

Отчёт по лабораторной работе

Кибербезопасность 3-А

группа 1е

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Уязвимость № 1 – SQL-инъекция (Web Server PHP)	7
3.2 Уязвимость № 2 – отключённая защита антивируса (Administrator Workstation	10
3.3 Уязвимость № 3 – слабый пароль учётной записи (MS Active Directory)	11
4 Выводы	14
Список литературы	15

Список иллюстраций

3.1	Описание атаки	7
3.2	меняю функцию	8
3.3	Уязвимость устранена	8
3.4	установленные соединения	9
3.5	Завершение сессии	9
3.6	Последствие устранено	9
3.7	Описание атаки	10
3.8	Удаление записи DisableAntiSpyware в реестре	10
3.9	все устранено	11
3.10	Описание атаки	11
3.11	Изменение пароля администратора	12
3.12	Удаление пользователя hacker в AD User & Computers	12
3.13	15	13

Список таблиц

1 Цель работы

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

2 Задание

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

3 Выполнение лабораторной работы

3.1 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.

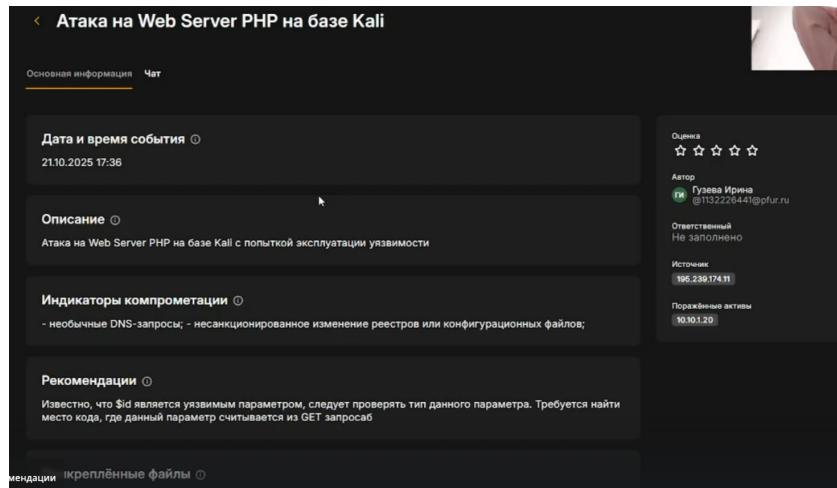


Рис. 3.1: Описание атаки

Добавляем проверку типа параметра \$id

```
2022-10-10 10:22:27 - [INFO] start - user@webportal: ~
[INFO] Кодирование: UTF-8
[INFO] Текущая рабочая директория: /var/www/html

?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();
    }
}

Format: controllers/NewsController.php
```

Рис. 3.2: меняем функцию

Готово)

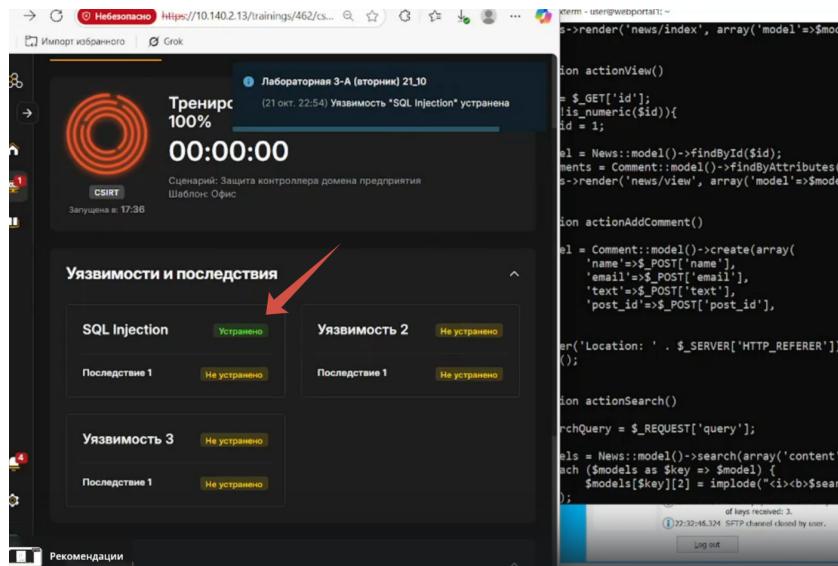


Рис. 3.3: Уязвимость устранена

Далее нужно устраниТЬ последствие. Проверяем сокеты уязвимой машины

Рисунок 7 – Список установленных соединений

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

Рис. 3.4: установленные соединения

Завершаем сессию с нарушителем

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

Рис. 3.5: Завершение сессии

Готово

Импорт избранного Grok

100%
00:00:00

Сценарий: Защита контроллера домена предприятия
Шаблон: Офис

Запущена в: 17:36

Уязвимости и последствия

SQL Injection Устранило

Web portal meterpreter Устранило

Уязвимость 2 Не устранило

Последствие 1 Не устранило

Уязвимость 3 Не устранило

Последствие 1 Не устранило

Ресурсы

jer@10.10.1.2022 - Bitvise xterm - user@webportal:~

```
s:(("server",pid=637,fd=8))
SENT 0 1 10.18.1.20:22
s:(("puppet",pid=13554,fd=6))
0 0 0 10.18.1.20:22
s:(("filebeat",pid=693,fd=5))
0 0 0 10.18.1.20:22
s:(("epp_agentd",pid=1248,fd=35))
@webportal1:/home/user# ss kill 13554
r: an inet prefix is expected rather
ot parse dst/src address.
@webportal1:/home/user# kill 13554
@webportal1:/home/user# ss -tp
e Recv-Q Send-Q Local Address: ...
0 204 10.18.1.20:22
s:(("sshd",pid=12987,fd=4),("sshd",pi
SENT 0 1 10.18.1.20:22
s:(("puppet",pid=13554,fd=5))
0 0 0 10.18.1.20:22
s:(("server",pid=637,fd=8))
0 0 0 10.18.1.20:22
s:(("filebeat",pid=693,fd=5))
0 0 0 10.18.1.20:22
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: ...
0 204 10.18.1.20:22
s:(("sshd",pid=12987,fd=4),("sshd",pi
0 0 0 10.18.1.20:22
s:(("server",pid=637,fd=8))
0 0 0 10.18.1.20:22
s:(("filebeat",pid=693,fd=5))
0 339 10.18.1.20:22
s:(("epp_agentd",pid=1248,fd=35))
@webportal1:/home/user# ss -tp
e Recv-Q Send-Q Local Address: ...
0 204 10.18.1.20:22
s:(("sshd",pid=12987,fd=4),("sshd",pi
0 0 0 10.18.1.20:22
s:(("server",pid=637,fd=8))
0 0 0 10.18.1.20:22
s:(("filebeat",pid=693,fd=5))
0 339 10.18.1.20:22
s:(("epp_agentd",pid=1248,fd=35))
```

Рис. 3.6: Последствие устранено

3.2 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 ①
21.10.2025 17:36

Описание ①
Атака на Administrator Workstation на базе Kali с попыткой эксплуатации уязвимости отключение защиты антивируса

Индикаторы компрометации ①
- необычные DNS-запросы; - подозрительные файлы, приложения или процессы;

Рекомендации ①
На узле Administrator Workstation вручную удалить запись в реестре или через консоль, используя команду REG DELETE <HKEY SOFTWARE\Policies\Microsoft\Windows Defender> /DisableAntiSpyware. Подтвердить действие, далее в Windows Defender перезапустить Virus & Threat Protection (Рисунок 10) и включить Real-time Protection

Рис. 3.7: Описание атаки

Удаляем запись

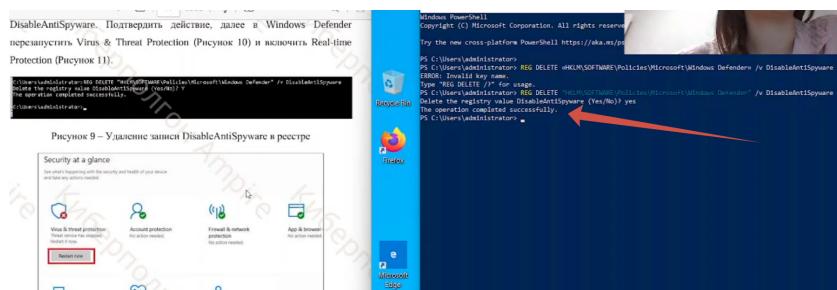


Рис. 3.8: Удаление записи DisableAntiSpyware в реестре

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

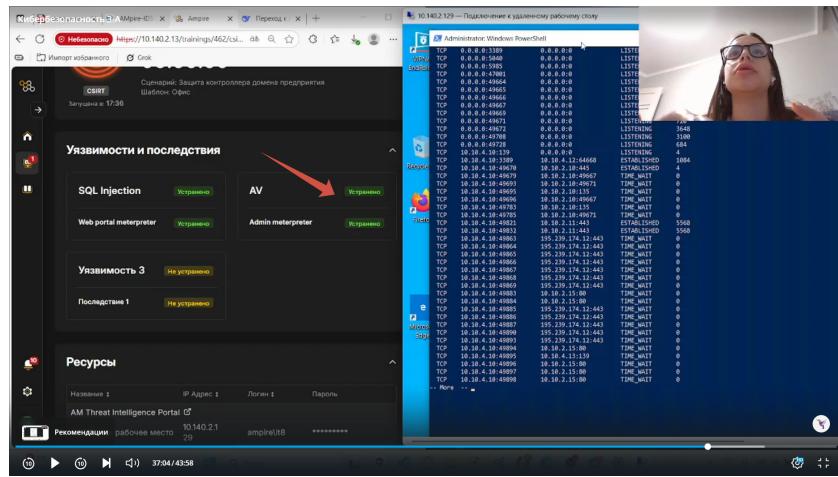


Рис. 3.9: все устранено

3.3 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

Основная информация

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

Рис. 3.10: Описание атаки

Меняем пароль к учетной записи администратора на более сложный, не содержит

жащийся в словарях

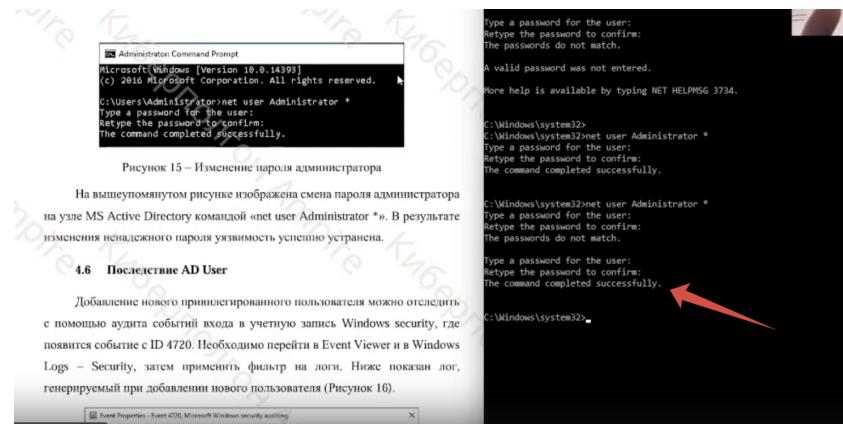


Рисунок 15 – Изменение пароля администратора

На вышеупомянутом рисунке изображена смена пароля администратора на узле MS Active Directory командой «net user Administrator *». В результате изменения несанкционированного 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 к логам. Ниже показан лог, генерируемый при добавлении нового пользователя (Рисунок 16).

Рисунок 16 – Лог добавления нового пользователя

Добавление нового привилегированного пользователя можно отследить с помощью аудита событий входа в учетную запись Windows security. Удаляем пользователя с именем “Hacker”

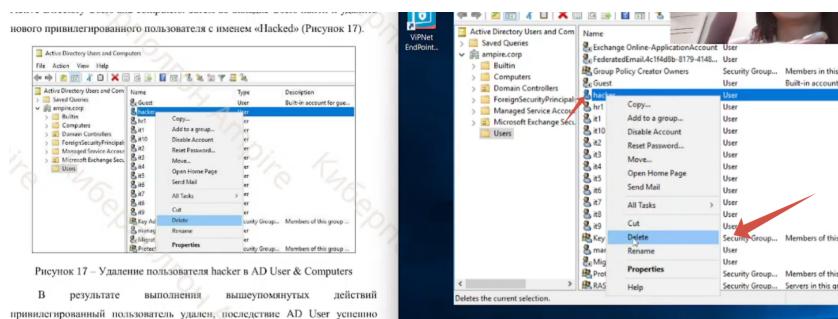


Рисунок 17 – Удаление пользователя hacker в AD User & Computers

В результате выполнения вышеупомянутых действий привилегированный пользователь удален, последствие AD User успешно

Рис. 3.12: Удаление пользователя hacker в AD User & Computers

Уязвимость и последствие успешно устранины!

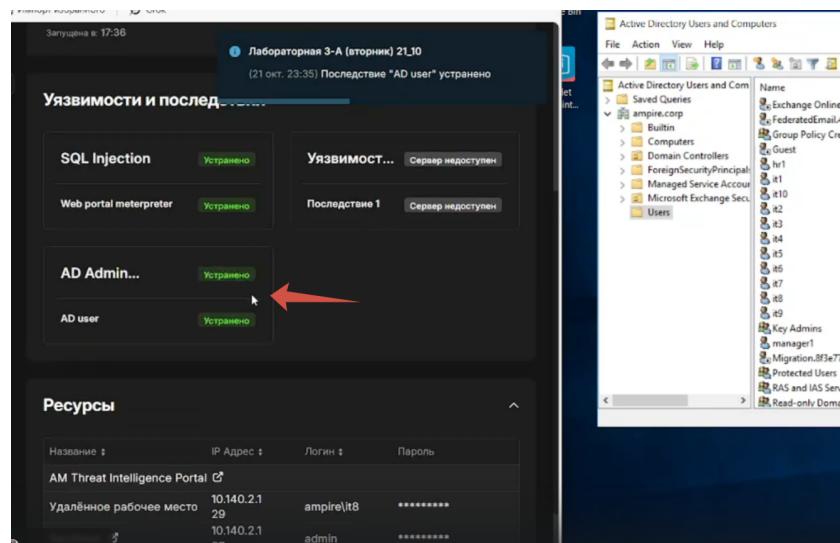


Рис. 3.13: 15

4 Выводы

В ходе лабораторной работы были:

- обнаружены и устранены 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.

Список литературы