

Лабораторная работа 2-А

Кибербезопасность предприятия

Ищенко Ирина Мишина Анастасия Дикач Анна Галацан Николай Амуничников Антон Барсегян Вардан Дудырев Глеб Дымченко Дмитрий

16 октября 2025 г.

Российский университет дружбы народов, Москва, Россия

- НПИбд-01-22
- Российский университет дружбы народов

Разобраться с сценарием действий нарушителя “Защита контроллера домена предприятия”.
Выявить и устранить уязвимости и их последствия.

Выявленные уязвимости и последствия

Лабораторная 2-А (НПИ) 09_10

Группа: НПИбд-01-22 (В) - суббота

Добавить инцидент

Основная информацияИнцидентыЦепочки кибератакиBetaСхема шаблонаМатериалы

ПоискФильтр

ПлиткаТаблица

В работе☆☆☆☆☆

Подбор паролей на хост Active Directory

Автор: Мишина Анастасия @1132226532@pf...
Ответственный: Ищенко Ирина @1132226529@pf...

Сообщений: 0
09.10.2025 14:07

В работе☆☆☆☆☆

SQL-инъекция

Автор: Ищенко Ирина @1132226529@pf...
Ответственный: Галацан Николай @1032225763@pf...

Сообщений: 0
09.10.2025 14:05

В работе☆☆☆☆☆

Отключенная защита антивируса

Автор: Мишина Анастасия @1132226532@pf...
Ответственный: Галацан Николай @1032225763@pf...

Сообщений: 0
09.10.2025 13:50

На узле Web Server PHP находится уязвимый веб-сервис на порту 80. Нарушитель использует уязвимый параметр `id` в GET-запросе для загрузки и выполнения `php reverse shell`.

Описание инцидента

Лабораторная 2-А (НПИ) 09_10
Группа: НПИбд-01-22 (В) - суббота

Добавление инцидента

Название ⓘ
SQL-инъекция

Дата и время события ⓘ
📅 09.10.2025 14:05

Источник ⓘ
195.239.174.11 (Kali) x

Поражённые активы ⓘ
10.10.1.20 (Web Server PHP) x

Описание ⓘ
Зафиксировано большое количество целенаправленных попыток проведения атаки типа SQL Injection

Рекомендации ⓘ

- Провести аудит атакуемого ресурса на наличие уязвимости к атакам типа SQL-Injection и устранить при обнаружении
- Отключить пораженный актив от вычислительной сети

Индикаторы компрометации ⓘ
ET SCAN Sqlmap SQL Injection Scan

Прикрепить файл ⓘ

🔄 IDS_packet_time-2025-10-09T11_05_41.808002Z_ruleid-2008538.pcap x

Выберите файл

Отмена

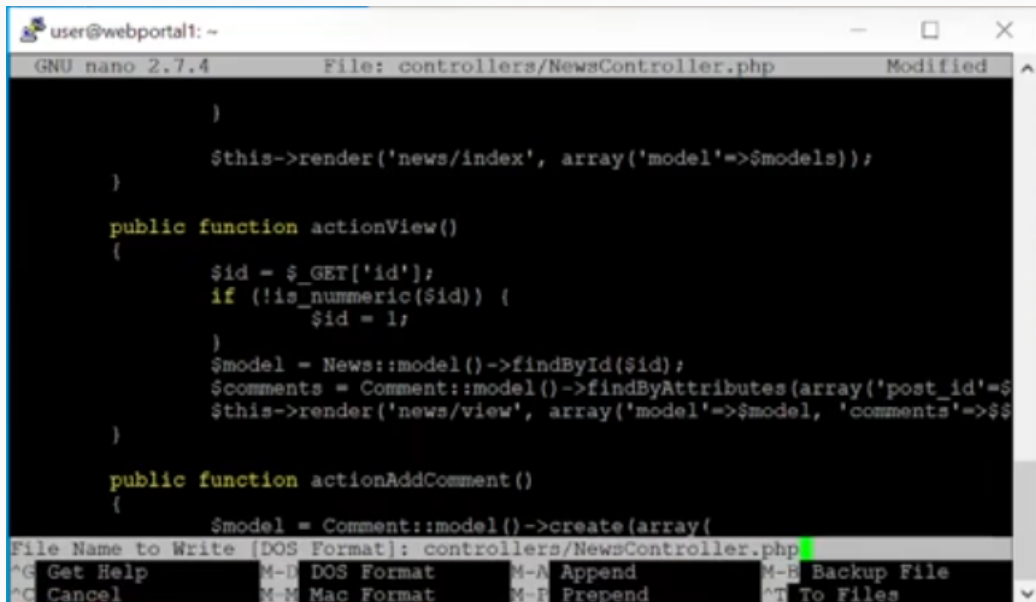
Добавить

Находим место кода, где `$id` считывается из GET запроса

Считываем параметр сайта в функции `actionView()` в файле `NewsController.php`

Используем функцию `is_numeric` для проверки типа `$id`. Она возвращает `True` в случае, если `$id` - число, иначе - `False`. В случае успешной проверки параметр будет передаваться в запрос, иначе - запрос будет статичным и независимым от `$id`.

После внесения изменений в файл конфигурации и проверки значения параметра `$id` уязвимость SQL-инъекции успешно устранена.



```
user@webportal1: ~
GNU nano 2.7.4 File: controllers/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(
File Name to Write [DOS Format]: controllers/NewsController.php
^G Get Help      M-B DOS Format  M-A Append      M-B Backup File
^C Cancel        M-M Mac Format  M-P Prepend     ^T To Files
```


Нарушитель устанавливает shell сессию с веб-порталом PHP. Для обнаружения последствия проверяем сокет уязвимой машины при помощи утилиты ss с ключами -tp.

Последствия Web portal meterpreter

```
user@webportal1: ~  
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/NewsController.php  
root@webportal1:/var/www/html/htdocs/polygon# nano controllers/NewsController.php  
root@webportal1:/var/www/html/htdocs/polygon# cd  
root@webportal1:~# ss -tp  
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port  
ESTAB      0      0      10.10.1.20:tpoxy           10.10.1.253:64811  
           users: ({"server",pid=626,fd=8})  
ESTAB      0      0      10.10.1.20:53246          10.10.1.25:5044  
           users: ({"filebeat",pid=705,fd=5})  
ESTAB      0      272    10.10.1.20:ssh            10.10.1.253:47737  
           users: ({"sshd",pid=9177,fd=4}, {"sshd",pid=9141,fd=4})  
ESTAB      0      339    10.10.1.20:43492          10.10.2.17:25004  
           users: ({"epp_agentd",pid=1531,fd=35})  
ESTAB      0      0      10.10.1.20:45306          195.239.174.11:4444  
           users: ({"chisel.sh",pid=20161,fd=3}, {"sh",pid=20160,fd=3}, {"Eq6sPL",pid=7447,fd=3})  
ESTAB      0      0      10.10.1.20:53304          195.239.174.11:1085  
           users: ({"chisel.sh",pid=20161,fd=11})  
CLOSE-WAIT 1      0      ::ffff:10.10.1.20:http      ::ffff:195.239.174.11:57486  
           users: ({"apache2",pid=1310,fd=13})  
root@webportal1:~#
```

Обнаруживаем то что есть активное соединение веб-портала с IP-адресом нарушителя. Для устранения пользуемся 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`. В результате выполнения команды сессия с нарушителем завершена.

```
user@webportal1: ~  
root@webportal1:~# ss -K dst '195.239.174.11' dport=4444  
Error: an inet prefix is expected rather than "dport=4444".  
Cannot parse dst/src address.  
root@webportal1:~# 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      10.10.1.20:45306        195.239.174.11:4  
444  
root@webportal1:~#
```

На рабочей станции администратора отключена защита в реальном времени Windows Defender (параметр `DisableAntiSpyware` в реестре), что позволяет запустить вредоносный скрипт.

Добавление инцидента

Название ⓘ

Отключенная защита антивируса

Дата и время события ⓘ

📅 09.10.2025 13:50

Источник ⓘ

195.239.174.11 (Kali) ✕

Поражённые активы ⓘ

10.10.4.10 (Administrator Workstation) ✕

Описание ⓘ

Отключена защита антивируса

Рекомендации ⓘ

Удалить запись в реестре. В Windows Defender перезапустить защиту. Завершить сессию с машиной нарушителя.

Индикаторы компрометации ⓘ

Windows Defender – в Powershell команда Get-MpP

Прикрепить файл ⓘ



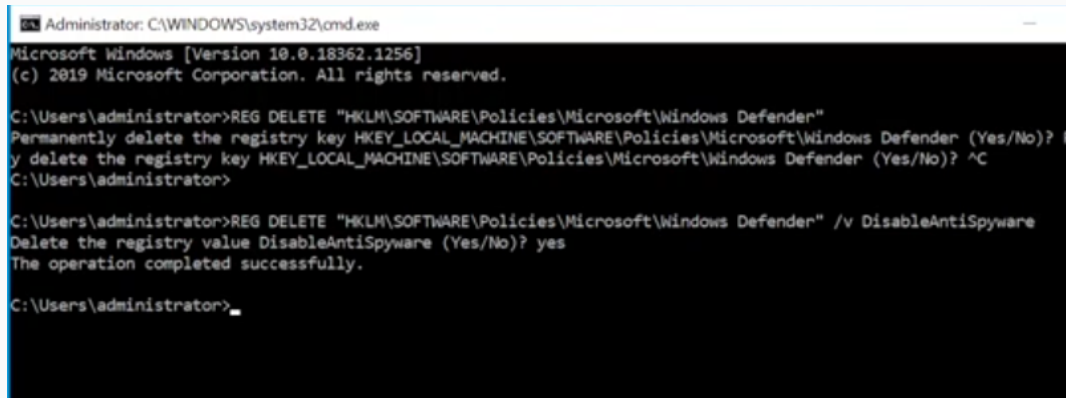
Перетяните файл в эту область или

Выберите файл

Отмена

Добавить

На узле Administrator Workstation вручную удаляем запись в реестре или через консоль с помощью команды.

A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\WINDOWS\system32\cmd.exe". The window content shows the following text:

```
Microsoft Windows [Version 10.0.18362.1256]  
(c) 2019 Microsoft Corporation. All rights reserved.  
  
C:\Users\administrator>REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender"  
Permanently delete the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender (Yes/No)? y  
y delete the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender (Yes/No)? ^C  
C:\Users\administrator>  
  
C:\Users\administrator>REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware  
Delete the registry value DisableAntiSpyware (Yes/No)? yes  
The operation completed successfully.  
  
C:\Users\administrator>_
```

Рис. 7: Удаление записи в реестре

Подтверждаем действие, далее в Windows Defender перезапускаем Virus & Threat Protection и включаем Real-time Protection.



После Удаления записи реестра и включения защиты антивирусной программы перезапускаем Windows.

Последствия Admin meterpreter

Установленную сессию с нарушителем находим при помощи утилиты netstat с ключами -ano

Для устранения завершаем сессию с машиной нарушителя.

```
TCP    10.10.4.10:50158      10.10.1.25:5044      ESTABLISHED    10916
TCP    10.10.4.10:52558      195.239.174.11:444    ESTABLISHED    11032
TCP    10.10.4.10:55385      10.10.2.11:443        ESTABLISHED    6476
TCP    10.10.4.10:55683      10.10.2.11:443        ESTABLISHED    6476
TCP    10.10.4.10:56540      10.10.2.15:80         ESTABLISHED    11252
TCP    10.10.4.10:57398      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57411      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57412      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57413      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57414      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57415      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57418      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57419      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57421      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57422      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57423      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57424      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57425      195.239.174.12:443    TIME_WAIT      0
TCP    10.10.4.10:57438      195.239.174.12:443    TIME_WAIT      0
```

```
PS C:\Users\administrator> taskkill /f /pid 11032
SUCCESS: The process with PID 11032 has been terminated.
```

```
PS C:\Users\administrator>
```

На узле MS Active Directory установлен слабый пароль учетной записи администратора, что позволяет нарушителю успешно подобрать его брутфорс-атакой (RDP Bruteforce). В журнале безопасности Windows событие с ID 1149 указывает на успешную аутентификацию.

Добавление инцидента

Название ⓘ

Подбор паролей на хост Active Directory

Дата и время события ⓘ

📅 09.10.2025 14:07

Источник ⓘ

10.10.1.20 (Web Server PHP) x

Поражённые активы ⓘ

10.10.2.10 (MS Active Directory) x

Описание ⓘ

Выявлены многочисленные попытки подбора пароля для доступа по RDP к узлу контролируемой сети

Рекомендации ⓘ

служб и закрыть неиспользуемые
Заблокировать на межсетевом экране IP-адрес атакующего
Провести интервьюирование владельца
Отключить пораженный актив от вычислительной сети

Индикаторы компрометации ⓘ

ICY MS Remote Desktop Administrator Login Request

Прикрепить файл ⓘ

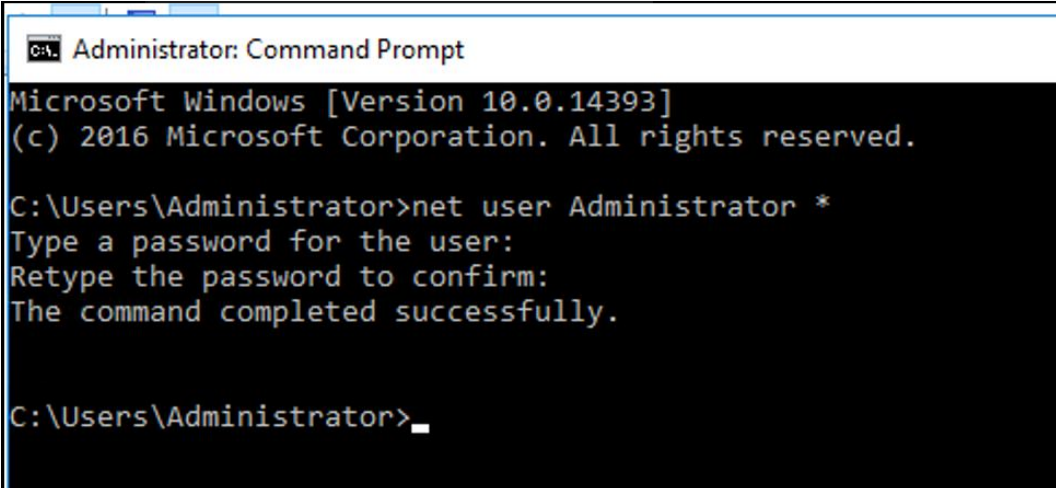
📎 IDS_packet_time-2025-10-09T11_07_45.939288Z_ruleid-2012709.pcap x

Выберите файл

Отмена

Добавить

Изменяем пароль к учётной записи администратора на более сложный, не содержащийся в словарях.



```
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>
```

Последствие AD User

Находим нового привилегированного пользователя с помощью аудита событий входа в учётную запись Windows security, где появилось событие с ID 4720. Переходим в Event Viewer и в Windows Logs - Security, затем применяем фильтр на логи.



Разобрались с сценарием действий нарушителя “Защита контроллера домена предприятия”.
Выявили и устранили уязвимости и их последствия

