

Отчет по этапу №4

Использование nikto

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	9
	Список литературы	10

Список иллюстраций

2.1	Справка	6
2.2	Сканирование веб-сайта	7
2.3	Сканирование локальной сети	7
2.4	Сканирование DVWA	8

1 Цель работы

Научиться использовать инструмент для сканирования на уязвимости nikto.

2 Выполнение лабораторной работы

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

Для сканирования цели необходимо ввести `nikto -h <цель> -p <порт>`, где `<цель>` — домен или IP-адрес целевого сайта, а `<порт>` — порт, на котором запущен сервис [1].

Для получения справки ввожу `nikto -h` (рис. 2.1).


```
(ngalacan@ngalacan)-[~]
$ 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: 2024-03-22 19:55:51 (GMT3)

+ Server: nginx/1.20.2
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: 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/
+ /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 cause false positives.
+ /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1243
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8770 requests: 1 error(s) and 9 item(s) reported on remote host
+ End Time: 2024-03-22 19:58:11 (GMT3) (140 seconds)

+ 1 host(s) tested
```

Рис. 2.2: Сканирование веб-сайта

Запускаю сканирование для локальной сети, введя `nikto -h 127.0.0.1`. В результате получаю замечая о работе сервера Apache (рис. 2.3).

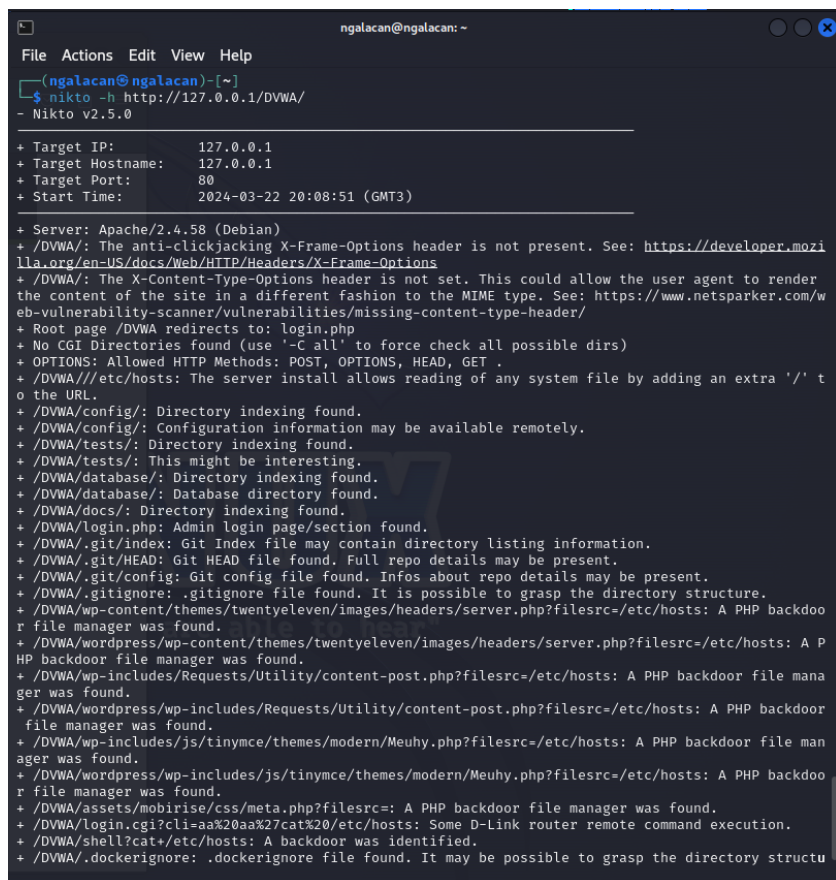
```
(ngalacan@ngalacan)-[~]
$ nikto -h 127.0.0.1
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-03-22 19:53:24 (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: 6124d1e7a22be, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ ///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 P
```

Рис. 2.3: Сканирование локальной сети

Далее приступаю к сканированию веб-приложения DVWA, запущенном в локальной сети [2] (рис. 2.4):



```
ngalacan@ngalacan: ~  
File Actions Edit View Help  
(ngalacan@ngalacan)~  
$ 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: 2024-03-22 20:08:51 (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: POST, OPTIONS, HEAD, GET .  
+ /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/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 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.  
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.  
+ /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-link router remote command execution.  
+ /DVWA/shell?cat+/etc/hosts: A backdoor was identified.  
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure
```

Рис. 2.4: Сканирование DVWA

nikto выводит информацию о структуре DVWA и находит возможные уязвимости. Среди них, например, PHP backdoor file manager.

3 Выводы

Приобретены навыки использования nikto для сканирования веб-серверов на уязвимости. Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения.

Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.
2. Scan for Vulnerabilities on Any Website Using Nikto. [Электронный ресурс].