

# Выполнение лабораторной работы 3

группа 1е

---

## Цель работы

---

## Цель работы

---

Закрепить практические навыки обнаружения уязвимостей, детектирования инцидентов и восстановления безопасного состояния корпоративных сервисов в рамках сценария «Защита контроллера домена предприятия».

## Задание

---

Провести анализ событий, выявить уязвимости и последствия атак, а также устраниТЬ их, используя средства мониторинга и реагирования, предусмотренные в учебном комплексе Ampire.

## Выполнение лабораторной работы

---

# Уязвимость № 1 – SQL-инъекция (Web Server PHP)

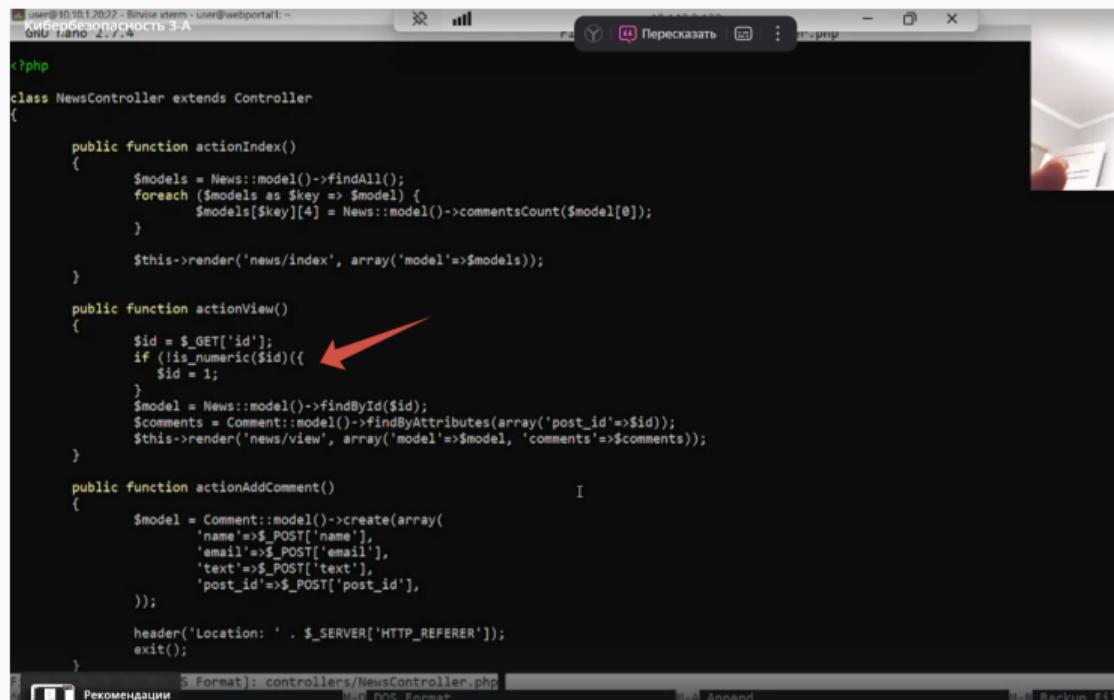
SQL-инъекция позволяла выполнять произвольные запросы к базе данных и загружать вредоносные файлы. Нарушитель использовал параметр id в URL-запросах.

The screenshot shows a dark-themed web interface for reporting a security incident. At the top, there's a navigation bar with a back arrow and the title 'Атака на Web Server PHP на базе Kali'. Below the title, there are two tabs: 'Основная информация' (selected) and 'Чат'. The main content area is divided into several sections:

- Дата и время события**: 21.10.2025 17:36
- Описание**: Атака на Web Server PHP на базе Kali с попыткой эксплуатации уязвимости
- Индикаторы компрометации**:
  - необычные DNS-запросы;
  - несанкционированное изменение реестров или конфигурационных файлов;
- Рекомендации**: Известно, что \$id является уязвимым параметром, следует проверять тип данного параметра. Требуется найти место кода, где данный параметр считывается из GET запроса!
- Оценка**: 5 звезд
- Автор**: Гузева Ирина @11322264-41@pfur.ru
- Ответственный**: Не заполнено
- Источник**: 195.239.174.11
- Пораженные активы**: 10.10.1.20

Figure 1: Описание атаки

## Добавляем проверку типа параметра \$id



```
<?php

class NewsController extends Controller
{
    public function actionIndex()
    {
        $models = News::model()->findAll();
        foreach ($models as $key => $model) {
            $models[$key][4] = News::model()->commentsCount($model[0]);
        }
        $this->render('news/index', array('model'=>$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()
    {
        $model = Comment::model()->create(array(
            'name'=>$_POST['name'],
            'email'=>$_POST['email'],
            'text'=>$_POST['text'],
            'post_id'=>$_POST['post_id'],
        ));
        header('Location: ' . $_SERVER['HTTP_REFERER']);
        exit();
    }
}
```

Figure 2: меняем функцию

Готово)

The screenshot shows a web browser window with a security training interface. At the top, the URL is <https://10.140.2.13/trainings/462/cs...>. The main content area displays a summary of a lab completion:

- Лабораторная 3-А (вторник) 21\_10**
- Тренинг 100%**
- 00:00:00**
- Сценарий:** Защита контроллера домена предприятия
- Шаблон:** Офис

The status bar indicates the lab was launched at 17:38. Below this, there's a section titled "Уязвимости и последствия" (Vulnerabilities and Consequences) with three items:

- SQL Injection** (Устранимо) - Status: Устранимо (Resolved)
- Уязвимость 2** (Не устранимо) - Status: Не устранимо (Not resolved)
- Уязвимость 3** (Не устранимо) - Status: Не устранимо (Not resolved)

A red arrow points from the text "Уязвимость устранена" to the "Устранимо" status of the SQL Injection item.

To the right of the browser window, a terminal window is open, showing PHP code and some log output:

```
lterm - user@webportal: ~
s->render('news/index', array('model'=>$model));
ion actionView()
{
    $id = $_GET['id'];
    if (!is_numeric($id)){
        $id = 1;
    }

    $news = News::model()->findById($id);
    $comments = Comment::model()->findByAttributes(
        array('news_id'=>$news->id));
    s->render('news/view', array('model'=>$model,
        'comments'=>$comments));
}

ion actionAddComment()

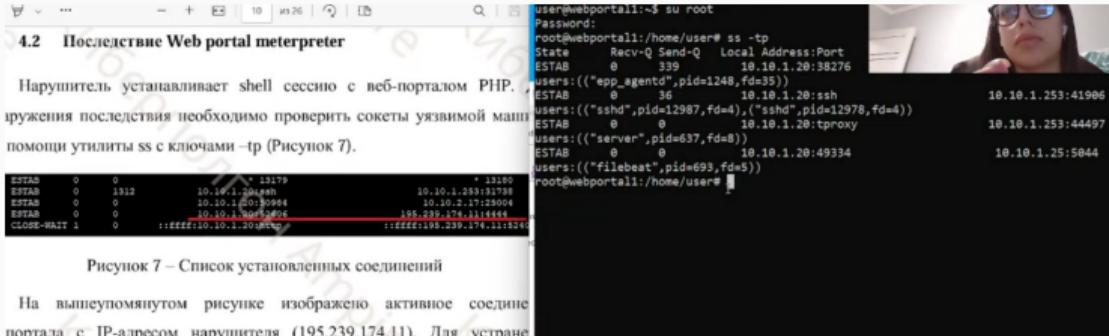
{
    $comment = Comment::model()->create(array(
        'name'=>$_POST['name'],
        'email'=>$_POST['email'],
        'text'=>$_POST['text'],
        'post_id'=>$_POST['post_id'],
        'parent_id'=>null));
    $comment->save();
    header('Location: ' . $_SERVER['HTTP_REFERER']);
    exit();
}

ion actionSearch()

{
    $query = $this->getRequest()->getQuery('query');
    $models = News::model()->search(array(
        'content'=>like($query),
        'status'=>notNull));
    foreach ($models as $key => $model) {
        $models[$key][2] = implode("<i><b>$search</b></i>", $models[$key][2]);
    }
}
of keys received: 2.
22:32:46.324 SFTP channel closed by user.
```

Figure 3: Уязвимость устранена

# Далее нужно устранить последствие. Проверяем сокеты уязвимой машины



4.2 Последствие Web portal meterpreter

```
user@webportal1:~$ su root
Password:
root@webportal1:/home/user# ss -tp
State      Recv-Q Send-Q Local Address:Port
ESTAB      0      399      10.10.1.20:38276
users:(("epp_agentd",pid=1248,fd=35))
ESTAB      0      36       10.10.1.20:ssh
users:(("sshd",pid=12987,fd=4),("sshd",pid=12978,fd=4))
ESTAB      0      0       10.10.1.20:tproxy
users:(("server",pid=637,fd=8))
ESTAB      0      0       10.10.1.20:49354
users:(("filebeat",pid=693,fd=5))
root@webportal1:/home/user#
```

Нарушитель устанавливает shell сессию с веб-порталом PHP. Для устранения последствия необходимо проверить сокеты уязвимой машины помоиутилиты ss с ключами -tp (Рисунок 7).

ESTAB	0	0	:x 19179	*	19180
ESTAB	0	1312	10.10.1.20:48000	10.10.1.235191798	
ESTAB	0	0	10.10.1.20:30984	10.10.2.17:23094	
ESTAB	0	0	10.10.1.20:52406	195.239.174.11:44444	
CLOSE-WAIT	1	0	::ffff:10.10.1.20:48000	::ffff:195.239.174.11:52406	

Рисунок 7 – Список установленных соединений

На вышеупомянутом рисунке изображено активное соединение портала с IP-адресом нарушителя (195.239.174.11). Для устрани

Figure 4: установленные соединения

# Завершаем сессию с нарушителем

Linux	
<команда> -help	Подробная информация о команде
<b>sudo</b>	Позволяет выполнять команды, требующие прав администратора или root
<b>ss</b>	Статистика сокетов, инструмент аналогичный netstat
<b>sudo ss -ltp</b> (Listening, tcp, Processes)	Команда позволяет узнать название и PID процесса, использующего сокет
<b>cd</b>	Переход между директориями. <b>cd ~</b> – перемещение в домашний каталог <b>cd ..</b> – перемещение в один каталог вверх <b>cd --</b> – возвращение в предыдущий каталог <b>cd /</b> – перемещение в корневую директорию
<b>ls</b>	Отображение содержимого директории. -a – отобразить скрытые файлы -l – подробная информация о файлах и каталогах
<b>cat file.txt</b>	Вывод содержимого файла
<b>nano file.txt</b>	Редактор файлов
<b>grep</b>	Поиск файлов в директориях и строк в файлах -t – поиск в директории и вложенных директориях
<b>chmod</b>	Установка прав на файл
<b>kill -9 &lt;pid&gt;</b>	Принудительное завершение процесса
<b>uname</b>	Подробная информация о системе
<b>passwd</b>	Позволяет изменить пароль учетной записи пользователя

25

```
users:(("server",pid=637,fd=8))
ESTAB      0      0          10.10.1.20:49334
users:(("filebeat",pid=693,fd=5))
root@webportal1:/home/user# ss -tp
State      Recv-Q Send-Q  Local Address:Port
ESTAB      0      204          10.10.1.20:ssh
users:(("sshd",pid=12987,fd=4),("sshd",pid=12978,fd=4))
ESTAB      0      0          10.10.1.20:tproxy
users:(("server",pid=637,fd=8))
SYN-SENT   0      1          10.10.1.20:36620
users:(("puppet",pid=13554,fd=6))
ESTAB      0      0          10.10.1.20:49334
users:(("filebeat",pid=693,fd=5))
ESTAB      0      0          10.10.1.20:38474
users:(("epp_agentd",pid=1248,fd=35))
root@webportal1:/home/user# ss kill 13554
Error: an inet prefix is expected rather than "kill".
Cannot parse dst/src address.
root@webportal1:/home/user# kill 13554
root@webportal1:/home/user# ss -tp
State      Recv-Q Send-Q  Local Address:Port
ESTAB      0      204          10.10.1.20:ssh
users:(("sshd",pid=12987,fd=4),("sshd",pid=12978,fd=4))
SYN-SENT   0      1          10.10.1.20:36404
users:(("puppet",pid=13554,fd=5))
ESTAB      0      0          10.10.1.20:tproxy
users:(("server",pid=637,fd=8))
ESTAB      0      0          10.10.1.20:49334
users:(("filebeat",pid=693,fd=5))
ESTAB      0      0          10.10.1.20:3887
users:(("epp_agentd",pid=1248,fd=35))
root@webportal1:/home/user# kill -9 13554
root@webportal1:/home/user#
```

Figure 5: Завершение сессии

Готово!

The screenshot shows a CSIRT dashboard interface. At the top, there's a header with tabs for 'Импорт избранного' and 'Grok'. Below the header, a large circular progress bar indicates '100%' completion with the text '00:00:00'. A message below the progress bar reads 'Сценарий: Защита контроллера домена предприятия' and 'Шаблон: Офис'. The date 'Запущена в: 17:36' is also present. The main content area is titled 'Уязвимости и последствия' (Vulnerabilities and Consequences). It lists three items:

- SQL Injection**: Status 'Устранено' (Resolved). Below it, 'Web portal meterpreter' is also marked as 'Устранено' (Resolved).
- Уязвимость 2**: Status 'Не устранено' (Not resolved). Below it, 'Последствие 1' is also marked as 'Не устранено' (Not resolved).
- Уязвимость 3**: Status 'Не устранено' (Not resolved). Below it, 'Последствие 1' is also marked as 'Не устранено' (Not resolved).

A red arrow points from the text 'Последствие 1' under 'Уязвимость 2' towards the bottom right of the screen, where a terminal window is visible. The terminal window displays several log entries related to network connections and processes on a host at 10.10.1.20. The log entries include:  
server@10.10.1.20:22 - Bitvise xterm - user@webportal1: ~  
s:(( "server", pid=637, fd=8 ))  
SENT 0 1 10.10.1.20:36  
s:(( "puppet", pid=13554, fd=6 ))  
B 0 0 10.10.1.20:49  
s:(( "filebeat", pid=693, fd=5 ))  
B 0 0 10.10.1.20:36  
s:(( "epp\_agentd", pid=1248, fd=35 ))  
@webportal1:/home/user# ss kill 13554  
r: an inet prefix is expected rather than a port  
at parse dst/src address.  
@webportal1:/home/user# kill 13554  
@webportal1:/home/user# ss -tp  
e Recv-Q Send-Q Local Address:Port  
B 0 204 10.10.1.20:36  
s:(( "sshd", pid=12987, fd=4 ), ("sshd", pid=12987, fd=4 ))  
SENT 0 1 10.10.1.20:36  
s:(( "puppet", pid=13554, fd=5 ))  
B 0 0 10.10.1.20:tp  
s:(( "server", pid=637, fd=8 ))  
B 0 0 10.10.1.20:49  
s:(( "filebeat", pid=693, fd=5 ))  
B 0 0 10.10.1.20:36  
s:(( "epp\_agentd", pid=1248, fd=35 ))  
@webportal1:/home/user# kill -9 13554  
@webportal1:/home/user# ss -tp  
e Recv-Q Send-Q Local Address:Port  
B 0 204 10.10.1.20:36  
s:(( "sshd", pid=12987, fd=4 ), ("sshd", pid=12987, fd=4 ))  
B 0 0 10.10.1.20:tp  
s:(( "server", pid=637, fd=8 ))  
B 0 0 10.10.1.20:49  
s:(( "filebeat", pid=693, fd=5 ))  
B 0 339 10.10.1.20:36  
s:(( "epp\_agentd", pid=1248, fd=35 ))  
@webportal1:/home/user#

Figure 6: Последствие устранено

## Уязвимость № 2 – отключённая защита антивируса (Administrator Workstation)

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

Атака на Administrator Workstation на базе Kali

Основная информация Чат

Дата и время события ⓘ  
21.10.2025 17:36

Описание ⓘ  
Атака на Administrator Workstation на базе Kali с попыткой эксплуатации уязвимости отключение защиты антивируса

Индикаторы компрометации ⓘ  
- необычные DNS-запросы; - подозрительные файлы, приложения или процессы;

Рекомендации ⓘ

Методика Атаки на Windows Workstation с использованием уязвимости отключения защиты антивируса (Windows Defender) в реальном времени.

10 / 17

# Удаляем запись

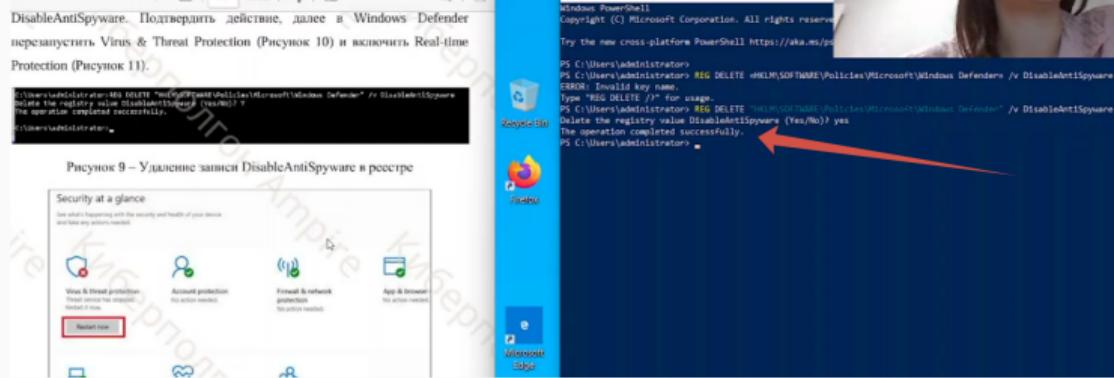


Рисунок 9 – Удаление записи DisableAntiSpyware в реестре



Figure 8: Удаление записи DisableAntiSpyware в реестре

И поскольку установленной сессии с нарушителем не обнаружилось, у нас устранились и уязвимость и последствие

Готово

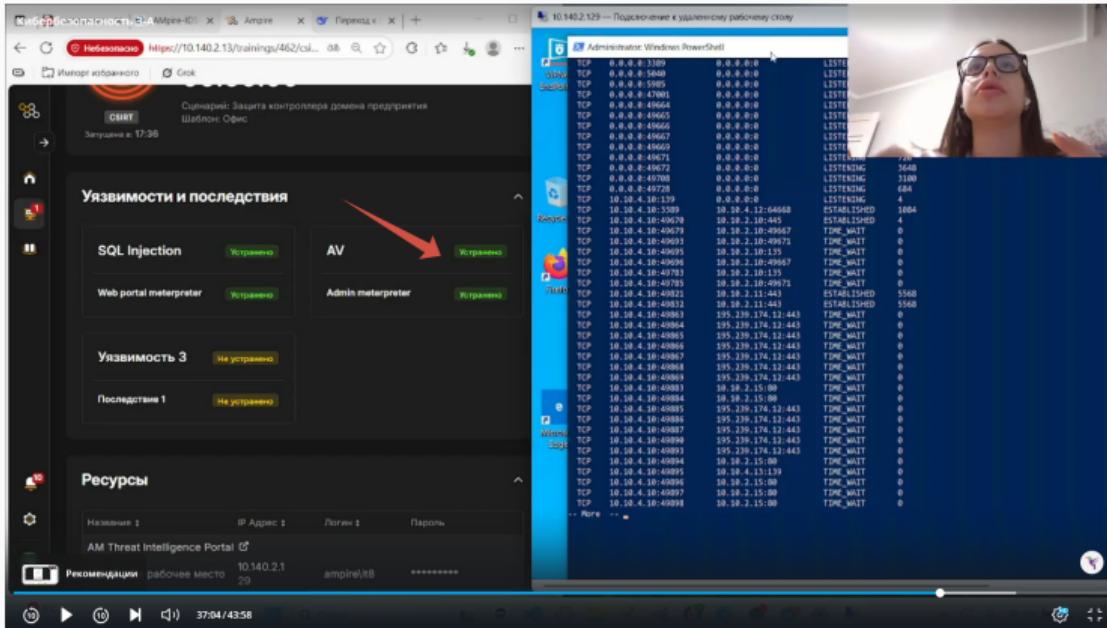


Figure 9: все устраниено

## Уязвимость № 3 – слабый пароль учётной записи (MS Active Directory)

На узле MS Active Directory установлен слабый пароль к учетной записи администратора, что позволяет нарушителю перебирать пароль

◀ Атака на MS Active Directory на базе Kali

Основная информация Чат

Дата и время события ⓘ  
21.10.2025 17:41

Описание ⓘ  
Атака на MS Active Directory на базе Kali с попыткой эксплуатации уязвимости слабый пароль учетной записи

Индикаторы компрометации ⓘ  
- подозрительная активность со стороны привилегированных записей; - внеплановое обновление ПО;

Рекомендации ⓘ  
Изменить пароль к учетной записи администратора на более сложный, не содержащийся в словарях

Прикреплённые файлы ⓘ

Оценка  
★ ★ ★

Автор  
Гузев @1132

Ответственный  
Не заполнено

Источник  
195.239.17

Поражённы  
10.10.2.10

# Меняем пароль к учетной записи администратора на более сложный, не содержащийся в словарях

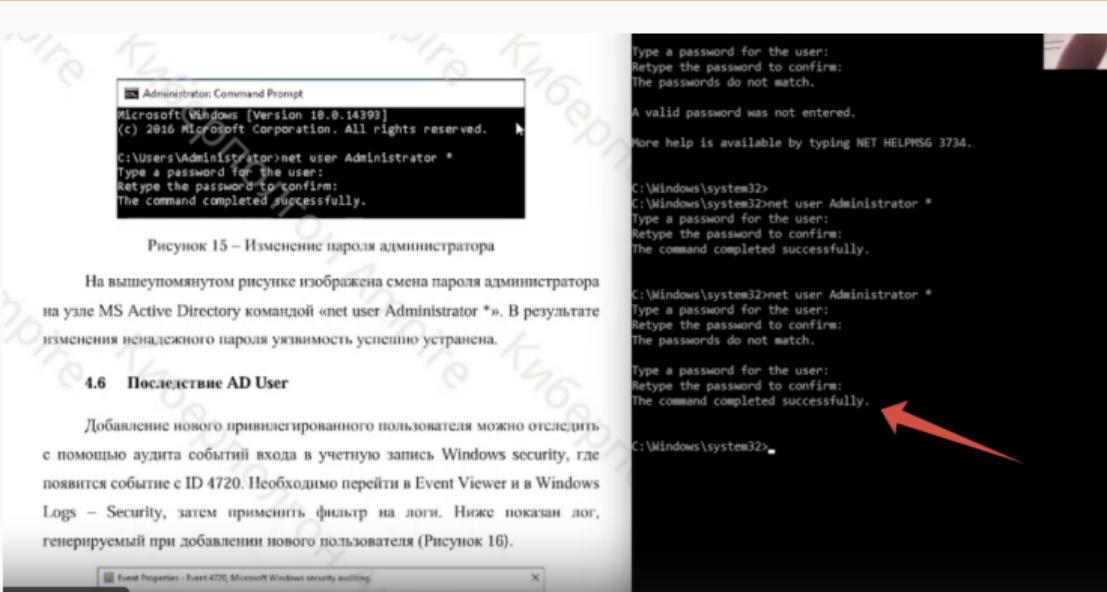


Рисунок 15 – Изменение пароля администратора

На вышеупомянутом рисунке изображена смена пароля администратора на узле MS Active Directory командой «`net user Administrator *`». В результате изменения недействительного пароля уязвимость успешно устранена.

## 4.6 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. Необходимо перейти в Event Viewer и в Windows Logs – Security, затем применить фильтр на логи. Ниже показан лог, генерируемый при добавлении нового пользователя (Рисунок 16).

Figure 11: Изменение пароля администратора

# Добавление нового привилегированного пользователя можно отследить

с помощью аудита событий входа в учетную запись Windows security. Удаляем пользователя с именем “Hacker”

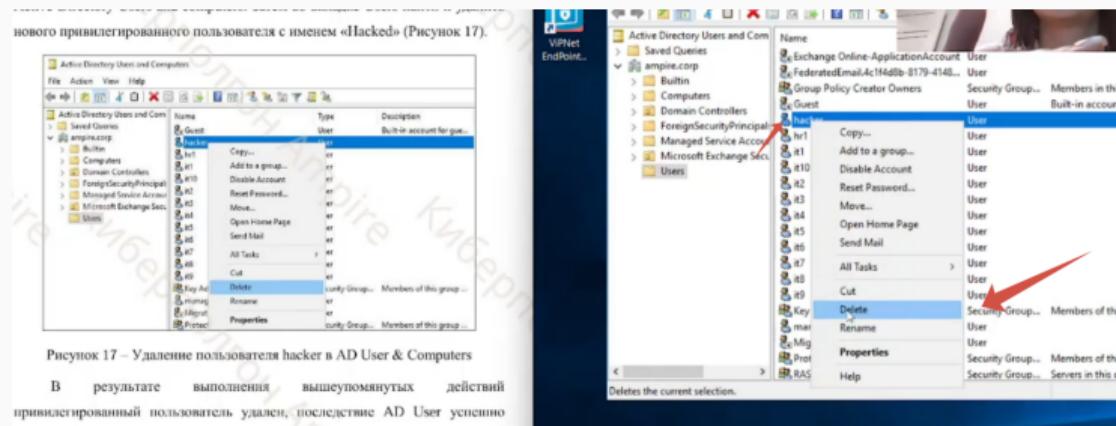


Figure 12: Удаление пользователя hacker в AD User & Computers

# Уязвимость и последствие успешно устранены!

The screenshot displays two windows side-by-side. On the left is the 'AM Threat Intelligence Portal' showing a summary of vulnerabilities and their status. On the right is the 'Active Directory Users and Computers' management console.

**Left Window (AM Threat Intelligence Portal):**

- Top Bar:** Запущена в: 17:36, Лабораторная 3-А (вторник) 21.10, (21 окт. 23:35) Последствие "AD user" устранено.
- Section: Уязвимости и последствия**
  - SQL Injection:** Устранено
  - Web portal meterpreter:** Устранено
  - Уязвимость:** Сервер недоступен
  - Последствие 1:** Сервер недоступен
  - AD Admin...:** Устранено
  - AD user:** Устранено
- Section: Ресурсы**

Название	IP Адрес	Логин	Пароль
AM Threat Intelligence Portal	10.140.2.1 29	ampire\lt8	*****
Удалённое рабочее место	10.140.2.1	admin	*****

A red arrow points from the 'Устранено' button next to the 'AD user' entry in the 'Уязвимости и последствия' section towards the 'Active Directory Users and Computers' window on the right.

**Right Window (Active Directory Users and Computers):**

- File Menu:** File, Action, View, Help
- Navigation:** Active Directory Users and Computers, Active Directory Users and Computers
- Tree View:** Active Directory Users and Computers, Active Directory Users and Computers, ampire.corp, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, Microsoft Exchange Security Groups, Users.
- List View (Users):**
  - Name
  - Exchange Online...
  - FederatedEmailA...
  - Group Policy Cre...
  - Guest
  - hr1
  - lt1
  - lt10
  - lt2
  - lt3
  - lt4
  - lt5
  - lt6
  - lt7
  - lt8
  - lt9
  - Key Admins
  - manager1
  - Migration.8f3e771
  - Protected Users
  - RAS and IAS Serv...
  - Read-only Domai...

Figure 13: 15

## Выводы

---

## Выводы

---

В ходе лабораторной работы были:

- обнаружены и устраниены уязвимости: SQL-инъекция, отключённая защита антивируса, слабый пароль администратора;
- ликвидированы последствия атак (веб-шелл, meterpreter-сессии, несанкционированные пользователи);
- восстановлена безопасность всех узлов системы;
- применены средства анализа и детектирования – ViPNet IDS NS, TIAS и Security Onion.

Система приведена в безопасное состояние.

:::