

# Лабораторная работа №1

Кибербезопасность предприятия

Пронякова Ольга Максимовна

## Содержание

### Список иллюстраций

### Список таблиц

## 1 Цель работы

Устранить действий нарушителя «Защита контроллера домена предприятия» для использования при проведении учебно-практических занятий на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

## 2 Выполнение лабораторной работы

### 2.1 1. SQL-инъекции

Детектирование SQL-инъекции. 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 и выставление права доступа на выполнение. Заходим на ViPNet IDS NS. (рис. 1).



Переход на ViPNet IDS NS

Нажимаем «События» и выставляем «За последние 24 часа». Ищем SQL-инъекции (как в методички), начиная просмотр по времени чуть ранее нашей атаки. (рис. 2).

The screenshot shows the NetworkMiner interface. On the left, a list of events is displayed with columns for Date & Time, Event ID, Class, and Protocol. A specific event is selected, highlighted in blue. On the right, a detailed view of this event is shown under the heading "Событие 08:27:15.794 23.09.2025". The detailed view includes tabs for General Information, Source, Destination, and Payload. Under General Information, details such as Date and time (08:27:15.794 23.09.2025), Interface (eth2), and Severity (High) are listed. The payload tab shows the raw HTTP request: "GET /?id=1 OR 1=1 HTTP/1.1".

### Применение фильтров и поиск SQL-инъекции

Создаем карточку инцидента по SQL-инъекции (рис. 3).

The screenshot shows a card incident creation form. The title is "SQL-инъекция" and the date is "23.09.2025 08:27". The form fields include:

- Источник:** 195.239.174.11 (Kali)
- Поражённые активы:** 10.10.1.20 (Web Server PHP)
- Описание:** Атака на Web Server PHP на базе Kali с попыткой эксплуатации уязвимости реляционной базы данных SQL. Атакующий - внешний нарушитель.
- Рекомендации:** параметр считывается из GET запроса в веб-сервисе на 80 порту  
2. внести изменения в файл конфигурации и проверить значения параметра \$id на уязвимость
- Индикаторы компрометации:** попытки загрузки эксплойтов из вредоносного ис
- Прикрепить файл:** IDS\_packet\_time-2025-09-23T05\_27.20.805705Z\_ruleid-3000706.pcap

### Создание карточки инцидента

У нас получилось 2 инцидента по SQL-инъекции (рис. 4).

< Лабораторная 1-А (вторник) 23\_09  
Группа: НФИбд-01-22 (В) - вторник

Основная информация Инциденты Цепочки кибератаки Beta Схема шаблона Материалы

Поиск Фильтр

**Новый** ☆☆☆☆☆

**SQL-инъекция**

Автор Сидорова Наталья  
SN @1132226432@pfur.ru

Сообщений 0 Сообщений 23.09.2025 08:27

**Новый** ☆☆☆☆☆

**SQL-инъекция**

Автор Сидорова Наталья  
SN @1132226432@pfur.ru

Сообщений 0 Сообщений 23.09.2025 08:27

### Готовые инциденты по SQL-инъекциям

Далее заходим на удаленный рабочий стол (рис. 5).

Уязвимость 1 Не устранено Уязвимость 2 Не устранено

Последствие 1

Подключение к удаленному рабочему столу

Компьютер: 10.140.2.129  
Пользователь: Не задано  
При подключении необходимо будет указать учетные данные

Доказать параметры Подключить Справка

Уязвимость 3

Последствие 1

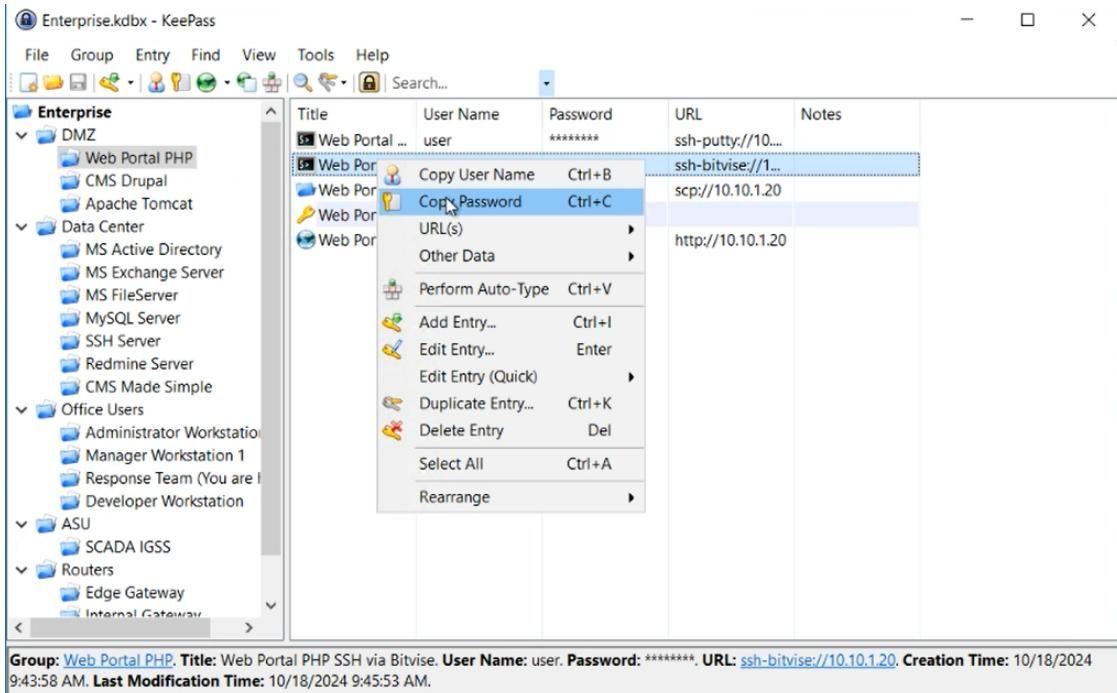
IP Адрес скопирован в буфер обмена

**Ресурсы**

Название	IP Адрес	Логин	Пароль
AM Threat Intelligence Portal	10.140.2.129	ampire it7	*****
Удалённое рабочее место	10.140.2.137	admin	*****
SecOnion	10.140.2.137	mon17	*****
ViPNet IDS NS	10.140.2.131		

### Вход на удаленный рабочий стол

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. Решение: известно, что \$id является уязвимым параметром, следует проверять тип данного параметра. Требуется найти место кода, где данный параметр считывается из GET запроса. Заходим на узел Web Server PHP (рис. 6).



*Открываем консоль на узле Web Server PHP*

Заходим не как user, а под root. Вводим следующие команды (рис. 7).

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

*Поиск места уязвимого параметра*

Считывание параметра сайта происходит в функции actionView() в файле NewsController.php (рис. 8).

```
public function actionView()
{
    $id = $_GET['id'];
    $model = News::model()->findById($id);
    $comments = Comment::model()->findByAttribu
```

*Параметры уязвимой функции*

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 (рис. 9).

```

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

```

*Измененная функция actionView с проверкой типа параметра \$id*

После внесения изменений в файл конфигурации и проверки значения параметра \$id уязвимость SQL-инъекции успешно устранена. 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. Для устранения необходимо воспользоваться 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. (рис. 10).

```

users:(("filebeat",pid=705,fd=5))
ESTAB      0      0          10.10.1.20:33054                               195.239.174.11:4444
users:(("chisel.sh",pid=8565,fd=3),("sh",pid=8564,fd=3),("iaG4M4",pid=7455,fd=3))
ESTAB      0      0          10.10.1.20:tproxy                           10.10.1.253:60808
users:(("server",pid=636,fd=8))
root@webportall:/home/user# 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          10.10.1.20:33054                195.239.174.11:4444
root@webportall:/home/user# ss -tp
State      Recv-Q Send-Q Local Address:Port                  Peer Address:Port
ESTAB      0      0          10.10.1.20:48390                195.239.174.11:1085
users:(("chisel.sh",pid=8565,fd=11))
ESTAB      0      0          10.10.1.20:45000                               10.10.2.17:25004
users:(("epp_agentd",pid=1256,fd=12))
ESTAB      0     288          10.10.1.20:ssh                           10.10.1.253:15356
users:(("sshd",pid=29177,fd=4),("sshd",pid=28898,fd=4))
ESTAB      0      0          10.10.1.20:tproxy                           10.10.1.253:30206
users:(("server",pid=636,fd=9))
ESTAB      0      0          10.10.1.20:38154                               10.10.1.25:5044
users:(("filebeat",pid=705,fd=5))
ESTAB      0      0          10.10.1.20:tproxy                           10.10.1.253:60808
users:(("server",pid=636,fd=8))
root@webportall:/home/user# █

```

*Завершение сессии с нарушителем*

В результате выполнения команды сессия с нарушителем завершена, последствие Web portal meterpreter успешно устранено. (рис. 11).

## Уязвимости и последствия

SQL Injection Устранено

Web portal meterpreter Устранено

Успешное устранение уязвимости и выполнение последствия

## 2.2 RDP Bruteforce (полный перебор паролей)

С помощью ViPNet IDS NS в сетевом трафике обнаруживаются множественные попытки подключения к хосту AD&DNS (рис. 12).

События

События за последние 24 часа

У...	Дата и время	Код события	К...	Название правила	Класс	Пр...
...	08:29:53.824 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:29:54.129 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:29:54.129 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:30:02.250 23...	2012709	1	ET POLICY MS Remote Desk...	protocol-command-decode	TCP
...	08:30:02.250 23...	2012709	1	ET POLICY MS Remote Desk...	protocol-command-decode	TCP
...	08:30:02.250 23...	2012709	1	ET POLICY MS Remote Desk...	protocol-command-decode	TCP
...	08:30:02.250 23...	2012709	1	ET POLICY MS Remote Desk...	protocol-command-decode	TCP
...	08:30:02.285 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:30:02.285 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:30:02.291 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:30:02.291 23...	2001330	1	ET INFO RDP - Response To ...	misc-activity	TCP
...	08:30:02.587 23...	3227018	1	ET SCAN Behavioral Unusual...	network-scan	TCP

Событие 08:30:02.250 23.09.2025

Событие Источник Получатель Пакет

**Правило анализа**

Класс protocol-command-decode  
Группа policy  
Название ET POLICY MS Remote Desktop Administrator Login Request  
Описание: Сигнатуры возможного нарушения политики информационной безопасности  
Текст: alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 3389 (msg: "ET POLICY MS Remote Desktop Administrator Login Request";flow: established,to\_server;content: "103 0 0 0 0";depth: 3;content: "e0 00 00 00 00 00";distance: 2;within: 6;content: "Cookie: 3ai mstshash=admin";distance: 0;nocase;reference: cve,CAN-2001-0540;classtype: protocol-command-decode;sid: 2012709;rev: 6;metadata: affected\_asset dst, affected\_product n/a, affected\_vendor n/a, attack\_target Client\_Endpoint, confidence Medium, created\_at 2011\_04\_22, signature\_severity Unknown, tias\_category Info, updated\_at 2012\_03\_10)

## RDP Bruteforce

Создаем карточку инцидента по «Полный перебор паролей» (рис. 13).

**Источник** 10.10.1.20 (Web Server PHP)

**Описание** Атака на Data Center (MS Active Directory) на базе Web Server PHP с попыткой эксплуатации уязвимости в виде слабого пароля . Атакующий - внутренний нарушитель

**Рекомендации** изменить пароль к учетной записи администратора на более сложный, не содержащийся в словарях

**Индикаторы компрометации** аномально большое количество попыток зайти под

**Прикрепить файл**

IDS\_packet\_time-2025-09-23T05\_30\_02.250526Z\_ruleid-2012709.pcap

Выберите файл

### Создание карточки инцидента

На узле MS Active Directory установлен слабый пароль к учетной записи администратора, что позволяет нарушителю перебирать пароль. В журнале безопасности Windows и логи подключений нарушителя на узел Active Directory по RDP мы вывели все записи с исключением кода события 4720. Этот код там присутствует, так как количество событий уменьшилось, по сравнению со всеми выведенными результатами (рис. 14).

Filtered: Log: Security; Level: Information; Source: ; Event ID: -4720 Date Range: Last 24 hours. Number of events: 138,818

Keywords	Date and Time
Audit Success	9/23/2025 8:19:04 P
Audit Success	9/23/2025 8:19:04 P
Audit Success	9/23/2025 8:19:03 P
Audit Success	9/23/2025 8:19:03 P
Audit Success	9/23/2025 8:19:03 P

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

- Security ID: SYSTEM
- Account Name: ADS
- Account Domain: AMPIRE
- Logon ID: 0x456147E

Logon Type: 3

This event is generated when a logon session is deleted on the same computer.

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4634  
Level: Information  
User: N/A

Filter Current Log

Logged: Last 24 hours

Event level: Critical, Warning, Verbose, Error,  Information

By log: Event logs: Security

By source: Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-/b

Task Category: Logoff, Group Membership, Logon, Special Logon

4720

Task Category:

Keywords:

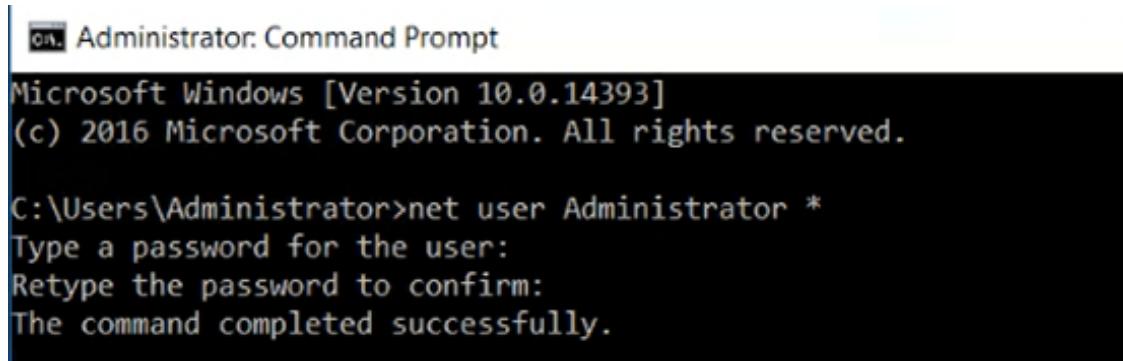
User: <All Users>

Computer(s): <All Computers>

OK Cancel

### Логи подключений по RDP и успешная аутентификация

Решение: изменить пароль к учетной записи администратора на более сложный, не содержащийся в словарях. Заходим в удаленный рабочий стол как администратор. Меняем пароль администратора на узле MS Active Directory командой «net user Administrator \*». В результате изменения ненадежного пароля уязвимость успешно устранена (рис. 15).

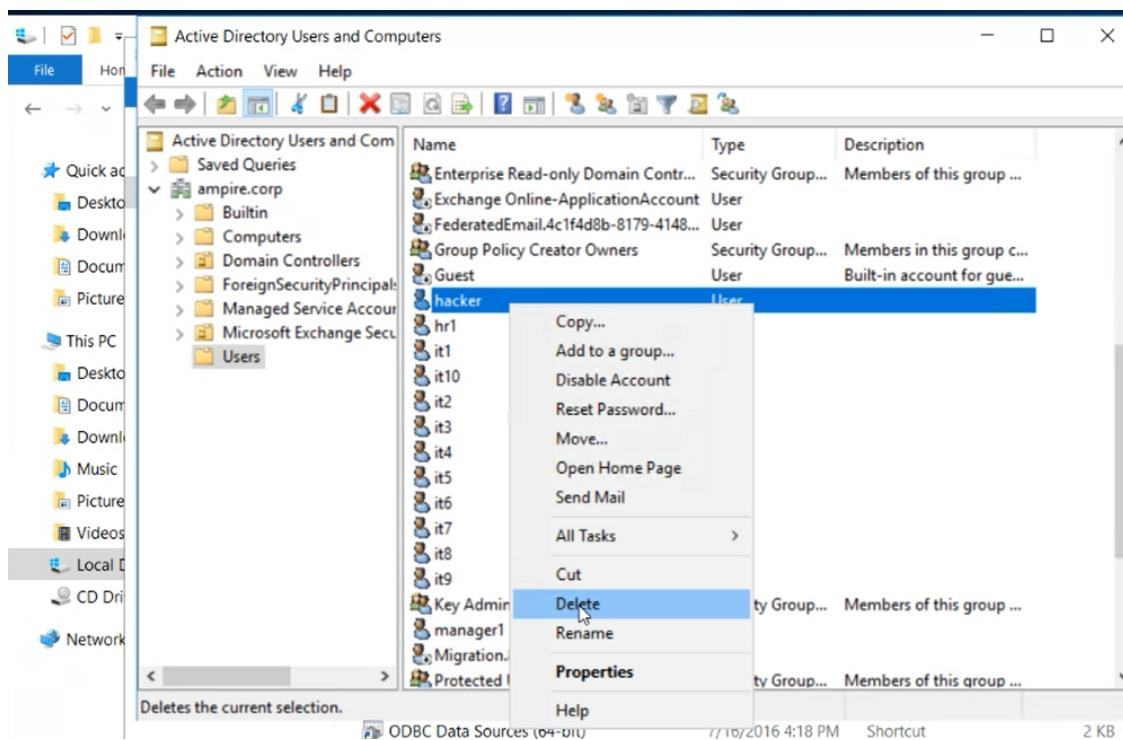


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

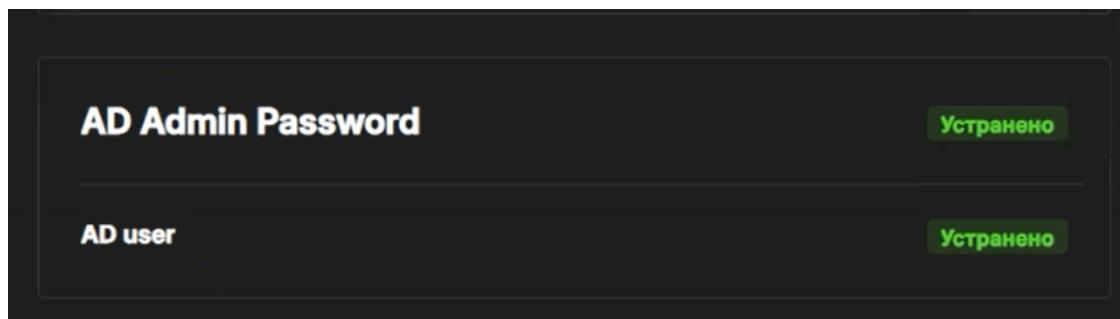
#### Изменение пароля администратора

Последствие: AD User Добавление нового привилегированного пользователя можно отследить с помощью аудита событий входа в учетную запись Windows security, где появится событие с ID 4720. Переходим в Event Viewer и в Windows Logs – Security, затем применяем фильтр на логи. Для удаления пользователя необходимо зайти в Administrative Tools – Active Directory Users and computers. Затем во вкладке Users находим и удаляем нового привилегированного пользователя с именем «Hacked» (рис. 16).



#### Удаление пользователя hacker в AD User & Computers

В результате выполнения вышеупомянутых действий привилегированный пользователь удален, последствие AD User успешно устранено (рис. 17).



*Успешное устранение уязвимости и выполнение последствия*

## 2.3 Отключенная защита антивируса

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. На рисунке изображено значение «true» параметра DisableRealtimeMonitoring, что означает отключенную защиту антивируса на узле (рис. 18).

The screenshot shows a Windows PowerShell window titled 'Select Administrator: Windows PowerShell'. The command 'Get-MpPreference' was run, and its output is displayed. The output shows various parameters and their values. One parameter, 'DisableRealtimeMonitoring', is highlighted with a yellow background and has a value of 'True', indicating that real-time monitoring is disabled. Other parameters shown include 'AttackSurfaceReductionOnlyExclusions', 'AttackSurfaceReductionRules\_Actions', 'AttackSurfaceReductionRules\_Ids', 'CheckForSignaturesBeforeRunningScan', 'CloudBlockLevel', 'CloudExtendedTimeout', 'ComputerID', 'ControlledFolderAccessAllowedApplications', 'ControlledFolderAccessProtectedFolders', 'DisableArchiveScanning', 'DisableAutoExclusions', 'DisableBehaviorMonitoring', 'DisableBlockAtFirstSeen', 'DisableCatchupFullScan', 'DisableCatchupQuickScan', 'DisableEmailScanning', 'DisableIntrusionPreventionSystem', 'DisableIOAVProtection', 'DisablePrivacyMode', and 'ExcludeExtension'.

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

AttackSurfaceReductionOnlyExclusions      :
AttackSurfaceReductionRules_Actions       :
AttackSurfaceReductionRules_Ids          :
CheckForSignaturesBeforeRunningScan      : False
CloudBlockLevel                          : 0
CloudExtendedTimeout                    : 0
ComputerID                             : 817F747C-5BC3-45A8-BE5F-09158DBFB3B7
ControlledFolderAccessAllowedApplications:
ControlledFolderAccessProtectedFolders   :
DisableArchiveScanning                 : False
DisableAutoExclusions                  : False
DisableBehaviorMonitoring              : True
DisableBlockAtFirstSeen                : True
DisableCatchupFullScan                 : True
DisableCatchupQuickScan                : True
DisableEmailScanning                   : True
DisableIntrusionPreventionSystem        :
DisableIOAVProtection                 : True
DisablePrivacyMode                     : False
DisableRealtimeMonitoring              : True
DisableRemovableDriveScanning         : True
DisableRestorePoint                   : True
DisableScanningMappedNetworkDrivesForFullScan: True
DisableScanningNetworkFiles           : False
DisableScriptScanning                 : False
EnableControlledFolderAccess           : 0
EnableFileHashComputation             : False
EnableLowCpuPriority                 : False
EnableNetworkProtection               : 0
ExcludeExtension                      : {ps1, py, zip}
ExclusionPath                         : {C:\}
ExclusionProcess                      :
```

*Настойки Windows Defender*

Создаем карточку инцидента по «Отключенная защита антивируса» (рис. 19).

### Добавление инцидента

Название ⓘ  
Отключена защита антивируса

Дата и время события ⓘ  
27.09.2025 15:30

Источник ⓘ  
10.10.4.10 (Administrator Workstation) ×

Поражённые активы ⓘ  
10.10.4.10 (Administrator Workstation) ×

Описание ⓘ  
Атака на administrator workstation с попыткой отключить антивирус

Рекомендации ⓘ  
на узле вручную удалить запись в реестре, перезапустить антивирус, включить защиту в реальном времени

Индикаторы компрометации ⓘ  
МОНИТОРИНГ ОТКЛЮЧЕН

Прикрепить файл ⓘ  
1.JPG ×  
Выберите файл

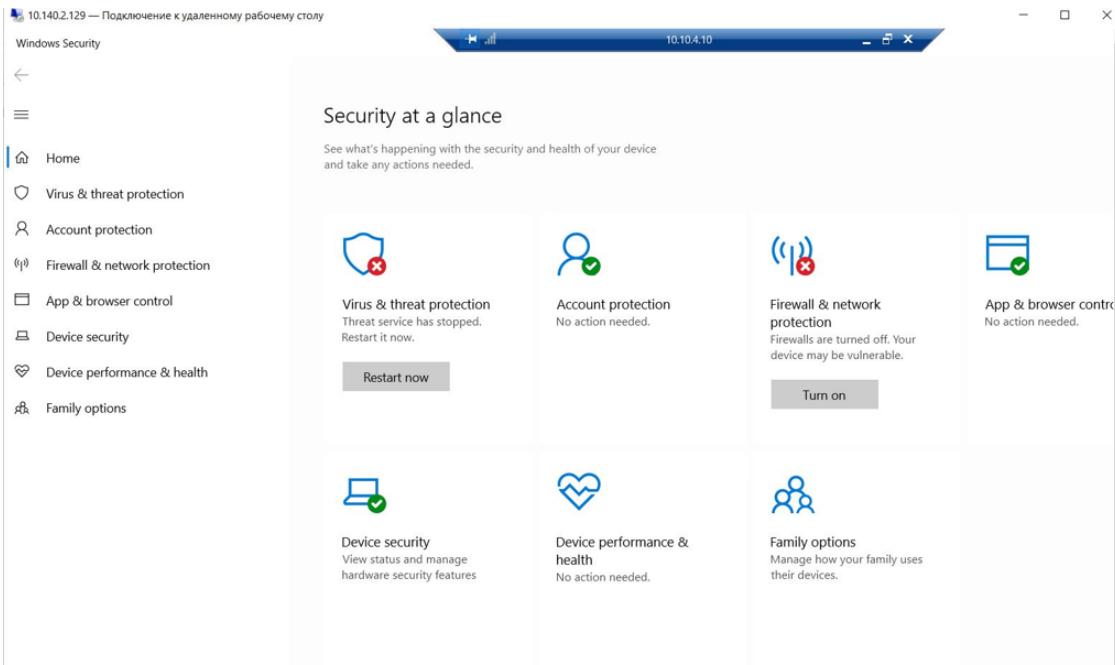
### Создание карточки инцидента

Решение: на узле Administrator Workstation удаляем запись в реестре через консоль, используя команду: REG DELETE (рис. 20).

```
C:\Users\administrator>REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware  
Delete the registry value DisableAntiSpyware (Yes/No)? Y  
The operation completed successfully.  
C:\Users\administrator>
```

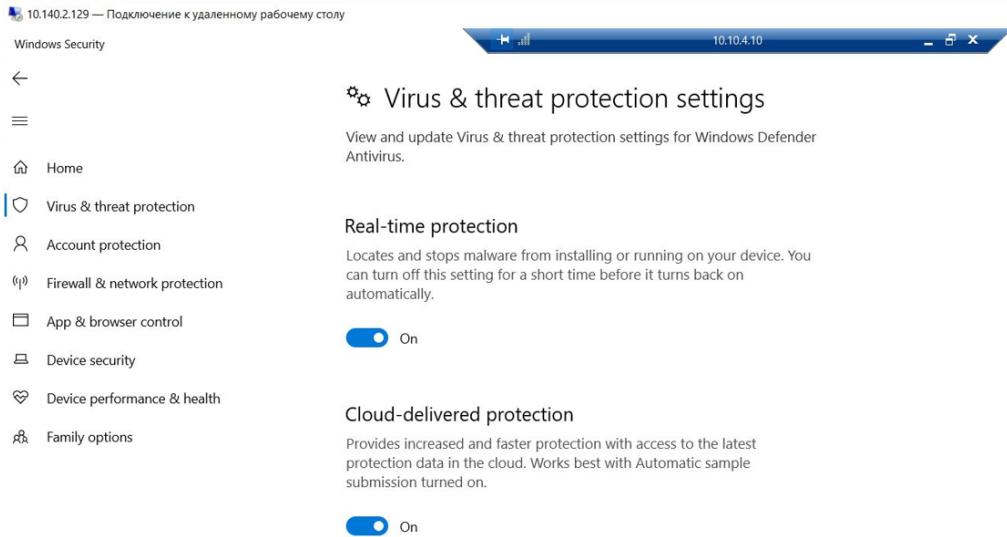
### Удаление записи DisableAntiSpyware в реестре

«HKLMDefender» /v DisableAntiSpyware. Подтвердить действие, далее в Windows Defender перезапускаем Virus & Threat Protection (рис. 21).



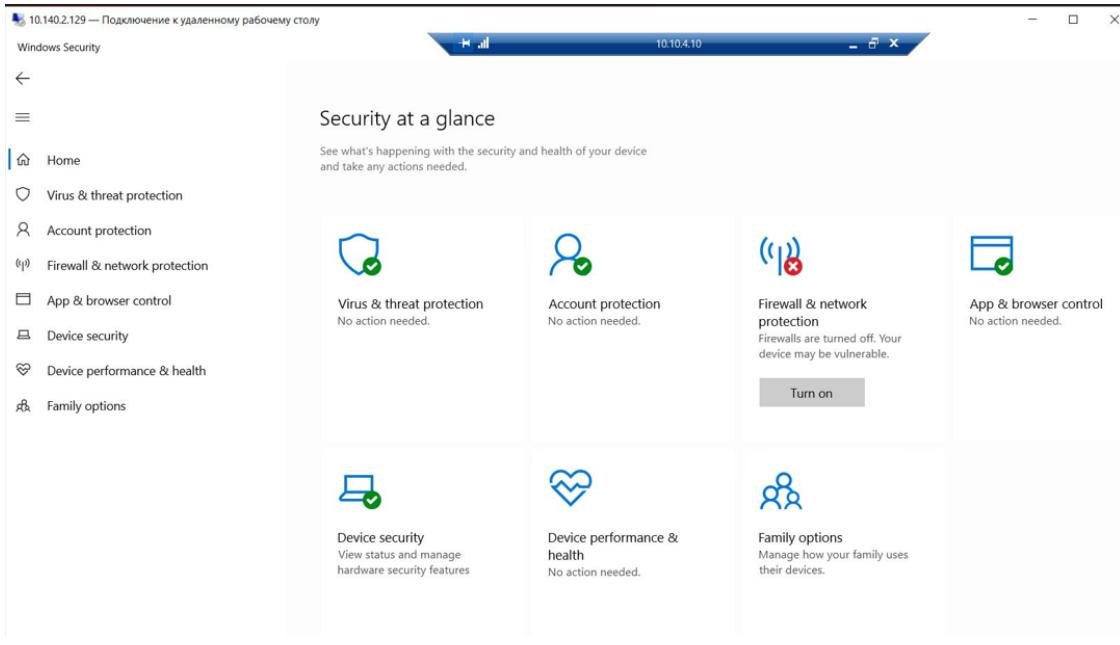
## Интерфейс Windows Defender

Включаем Real-time Protection (рис. 22).



## Включение Real-time Protection

После удаления записи реестра и включения защиты антивирусной программы Microsoft Defender необходимо перезагрузить Windows (рис. 23).



### Проверка включенного Антивируса

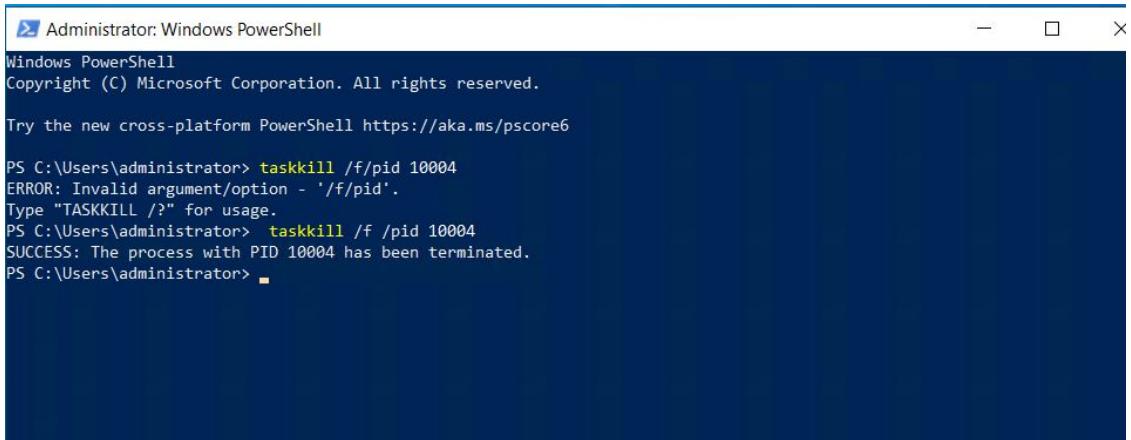
Последствие: Admin meterpreter Установленную сессию с нарушителем можно обнаружить при помощи утилиты netstat с ключами –ano (рис. 24).

```
PS C:\Users\administrator> netstat -ano | more
```

Active Connections				
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	960
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	612
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	7708
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	692
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	1200
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	1856
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	2172
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING	2772
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING	692
TCP	0.0.0.0:49692	0.0.0.0:0	LISTENING	672
TCP	0.0.0.0:49703	0.0.0.0:0	LISTENING	2128
TCP	10.10.4.10:139	0.0.0.0:0	LISTENING	4
TCP	10.10.4.10:3389	10.10.4.12:64891	ESTABLISHED	612
TCP	10.10.4.10:49813	10.10.2.11:443	ESTABLISHED	10068
TCP	10.10.4.10:49824	10.10.2.11:443	ESTABLISHED	10068
TCP	10.10.4.10:49855	10.10.2.11:443	ESTABLISHED	6536
TCP	10.10.4.10:49922	10.10.2.11:443	ESTABLISHED	6536
TCP	10.10.4.10:50158	10.10.1.25:5044	ESTABLISHED	7476
TCP	10.10.4.10:51048	195.239.174.11:443	ESTABLISHED	10004
TCP	10.10.4.10:51512	10.10.2.15:80	ESTABLISHED	1164
TCP	10.10.4.10:52379	10.10.2.15:80	TIME_WAIT	0
TCP	10.10.4.10:52380	10.10.2.15:80	TIME_WAIT	0
TCP	10.10.4.10:52381	10.10.2.15:80	TIME_WAIT	0
TCP	10.10.4.10:52382	10.10.2.15:80	TIME_WAIT	0
TCP	10.10.4.10:52393	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:52394	195.239.174.12:443	TIME_WAIT	0

### Соединение с машиной нарушителя

Для устранения необходимо завершить сессию с машиной нарушителя. Например, при помощи команды taskkill /f /pid. (рис. 25).



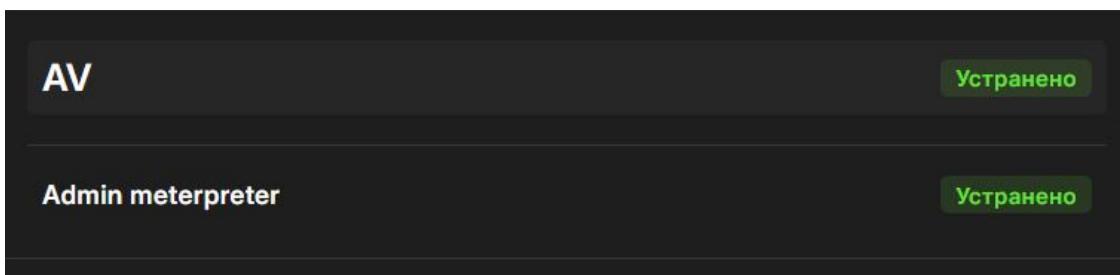
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\administrator> taskkill /f/pid 10004
ERROR: Invalid argument/option - '/f/pid'.
Type "TASKKILL /?" for usage.
PS C:\Users\administrator> taskkill /f /pid 10004
SUCCESS: The process with PID 10004 has been terminated.
PS C:\Users\administrator>
```

### *Остановка процесса*

В результате выполнения команды сессия с машиной нарушителя завершена, последствие Admin meterpreter успешно устранено (рис. 25).



*Успешное устранение уязвимости и выполнение последствия*

## 3 Выводы

В ходе данной лабораторной работы мы смогли устраниить действия нарушителя «Защита контроллера домена предприятия», а так же выполнить последствия к каждой уязвимости.