Отчёт по этапу №4

Дисциплина: Основы информационной безопасности

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

Научиться использовать инструмент для сканирования на уязвимости nikto.

# 2 Выполнение лабораторной работы

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Для сканирования цели необходимо ввести nikto -h -p , где — домен или IP-адрес целевого сайта, а — порт, на котором запущен сервис [1].

Для начала получаем справку по команде, вводим nikto -h (рис. 1).

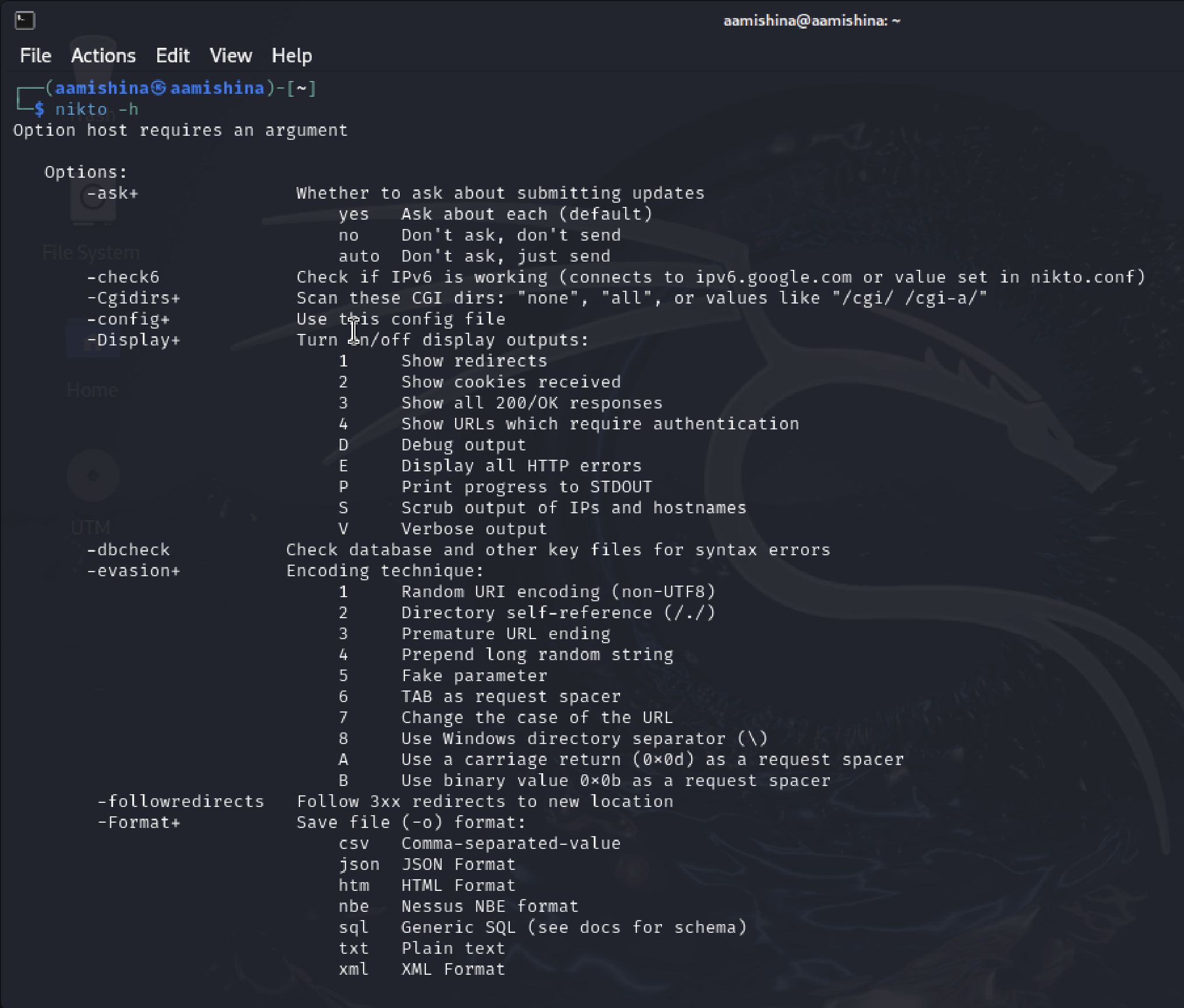


Рис. 1: Справка по nikto

Запускаем сканирование для веб-сайта gazel.me. В результате видим, что выводятся различные замечания и потенциальные уязвимости (например уязвимость с кодом CVE-2003-1243) (рис. 2).

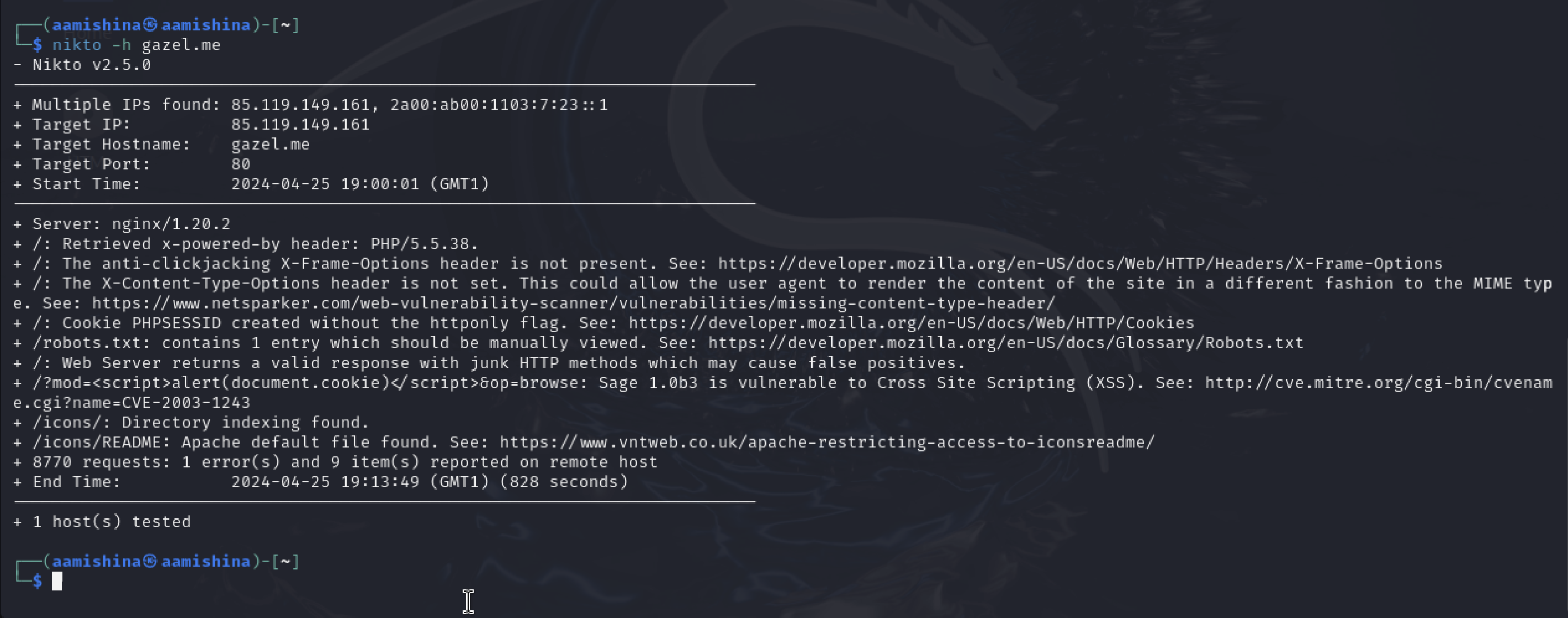


Рис. 2: Сканирование веб-сайта

Запускаем наш сервер apache и выполняем сканирование для локальной сети, введя nikto -h 127.0.0.1. В результате видим замечания о работе сервера (рис. 3).



Рис. 3: Сканирование локальной сети

Затем приступаем к сканированию веб-приложения DVWA, запущенном в локальной сети [2] (рис. 4). Получаем информацию о структуре DVWA и находим возможные уязвимости, например, PHP backdoor file manager.



Рис. 4: Сканирование DVWA

# 3 Выводы

В ходе выполнения данной лабораторной работы, я научилась использовать инструмент для сканирования на уязвимости nikto. Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация ПО.

# Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.

2. [Scan for Vulnerabilities on Any Website Using Nikto](https://null-byte.wonderhowto.com/how-to/scan-for-vulnerabilities-any-website-using-nikto-0151729/). [Электронный ресурс].