

# Отчёт по индивидуальному проекту. Этап 4

---

Бансимба Клодели Дьегра НПИбд-02-22<sup>1</sup>

27 апреля, Москва, Россия

<sup>1</sup>Российский Университет Дружбы Народов

# Информация

---

- Бансимба Клодели Дьегра
- Студент, НПИбд-02-22
- Российский университет дружбы народов
- 1032215651@pfur.ru



## Цели и задачи работы

---

## Цель лабораторной работы

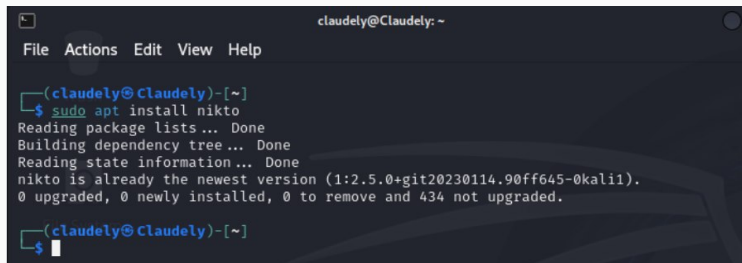
Научиться использовать nikto (базовый сканер безопасности веб-сервера).

# **Процесс выполнения лабораторной работы**

---

## Запустим Nikto

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

A terminal window titled 'claudely@Claudely: ~' with a menu bar containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command 'sudo apt install nikto' being executed. The output indicates that Nikto is already installed as the newest version (1:2.5.0+git20230114.90ff645-0kali1) and no action is required. The prompt returns to the user.

```
(claudely@Claudely)-[~]  
$ sudo apt install nikto  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).  
0 upgraded, 0 newly installed, 0 to remove and 434 not upgraded.  
  
(claudely@Claudely)-[~]  
$
```

**Рис. 1:** Nikto предустановлен

# Nikto help

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

```
(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)
```



# Использование базовый синтаксис

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.

```
(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.
```

# Использование базовый синтаксис

http://127.0.0.1/DVWA/ .

```
(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.
```

## **Выводы по проделанной работе**

---

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

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.