Индивидуальный проект. Отчёт о выполнении №4
Информационная безопасность

Использование Nikto

Выполнил: Мальков Роман Сергеевич,
НФИбд-02-21, 1032217048

Содержание

Список иллюстраций

Цель работы

Рассмореть и применить утилиту nikto для просмотра уязвимостей веб приложения DVWA.

Использование Nikto

Просмотрим версию nikto и проверим базы данных на ошибки.

Рис. 1: Проверка

Попробуем просканировать DVWA

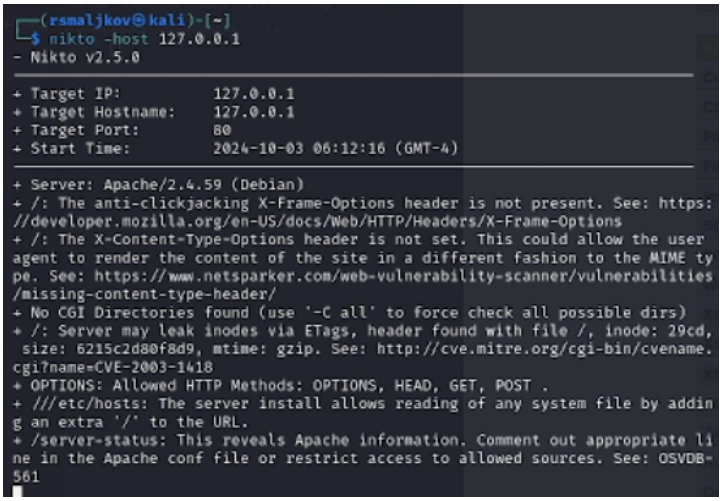

Рис. 2: сканирование DVWA

Также дополнительно можно указать порт

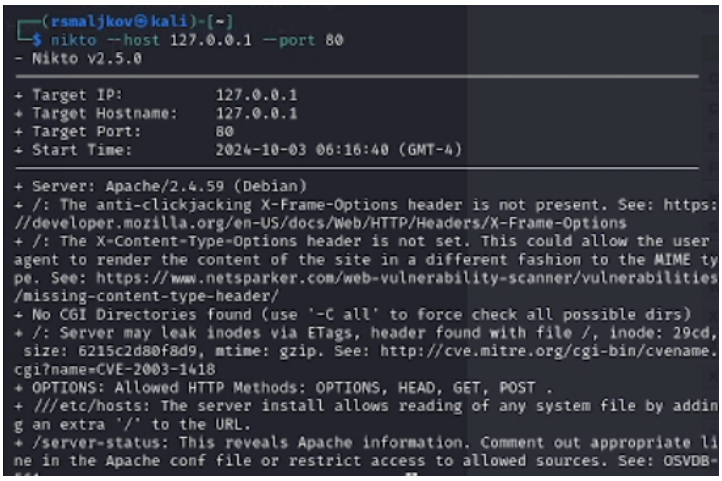

Рис. 3: сканирование с указанием порта

Укажем параметр maxtime, отвечающий за длительность работы сканирования, а также параметр Pause, отвечающий за паузу между вполнением запросов

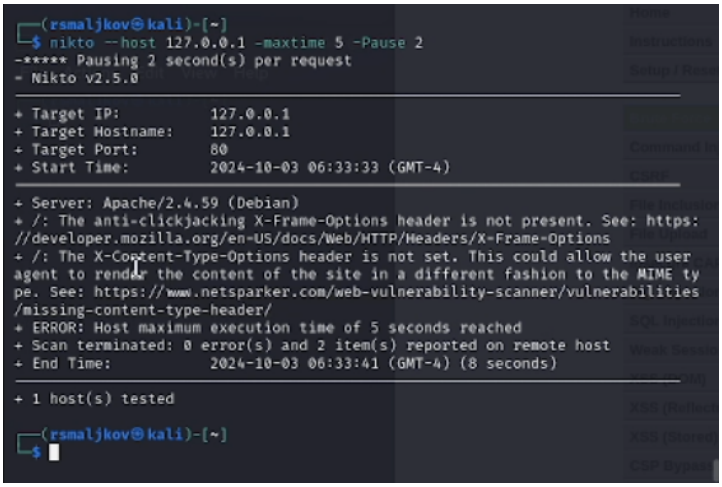

Рис. 4: сканирования с maxtime и Pause

При помощи параметра Tuning можно выбрать тип теста приложения:

0 - File Upload

1 - Interesting File / Seen in Logs

2 - Misconfiguration / Default File

3 - Information Disclosure

4 - (XSS/Script/HTML) Injection

5 - Remote file retrival Inside web root

6 - Denial of service

7 - Remote file retrival / Server wide

8 - Command exec / Remote shell

9 - SQL Injection

a - Authentication Bypass

b - Software Indetification

c - Remote source Inclusion

x - Reverse tuning options

Рис. 5: сканирование с Tuning

Для того чтобы обойти систему обнаружения вторжения, можно воспользоваться параметром evasion:

1 - Random URI encoding

2 - Directory self reference (/./)

3 - Premature URL ending

4 - Prepend long random string

5 - Fake parameter

6 - TAB as request spacer

7 - Change case of URL

8 - Use Windows directory separator

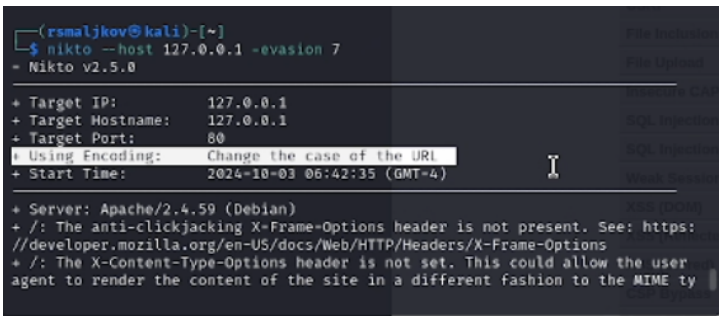

Рис. 6: сканирование с evasion

Сохраним отчет в определенном формате используя параметры o и Format

Рис. 7: Сохраним отчет

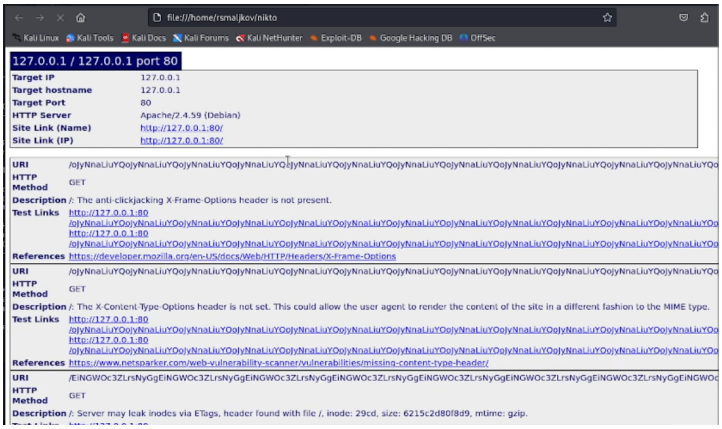

Рис. 8: Отчет

Заключение

Были полученны базовые навыки работы с утилитой nikto.

Ссылки

“Nikto vulnerability scanner: Complete guide”: https://www.hackercoolmagazine.com/nikto-vulnerability-scanner-complete-guide/