

# **Отчёт по этапу №4**

**Дисциплина: Основы информационной безопасности**

Мишина Анастасия Алексеевна

# Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	9
	Список литературы	10

## Список иллюстраций

2.1	Справка по nikto . . . . .	6
2.2	Сканирование веб-сайта . . . . .	7
2.3	Сканирование локальной сети . . . . .	7
2.4	Сканирование DVWA . . . . .	8

## Список таблиц

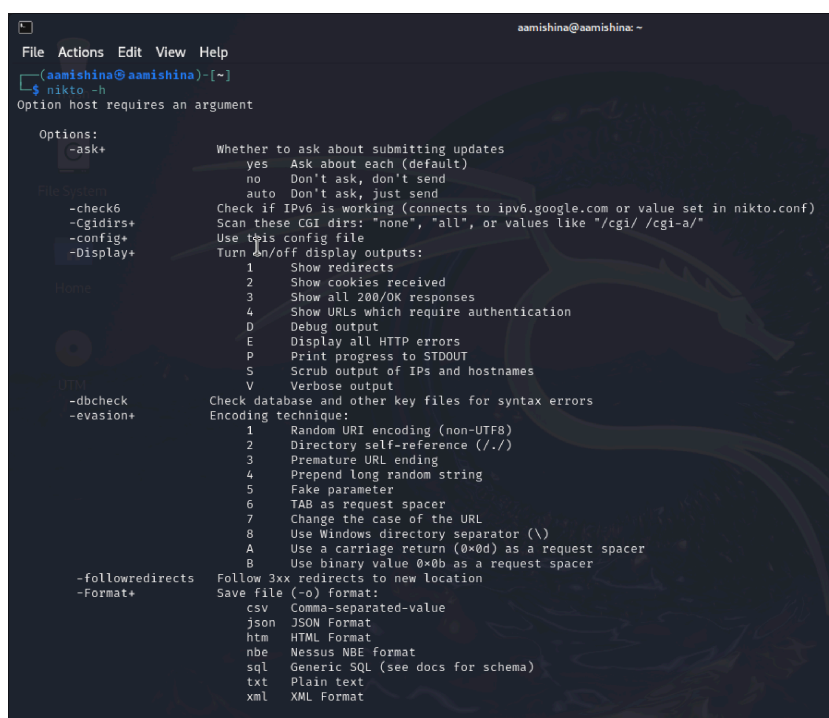
# 1 Цель работы

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. 2.1).



```
aamishina@aamishina: ~  
File Actions Edit View Help  
aamishina@aamishina: ~  
$ 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 ipv6.google.com or value set in nikto.conf)  
-cgidir+       Scan these CGI dirs: "none", "all", or values 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 authentication  
                D     Debug output  
                E     Display all HTTP errors  
                P     Print progress to STDOUT  
                S     Scrub output of IPs and hostnames  
                V     Verbose output  
-dbcheck       Check database and other key files for syntax errors  
-evasion+      Encoding technique:  
                1     Random URI encoding (non-UTF8)  
                2     Directory self-reference (../)  
                3     Premature URL ending  
                4     Prepend long random string  
                5     Fake parameter  
                6     TAB as request spacer  
                7     Change the case of the URL  
                8     Use Windows directory separator (\)  
                A     Use a carriage return (0x0d) as a request spacer  
                B     Use binary value 0x0b as a request spacer  
-followredirects Follow 3xx redirects to new location  
-format+       Save file (-o) format:  
                csv   Comma-separated-value  
                json  JSON Format  
                htm   HTML Format  
                nbe   Nessus NBE format  
                sql   Generic SQL (see docs for schema)  
                txt   Plain text  
                xml   XML Format
```

Рис. 2.1: Справка по nikto

Запускаем сканирование для веб-сайта `gazel.me`. В результате видим, что вы-

водятся различные замечания и потенциальные уязвимости (например уязвимость с кодом CVE-2003-1243) (рис. 2.2).

```
amishina@amishina:~$ nikto -h gazel.me
- Nikto v2.5.0

+ Multiple IPs found: 85.119.149.161, 2a00:ab00:103:7:23::1
+ Target IP: 85.119.149.161
+ Target Hostname: gazel.me
+ Target Port: 80
+ Start Time: 2024-04-25 19:00:01 (GMT1)

+ Server: nginx/1.20.2
+ /: Retrieved x-powered-by header: PHP/5.5.38.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/
+ /: Cookie (PHPSESSID) created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /found=scriptalert(document.cookie)/script-ftp-browse: Sage 1.0b1 is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1243
+ /icons/: Directory indexing found.
+ /icons/README: apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconreadme/
+ 8/70 requests: 1 error(s) and 9 item(s) reported on remote host
+ End Time: 2024-04-25 19:13:49 (GMT1) (828 seconds)

+ 1 host(s) tested
```

Рис. 2.2: 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. 2.3).

```
amishina@amishina:~$ sudo service apache2 start
[sudo] password for amishina:
amishina@amishina:~$ 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: 2024-04-25 19:15:51 (GMT1)

+ 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
+ /: 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/
+ No CGI Directories found (use "-C all" to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 61289c971e220, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ Server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Menu.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Menu.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobileise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?ll=ask38aa37ca530/etc/hosts: Some 0-link router remote command execution.
+ /shellcat/etc/hosts: A backdoor was identified.
+ 8/74 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-04-25 19:15:58 (GMT1) (7 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.58) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
```

Рис. 2.3: Сканирование локальной сети

Затем приступаем к сканированию веб-приложения DVWA, запущенном в локальной сети [2] (рис. 2.4). Получаем информацию о структуре DVWA и находим возможные уязвимости, например, PHP backdoor file manager.

```
ami@ami:~$ 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:     2024-04-25 19:16:51 (GMT1)

+ 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
+ No .git Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /DVWA//etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/.git/index: Git Index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meahy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meahy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=aa2baa2?cat20/etc/hosts: Some D-Link router remote command execution.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 878 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time:     2024-04-25 19:16:59 (GMT1) (8 seconds)
```

Рис. 2.4: 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. [Электронный ресурс].