

Отчёт по индивидуальному проекту.

Этап 4

Дисциплина: Основы информационной безопасности

Бансимба Клодели Дьегра НПИбд-02-22

Содержание

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

Список иллюстраций

2.1	Nikto предустановлен	6
2.2	Nikto -h	7
2.3	использование базовый синтаксис	7
2.4	использование базовый синтаксис	8

Список таблиц

1 Цель работы

Научиться использовать nikto (базовый сканер безопасности веб-сервера).

2 Выполнение лабораторной работы

Мы используем Kali Linux, то Nikto будет предустановлен, поэтому нам ничего скачивать и устанавливать не придется. Он будет расположен в категории «Анализ уязвимостей». (рис. 2.1)

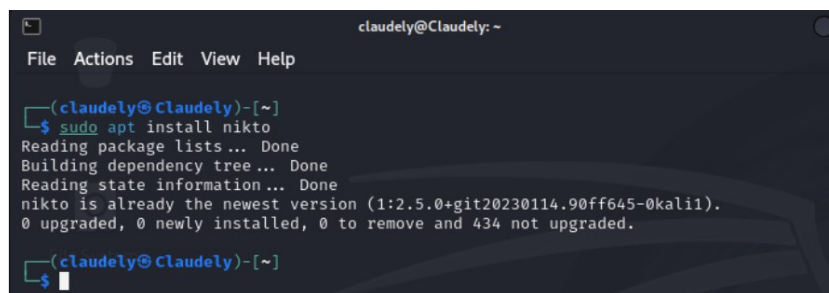
A screenshot of a terminal window titled 'claudely@Claudely: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command '\$ sudo apt install nikto' being executed. The output indicates that the package lists are read, the dependency tree is built, and state information is read. It then states that Nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1) and that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 434 not upgraded. The prompt returns to '\$ '.

Рис. 2.1: Nikto предустановлен

Перед сканированием веб-серверов с помощью Nikto, давайте воспользуемся параметром -Help, чтобы увидеть все, что мы можем делать с этим инструментом. (рис. 2.2)

```
(claudely@claudely)-[~]
$ 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)
  -Cgidirs+       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
```

Рис. 2.2: Nikto -h

Как вы видите из предыдущего шага, у Nikto есть много вариантов использования, но для наших целей мы будем использовать базовый синтаксис <127.0.0.1 или http://127.0.0.1/DVWA/> с фактическим IP-адресом или именем хоста без угловых скобок.” (рис. 2.3).

```
(claudely@claudely)-[~]
$ 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 15:09:40 (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
+ /: 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.net-sparker.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: 6128f3c4d8c1c, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ///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/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
```

Рис. 2.3: использование базовый синтаксис

http://127.0.0.1/DVWA/ (рис. 2.4).

```
(claudely@claudely)-[~]
$ 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 15:12:08 (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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /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/wordpress/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.
```

Рис. 2.4: использование базовый синтаксис

3 Выводы

В ходе этапа проекта мы узнали как использовать nikto (базовый сканер безопасности веб-сервера).

Список литературы

1. Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.