

Отчёт по лабораторной работе 1-А (НФИ-2)

Julia. Установка и настройка. Основные принципы.

Козлов В.П. Гэинэ А. Шуваев С. Джахангиров И.З Хватов М.Г.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

- Козлов В.П., Гэинэ А., Шуваев С., Джахангиров И.З, Хватов М.Г.
- НФИбд-02-22
- Российский университет дружбы народов

Выполнение лабораторной работы

Отработать сценарий действий нарушителя «Защита контроллера домена предприятия» на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

Задание

1. Обнаружить SQL-injection на PHP Server.
2. Устранить уязвимость в контроллере NewsController.php.
3. Устранить последствие (Web portal meterpreter). Убиваем сессию нарушителя.
4. Обнаружить сессию нарушителя на узле администратора.
5. Запустить защиту в реальном времени Windows defender, очистить регистр.
6. Устранить последствие (Admin meterpreter). Убиваем сессию нарушителя.
7. Обнаружить попытку подбора паролей на узле MS Active Directory.
8. Изменить пароль к учетной записи администратора на более сложный.

На сайте ViPNet IDS NS просмотрели атакованные активы и суть атак

The screenshot displays the ViPNet IDS NS interface. On the left, a table lists recent events. The event with ID 3297187 is highlighted, showing it is an 'AM SQL Generic SQLi in HTTP' attack. On the right, a detailed view of this event is shown, including its classification as a 'web-application-attack' and the specific SQL injection payload used.

№	Date and time	Event code	Q...	Rule name	Class	Pr...
•	17:13:55.213 10/...	3023542	1	AM EXPLOIT Generic URL XS...	web-application-attack	TC
•	17:13:55.213 10/...	2006446	1	ET WEB_SERVER Possible S...	web-application-attack	TC
•	17:13:55.213 10/...	3106349	1	AM EXPLOIT Generic Path Tr...	web-application-attack	TC
•	17:13:55.213 10/...	3297187	1	AM SQL Generic SQLi in HTT...	web-application-attack	TC
•	17:13:55.045 10/...	3061279	1	AM USER_AGENTS Suspicio...	bad-unknown	TC
•	17:13:53.330 10/...	3194701	1	ET POLICY Possible Web Cra...	attempted-recon	TC
•	17:13:21.810 10/...	3200655	1	AM EXPLOIT Possible Googl...	client-side-exploit	TC
•	17:13:00.941 10/...	2010939	1	ET SCAN Suspicious Inboun...	bad-unknown	TC
•	17:13:00.837 10/...	2010939	1	ET SCAN Suspicious Inboun...	bad-unknown	TC
•	17:12:59.652 10/...	2010936	1	ET SCAN Suspicious Inboun...	bad-unknown	TC
•	17:12:59.559 10/...	2010936	1	ET SCAN Suspicious Inboun...	bad-unknown	TC
•	17:12:59.410 10/...	2010935	1	ET SCAN Suspicious Inboun...	bad-unknown	TC
•	17:12:59.310 10/...	2010935	1	ET SCAN Suspicious Inboun...	bad-unknown	TC

Event 17:13:55.213 10/10/2025

Event type: Signature event
Protocol: TCP
Event code: 3297187

Analysis rule

Class: web-application-attack
Group: sql
Name: AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query var2
Description: This rule detects attacks against the SQL database
Text: alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg: 'AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query var2'; flow: established, to_server; content: 'UNION'; offset: \$nocase; fast_pattern; content: 'SELECT'; nocase; distance: 0; content: '120'; HTTP'; flowbits: set, AM.Generic.sql; reference: cve.NA; reference: url:owasp.org/index.php/SQL_injection; classtype: web-application-attack; sid: 3297187; rev: 1; metadata: affected asset dst affected os any affected product n/a affected vendor n/a attack

Figure 1: Атакованные ip-адреса

Добавили карточку инцидента “SQL Инъекция”

Добавление инцидента

Название ⓘ
SQL Инъекция

Дата и время события ⓘ
10.10.2025 17:14

Источник ⓘ
195.239.174.11 (Kali) x

Поражённые активы ⓘ
10.10.1.20 (Web Server PHP) x

Описание ⓘ
Нарушитель за счёт уязвимого параметра id успешно загружает вредоносный файл на веб сервер, и устанавливает с ним shell сессию

Рекомендации ⓘ
Добавить санитизацию в код контроллера NewsController, убить сессию нарушителя

Индикаторы компрометации ⓘ
ip файла), shell сессия нарушителя на веб сервере

Прикрепить файл ⓘ
Перетяните файл в эту область или
Выберите файл

Figure 2: Карточка инцидента “SQL Инъекция”

Добавили карточку инцидента “Отключённый антивирус”

Добавление инцидента

Название ⓘ
Отключенный антивирус

Дата и время события ⓘ
10.10.2025 17:14

Источник ⓘ
195.239.174.11 (Kali) x

Поражённые 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 вредоносного скрипта

Рекомендации ⓘ
Удалить запись
"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware в реестре, включить Real-time protection в Windows Defender, убить сессию нарушителя

Индикаторы компрометации ⓘ
кем увидеть сессию с нарушителем на Administrato

Прикрепить файл ⓘ
Перетяните файл в эту область или
Выберите файл

Figure 3: Карточка инцидента “Отключённый антивирус”

Добавили карточку инцидента “Слабый пароль сервера AD”

Дата и время события ⓘ

10.10.2025 19:14

Описание ⓘ

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

Индикаторы компрометации ⓘ

Добавление нового пользователя в логах, его присутствие в AD Users and Computers

Рекомендации ⓘ

Сменить пароль на более надёжный, удалить нового пользователя

Прикреплённые файлы ⓘ

ad.pcap

Figure 4: Добавили карточку инцидента “Слабый пароль сервера AD”

SQL Инъекция. Открыли контроллер NewsController, добавили простейший фильтр для id

```
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));
}
```

Figure 5: NewsController.php

SQL Инъекция. Убиваем сессию нарушителя

```
root@webportall:~# ss -K dst '195.239.174.11' dport = 4444
Netid State      Recv-Q Send-Q                               Local Address:Port
tcp    ESTAB        0      0                               10.10.1.20:5419
root@webportall:~#
```

Figure 6: Убиваем сессию

Отключённый антивирус. Заходим на узел администратора, удаляем запись из регистра

```
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.
```

Figure 7: Удаление из регистра

Отключённый антивирус. Включаем защиту в настоящем времени



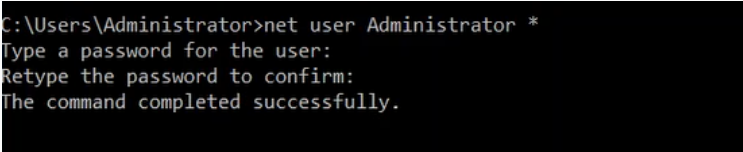
Figure 8: Включаем антивирус

Отключённый антивирус. Находим PID сессии с нарушителем, убиваем её

```
C:\Users\administrator>taskkill /f /pid 10952  
SUCCESS: The process with PID 10952 has been terminated.
```

Figure 9: Сессия нарушителя устранена

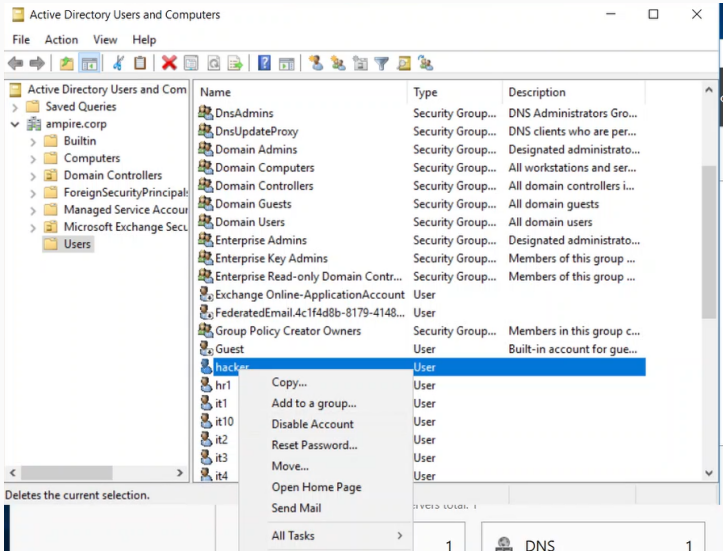
Слабый пароль. Заходим на MS AD, меняем пароль администратора



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

Figure 10: Меняем пароль

Слабый пароль. В Active directory users and computers, удаляем нового пользователя



Отработали сценарий действий нарушителя «Защита контроллера домена предприятия» на базе «Ampire».