

Четвертый этап проекта

Основы информационной безопасности

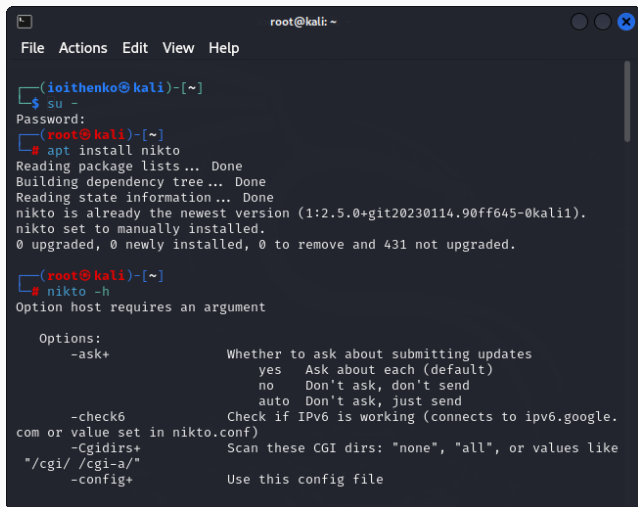
Ищенко Ирина

Российский университет дружбы народов, Москва, Россия

- Ищенко Ирина Олеговна
- НПИбд-02-22

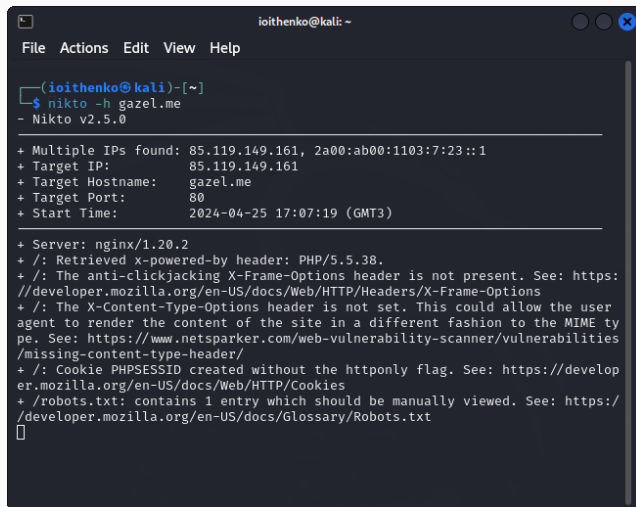
Получить навыки работы с nikto, отображающем информацию об уязвимостях.

Выполнение проекта



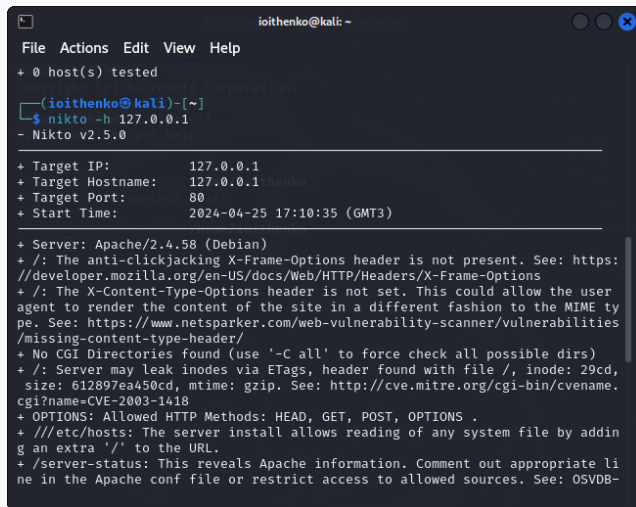
```
root@kali: ~  
File Actions Edit View Help  
  
(ioithenko@kali)-[~]  
$ su -  
Password:  
(root@kali)-[~]  
# apt install nikto  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).  
nikto set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 431 not upgraded.  
  
(root@kali)-[~]  
# 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)  
  -Cgидirs+            Scan these CGI dirs: "none", "all", or values like  
"/cgi/" /cgi-a/"  
  -config+             Use this config file
```

Рис. 1: Справка по команде



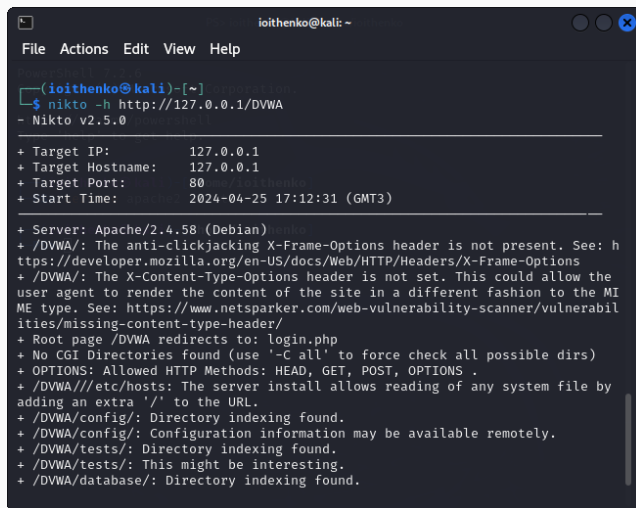
```
ioithenko@kali: ~  
File Actions Edit View Help  
  
(ioithenko@kali)-[~]  
$ nikto -h gazel.me  
- Nikto v2.5.0  
  
+ Multiple IPs found: 85.119.149.161, 2a00:ab00:1103:7:23::1  
+ Target IP:      85.119.149.161  
+ Target Hostname: gazel.me  
+ Target Port:    80  
+ Start Time:     2024-04-25 17:07:19 (GMT3)  
  
+ 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  
□
```

Рис. 2: Для веб-сайта



```
ioithenko@kali: ~  
File Actions Edit View Help  
+ 0 host(s) tested  
Copyright (c) 2004-2014, Microsoft Corporation.  
(ioithenko@kali)~  
$ nikto -h 127.0.0.1  
- Nikto v2.5.0  
+-----+  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1:henko  
+ Target Port: 80  
+ Start Time: 2024-04-25 17:10:35 (GMT3)  
+-----+  
+ 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: 612897ea450cd, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .  
+ ///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-
```

Рис. 3: Для локальной сети



```
ioithenko@kali: ~  
File Actions Edit View Help  
  
(ioithenko@kali)-[~]  
$ nikto -h http://127.0.0.1/DVWA  
- Nikto v2.5.0 powershell  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Start Time: 2024-04-25 17:12:31 (GMT3)  
  
+ 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: HEAD, GET, POST, OPTIONS .  
+ /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.
```

Рис. 4: Для веб-сервера в локальной сети

В ходе проекта я получила навыки работы с nikto, отображающем информацию об уязвимостях.