

# **Лабораторная работа №3**

**Кибербезопасность предприятия**

Аскеров Александр Эдуардович

Замбалова Дина Владимировна

Кузнецова София Вадимовна

Поляков Глеб Сергеевич

Скандарова Полина Юрьевна

Тарутина Кристина Еленовна

Цвелев Сергей Андреевич

Шулуужук Айраана Вячеславовна

Учебная группа: НПИбд-01-22

# Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Вывод	19
	Список литературы	20

## Список иллюстраций

3.1	Подключение к удалённому рабочему столу . . . . .	6
3.2	Подключение к узлу Web Portal PHP . . . . .	7
3.3	Поиск места уязвимого параметра . . . . .	7
3.4	Добавление условия в файл NewsController.php . . . . .	7
3.5	Уязвимость 1 устранена . . . . .	8
3.6	Команда ss -tp . . . . .	9
3.7	Завершение сессии с нарушителем . . . . .	9
3.8	Последствие 1 устранено . . . . .	9
3.9	Подключение к узлу Administrator Workstation . . . . .	10
3.10	Удаление записи DisableAntiSpyware в реестре . . . . .	10
3.11	Перезагрузка системы защиты компьютера . . . . .	11
3.12	Перезагрузка компьютера . . . . .	12
3.13	Включение параметра Real-time protection . . . . .	13
3.14	Список соединений . . . . .	14
3.15	Нужное соединение . . . . .	14
3.16	Завершение сессии с машиной нарушителя . . . . .	14
3.17	Уязвимость 2 и последствие 2 устранены . . . . .	15
3.18	Подключение к узлу MS Active Directory . . . . .	15
3.19	Изменение пароля администратора . . . . .	15
3.20	Уязвимость 3 устранена . . . . .	16
3.21	Удаление пользователя hacker . . . . .	16
3.22	Последствие 3 устранено . . . . .	16
3.23	Все задания выполнены . . . . .	17
3.24	Инцидент 1 . . . . .	17
3.25	Команда Get-MpPreference . . . . .	17
3.26	Значение параметра DisableRealtimeMonitoring . . . . .	18
3.27	Инцидент 3 . . . . .	18

# 1 Цель работы

Защитить контроллер домена предприятия. Устранить три уязвимости и три последствия.

## 2 Теоретическое введение

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.

### 3 Выполнение лабораторной работы

Подключимся к удалённому рабочему столу [1].

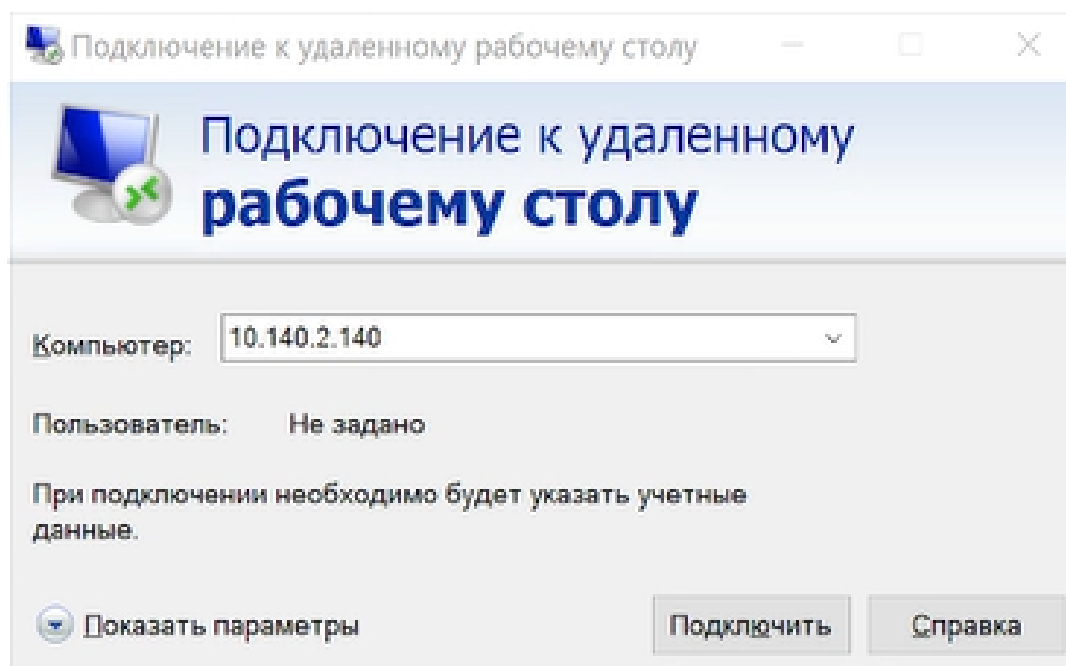


Рис. 3.1: Подключение к удалённому рабочему столу

Подключимся к Web Portal PHP через SSH.

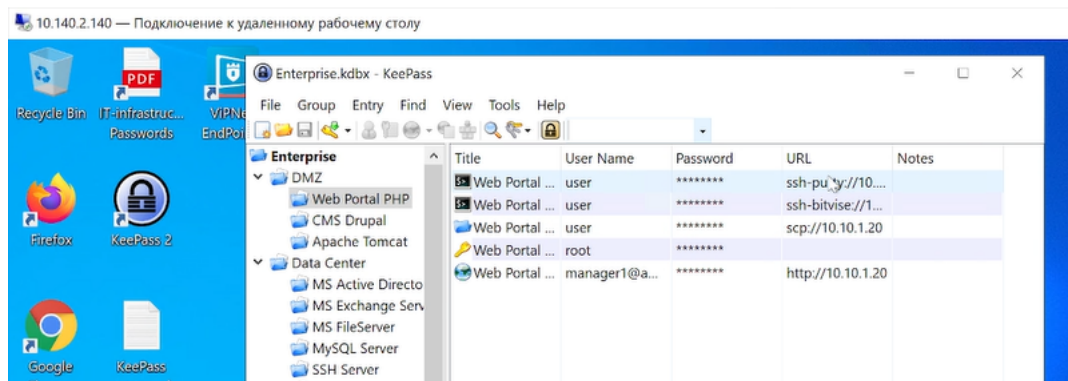


Рис. 3.2: Подключение к узлу Web Portal PHP

Выполним поиск места уязвимого параметра.

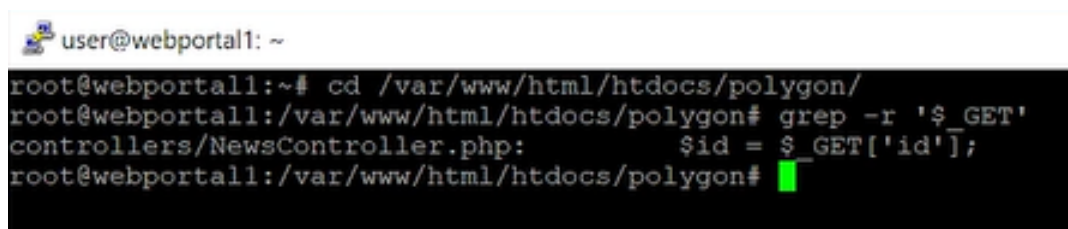


Рис. 3.3: Поиск места уязвимого параметра

Отредактируем файл NewsController.php.

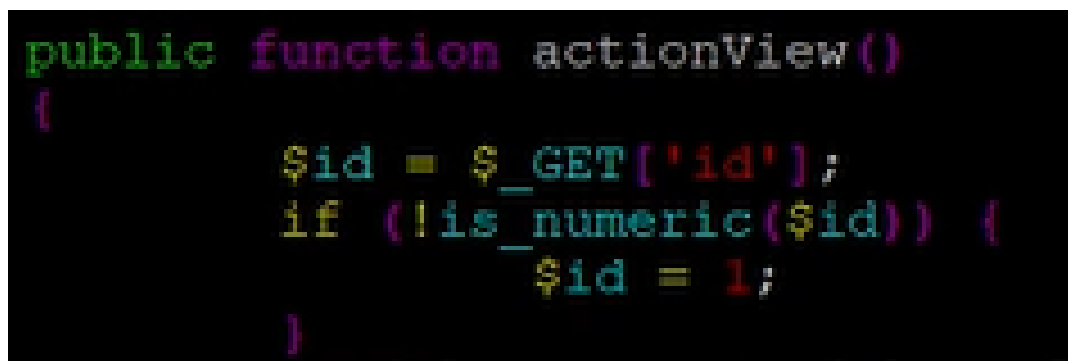


Рис. 3.4: Добавление условия в файл NewsController.php

Уязвимость 1 устранена.

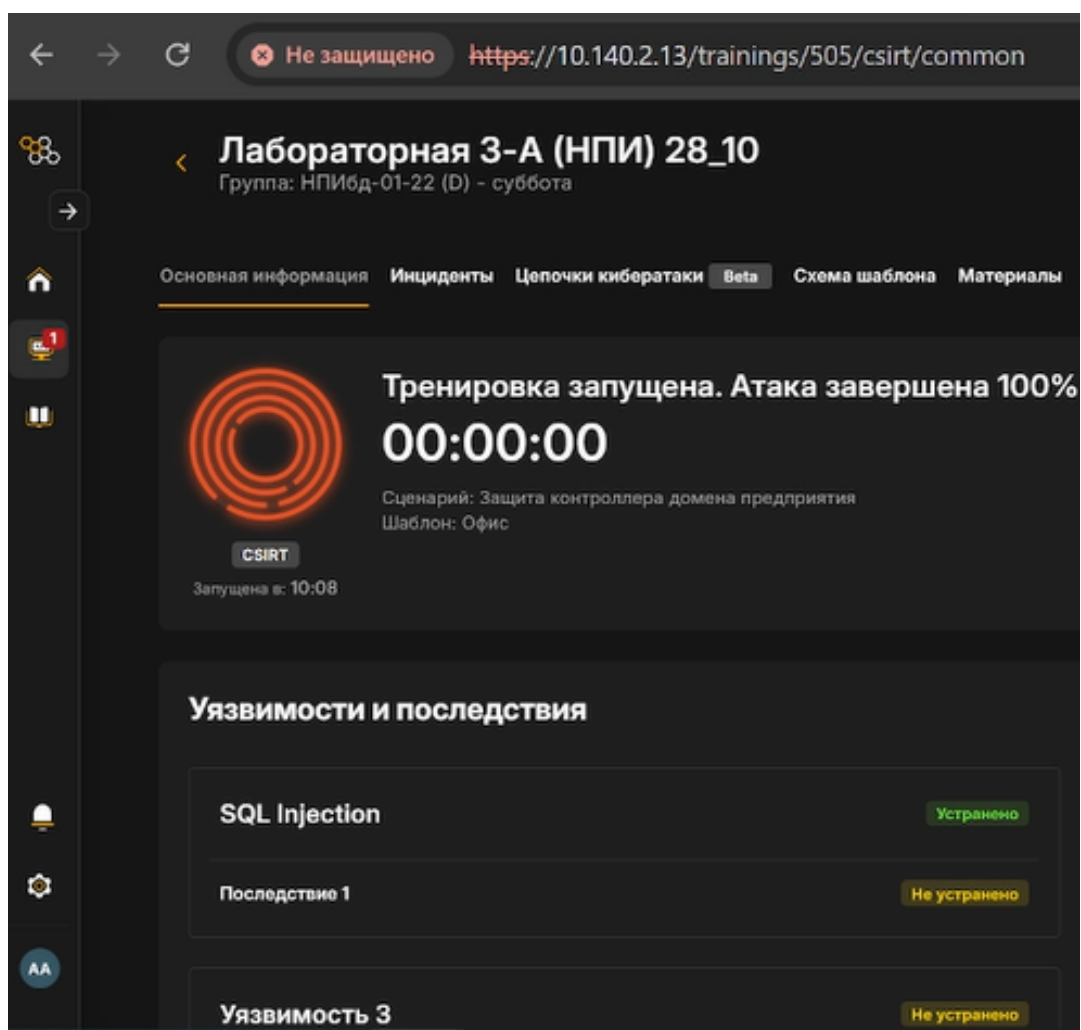


Рис. 3.5: Уязвимость 1 устранена

Устраним последствие 1.

Выполним команду `ss` с параметром `-tp`, чтобы посмотреть подсоединённые ip-адреса.



```
user@webportal1: ~  
root@webportal1:/var/www/html/htdocs/polygon/controllers# ss -tp  
State      Recv-Q Send-Q           Local Address:Port           Peer Address:Port  
ESTAB      0      0           10.10.1.20:60982             195.239.174.11:1085  
users: (("chisel.sh",pid=14055,fd=11))  
ESTAB      0      304           10.10.1.20:ssh              10.10.1.253:20890  
users: (("sshd",pid=666,fd=4), ("sshd",pid=630,fd=4))  
ESTAB      0      0           10.10.1.20:51550             195.239.174.11:4444  
users: (("chisel.sh",pid=14055,fd=3), ("sh",pid=14054,fd=3), ("hRt51J",pid=12953,fd=3))  
ESTAB      0      0           10.10.1.20:40680             10.10.1.25:5044  
users: (("filebeat",pid=701,fd=5))  
ESTAB      0      0           10.10.1.20:60328             10.10.2.17:25004  
users: (("epp_agentd",pid=11489,fd=36))  
ESTAB      0      0           10.10.1.20:tpoxy             10.10.1.253:14010  
users: (("server",pid=621,fd=8))  
root@webportal1:/var/www/html/htdocs/polygon/controllers#
```

Рис. 3.6: Команда ss -tp

Завершим сессию с нарушителем.

```
root@webportal1:/var/www/html/htdocs/polygon/controllers# 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           10.10.1.20:51550             195.239.174.11:4444  
root@webportal1:/var/www/html/htdocs/polygon/controllers#
```

Рис. 3.7: Завершение сессии с нарушителем

Последствие 1 устранено.

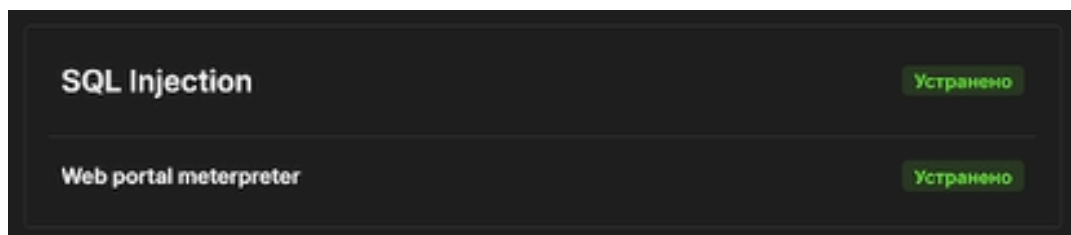


Рис. 3.8: Последствие 1 устранено

Устраним уязвимость 2.

Подключимся к узлу Administrator Workstation через rdp.

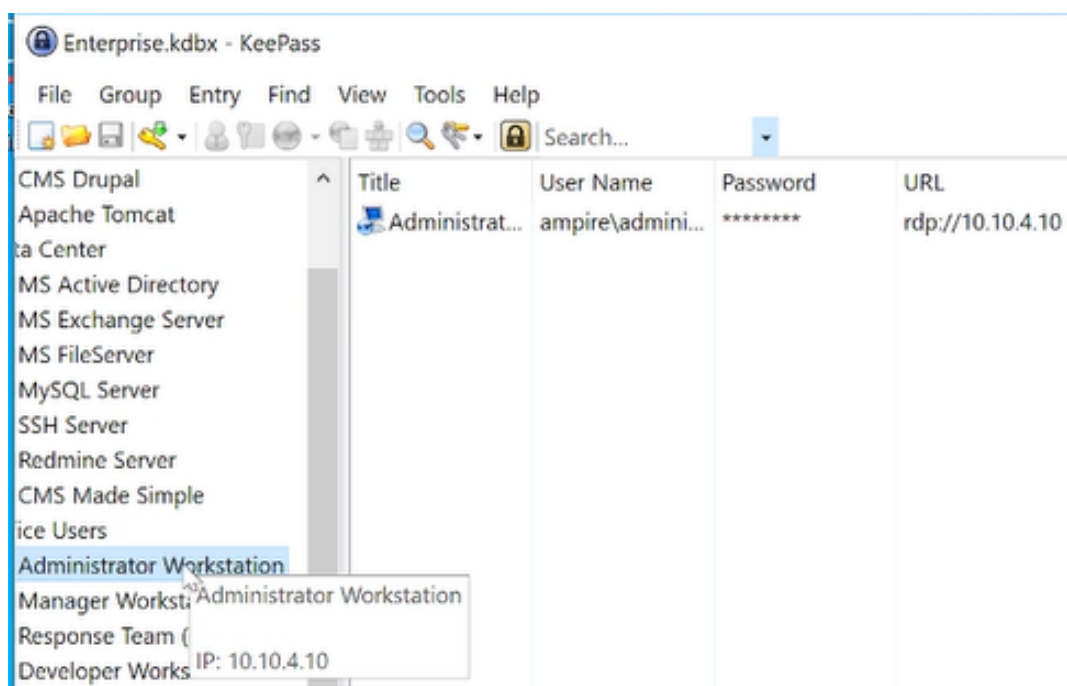


Рис. 3.9: Подключение к узлу Administrator Workstation

Удалим запись DisableAntiSpyware в реестре.

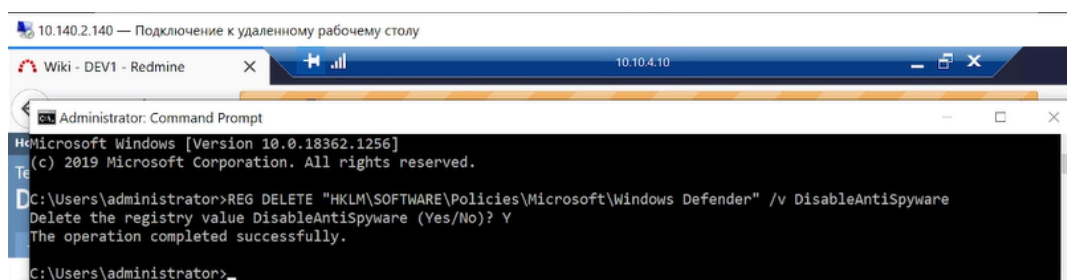


Рис. 3.10: Удаление записи DisableAntiSpyware в реестре

Откроем настройки антивируса Windows и перезагрузим параметр Virus & threat protection.

# Security at a glance

See what's happening with the security and take any actions needed.



Virus & threat protection  
No action needed.

Рис. 3.11: Перезагрузка системы защиты компьютера

Перезагрузим компьютер.

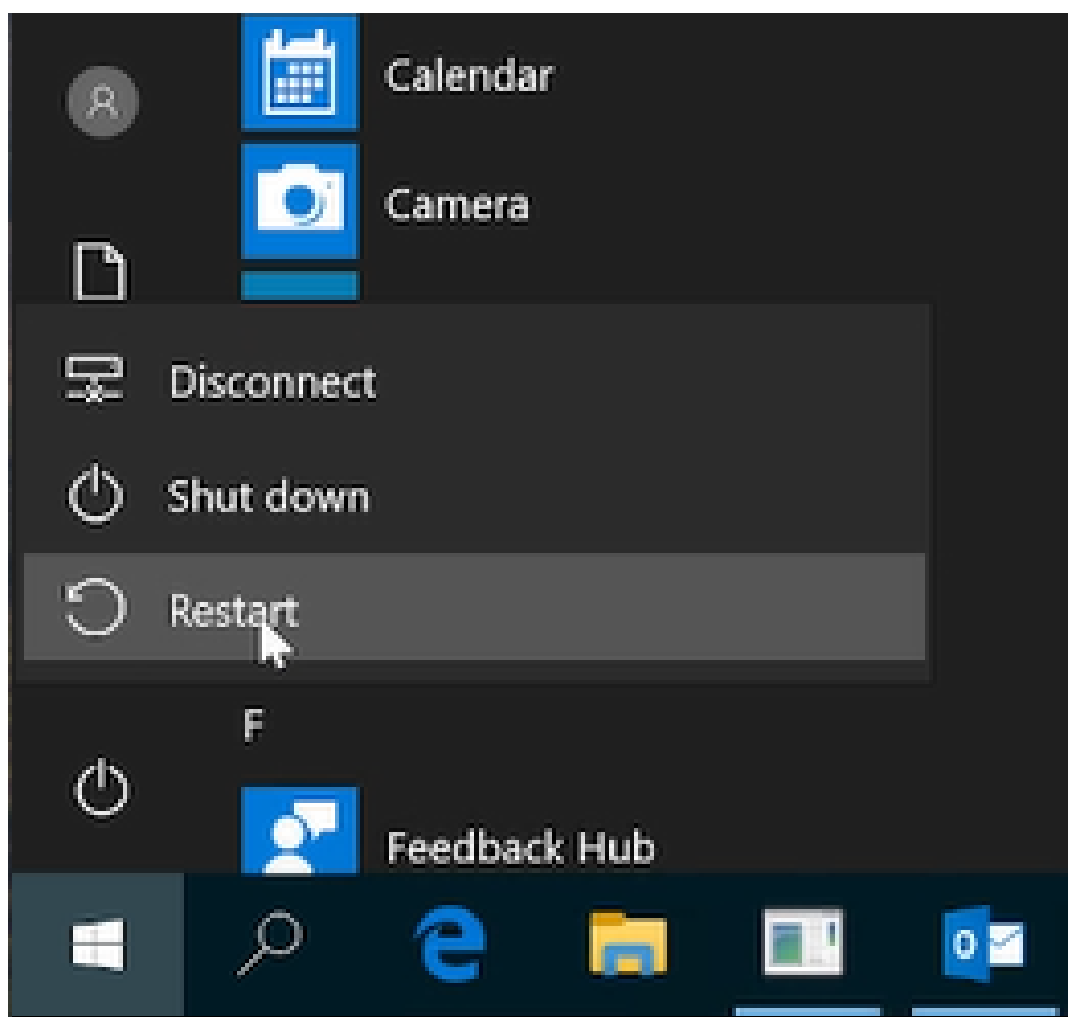


Рис. 3.12: Перезагрузка компьютера

Включим параметр Real-time protection. Он включён.

# 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. 3.13: Включение параметра Real-time protection

Уязвимость 2 устранена.

Устраним последствие 2.

Найдём соединение с машиной нарушителя.

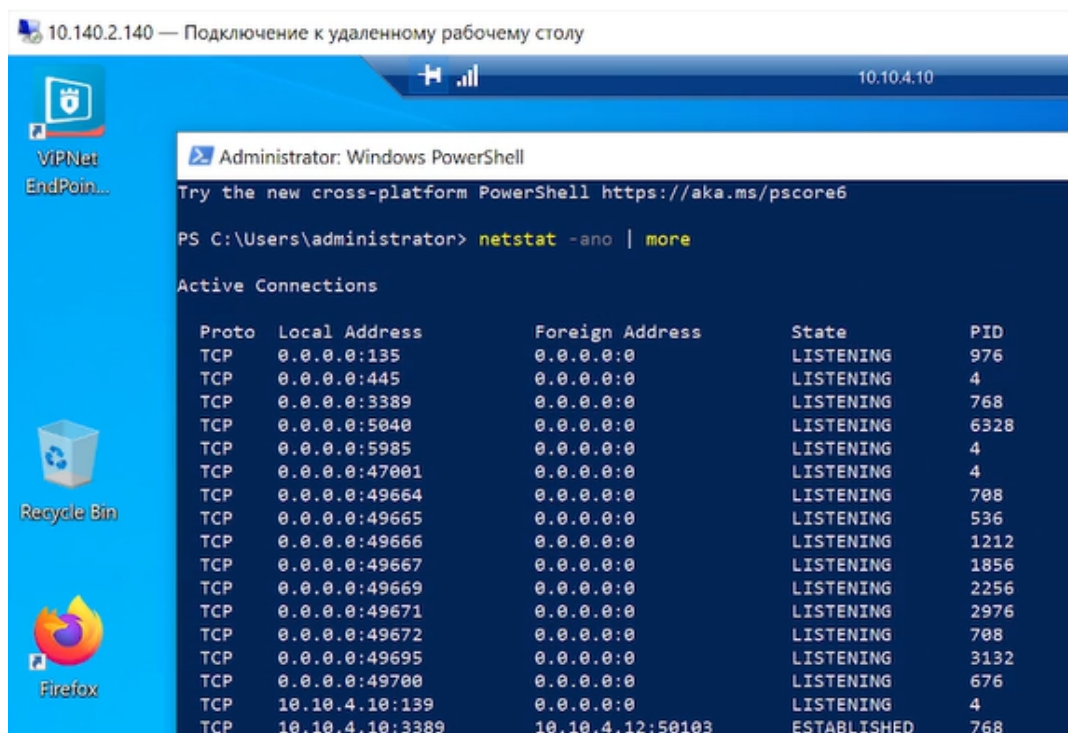


Рис. 3.14: Список соединений

Нужное соединение.

TCP	10.10.4.10:50171	10.10.1.25:5044	ESTABLISHED	6428
TCP	10.10.4.10:52131	10.10.2.15:80	ESTABLISHED	7364
TCP	10.10.4.10:52518	195.239.174.11:444	ESTABLISHED	<u>7212</u>
TCP	10.10.4.10:52654	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:52655	195.239.174.12:443	TIME_WAIT	0

Рис. 3.15: Нужное соединение

Завершим сессию с машиной нарушителя.

```
PS C:\Users\administrator> taskkill /f /pid 7212
SUCCESS: The process with PID 7212 has been terminated.
PS C:\Users\administrator>
```

Рис. 3.16: Завершение сессии с машиной нарушителя

Последствие 2 устранено.

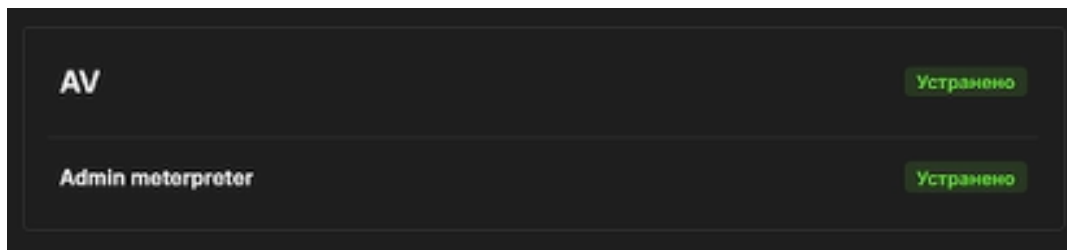


Рис. 3.17: Уязвимость 2 и последствие 2 устранены

Устраним уязвимость 3.

Подключимся к узлу MS Active Directory через rdp.

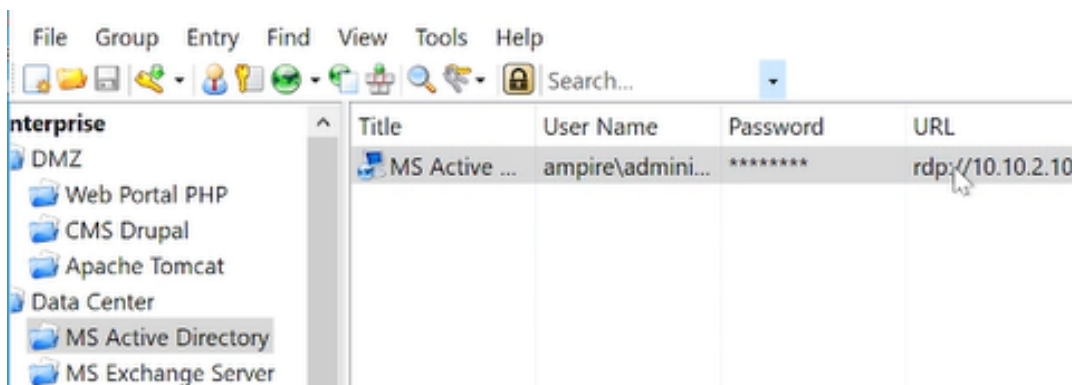


Рис. 3.18: Подключение к узлу MS Active Directory

Изменим пароль администратора.

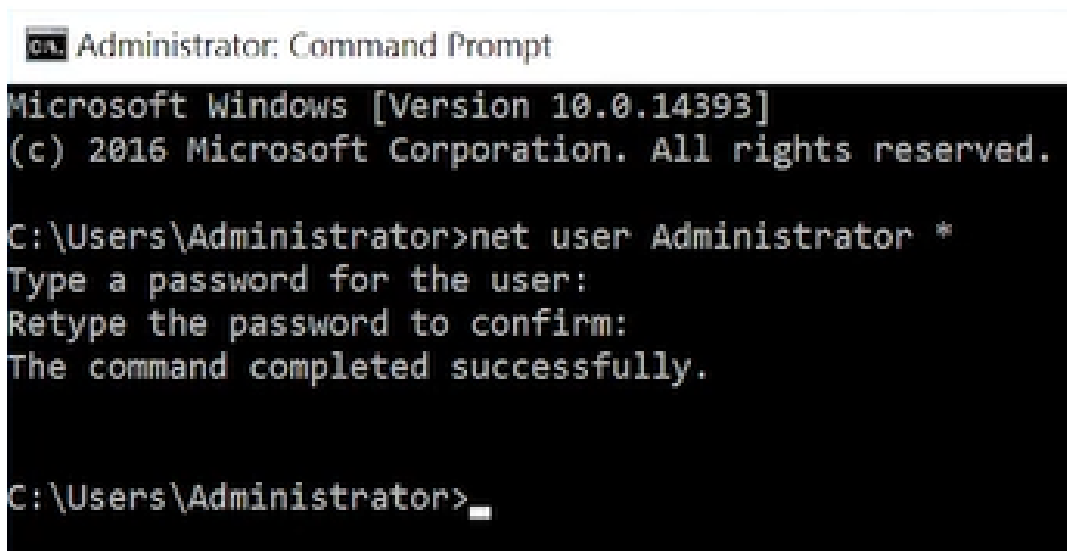


Рис. 3.19: Изменение пароля администратора

Уязвимость 3 устранена.

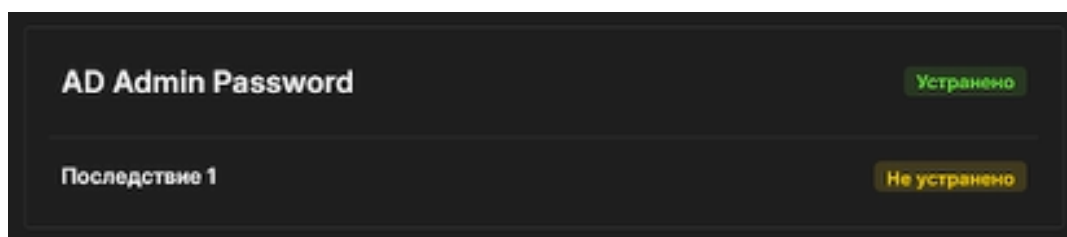


Рис. 3.20: Уязвимость 3 устранена

Устраним последствие 3.

Откроем приложение Active Directory Users and Computers. Найдём пользователя hacker и удалим его.

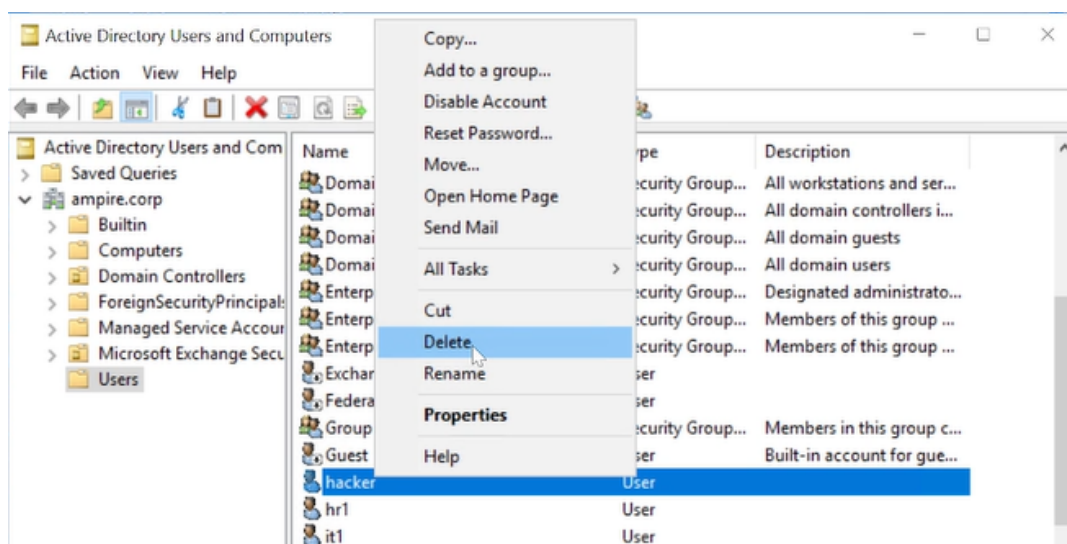


Рис. 3.21: Удаление пользователя hacker

Последствие 3 устранено.

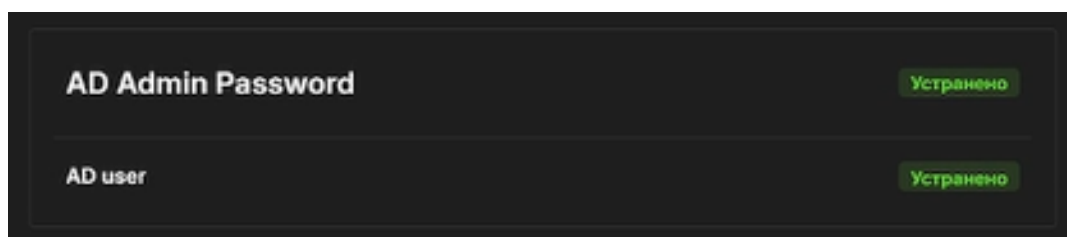


Рис. 3.22: Последствие 3 устранено



Все уязвимости и последствия устранены.

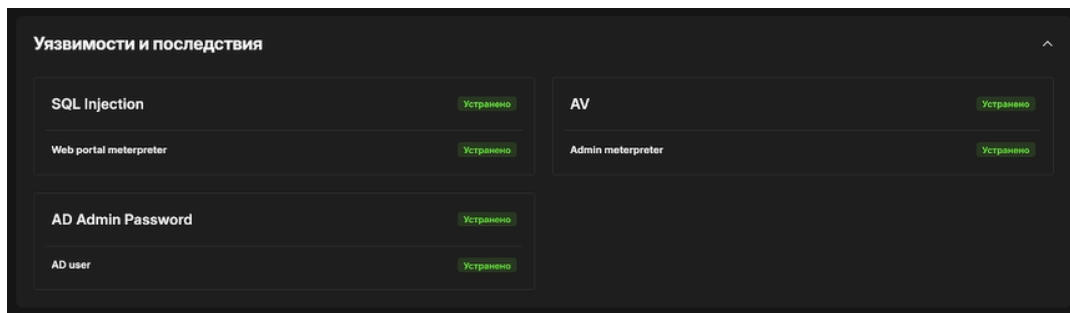


Рис. 3.23: Все задания выполнены

Добавим карточки инцидентов.

Инцидент 1.

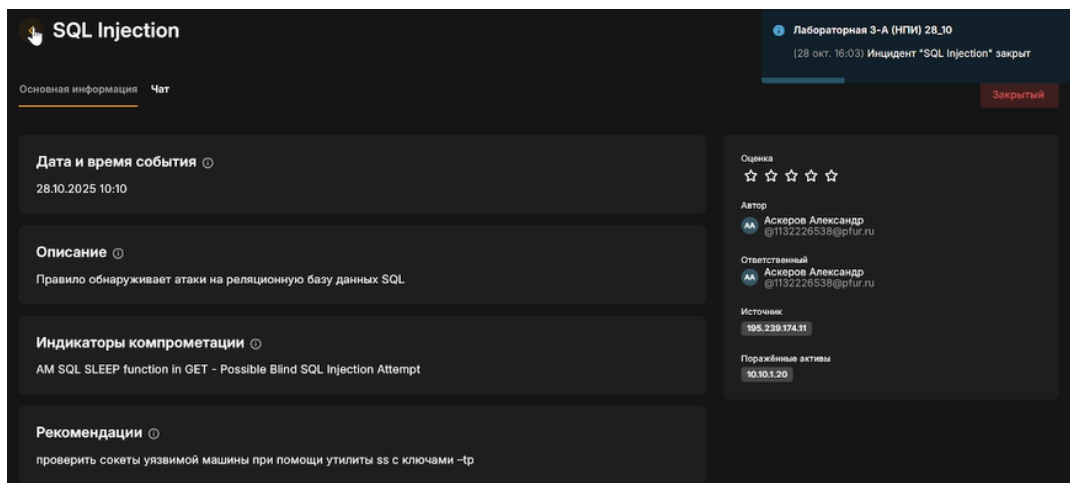


Рис. 3.24: Инцидент 1

Инцидент 2.

Выполним команду Get-MpPreference, чтобы проверить значение параметра DisableRealtimeMonitoring.



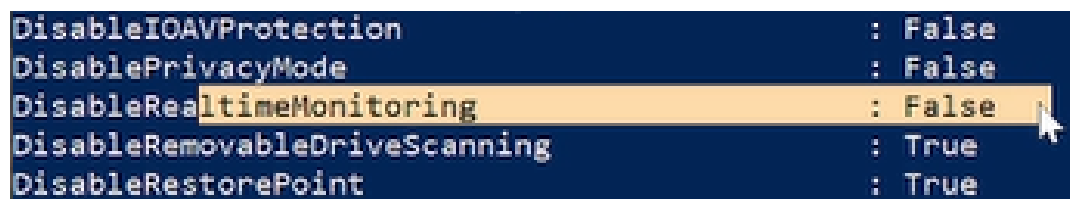
Рис. 3.25: Команда Get-MpPreference



DisableIOAVProtection	: False
DisablePrivacyMode	: False
DisableRealtimeMonitoring	: False
DisableRemovableDriveScanning	: True
DisableRestorePoint	: True

Рис. 3.26: Значение параметра DisableRealtimeMonitoring

Инцидент 3.



DisableIOAVProtection	: False
DisablePrivacyMode	: False
DisableRealtimeMonitoring	: False
DisableRemovableDriveScanning	: True
DisableRestorePoint	: True

Рис. 3.27: Инцидент 3

## 4 Вывод

Защищён контроллер домена предприятия. Устранены три уязвимости и три последствия.

# Список литературы

1. IEEE. POSIX // Wikipedia.