

Отчёт по четвёртому этапу индивидуального проекта

Использование nikto

Тарутина Кристина Олеговна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	8
	Список литературы	9

Список иллюстраций

2.1	Справка	6
2.2	Результат для github.com	7
2.3	Результат для локальной сети	7

Список таблиц

1 Цель работы

Научиться использовать базовый сканер безопасности веб-сервера nikto

2 Выполнение лабораторной работы

Получаем справку по работе nikto (рис. 2.1).

nikto -h

```
L$ 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
  -evasion+     Encoding technique:
                  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
```

Рис. 2.1: Справка

Далее для примера запустим сканирование всем известного сайта github.com на пример уязвимостей(рис. 2.2).

nikto -h github.com

```
(kotarutina@kotarutina)~$ nikto -h github.com
- Nikto v2.5.0

+ Target IP: 69.162.95.6
+ Target Hostname: github.com
+ Target Port: 80
+ Start Time: 2024-04-27 15:08:29 (GMT3)

+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version, Sec-CH-UA-Mobile.
+ /: 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/
```

Рис. 2.2: Результат для github.com

И теперь отсканируем собственную локальную сеть(рис. 2.3).

nikto -h 127.0.0.1

```
$ 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: 2024-04-27 15:09:45 (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: 61703ee9fb635, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /etc/passwd: 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-561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/passwd: Some D-Link router remote command execution.
```

Рис. 2.3: Результат для локальной сети

3 Выводы

Мы успешно изучили базовый сканер безопасности веб-сервера nikto

Список литературы