

Индивидуальный проект.

Этап 4. Использование nikto

Стариков Данила НПИбд-02-22

Содержание

1	Цель работы	3
2	Теоретическое введение	4
3	Выполнение лабораторной работы	6
4	Выводы	10
	Список литературы	11

1 Цель работы

Познакомиться с утилитой `nikto` для поиска уязвимостей веб-серверов, проверить ее работу на ранее установленном сервере DVWA.

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.

Для запуска `nikto` в командной строке необходимо указать несколько параметров (Табл. 2.1):

Таблица 2.1: Основные параметры запуска `nikto`

Ключ	Описание ключа
<code>-host</code>	Указание IP-адрес сервера, для которого необходимо выполнить проверку на уязвимости. Передав текстовый файл можно указать список адресов для проверки.
<code>-Display</code>	Определение сообщения <code>nikto</code> будет выводить в консоль. Возможные значения: 1 – показывать перенаправления 2 – показывать полученные файлы cookie 3 – показывать все ответы 200/OK 4 – показывать URL-адреса, для которых требуется аутентификация D – вывод для отладки V – подробный вывод E – показывать все HTTP ошибки P – выводить прогресс в стандартный вывод (STDOUT)

Ключ	Описание ключа
-Tuning	<p>Контроль над тестами, которые nikto будет проводить. Возможные значения:</p> <ul style="list-style-type: none"> 1 –Интересный файл / Замеченный в логах 2 –Неправильная настройка / Файл по умолчанию 3 –Раскрытие информации 4 –Внедрение (XSS/Script/HTML) 5 –Удаленный поиск файлов - Внутри корневого веб-каталога 6– Отказ в обслуживании 7– Удаленный поиск файлов - на сервере 8 –Выполнение команд / Удаленная оболочка 9 –SQL-инъекция 0 –Загрузка файла a –Обход проверки подлинности b– Идентификация программного обеспечения c – Включение удаленного источника d –Веб-сервис e – Административная консоль x – Параметры обратной настройки (т.е. включить все, кроме указанных)
-o	Указание, в какой файл записать результаты проверки.
-Format	Указание формата файла результатов (htm, csv, json, nbe, sql, txt, xml)

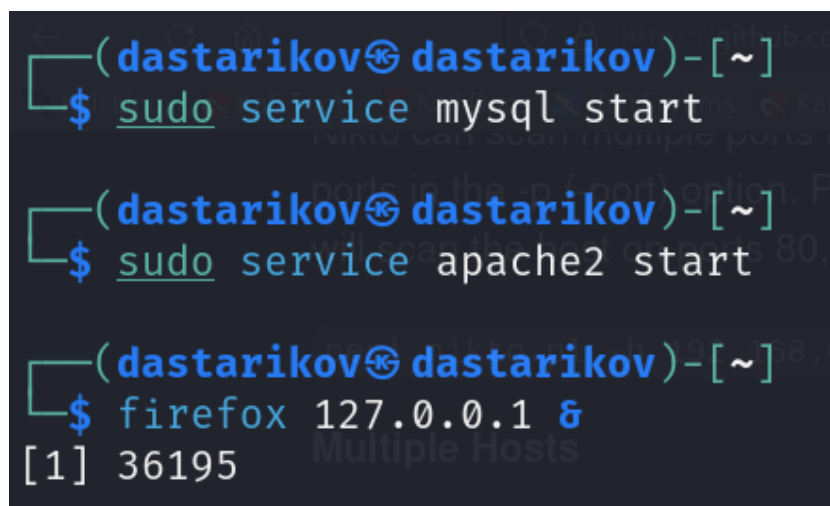
Более подробная информация может быть найдена на man-pages [1].

3 Выполнение лабораторной работы

1. Запустили веб-сервер DVWA, который будем тестировать (Рис. 3.1):

```
sudo service mysql start
```

```
sudo service apache2 start
```

A screenshot of a terminal window with a dark background. The prompt is '(dastarikov@dastarikov)-[~]'. The first command entered is 'sudo service mysql start'. The second command is 'sudo service apache2 start'. The third command is 'firefox 127.0.0.1 &'. The output of the last command is '[1] 36195'.

```
(dastarikov@dastarikov)-[~]  
$ sudo service mysql start  
  
(dastarikov@dastarikov)-[~]  
$ sudo service apache2 start  
  
(dastarikov@dastarikov)-[~]  
$ firefox 127.0.0.1 &  
[1] 36195
```

Рис. 3.1: Запуск веб-сервера DVWA.

2. Открыли веб-страницу запущенного сервера, чтобы убедиться, что он работает (Рис. 3.3):

```
firefox 127.0.0.1/DVWA
```

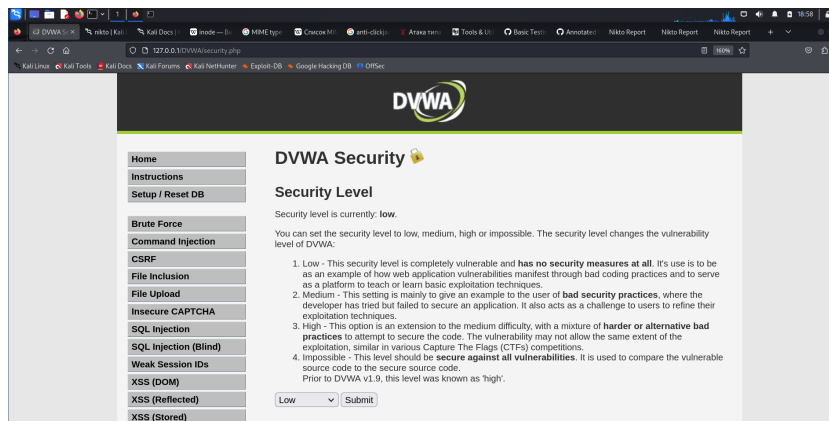


Рис. 3.2: Проверка работы сервера.

3. Открыли описание утилиты `nikto` для составления команды (Рис. 3.1):

`man nikto`

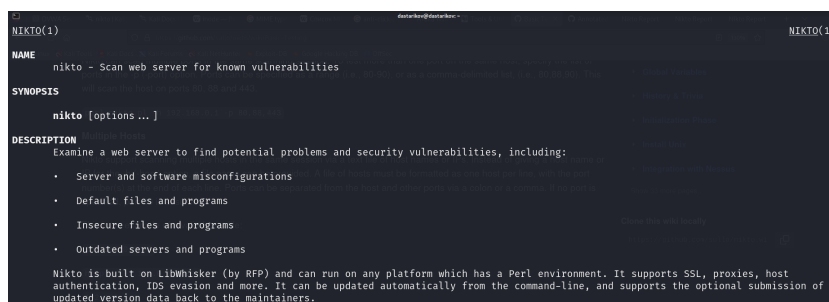


Рис. 3.3: Man-page `nikto`.

4. Запустили утилиту `nikto` со следующими параметрами (Рис. 3.4):

`nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host 127.0.0.1`

```
(dastarikov@dastarikov) ~
$ nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host 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: 2024-04-19 18:21:15 (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: 612b112e93ec6, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /./ - 200/OK Response could be Appending '././' to a directory may reveal PHP source code.
+ /mod=nodesnid-some_thingsop-view - 200/OK Response could be Sage 1.0b3 may reveal system paths with invalid module names.
+ /?mod=some_thingsop-browse - 200/OK Response could be Sage 1.0b3 reveals system paths with invalid module names.
- STATUS: Completed 1000 requests (~29% complete, 12 seconds left): currently in plugin 'Nikto Tests'
- STATUS: Running average: Not enough data.
+ /./ - 200/OK Response could be Appending '././' to a directory allows indexing
+ / - 200/OK Response could be Appears to be a default Apache Tomcat install.
```

Рис. 3.4: Консольный вывод программы во время работы.

Помимо вывода в консоль указали утилите сохранить отчет в файле `output.html`, приведен пример найденной уязвимости (Рис. 3.5) и итог по тестированию (Рис. 3.6).

127.0.0.1 / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	127.0.0.1
Target Port	80
HTTP Server	Apache/2.4.58 (Debian)
Site Link (Name)	http://127.0.0.1:80/
Site Link (IP)	http://127.0.0.1:80/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 612b112e93ec6, mtime: gzip.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/ http://127.0.0.1:80/
References	CVE-2003-1418
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	

Рис. 3.5: Пример найденной уязвимости веб-сервера.

Host Summary	
Start Time	2024-04-19 18:37:42
End Time	2024-04-19 18:38:01
Elapsed Time	19 seconds
Statistics	4300 requests, 0 errors, 5 findings
Scan Summary	
Software Details	Nikto 2.5.0
CLI Options	-Display 1234EP -o report.html -Format htm -Tuning 123bde -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:37:41 2024
End Time	Fri Apr 19 18:38:01 2024
Elapsed Time	20 seconds

Рис. 3.6: Итоговый отчет по тестированию веб-сервера.

5. Также запустили другой тест, на этот раз не уточняя параметр `Tuning`, поэтому были проведены все варианты тестов. Обратим внимание, что в этот тест занял больше времени, и нашел больше уязвимостей (Рис. 3.7)

```
nikto -Display 1234EP -o report.html -Format htm -host 127.0.0.1
```


Host Summary	
Start Time	2024-04-19 18:35:45
End Time	2024-04-19 18:36:17
Elapsed Time	32 seconds
Statistics	8074 requests, 0 errors, 15 findings

Scan Summary	
Software Details	Nikto 2.5.0
CLI Options	-Display 1234EP -o report.html -Format htm -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:35:44 2024
End Time	Fri Apr 19 18:36:17 2024
Elapsed Time	33 seconds

Рис. 3.7: Итоговый отчет по тестированию веб-сервера с большим числом тестов.

4 Выводы

В результате работы познакомились с утилитой `nikto` и проверили уязвимости веб-сервера DVWA с разными параметрами теста.

Список литературы

1. Sullo C., Lodge D. nikto(1) Linux User's Manual. 2010.