

# Лабораторная работа №1

Кибербезопасность предприятия

---

Абакумова Олеся    Герра Гарсия Максимиано Антонио    Канева Екатерина    Клюкин  
Михаил    Ланцова Яна

24 сентября 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

Студенты группы НФИбд-02-22:

- Абакумова Олеся
- Герра Гарсия Максимиано Антонио
- Канева Екатерина
- Ключин Михаил
- Ланцова Яна

Устранить уязвимости информационных систем Компании.

# Выполнение лабораторной работы

---

# Первая уязвимость ET SCAN.

События

События за последние 24 часа

У...	Дата и время	ИД	Код событ...	К...	Название правила	Класс
•	13:20:34.348 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:20:05.108 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:19:28.013 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:19:00.016 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:18:19.167 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:17:51.424 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:17:22.625 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:17:21.578 19...		3227018	1	ET SCAN Behavioral Unusu...	network-scan
•	13:16:43.019 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:16:16.084 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:15:35.470 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:15:08.779 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit
•	13:14:36.825 19...		3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit

« < Страница 1 > »

Событие 13:17:21.578 19.09.2025

Событие | Источник | Получатель | Пакет

Тип события	Сигнатурное событие
Протокол	TCP
Код события	3227018

Правило анализа

Класс	network-scan
Группа	scan
Название	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound) var1

Описание:  
Правило обнаруживает факт сканирования

Текст:  
alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 3389 (msg:"ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound) var1";flow: to\_server,flags: S,12,threshold: type both, track by\_src, count 20, seconds 360;reference: url,doc.emergingthreats.net/2001972;classtype: network-scan;sid: 3227018;rev: 3;metadata: affected\_asset dst, affected\_os any, affected\_product n/a, affected\_vendor n/a, attack\_target Client\_and\_Server, tias\_category Scan)

Описание уязвимостей  
url: doc.emergingthreats.net/2001972

Рис. 1: Первая уязвимость ET SCAN.

# Описание первой уязвимости.

The screenshot displays the CVE 25 Years website interface. The top navigation bar includes links for 'About', 'Partner Information', 'Program Organization', 'Downloads', 'Resources & Support', and 'Report/Request'. The main content area is titled 'Required CVE Record Information' and features a 'Collapse all' button. A sidebar on the right, titled 'On This Page', lists 'Required CVE Record Information', 'CNA: Chrome', and 'CVE Program'. The central content area shows details for 'CNA: Chrome', including publication and update dates, a description of the vulnerability, product status, and a table of affected versions.

**Required CVE Record Information**

**Collapse all**

**CNA: Chrome**

**Published:** 2022-02-12 **Updated:** 2022-03-30

**Description**

Use after free in Safe browsing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

**Product Status**  
[Learn more](#)

Vendor	Product
Google	Chrome

**Versions** 1 Total

Default Status: unknown  
Affected

- affected before 97.0.4692.99

Рис. 2: Описание первой уязвимости.

## Вторая уязвимость

У.	Дата и время	ID	Код событ...	K..	Название правила	Класс
•	13:42:22.452 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:41:52.568 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:41:36.178 19...	3227018	1	ET SCAN Behavioral Unusu...	network-scan	
•	13:41:16.367 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:40:48.701 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:40:05.770 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:39:39.574 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:39:10.020 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:38:34.599 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:38:06.562 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:37:22.054 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:36:52.325 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:36:22.947 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	
•	13:36:44.024 19...	3200655	1	AM EXPLOIT Possible Goog...	client-side-exploit	

« < Страница 1 »

**Рис. 3: Вторая уязвимость - клиент сканировал сеть.**



# Добавление инцидента

## Добавление инцидента

Название ⓘ

SQL-инъекция

Дата и время события ⓘ

19.09.2025 13:17

Источник ⓘ

195.239.174.96 (CMS Drupal) ×

Пораженные активы ⓘ

10.10.4.11 (Manager Workstation 1) ×

Описание ⓘ

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

Рекомендации ⓘ

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

Индикаторы компрометации ⓘ

Сканирование сети

Прикрепить файл ⓘ

IDS\_packet\_time-2025-09-19T10\_17\_21.578737Z\_ruleid-3227018.pcap ×

Выберите файл

Рис. 4: Добавление инцидента.

# Подключение к удалённому ПК

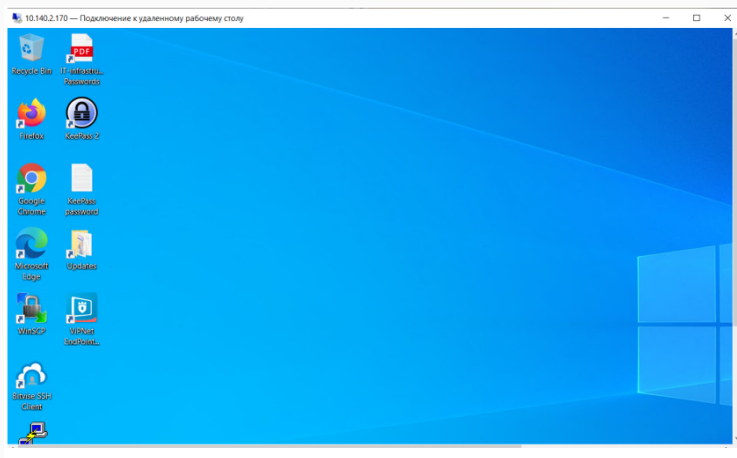
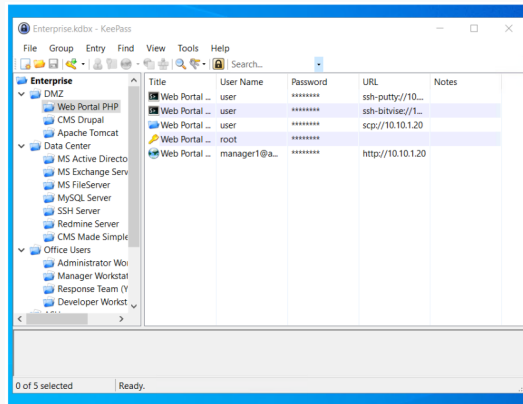


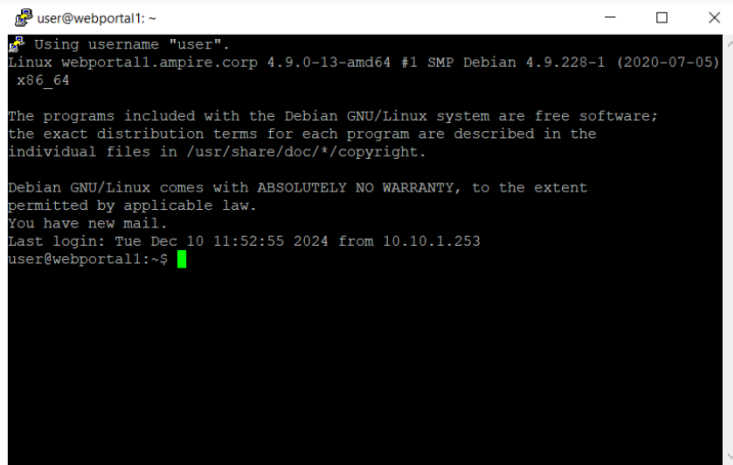
Рис. 5: Подключение к удалённому ПК.

# Посещение веб-портала



**Рис. 6:** Посещение веб-портала.

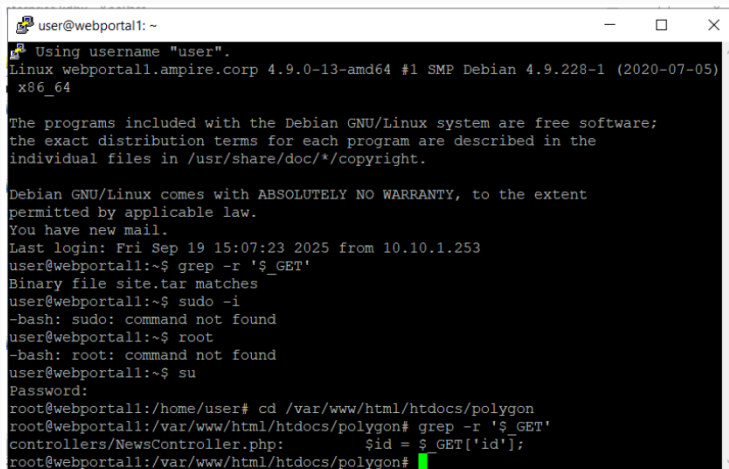
# Командная строка



The image shows a terminal window with a title bar that includes a window icon, the text "user@webportal1: ~", and standard window controls (minimize, maximize, close). The terminal content is as follows:

```
user@webportal1: ~  
Using username "user".  
Linux webportal1.ampire.corp 4.9.0-13-amd64 #1 SMP Debian 4.9.228-1 (2020-07-05)  
x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
Last login: Tue Dec 10 11:52:55 2024 from 10.10.1.253  
user@webportal1:~$
```

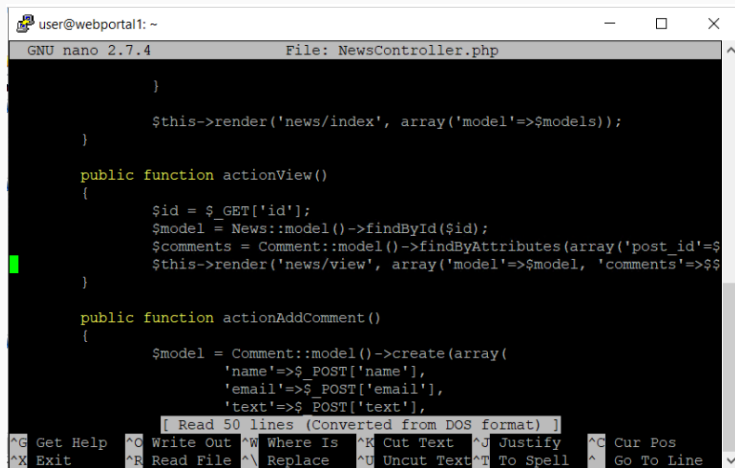
Рис. 7: Командная строка.



```
user@webportal1: ~  
Using username "user".  
Linux webportal1.ampire.corp 4.9.0-13-amd64 #1 SMP Debian 4.9.228-1 (2020-07-05)  
x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
Last login: Fri Sep 19 15:07:23 2025 from 10.10.1.253  
user@webportal1:~$ grep -r '$_GET'  
Binary file site.tar matches  
user@webportal1:~$ sudo -i  
-bash: sudo: command not found  
user@webportal1:~$ root  
-bash: root: command not found  
user@webportal1:~$ su  
Password:  
root@webportal1:/home/user# 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#
```

Рис. 8: Поиск уязвимости.

# Параметры уязвимой функции



```
user@webportal1: ~
GNU nano 2.7.4 File: NewsController.php

    }

    $this->render('news/index', array('model'=>$models));
}

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

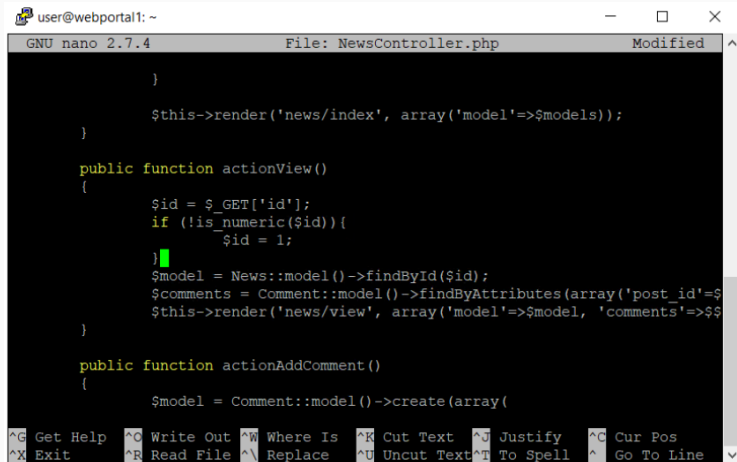
}

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

[ Read 50 lines (Converted from DOS format) ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Рис. 9: Параметры уязвимой функции.

# Исправление уязвимости



```
user@webportal1: ~  
GNU nano 2.7.4 File: 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);  
    $comments = Comment::model()->findByAttributes(array('post_id'=>$id));  
    $this->render('news/view', array('model'=>$model, 'comments'=>$comments));  
}  
  
public function actionAddComment()  
{  
    $model = Comment::model()->create(array(  
        'post_id' => $id,  
        'text' => $_POST['comment'],  
        'user_id' => $user_id,  
        'parent_id' => $parent_id,  
        'status' => 1,  
        'created_at' => time(),  
        'updated_at' => time(),  
    ));  
    $this->render('news/view', array('model'=>$model, 'comments'=>$comments));  
}
```

Рис. 10: Исправляем уязвимости.

# Результат устранения инцидента

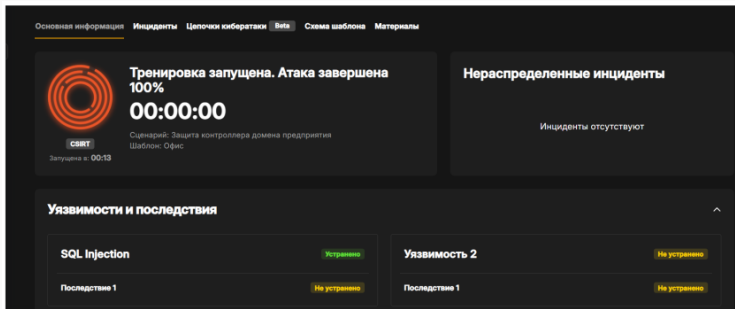


Рис. 11: Результат устранения инцидента.



# Список установленных соединений

```
user@webportal1: ~  
components controllers images js shell.php  
config css index.php models views  
root@webportal1:/var/www/html/htdocs/polygon# cd controllers  
root@webportal1:/var/www/html/htdocs/polygon/controllers# ls  
NewsController.php SiteController.php  
root@webportal1:/var/www/html/htdocs/polygon/controllers# nano NewsController.ph  
P  
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:tpoxy        10.10.1.253:7960  
            users: (("server",pid=644,fd=8))  
ESTAB      0      0      10.10.1.20:44342        195.239.174.11:1085  
            users: (("chisel.sh",pid=7822,fd=11))  
ESTAB      0      0      10.10.1.20:56240        10.10.1.25:5044  
            users: (("filebeat",pid=695,fd=5))  
ESTAB      0      0      10.10.1.20:51720        195.239.174.11:4444  
            users: (("chisel.sh",pid=7822,fd=3), ("sh",pid=7821,fd=3), ("lf0NNR",  
pid=7252,fd=3))  
ESTAB      0      272    10.10.1.20:ssh          10.10.1.253:24376  
            users: (("sshd",pid=7351,fd=4), ("sshd",pid=7342,fd=4))  
ESTAB      0      0      10.10.1.20:58298        10.10.2.17:25004  
            users: (("epp_agentd",pid=32334,fd=37))  
root@webportal1:/var/www/html/htdocs/polygon/controllers#
```

Рис. 12: Список установленных соединений.

# Разрыв соединения 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           10.10.1.20:51720             195.239.174.11:4444
root@webportal1:/var/www/html/htdocs/polygon/controllers#
```

Рис. 13: Разрыв соединения с нарушителем.

# Последствия первой уязвимости устранены

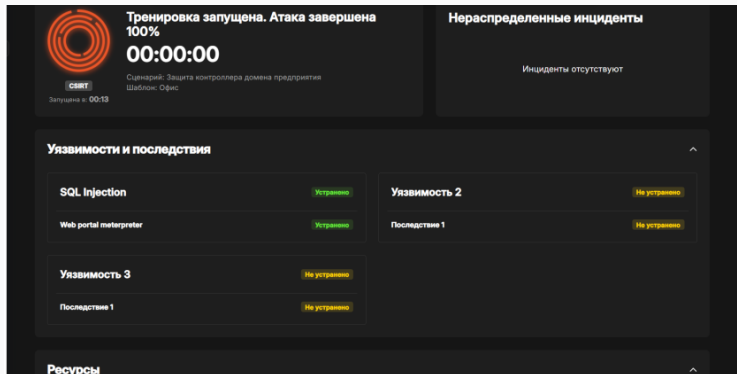


Рис. 14: Последствия первой уязвимости устранены.

# Создание записи об инциденте

Название ⓘ

Отключенная защита антивируса.

Дата и время события ⓘ

19.09.2025 13:17

Источник ⓘ

195.239.174.11 (Kali) x

Пораженные активы ⓘ

10.10.4.10 (Administrator Workstation) x

Описание ⓘ

На узле администратора выключена защита в реальном времени Windows Defender, что дает нарушителю возможность получить контроль над компьютером администратора при запуске им

Рекомендации ⓘ

Решение: на узле Administrator Workstation вручную удалить запись в реестре или через консоль, используя команду. Подтвердить действие, далее в Windows Defender перезапустить Virus & Threat Protection

Индикаторы компрометации ⓘ

Отключена защита

Прикрепить файл ⓘ

IDS\_packet\_time-2025-09-19T10\_17\_22.625628Z\_ruleid-3200655.pcap x

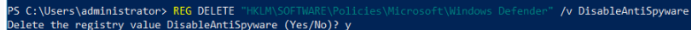
Выберите файл

Отмена

Добавить

Рис. 15: Создание записи об инциденте.

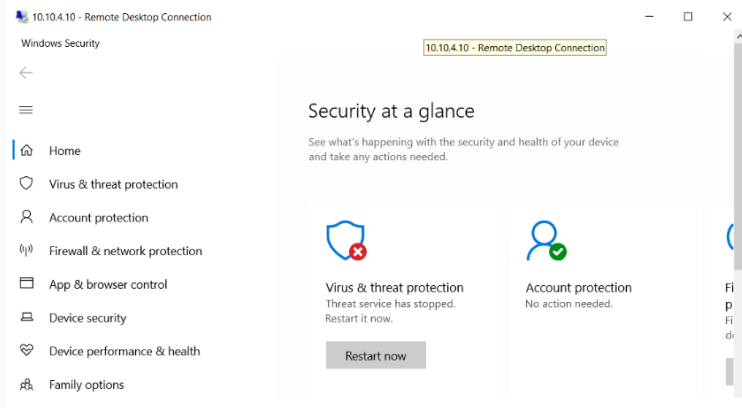
## Удаление записи DisableAntiSpyware в реестре



```
PS C:\Users\administrator> REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware
Delete the registry value DisableAntiSpyware (Yes/No)? y
```

**Рис. 16:** Удаление записи DisableAntiSpyware в реестре.

# Интерфейс Windows Defender



**Рис. 17:** Интерфейс Windows Defender.

# Включение Real-time Protection



**Рис. 18:** Включение Real-time Protection.

# Функционирование антивируса

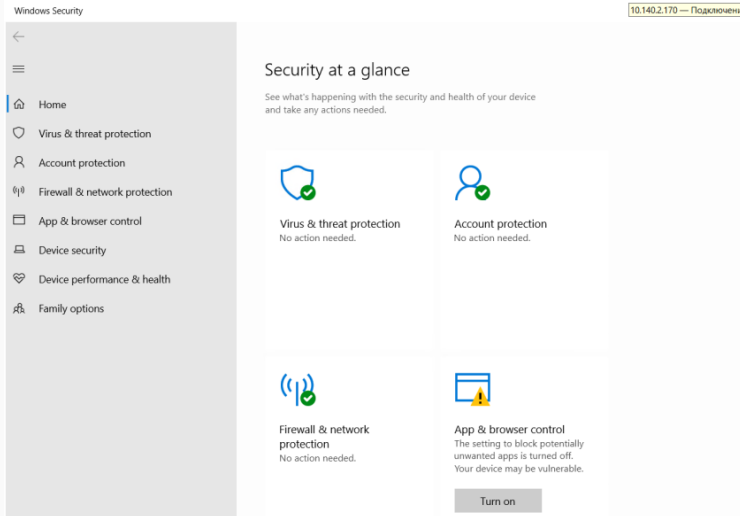
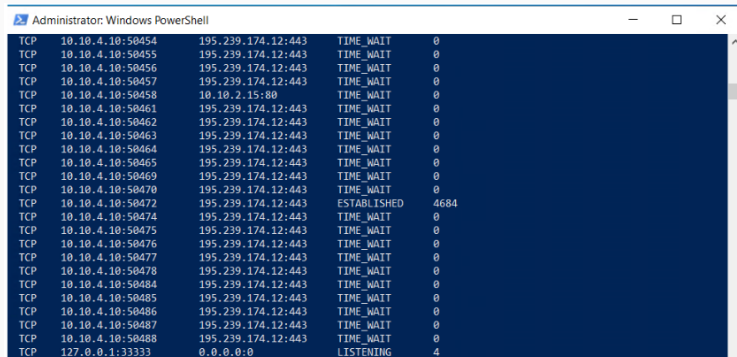


Рис. 19: Функционирование антивируса.




# Соединение с машиной нарушителя



TCP	10.10.4.10:50454	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50455	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50456	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50457	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50458	10.10.2.15:80	TIME_WAIT	0
TCP	10.10.4.10:50461	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50462	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50463	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50464	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50465	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50469	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50470	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50472	195.239.174.12:443	ESTABLISHED	4684
TCP	10.10.4.10:50474	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50475	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50476	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50477	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50478	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50484	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50485	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50486	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50487	195.239.174.12:443	TIME_WAIT	0
TCP	10.10.4.10:50488	195.239.174.12:443	TIME_WAIT	0
TCP	127.0.0.1:33333	0.0.0.0:0	LISTENING	4

Рис. 20: Соединение с машиной нарушителя.

# Остановка процесса



```
PS C:\Users\administrator> taskkill /f /pid 4684  
SUCCESS: The process with PID 4684 has been terminated.  
PS C:\Users\administrator> █
```

Рис. 21: Остановка процесса.

# Логи подключений по RDP и успешная аутентификация

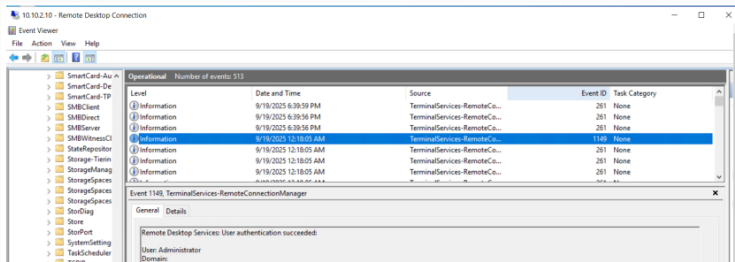
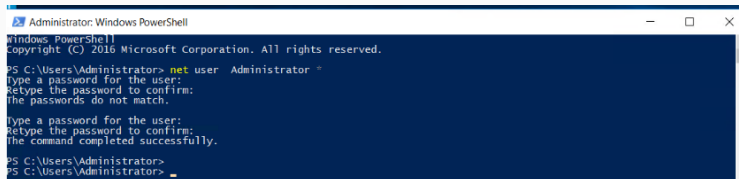


Рис. 22: Логи подключений по RDP и успешная аутентификация.

# Изменение пароля администратора



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> net user Administrator *
Type a password for the user:
Retype the password to confirm:
The passwords do not match.

Type a password for the user:
Retype the password to confirm:
The command completed successfully.

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

Рис. 23: Изменение пароля администратора.

# Удаление привилегированного пользователя

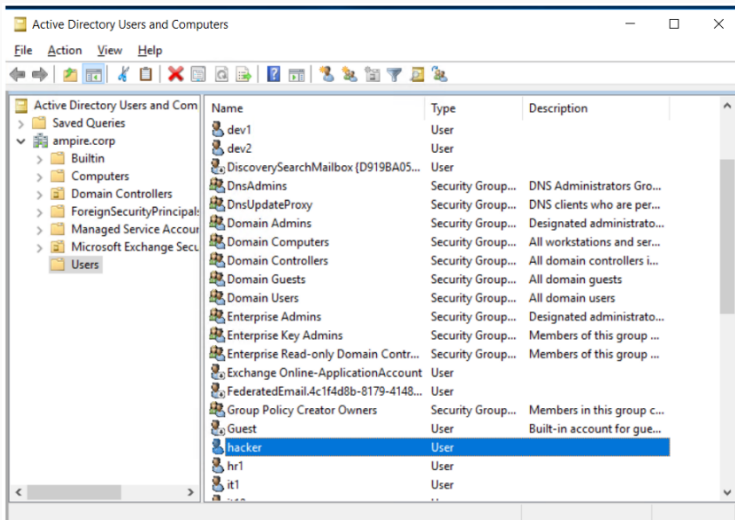


Рис. 24: Удаление привилегированного пользователя.

# Все уязвимости устранены

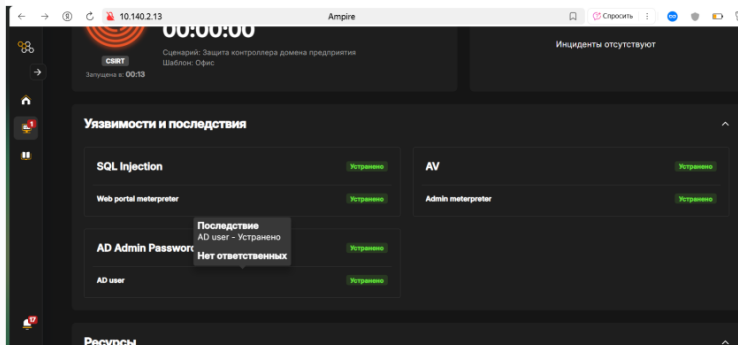


Рис. 25: Все уязвимости устранены.

## Выводы

---

Устранили уязвимости сайта Компании.