

Отчет по четвертому этапу индивидуального проекта

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	9
	Список литературы	10

Список иллюстраций

2.1	Справка по команде	6
2.2	Для веб-сайта	7
2.3	Для локальной сети	7
2.4	Для веб-сервера в локальной сети	8

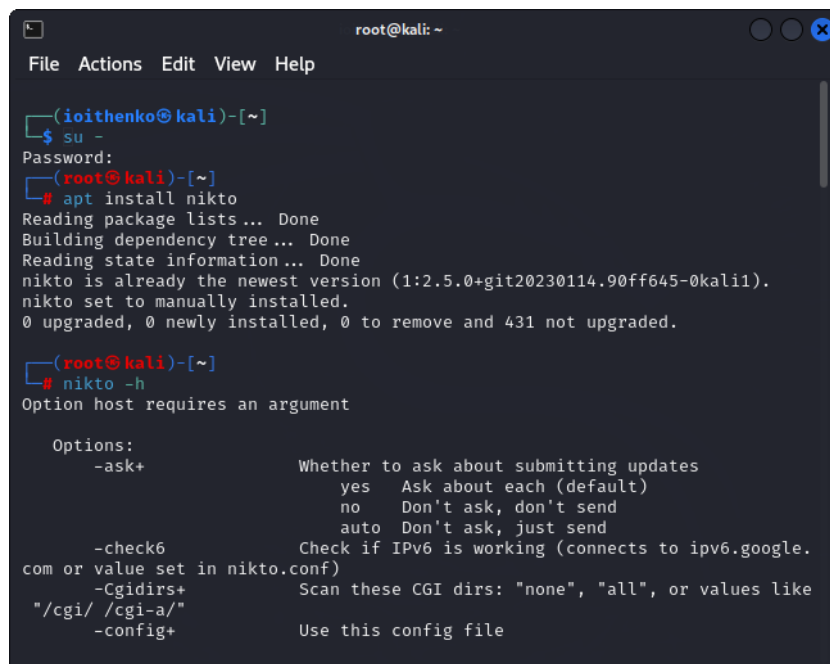
Список таблиц

1 Цель работы

Получить навыки работы с nikto, отображающем информацию об уязвимостях [1].

2 Выполнение лабораторной работы

Проверим, что сервер установлен и посмотрим справку (рис. 2.1).



```
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. 2.1: Справка по команде

С помощью команды `nikto -h gazel.me` узнаем об уязвимостях веб-сайта `gazel.me`. Пример уязвимости: отсутствие the anti-clickjacking `X-Frame_Options` header (рис. 2.2).

```
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. 2.2: Для веб-сайта

Для вывода информации о локальной сети введем в качестве аргумента IP. Предварительно арасче сервер (рис. 2.3).

```
ioithenko@kali: ~  
File Actions Edit View Help  
  
+ 0 host(s) tested  
  
(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. 2.3: Для локальной сети

Запросим уязвимости веб-сервера dvwa в локальной сети. Пример уязвимости: no CGI directories found (рис. 2.4).

Рис. 2.4: Для веб-сервера в локальной сети

3 Выводы

В ходе этапа проекта я получила навык работы с сервером nikto.

Список литературы

1. Ш. Парасрам Т.Х. А. Замм. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.