

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

2025-10-30

Российский университет дружбы народов

Москва, Россия

Цель работы

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

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.

Выполнение лабораторной работы

Подключимся к удалённому рабочему столу.

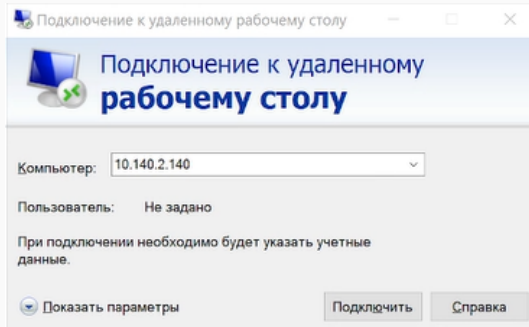


Figure 1: Подключение к удалённому рабочему столу

Выполнение лабораторной работы

Выполнение лабораторной работы

Подключимся к Web Portal PHP через SSH.

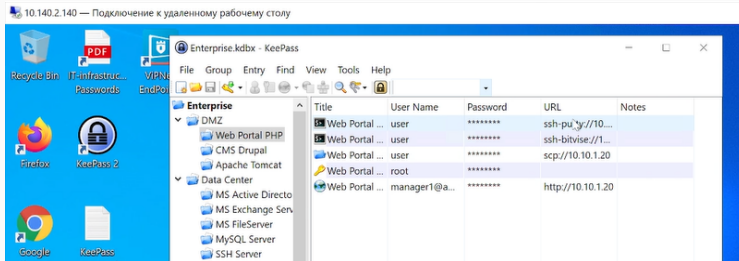
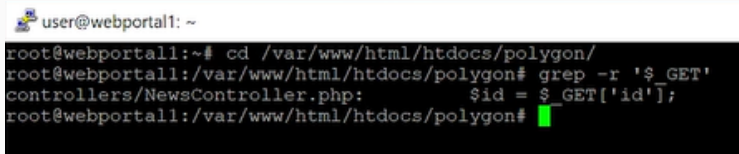


Figure 2: Подключение к узлу Web Portal PHP

Выполним поиск места уязвимого параметра.



```
user@webportal1: ~  
root@webportal1:~# cd /var/www/html/htdocs/polygon/  
root@webportal1:/var/www/html/htdocs/polygon# grep -r '$_GET'  
controllers/NewsController.php:         $id = $_GET['id'];  
root@webportal1:/var/www/html/htdocs/polygon#
```

Figure 3: Поиск места уязвимого параметра

Отредактируем файл NewsController.php.

```
public function actionView()
{
    $id = $_GET['id'];
    if (!is_numeric($id)) {
        $id = 1;
    }
}
```

Figure 4: Добавление условия в файл NewsController.php

Уязвимость 1 устранена.

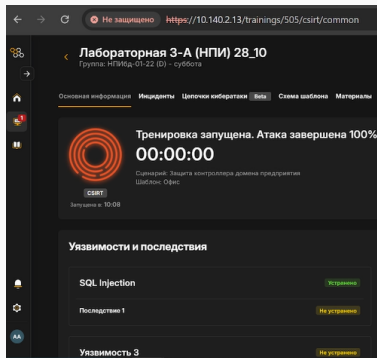


Figure 5: Уязвимость 1 устранена

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#
```

Figure 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#
```

Figure 7: Завершение сессии с нарушителем

Последствие 1 устранено.

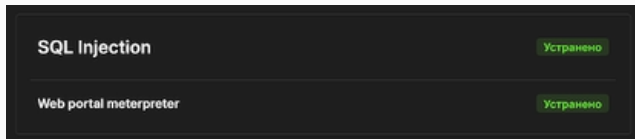


Figure 8: Последствие 1 устранено

Устраним уязвимость 2.

Подключимся к узлу Administrator Workstation через rdp.

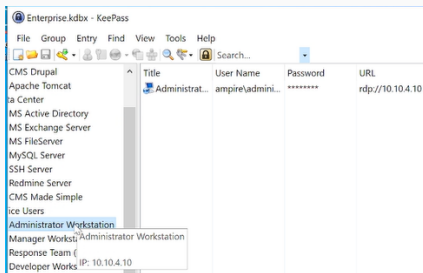


Figure 9: Подключение к узлу Administrator Workstation

Удалим запись DisableAntiSpyware в реестре.

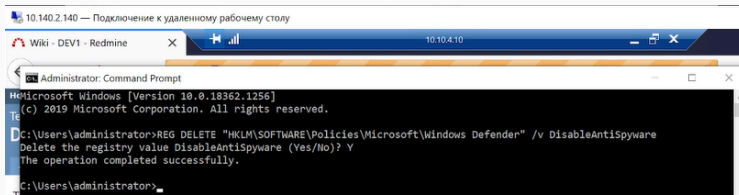


Figure 10: Удаление записи DisableAntiSpyware в реестре

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

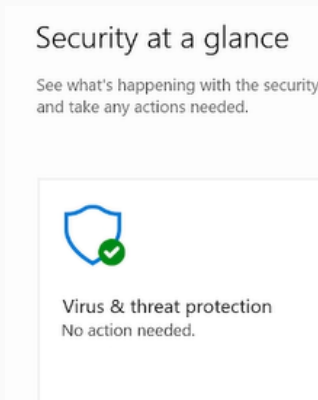


Figure 11: Перезагрузка системы защиты компьютера

Перезагрузим компьютер.

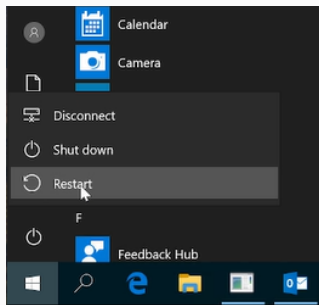


Figure 12: Перезагрузка компьютера

Включим параметр Real-time protection. Он включён.



Figure 13: Включение параметра Real-time protection

Уязвимость 2 устранена.

Выполнение лабораторной работы

Устраним последствие 2.

Найдём соединение с машиной нарушителя.

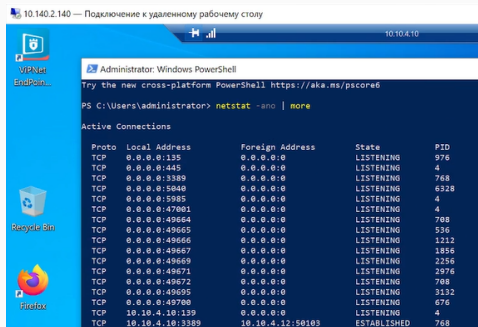


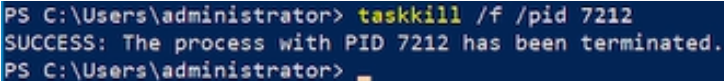
Figure 14: Список соединений

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

Figure 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> _
```

Figure 16: Завершение сессии с машиной нарушителя

Последствие 2 устранено.

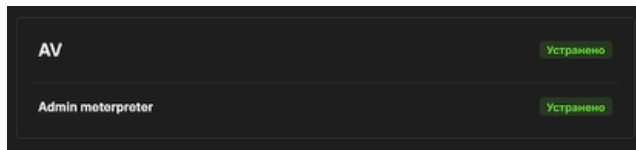


Figure 17: Уязвимость 2 и последствие 2 устранены

Выполнение лабораторной работы

Устраним уязвимость 3.

Подключимся к узлу MS Active Directory через rdp.

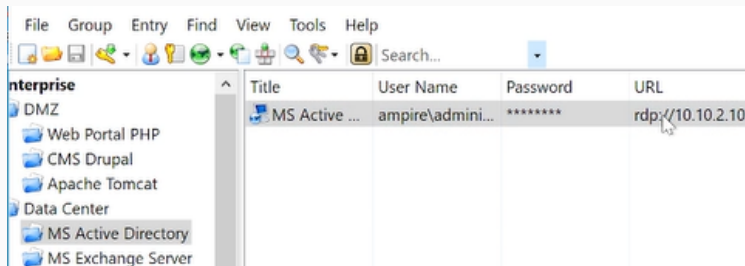
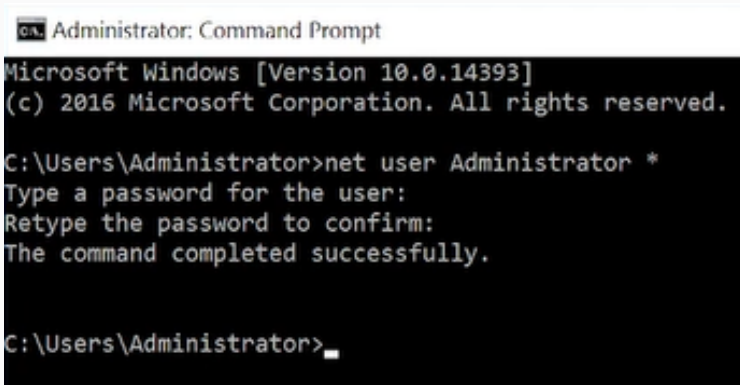


Figure 18: Подключение к узлу MS Active Directory

Изменим пароль администратора.

A screenshot of a Windows Command Prompt window. The title bar reads "Administrator: Command Prompt". The window content shows the following text: "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>".

```
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>
```

Figure 19: Изменение пароля администратора

Уязвимость 3 устранена.

AD Admin Password	Устранено
Последствие 1	Не устранено

Figure 20: Уязвимость 3 устранена

Выполнение лабораторной работы

Устраним последствие 3.

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

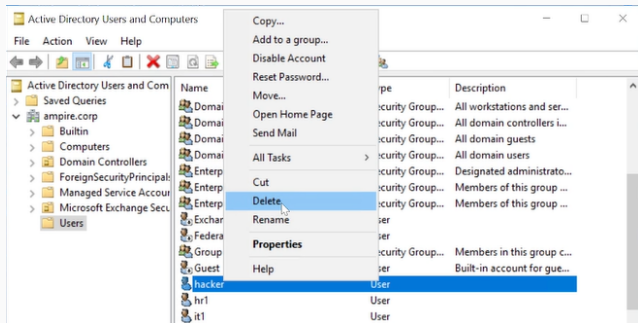


Figure 21: Удаление пользователя hacker

Последствие 3 устранено.

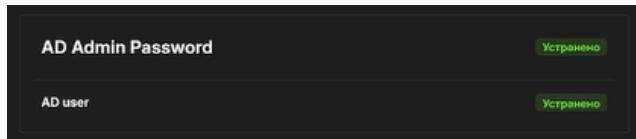


Figure 22: Последствие 3 устранено

Все уязвимости и последствия устранены.

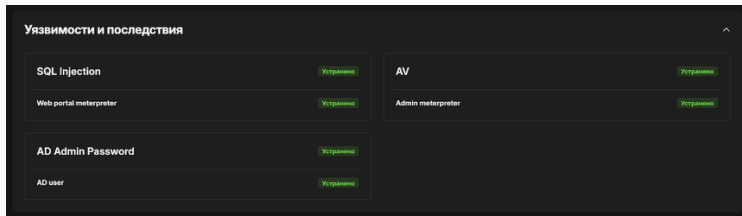


Figure 23: Все задания выполнены

Выполнение лабораторной работы

Добавим карточки инцидентов.

Инцидент 1.

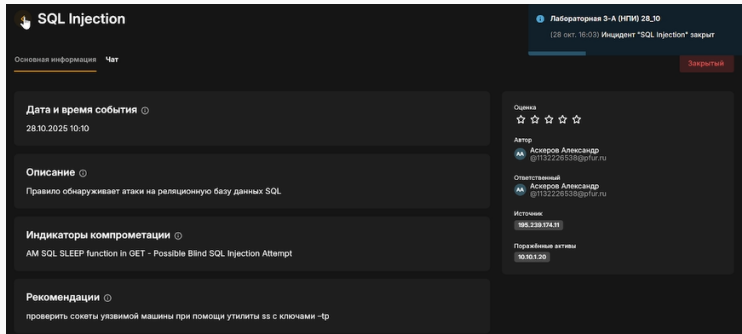


Figure 24: Инцидент 1

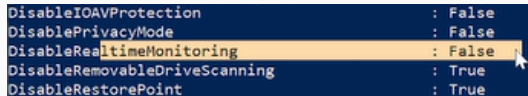
Инцидент 2.

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



```
PS C:\Users\administrator> Get-MpPreference
```

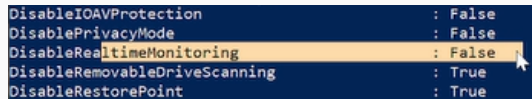
Figure 25: Команда Get-MpPreference



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

Figure 26: Значение параметра DisableRealtimeMonitoring

Инцидент 3.



A screenshot of a Windows command prompt window with a dark blue background and white text. It displays a list of system security settings. The line 'DisableRealtimeMonitoring : False' is highlighted with a yellow background. A mouse cursor is positioned at the end of this line.

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

Figure 27: Инцидент 3

Вывод

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