

Индивидуальный проект. Этап 4.

Использование nikto

Аскеров Александр Эдуардович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	8
	Список литературы	9

Список иллюстраций

2.1	Справка по nikto	5
2.2	Сканирование сайта	6
2.3	Запуск apache-сервера	6
2.4	Сканирование локальной сети	6
2.5	Сканирование DVWA	7
2.6	Выключение apache-сервера	7

1 Цель работы

Познакомиться с nikto.

2 Выполнение лабораторной работы

Посмотрим справку по nikto.

```
(aeaskerov@aeaskerov)-[~]
$ nikto -h
Option host requires an argument

Options:
  -ask+           Whether to ask about submitting updates
                   yes   Ask about each (default)
                   no    Don't ask, don't send
                   auto  Don't ask, just send
  -check6         Check if IPv6 is working (connects to ipv
6.google.com or value set in nikto.conf)
  -Cgидirs+       Scan these CGI dirs: "none", "all", or va
lues like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
                   1     Show redirects
                   2     Show cookies received
                   3     Show all 200/OK responses
                   4     Show URLs which require authent
ication
                   D     Debug output
                   E     Display all HTTP errors
                   P     Print progress to STDOUT
                   S     Scrub output of IPs and hostnam
es
```

Рис. 2.1: Справка по nikto

Просканируем сайт gazel.me.

```

(aeaskerov@aeaskerov)-[~]
$ nikto -h gazel.me
- Nikto v2.5.0

+ Multiple IPs found: 85.119.149.161, 2a00:ab00:1103:7:23::1
+ Target IP:      85.119.149.161
+ Target Hostname: gazel.me
+ Target Port:    80
+ Start Time:     2024-04-27 06:49:17 (GMT-4)

+ Server: nginx/1.20.2
+ /: Retrieved x-powered-by header: PHP/5.5.38.

```

Рис. 2.2: Сканирование сайта

Запустим apache-сервер.

```

(aeaskerov@aeaskerov)-[~]
$ sudo service apache2 start
[sudo] password for aeaskerov:

```

Рис. 2.3: Запуск apache-сервера

Просканируем локальную сеть.

```

(aeaskerov@aeaskerov)-[~]
$ nikto -h 127.0.0.1
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-04-27 06:58:06 (GMT-4)

+ Server: Apache/2.4.58 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

```

Рис. 2.4: Сканирование локальной сети

Просканируем DVWA.

```
(aeaskerov@aeaskerov)-[~]
$ nikto -h http://127.0.0.1/DVWA/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-04-27 06:58:48 (GMT-4)

+ Server: Apache/2.4.58 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /DVWA redirects to: login.php
```

Рис. 2.5: Сканирование DVWA

Выключим apache-сервер.

```
(aeaskerov@aeaskerov)-[~]
$ sudo service apache2 stop
```

Рис. 2.6: Выключение apache-сервера

3 Выводы

Изучен сервис nikto.

Список литературы

1. An introduction to web-server scanning with nikto