

Отчет по индивидуальному проекту 4

Дисциплина: Информационная безопасность

Хрусталев Влад Николаевич

Содержание

| | | |
|---|--------------------------------|---|
| 1 | Цель работы | 5 |
| 2 | Выполнение лабораторной работы | 6 |
| 3 | Выводы | 8 |

Список иллюстраций

| | | |
|-----|---|---|
| 2.1 | Вывод команды “nikto -h” | 6 |
| 2.2 | Вывод команды “nikto -h vsosh.rudn.ru” | 7 |
| 2.3 | Вывод команды “nikto -h 127.0.0.1/DVWA” | 7 |

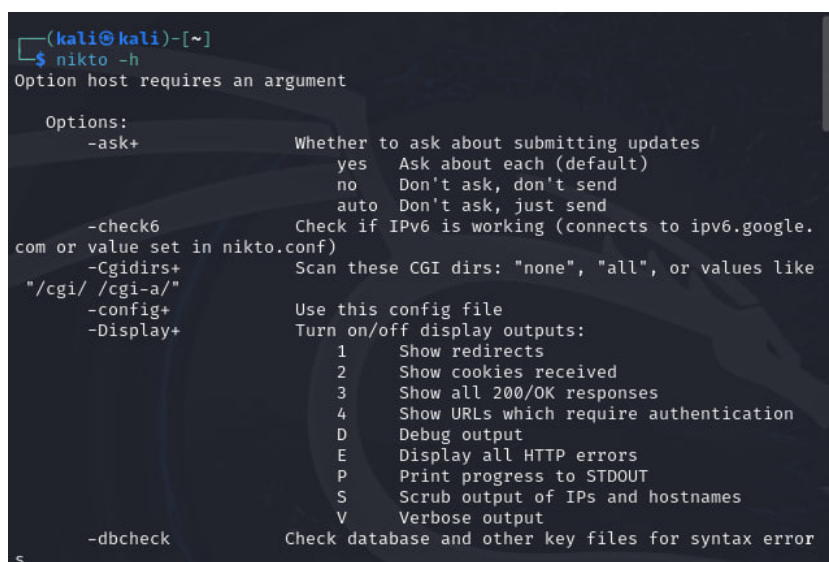
Список таблиц

1 Цель работы

Знакомство с базовым сканером безопасности nikto.

2 Выполнение лабораторной работы

1. Посмотрим основную информацию об данном ПО и посмотрим возможные аргументы для команды `nikto -h`.



```
(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)
  -Cgdirs+       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
```

Рис. 2.1: Вывод команды “nikto -h”

2. Протестируем его на сайте моей разработки `nikto -h vsosh.rudn.ru`.

```
File Actions Edit View Help
(kali@kali)-[~]
$ nikto -h vsosh.rudn.ru
- Nikto v2.5.0

+ Target IP: 89.232.160.167
+ Target Hostname: vsosh.rudn.ru
+ Target Port: 80
+ Start Time: 2024-04-27 12:37:56 (GMT-4)

+ Server: Apache/2.4.52 (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/
+ Root page / redirects to: https://vsosh.rudn.ru
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). A patch 2.2.34 is the EOL for the 2.x branch.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
+ 8052 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2024-04-27 12:40:30 (GMT-4) (154 seconds)

+ 1 host(s) tested
```

Рис. 2.2: Вывод команды “nikto -h vsosh.rudn.ru”

3. Так же протестируем на поднятом уязвимом сервере nikto -h 127.0.0.1/DVWA.

```
(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: 2024-04-27 12:42:02 (GMT-4)

+ 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: GET, POST, OPTIONS, HEAD .
+ /DVWA//etc/passwd: 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.
```

Рис. 2.3: Вывод команды “nikto -h 127.0.0.1/DVWA”

3 Выводы

В результате выполнения лабораторной работы на практике опробовали базовым сканером безопасности nikto.