

Индивидуальный проект №4

Основы информационной безопасности

Барсегян В.Л.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

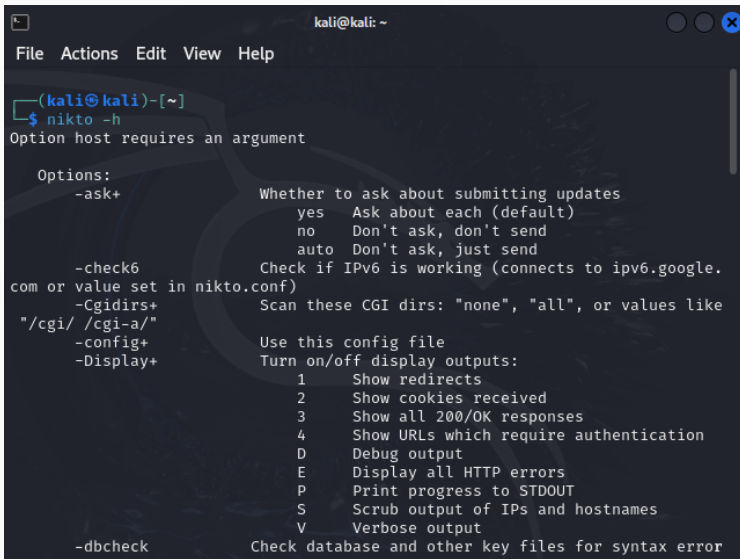
- Барсегян Вардан Леонович
- НПИбд-01-22
- Российский университет дружбы народов
- [1132222005@pfur.ru]
- https://github.com/VARdamn/study_2023-2024_infosec/tree/master/project-personal

Вводная часть

Знакомство с базовым сканером безопасности nikto, его применение.

Выполнение лабораторной работы

Вывожу справку об утилите nikto командой *nikto -h*



```
kali@kali: ~  
File Actions Edit View Help  
  
(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
```

Figure 1: nikto -h

Сканирую веб-сайт gosuslugi.ru на наличие уязвимостей с помощью команды *nikto -h gosuslugi.ru*. Утилита показала отсутствие некоторых важных для безопасности заголовков

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nikto -h gosuslugi.ru  
- Nikto v2.5.0  
  
+ Multiple IPs found: 213.59.254.7, 213.59.253.7  
+ Target IP: 213.59.254.7  
+ Target Hostname: gosuslugi.ru  
+ Target Port: 80  
+ Start Time: 2024-03-28 10:46:18 (GMT-4)  
  
+ Server: BigIP  
+ /: 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://gosuslugi.ru/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ 7962 requests: 0 error(s) and 2 item(s) reported on remote host  
+ End Time: 2024-03-28 10:47:22 (GMT-4) (64 seconds)  
  
+ 1 host(s) tested
```

Сканирую локальный хост на наличие уязвимостей с помощью команды *nikto -h 127.0.0.1*

```
kali@kali: ~  
File Actions Edit View Help  
  
(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: 2024-03-28 10:48:32 (GMT-4)  
  
+ 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: 61236d1d67a20, 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 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-
```


Сканирую приложение DVWA с помощью команды *nikto -h http://127.0.0.1/DVWA*. *nikto* также указывает на отсутствие важных заголовков и выводит информацию о различных доступных эндпоинтах

```
kali@kali: ~  
File Actions Edit View Help  
  
(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: 2024-03-28 10:49:52 (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/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.
```

Я познакомился с nikto, научился его применять на практике для проверки уязвимостей различных сайтов

Список литературы

Список литературы