

Презентация по этапу №4

Использование nikto

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Научиться использовать инструмент для сканирования на уязвимости nikto.

Выполнение лабораторной работы

```
ngalacan@ngalacan: ~  
File Actions Edit View Help  
$ 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)  
-Cgkdirs+      Scan these CGI dirs: "none", "all", or values like "/c  
gi/ /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 errors  
-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 sp  
acer
```

Рис. 1: Справка

Выполнение лабораторной работы

```
(ngalacan@ngalacan)-[~]  
$ 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:     2024-03-22 19:55:51 (GMT3)  
  
+ Server: nginx/1.20.2  
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mo  
zilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: Retrieved x-powered-by header: PHP/5.5.38.  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev  
eloper.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: h  
ttps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten  
t-type-header/  
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://deve  
loper.mozilla.org/en-US/docs/Glossary/Robots.txt  
+ /: Web Server returns a valid response with junk HTTP methods which may cause fa  
lse positives.  
+ /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerabl  
e to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?nam  
e=CVE-2003-1243  
+ /icons/: Directory indexing found.  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-r  
estricting-access-to-iconsreadme/  
+ 8770 requests: 1 error(s) and 9 item(s) reported on remote host  
+ End Time:      2024-03-22 19:58:11 (GMT3) (140 seconds)  
  
+ 1 host(s) tested
```

Рис. 2: Сканирование веб-сайта

Выполнение лабораторной работы

```
(ngalacan@ngalacan)-[~]  
$ 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: 2024-03-22 19:53:24 (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: 6124d1e7a22be, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .  
+ ///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-561  
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A P
```

Рис. 3: Сканирование локальной сети

Выполнение лабораторной работы

```
ngalacan@ngalacan: ~  
File Actions Edit View Help  
ngalacan@ngalacan:~$ 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: 2024-03-22 20:08:51 (GMT+3)  
  
+ 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: POST, OPTIONS, HEAD, GET .  
+ /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.  
+ /DVWA/tests/: Directory indexing found.  
+ /DVWA/tests/: This might be interesting.  
+ /DVWA/database/: Directory indexing found.  
+ /DVWA/database/: Database directory found.  
+ /DVWA/docs/: Directory indexing found.  
+ /DVWA/login.php: Admin login page/section found.  
+ /DVWA/.git/index: Git Index file may contain directory listing information.  
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.  
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.  
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.  
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wp-includes/js/tinymce/themes/modern/Mouhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Mouhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/assets/mobile/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/login-shellcat.sh: A backdoor was identified.  
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure.
```

Рис. 4: Сканирование DVWA

Приобретены навыки использования nikto для сканирования веб-серверов на уязвимости. Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения.