Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ СТРУКТУРЫ WEB ПРИЛОЖЕНИЙ**

отчет о   
лабораторной работе №6

по дисциплине

*ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ*

***ВАРИАНТ 13***

|  |  |  |
| --- | --- | --- |
| Выполнила: | ст. гр. 230711 | Павлова В.С. |
| Проверил: | асс. каф. ИБ | Греков М.М. |

Тула, 2023 г.

# **ЦЕЛЬ РАБОТЫ**

**Цель:** ознакомиться с основными методами анализа структуры WEB приложений, и методами оценки результатов анализа.

# **ЗАДАНИЕ НА РАБОТУ**

1. Установить Metasploitable 2 в комплекте с платформой DVWA. Выполнить привязку двух машин (Kali Linux и Metasploitable).
2. Зайти через браузер Kali Linux на Metasploitable. Ввести в строку запросов IP-адрес машины, на которую установлен Metasploitable. Выбрать тренировочную площадку DVWA.
3. Просканировать площадку DVWA с помощью DirBuster и представить скриншот и отчёт.
4. Просканировать DVWA при помощи DirSearch, предоставить скриншот и отчёт.
5. Просканировать DVWA в рекурсивном режиме с анализом подкаталогов и предоставить скриншот и отчёт. В качестве дополнительного задания просканировать сайт scanme.org

**ХОД РАБОТЫ**

1. Привязка Kali и Metasploitable (10.0.2.5) друг к другу (рисунок 1):

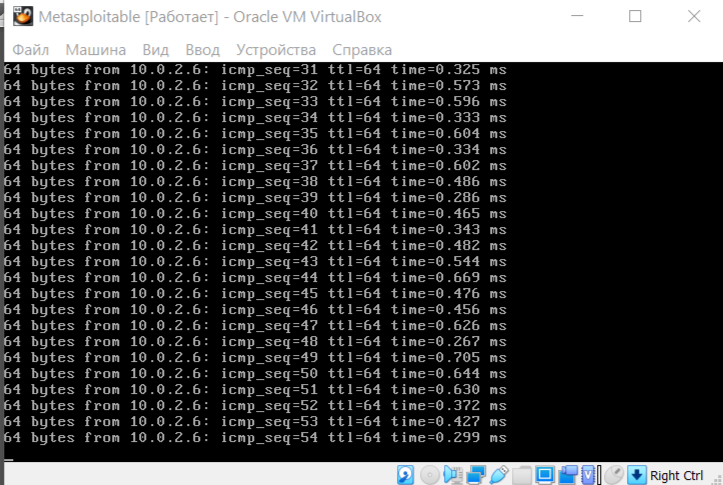


Рисунок 1 – Результат выполнения команды ping

1. Сканирование площадки DVWA с помощью DirBuster показано на рисунке 2. Результат приведен ниже:

|  |  |  |  |
| --- | --- | --- | --- |
| Directories found during testing:  Dirs found with a 302 response:  /dvwa/  /dvwa/index/  /dvwa/security/ | Dirs found with a 200 response:  /dvwa/login/  /dvwa/docs/  /  /icons/  /dvwa/external/ | Files found during testing:  Files found with a 302 responce:  /dvwa/index.php  /dvwa/about.php  /dvwa/security.php | Files found with a 200 responce:  /dvwa/login.php  /dvwa/docs/DVWA-Documentation.pdf  /dvwa/setup.php  /dvwa/config/config.inc.php  /dvwa/external/phpids/0.6/LICENSE |

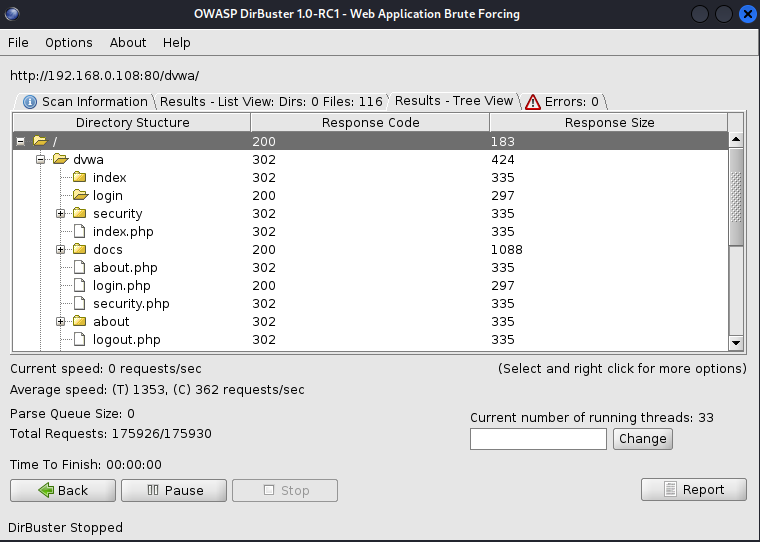


Рисунок 2 – Результат сканирования DVWA с помощью DirBuster

1. Сканирование площадки DVWA с помощью DirSearch (рисунок 3).

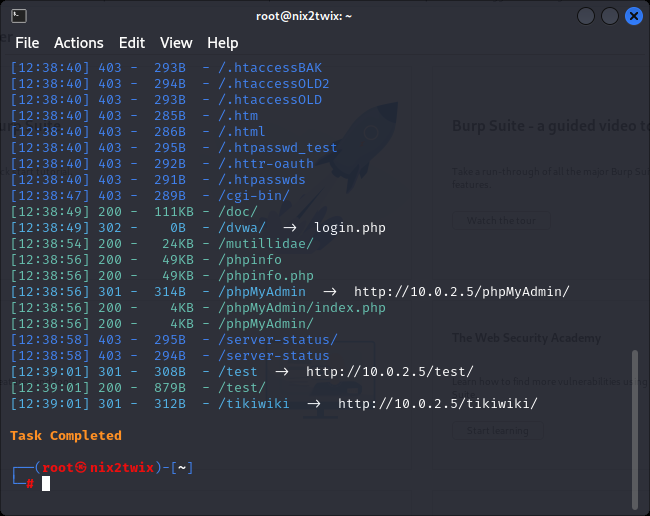


Рисунок 3 – Результат сканирования DVWA с помощью DirSearch

1. На рисунке 4 приведен результат сканирования площадки DVWA в рекурсивном режиме с анализом подкаталогов:

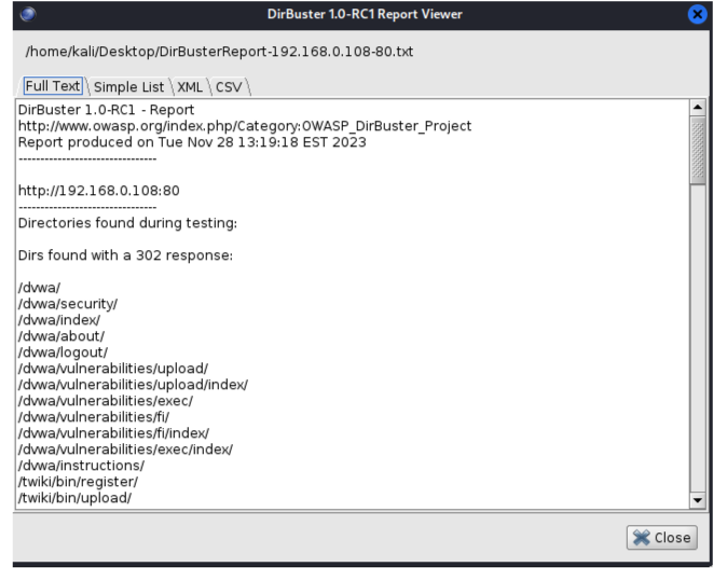


Рисунок 4 – Результат сканирования в рекурсивном режиме

# **ВЫВОД**

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами анализа структуры WEB приложений, и методами оценки результатов анализа.