

Отчет 4 этапу индивидуального проекта

Использование Nikto

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	11

Список иллюстраций

3.1	Просмотр справочной информации	7
3.2	Проверка <code>gazel.me</code>	8
3.3	Поиск уязвимостей на локальном сервере	9
3.4	Проверка DVWA	10

Список таблиц

1 Цель работы

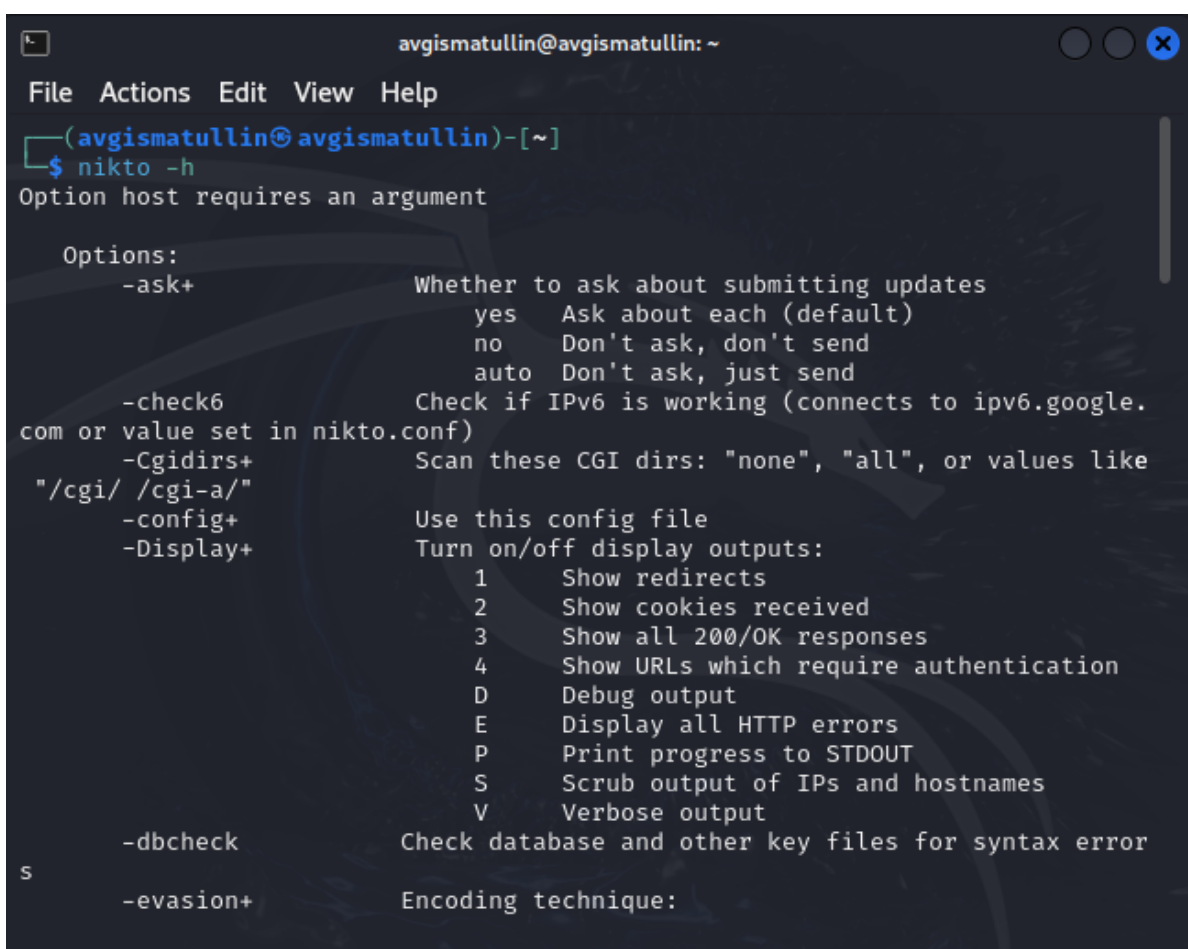
Получение практических навыков работы с Nikto и нахождению уязвимостей.

2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

3 Выполнение лабораторной работы

1. Первым делом получим справочную информацию по сканеру безопасности Nikto командой `nikto -h` (рис. 3.1)



```
avgismatullin@avgismatullin: ~
File Actions Edit View Help
(avgismatullin@avgismatullin)-[~]
$ 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)
  -Cgkdirs+            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
  -evasion+            Encoding technique:
```

Рис. 3.1: Просмотр справочной информации

2. После этого попробуем найти уязвимости сайта `gazel.me`, где обнаружится 20 уязвимостей (рис. 3.2)

```
avgismatullin@avgismatullin: ~  
File Actions Edit View Help  
  
(avgismatullin@avgismatullin)-[~]  
$ 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: 2024-04-26 21:01:18 (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 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  
  
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response  
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
```

Рис. 3.2: Проверка gazel.me

- Затем запустим свой веб-сервис командой `service apache2 start`, как в предыдущей стадии и попробуем найти уязвимости здесь (не обнаружено) (метод GET) (рис. 3.3)


```

cgitname=CVE-2003-1410
+ 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.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-04-26 21:14:56 (GMT-4) (31 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.58) are not in

```

Рис. 3.3: Поиск уязвимостей на локальном сервере

4. Далее испытаем ранее установленную DVWA и проанализируем на предмет уязвимостей командой `nikto -h http://127.0.0.1/DVWA/` (Уязвимостей снова не было обнаружено) (рис. 3.4)

```
+ /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.
+ /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 and learn more about the site.
+ 8074 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time: 2024-04-26 21:16:43 (GMT-4) (38 seconds)

+ 1 host(s) tested
```

Рис. 3.4: Проверка DVWA

4 Выводы

В ходе выполнения данного этапа были получены практические навыки работы с Nikto и поиском уязвимостей