

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

**Программный комплекс обучения методам обнаружения,
анализа и устранения последствий компьютерных атак
«Ampire»**

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

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	12
5	Список литературы	13

Список иллюстраций

3.1	Атакованные ip-адреса	7
3.2	Карточка инцидента “SQL Инъекция”	8
3.3	Карточка инцидента “Отключённый антивирус”	8
3.4	Добавили карточку инцидента “Слабый пароль сервера AD”	9
3.5	NewsController.php	9
3.6	Убиваем сессию	9
3.7	Удаление из регистра	10
3.8	Включаем антивирус	10
3.9	Сессия нарушителя устранена	10
3.10	Меняем пароль	10
3.11	Удалили hacker'а	11

Список таблиц

1 Цель работы

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

2 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.
9. Устранить последствие (AD User). Удалить нового привилегированного пользователя.

3 Выполнение лабораторной работы

На сайте VipNet IDS NS просмотрели атакованные активы и суть атак (рис. 3.1)

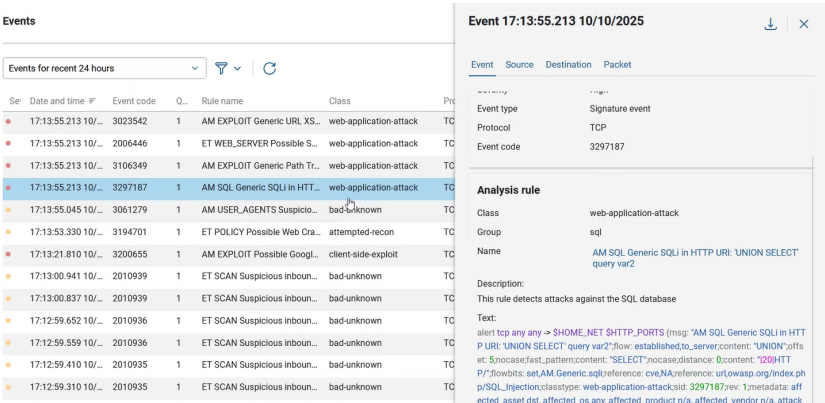


Рис. 3.1: Атакованные ip-адреса

Добавили карточку инцидента “SQL Инъекция” (рис. 3.2)

Добавление инцидента

Название

SQL Инъекция

Дата и время события

10.10.2025 17:14

Источник

195.239.174.11 (Kali)

Поражённые активы

10.10.1.20 (Web Server PHP)

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 файлах), shell сессия нарушителя на веб сервере

Прикрепить файл

Перетащите файл в эту область или

Выберите файл

Рис. 3.2: Карточка инцидента “SQL Инъекция”

Добавили карточку инцидента “Отключённый антивирус” (рис. 3.3)

Добавление инцидента

Название

Отключенный антивирус

Дата и время события

10.10.2025 17:14

Источник

195.239.174.11 (Kali)

Поражённые активы

10.10.4.10 (Administrator Workstation)

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 Administrator

Прикрепить файл

Перетащите файл в эту область или

Выберите файл

Рис. 3.3: Карточка инцидента “Отключённый антивирус”

Добавили карточку инцидента “Слабый пароль сервера AD” (рис. 3.4)

8

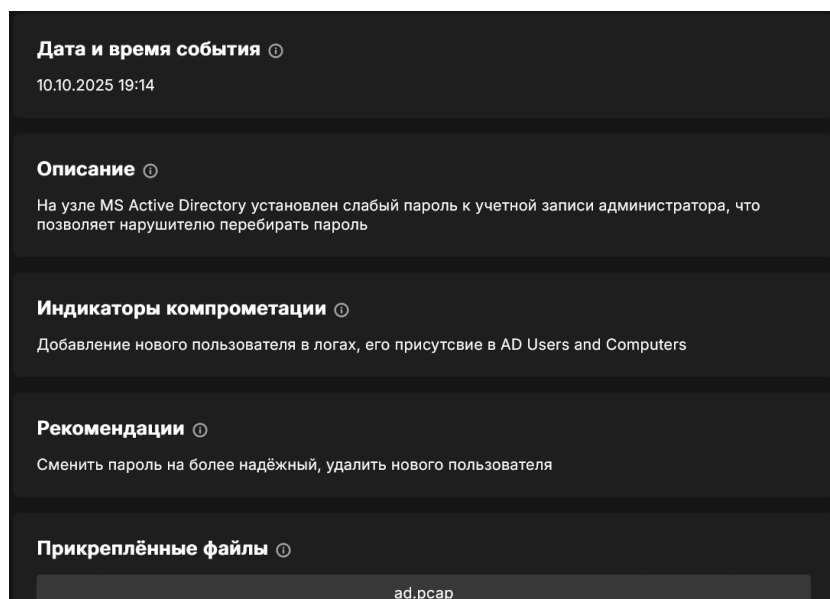


Рис. 3.4: Добавили карточку инцидента “Слабый пароль сервера AD”

SQL Инъекция. Открыли контроллер NewsController, добавили простейший фильтр для id (рис. 3.5)

```
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));
}
```

Рис. 3.5: NewsController.php

SQL Инъекция. Убиваем сессию нарушителя (рис. 3.6)

```
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:~#
```

Рис. 3.6: Убиваем сессию

Отключённый антивирус. Заходим на узел администратора, удаляем запись из регистра (рис. 3.7)

```
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.
```

Рис. 3.7: Удаление из регистра

Отключённый антивирус. Включаем защиту в настоящем времени (рис. 3.8)



Рис. 3.8: Включаем антивирус

Отключённый антивирус. Находим PID сессии с нарушителем, убиваем её (рис. 3.9)

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

Рис. 3.9: Сессия нарушителя устранена

Слабый пароль. Заходим на MS AD, меняем пароль администратора (рис. 3.10)

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

Рис. 3.10: Меняем пароль

Слабый пароль. В Active directory users and computers, удаляем нового пользователя (рис. 3.11)

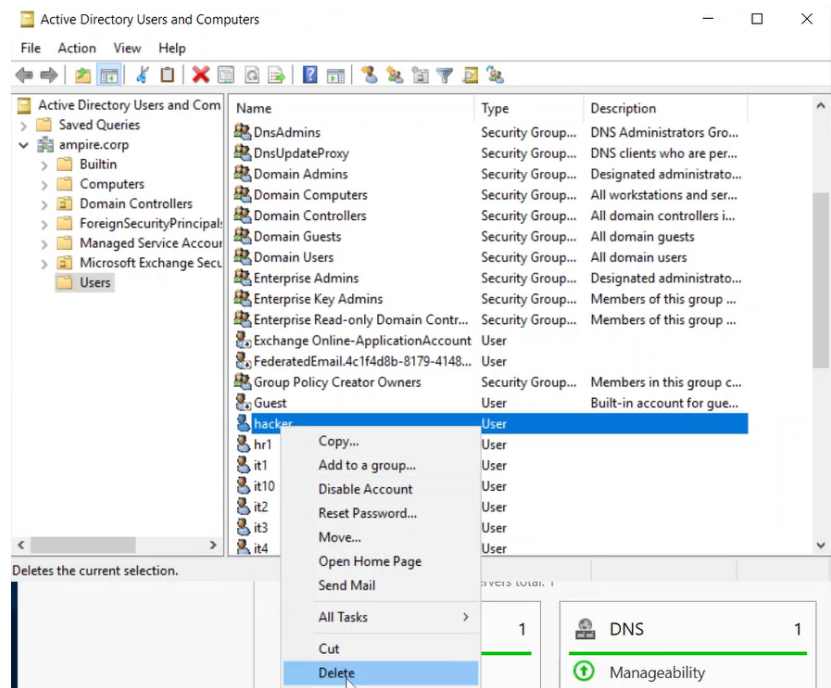


Рис. 3.11: Удалили hacker'а

Все атаки и их последствия успешно устранены

4 Выводы

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

5 Список литературы

1. **CVE-2019-0630** — Common Vulnerabilities and Exposures.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0630>
2. **CVE-2019-17427** — Уязвимость XSS в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17427>
3. **CVE-2019-18890** — Уязвимость Blind SQL-инъекции в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18890>