

# Индивидуальный проект этап 4

## Информационная безопасность

---

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

## Цели и задачи

---

Установить nikto и просканировать локальный веб-сервер

## Выполнение работы

---

## Установил nikto на kali linux

```
(ksudzuki@KSudzuki)-[~]  
$ sudo apt-get install nikto -y  
[sudo] password for ksudzuki:  
Sorry, try again.  
[sudo] password for ksudzuki:  
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).  
nikto set to manually installed.  
The following packages were automatically installed and are no longer required:  
  chrome-gnome-shell fonts-liberation2 gnome-backgrounds ibverbs-providers  
  libarmadillo12 libassuan0 libavfilter9 libavformat60 libblosc2-3  
  libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdisplay-info1  
  libgdal34t64 libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0  
  libibverbs1 libimobiledevice6 libjsoncpp25 liblua5.2-0 libnghttp3-3  
  libplacebo338 libplist3 libpoppler134 libpostproc57  
  libproxy1-plugin-gsettings libproxy1-plugin-networkmanager  
  libproxy1-plugin-webkit libpython3.11-dev libpython3.11-minimal  
  libpython3.11-stdlib libpython3.11t64 libqt6dbus6t64 libqt6gui6t64  
  libqt6network6t64 libqt6opengl6t64 libqt6openglwidgets6t64  
  libqt6printsupport6t64 libqt6sql6t64 libqt6test6t64 libqt6widgets6t64  
  libqt6xml6t64 librados2 librdmacm1t64 libssh-gcrypt-4 libusbmuxd6  
  libwireshark17t64 libwiretap14t64 libwsutil15t64 openjdk-17-jre  
  openjdk-17-jre-headless python3-jose python3-lib2to3 python3-rsa python3.11  
  python3.11-dev python3.11-minimal rwho rwhod samba-vfs-modules  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Проверил установилась ли nikto и её версию

```
(ksudzuki@KSudzuki)-[~]  
$ nikto  
- Nikto v2.5.0
```

Запустил локальный веб-сервер (рис. [-@fig:003])

```
(ksudzuki@KSudzuki)-[~]  
$ sudo systemctl start mysql  
  
(ksudzuki@KSudzuki)-[~]  
$ sudo systemctl start apache2
```

# Просканировал веб-сервер по полному URL

```
---(kxatrak10@kxatrak1)-[~]
$ curl -s 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: 2024-08-05 17:51:26 (GMT)
-----
+ Server: Apache/2.4.62 (Debian)
+ /dvwa/: The x-mll-clickjacking P-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/w
issing-content-type-header/
+ Root page /dvwa redirects to: login.php
+ No CUI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /dvwa//etc/hosts: The server default 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/login.php: Admin login page/section 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 guess 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-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-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/assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/login.cgi?cli=awk23art23art23/etc/hosts: Some 0-link router remote command execution.
+ /dvwa/shell?cat=/etc/hosts: A backdoor was identified.
+ /dvwa/.dockerignore: .dockerignore file found. It may be possible to guess the directory structure and learn more about the site.
+ HTTP requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2024-08-05 17:51:46 (GMT) (16 seconds)
-----
+ 1 host(s) tested
```



# Просканировал веб-сервер по порту и ip-адресу

```
---(khozrakh@khozrakh):[~]
$ nmap -sS 127.0.0.1 -p 80
Nmap v2.5.0

-----
+ Target IP: 127.0.0.1
+ Target hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-05 17:55:25 (GMT)
-----

+ Server: Apache/2.4.42 (Ubuntu)
+ /: 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: 28cf, nsize: 422178c4bcc49, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1618
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /etc/passwd: The server doesn't allow 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/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Moday.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Moday.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/: A PHP backdoor file manager was found.
+ /login.cgi?cli=ma8baas27ca3b9:/etc/passwd: Some 0-link router remote command execution.
+ /shell?cat=/etc/passwd: A backdoor was identified.
+ 80% requests: 0 error(s) and 15 item(s) reported as remote host
+ End Time: 2024-10-05 17:56:01 (GMT) (36 seconds)

+ 1 host(s) tested
```

Установил nikto на kali linux. Просканировал локальный веб-сервер с помощью nikto двумя способами. При сканировании по полному URL, дается больше информации.