

Отчёт по индивидуальному проекту

Этап 4

Надежда Александровна Рогожина

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение	7
	Список литературы	11

Список иллюстраций

3.1	Установка nikto	7
3.2	nikto -h	8
3.3	nikto -h eystem.rudn.ru	8
3.4	nikto -h school1366.ru	9
3.5	nikto -h school1366.ru	9
3.6	nikto -h school1366.ru	10

Список таблиц

1 Цель работы

Получить начальные практические навыки работы с nikto.

2 Теоретическое введение

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. Утилита относится к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения. Помимо поиска уязвимостей, сканер производит поиск на наличие устаревших версий, используемых библиотек и фреймворков. Nikto не позиционируется как стелс сканер (стелс сканеры никогда не устанавливают TCP-соединения до конца, тем самым сканирование происходит скрытно) – при сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если она используется, будет отображена информация о том, что сайт подвергается сканированию.

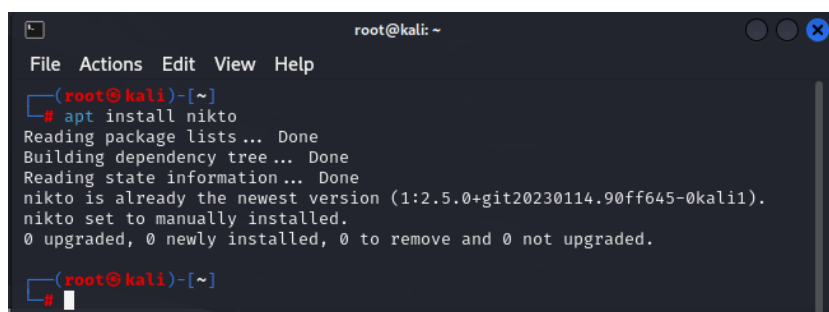
Минимальный синтаксис для запуска сканирования выглядит следующим образом:

```
nikto -h [доменное_имя или IP_адрес]
```

Более подробно можно почитать в [тут](#) и [тут](#).

3 Выполнение

1. От имени суперпользователя установим необходимую программу (рис. [3.3]):



```
root@kali: ~  
File Actions Edit View Help  
(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 0 not upgraded.  
(root@kali)-[~]  
#
```

Рис. 3.1: Установка nikto

2. Изучим справку по команде (рис. [3.2]):

```
(kali@kali)-[~]
└─$ nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

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: Actions, 2: Cookies, 3: HTTP, 4: Redirects, 5: Status, 6: Syntax, 7: Verbose, 8: All
                  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 errors
  -evasion+      Encoding techniques:
                  1     Random URI encoding (non-UTF8)
                  2     Directory self-reference (../)
                  3     Premature URL ending
                  4     Prepend long random string
                  5     Fake parameter
                  6     TAB as request spacer
                  7     Change the case of the URL
                  8     Use Windows directory separator (\)
                  A     Use a carriage return (0x0d) as a request spacer
                  B     Use binary value 0x0b as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+       Save file (-o) format:
                  csv   Comma-separated-value
                  json  JSON Format
                  htm   HTML Format
                  nbe   Nessus NBE format
                  sql   Generic SQL (see docs for schema)
                  txt   Plain text
                  xml   XML Format
                  (if not specified the format will be taken from the file extension passed to -output)
```

Рис. 3.2: nikto -h

3. Протестируем сайт ТУИС (рис. [??]):

```
(kali@kali)-[~]
└─$ nikto -h esystem.rudn.ru
- Nikto v2.5.0

+ Target IP:      37.238.195.241
+ Target Hostname: esystem.rudn.ru
+ Target Port:    80
+ Start Time:     2024-04-27 18:57:46 (GMT+4)

+ Server: nginx/1.18.0 (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://esystem.rudn.ru/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ nginx/1.18.0 appears to be outdated (current is at least 1.20.1).
+ 8040 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2024-04-27 18:59:19 (GMT+4) (93 seconds)

+ 1 host(s) tested
```

Рис. 3.3: nikto -h esystem.rudn.ru

4. Протестируем сайт московской школы №1366 (рис. [3.4], рис. [3.5], рис. [3.3]):

Рис. 3.4: nikto -h school1366.ru

Рис. 3.5: nikto -h school1366.ru

```

File Actions Edit View Help
+ /administr.php: Admin login page/section found.
+ /administr/?: Admin login page/section found.
+ /administracao.php: Admin login page/section found.
+ /administracao.php: Admin login page/section found.
+ /administracao/?: Admin login page/section found.
+ /administracao/?: Admin login page/section found.
+ /administracion.php: Admin login page/section found.
+ /administracion/?: Admin login page/section found.
+ /administrateur.php: Admin login page/section found.
+ /administrateur/?: Admin login page/section found.
+ /administratie/?: Admin login page/section found.
+ /administration.html: Admin login page/section found.
+ /administration.php: Admin login page/section found.
+ /administration/?: Admin login page/section found.
+ /administrator.asp: Admin login page/section found.
+ /administrator.html: Admin login page/section found.
+ /administrator.php: Admin login page/section found.
+ /administrator/account.asp: Admin login page/section found.
+ /administrator/account.html: Admin login page/section found.
+ /administrator/account.php: Admin login page/section found.
+ /administrator/index.asp: Admin login page/section found.
+ /administrator/index.html: Admin login page/section found.
+ /administrator/index.php: Admin login page/section found.
+ /administrator/login.asp: Admin login page/section found.
+ /administrator/login.html: Admin login page/section found.
+ /administrator/login.php: Admin login page/section found.
+ /administratoraccounts/?: Admin login page/section found.
+ /administrators/?: Admin login page/section found.
+ /administrivia/?: Admin login page/section found.
+ /administratortora.php: Admin login page/section found.
+ /adminisztratora/?: Admin login page/section found.
+ /adminpanel.asp: Admin login page/section found.
+ /adminpanel.html: Admin login page/section found.
+ /adminpanel.php: Admin login page/section found.
+ /adminpro/?: Admin login page/section found.
+ /admins.asp: Admin login page/section found.
+ /admins.html: Admin login page/section found.
+ /admins.php: Admin login page/section found.
+ /admins/?: Admin login page/section found.
+ /admin-console: JBoss admin console is visible.
+ /admin/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /admin/status: Tomcat Server Status interface found (pass protected).
+ /admin/sites/new: ComfortableMexicanSofa CMS Engine Admin Backend (pass protected).
+ /core/modules/config/config.info.yml: Drupal version number revealed in config.info.yml.
+ 8770 requests: 1 error(s) and 147 item(s) reported on remote host
+ End Time: 2024-04-27 11:36:25 (GMT+3) (2214 seconds)

+ 1 host(s) tested

```

Рис. 3.6: nikto -h school1366.ru

Список литературы