10.1.20:43492        10.10.2.17:25004  
            users: ({"epp_agentd",pid=1531,fd=35})  
ESTAB      0      0      10.10.1.20:45306        195.239.174.11:4444  
            users: ({"chisel.sh",pid=20161,fd=3}, {"sh",pid=20160,fd=3}, {"Eq6sPL",pid=7447,fd=3})  
ESTAB      0      0      10.10.1.20:53304        195.239.174.11:1085  
            users: ({"chisel.sh",pid=20161,fd=11})  
CLOSE-WAIT 1      0      ::ffff:10.10.1.20:http  ::ffff:195.239.174.11:57486  
            users: ({"apache2",pid=1310,fd=13})  
root@webportal1:~#
```

Рис. 2.4: 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.



```
user@webportall1: ~  
root@webportall1:~# ss -K dst '195.239.174.11' dport=4444  
Error: an inet prefix is expected rather than "dport=4444".  
Cannot parse dst/src address.  
root@webportall1:~# ss -K dst '195.239.174.11' dport = 4444  
Netid  State      Recv-Q  Send-Q  Local Address:Port      Peer Address:  
Port  
tcp    ESTAB      0        0      10.10.1.20:45306        195.239.174.11:4444  
root@webportall1:~#
```

Рис. 2.5: 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

#### Добавление инцидента

Название ⓘ  
Отключенная защита антивируса

Дата и время события ⓘ  
09.10.2025 13:50

Источник ⓘ  
195.239.174.11 (Kali) x

Поражённые активы ⓘ  
10.10.4.10 (Administrator Workstation) x

Описание ⓘ  
Отключена защита антивируса

Рекомендации ⓘ  
Удалить запись в реестре. В Windows Defender перезапустить защиту. Завершить сессию с машиной нарушителя.

Индикаторы компрометации ⓘ  
Windows Defender – в Powershell команда Get-MpP

Прикрепить файл ⓘ  
Перетяните файл в эту область или  
Выберите файл

ОтменаДобавить

Рис. 2.6: Описание инцидента

### 2.2.2 Решение

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

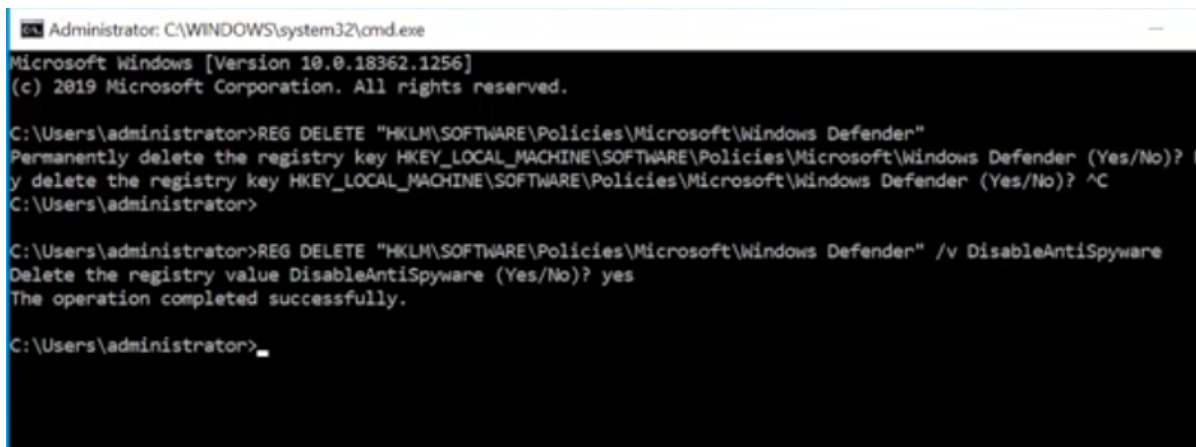


Рис. 2.7: Удаление записи в реестре

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

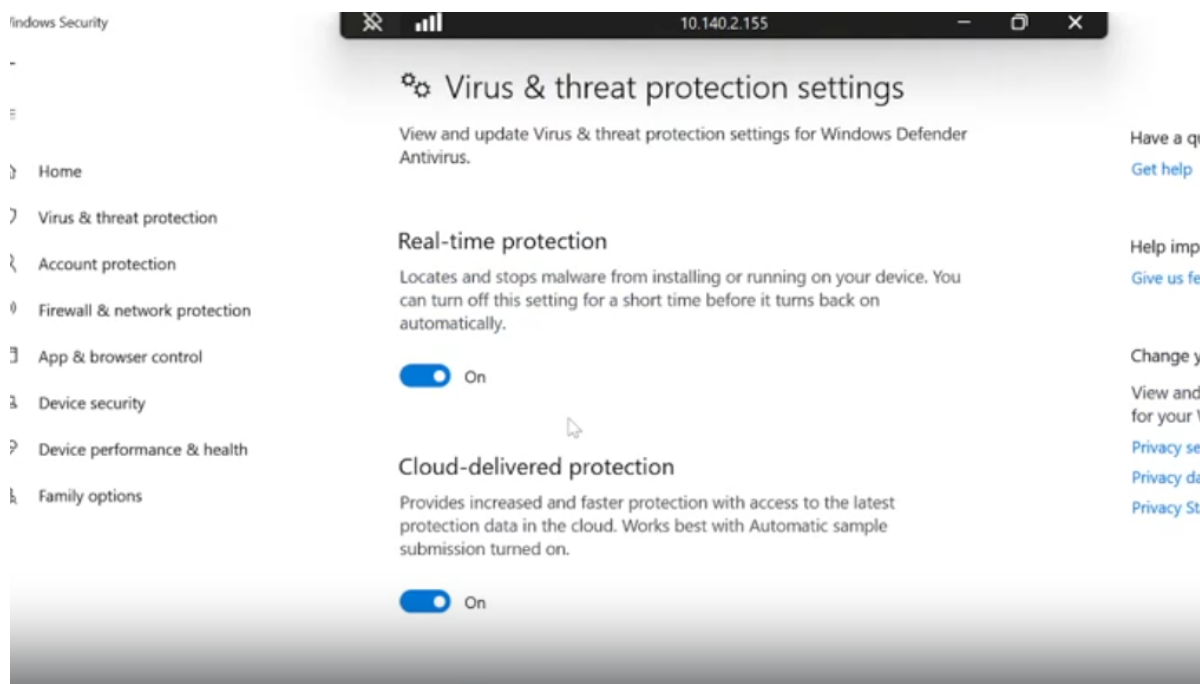


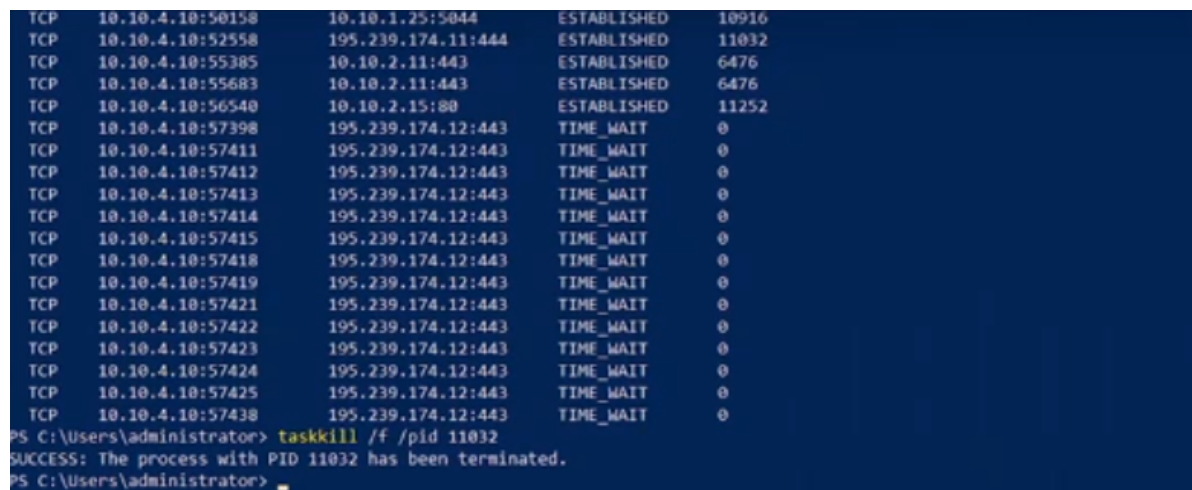
Рис. 2.8: Virus & Threat Protection и Real-time Protection

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.



```
TCP 10.10.4.10:50150 10.10.1.25:5044 ESTABLISHED 10916
TCP 10.10.4.10:52558 195.239.174.11:444 ESTABLISHED 11032
TCP 10.10.4.10:55385 10.10.2.11:443 ESTABLISHED 6476
TCP 10.10.4.10:55683 10.10.2.11:443 ESTABLISHED 6476
TCP 10.10.4.10:56540 10.10.2.15:80 ESTABLISHED 11252
TCP 10.10.4.10:57398 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57411 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57412 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57413 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57414 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57415 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57418 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57419 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57421 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57422 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57423 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57424 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57425 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.10:57438 195.239.174.12:443 TIME_WAIT 0
PS C:\Users\administrator> taskkill /f /pid 11032
SUCCESS: The process with PID 11032 has been terminated.
PS C:\Users\administrator>
```

Рис. 2.9: 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

#### Добавление инцидента

Название ⓘ  
Подбор паролей на хост Active Directory

Дата и время события ⓘ  
09.10.2025 14:07

Источник ⓘ  
10.10.1.20 (Web Server PHP)

Поражённые активы ⓘ  
10.10.2.10 (MS Active Directory)

Описание ⓘ  
Выявлены многочисленные попытки подбора пароля для доступа по RDP к узлу контролируемой сети

Рекомендации ⓘ  
служб и закрыть неиспользуемые  
Заблокировать на межсетевом экране IP-адрес атакующего  
Провести интервьюирование владельца  
Отключить пораженный актив от вычислительной сети

Индикаторы компрометации ⓘ  
ICY MS Remote Desktop Administrator Login Request

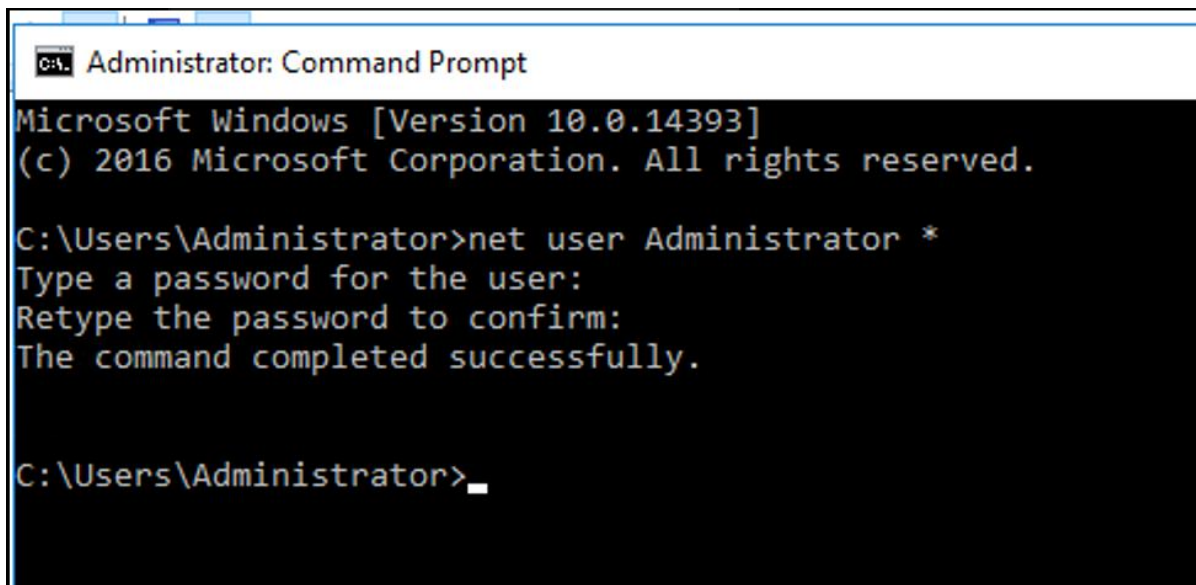
Прикрепить файл ⓘ  
IDS\_packet\_time-2025-10-09T11\_07\_45.939288Z\_ruleid-2012709.pcap  
Выберите файл

ОтменаДобавить

Рис. 2.10: Описание инцидента

### 2.3.2 Решение

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



```
C:\> Administrator: Command Prompt

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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. 2.11: 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 Event Viewer и в Windows Logs - Security, затем применяем фильтр на логи.

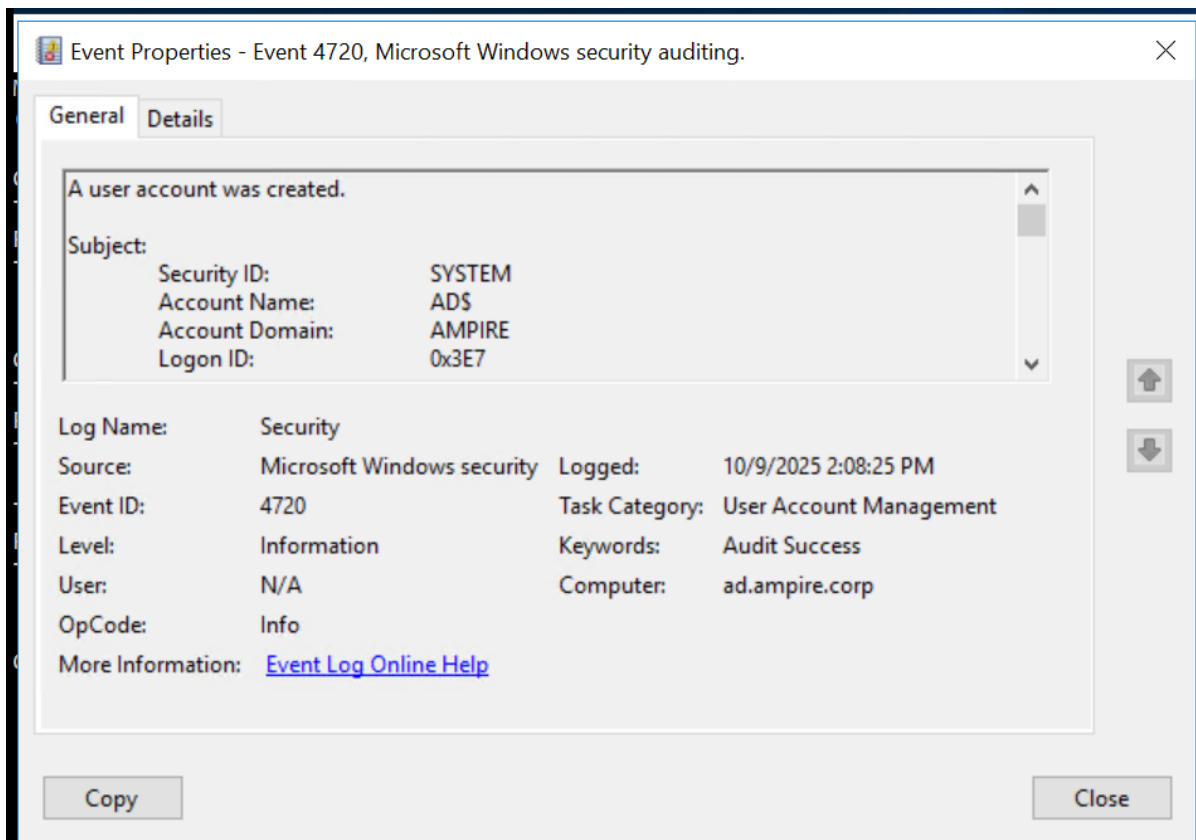


Рис. 2.12: Аудит событий

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



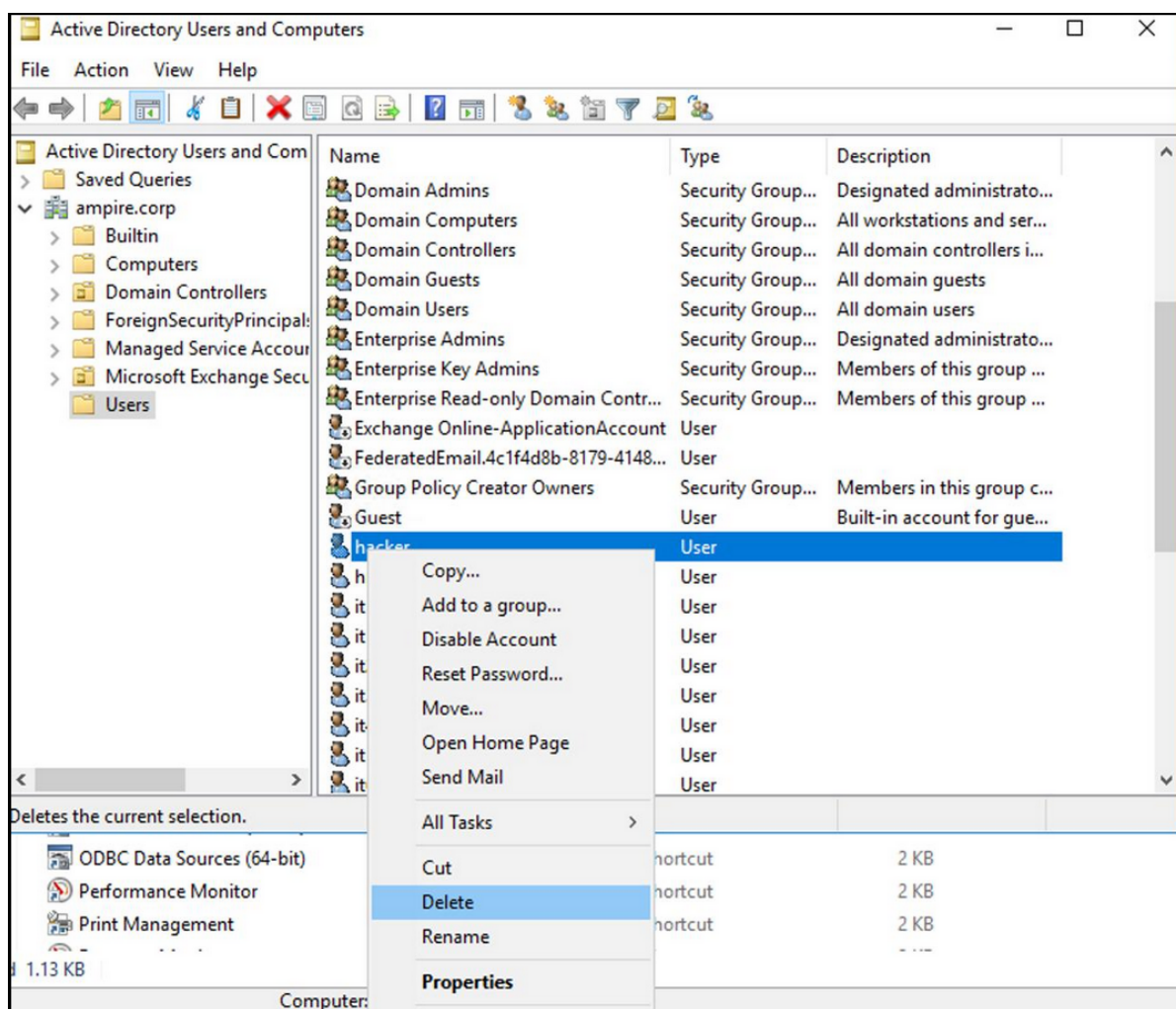
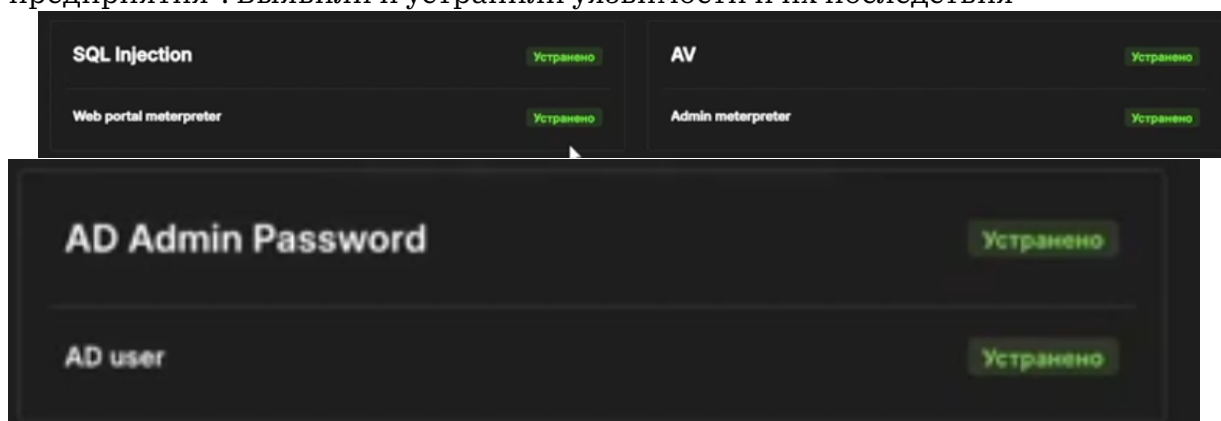


Рис. 2.13: Удаление пользователя

В результате выполнения 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**