Введение в Nikto

Nikto — очень популярный инструмент сканирования веб-серверов с открытым исходным кодом, который в основном используется для выявления уязвимостей безопасности на веб-серверах. Он может обнаруживать различные проблемы, включая, помимо прочего:

- Опасные или устаревшие файлы, которые можно использовать для получения несанкционированного доступа к серверу.
- Неправильно настроенные параметры сервера, например настройки, разрешающие просмотр списков каталогов.
- Отсутствуют обновления или исправления безопасности.
- Раскрытие информации о сервере, такой как номера версий или другие метаданные.
- Слабые пароли.
- Известные уязвимости сценариев CGI и другие угрозы безопасности на уровне веб-приложений.

Nikto написан на Perl и работает на различных операционных системах, включая Kali Linux, операционную систему, широко используемую для тестирования на проникновение и аудита безопасности.

Как использовать
Обычно Nikto можно использовать через командную строку. Основной формат команды следующий:

```
nikto -h <target_host>
```

Где <target_host> — это адрес целевого веб-сервера, который вы хотите сканировать.

использование

Шаг 1: Убедитесь, что Nikto установлен

Сначала откройте терминал и проверьте, установлен ли Nikto. Вы можете это сделать с помощью следующей команды:

```
nikto -h
```

Если Nikto уже установлен, вы увидите справочную информацию. Если нет, вы можете установить его с помощью следующих команд:

```
sudo apt update
sudo apt install nikto
```

Шаг 2: Базовый скан

Далее, используйте Nikto для базового сканирования целевого веб-сервера. Предположим, что IP-адрес или доменное имя целевого сервера — example.com. Вы можете запустить следующую команду:

```
nikto -h example.com
```

Эта команда выполнит сканирование целевого сервера и выведет все обнаруженные проблемы.

Шаг 3: Настройка опций сканирования

Nikto предлагает множество опций для настройки сканирования. Вот некоторые из них:

- Указание порта:

  nikto -h example.com -p 8080
- Вывод результатов в файл:

```
nikto -h example.com -o /path/to/output.txt
```

Установка User-Agent:

```
nikto -h example.com -useragent "Mozilla/5.0"
```

Установка максимального времени сканирования:

```
nikto -h example.com -maxtime 60
```

Использование Cookie:

```
nikto -h example.com -C "session=12345"
```

Пример

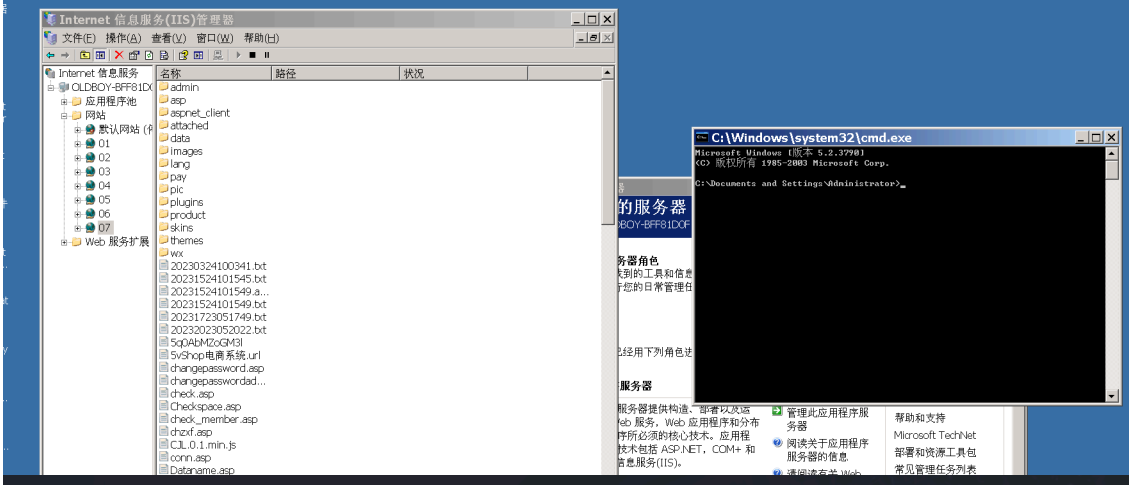
Предположим, вы хотите выполнить базовое сканирование example.com и сохранить результаты в файле. Вы можете использовать следующую команду:

```
nikto -h example.com -o /tmp/nikto_results.txt
```

Это сохранит результаты сканирования в файл /tmp/nikto_results.txt.

```
┌──(root㉿kali)-[~]
└─# nikto
- Nikto v2.5.0
---------------------------------------------------------------------------

---------------------------------------------------------------------------
+ ERROR: No host (-host) specified
```




```
┌──(root㉿kali)-[~]
└─# nikto -h 192.168.159.131 -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------

---------------------------------------------------------------------------
+ Target IP:          192.168.159.131
+ Target Hostname:    192.168.159.131
+ Target Port:        80
+ Start Time:         2024-09-30 02:09:07 (GMT-4)
---------------------------------------------------------------------------

---------------------------------------------------------------------------
```