Индивидуальный проект

Этап 4. Использование Nikto

Артамонов Т. Е.

5 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/teartamonov

Цель работы

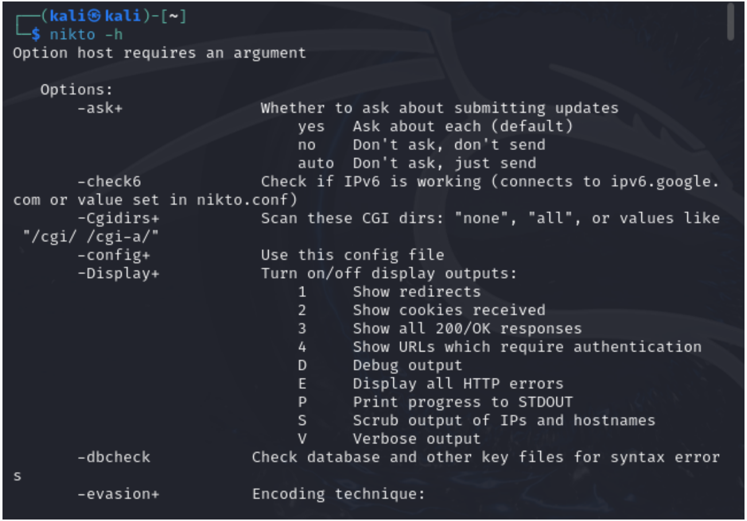
Исспользовать Nikto для поиска уязвимостей в системе.

Теоретеческое введение

Nikto — веб-сканер, проверяющий веб-серверы на самые частые ошибки, возникающие обычно из-за человеческого фактора. Проверяет целевой веб-сервер на наличие опасных файлов и исполняемых сценариев, инструментов администрирования базами данных, устаревшего программного обеспечения.

Выполнение лабораторной работы

Посмотрим список опций для команды nikto. (рис. (fig:001?))

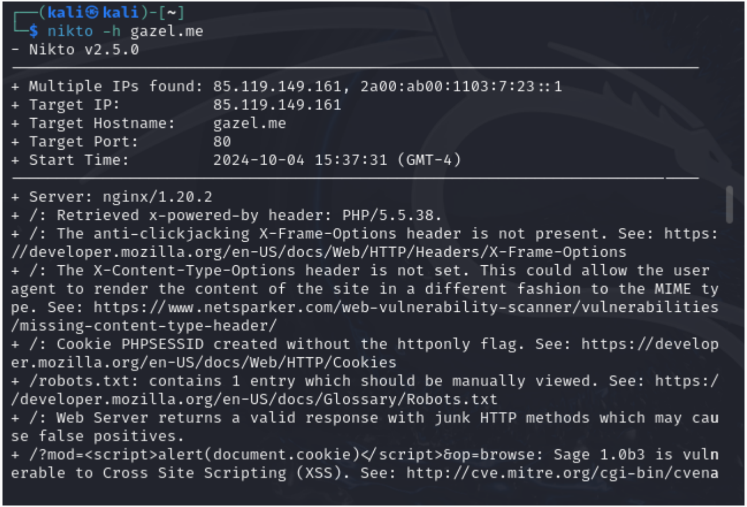


```
┌──(kali㉿kali)-[~]
└─$ nikto -h
Option host requires an argument

   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)
       -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 error
s
       -evasion+                Encoding technique:
```

Рис. 1: Опции для команды nikto

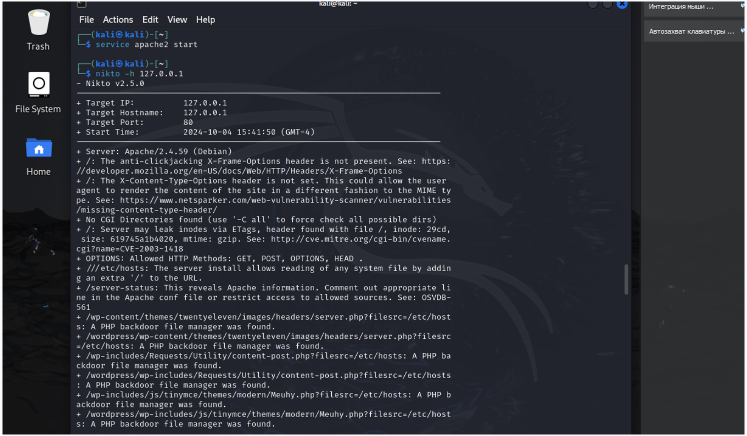
Запустим nikto для поиска уязвиомстей в системе. (рис. (fig:002?))



```
┌──(kali㉿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:         2024-10-04 15:37:31 (GMT-4)
---------------------------------------------------------------------------
+ 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 ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://develop
er.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 cau
se false positives.
+ /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vuln
erable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvena
```

Рис. 2: Нашли несколько уязвимостей, например, Sage 1.0b3

Проверим apache2 на уязвимости. (рис. (fig:003?))

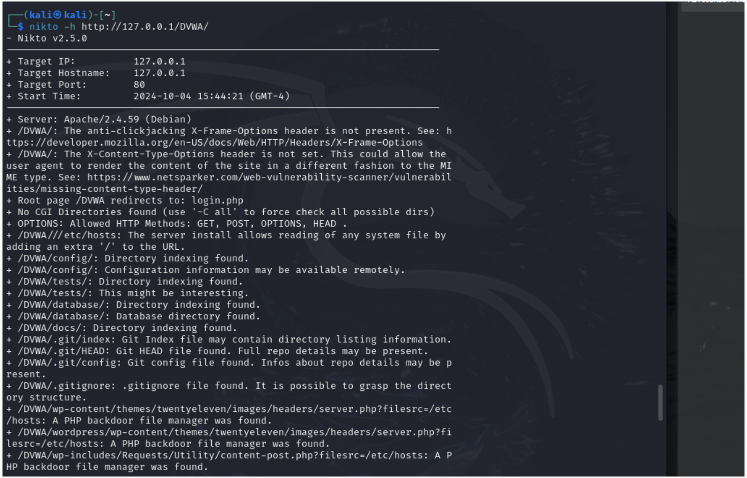


```
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ 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:         2024-10-04 15:41:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.59 (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 ty
pe. 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: 619745a1b4020, mtime: gzip. 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 addin
g an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate li
ne in the Apache conf file or restrict access to allowed sources. See: OSVDB-
561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/host
s: 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 ba
ckdoor 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 b
ackdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
```

Рис. 3: Здесь также нашли несколько уязвимостей, например, несколько backdoor file manager

Проверим DVWA на уязвимости. (рис. (fig:004?))



```
┌──(kali㉿kali)-[~]
└─$ 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:         2024-10-04 15:44:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.59 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: h
ttps://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 MI
ME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabil
ities/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: 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 p
resent.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the direct
ory 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?fi
lesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A P
HP backdoor file manager was found.
```

Рис. 4: Также нашли уязвимости и в DVWA, те же backdoor file manager

Выводы

Использовали nikto для поиска уязвимостей в системе и приложениях.

Список литературы

1. Nikto [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: https://ru.wikipedia.org/wiki/Nikto.