

Презентация по 4 этапу индивидуального проекта.

Основы информационной безопасности.

Рогожина Н.А.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Рогожина Надежда Александровна
- Студентка 2го курса, НКАбд-02-22
- Компьютерные и информационные науки
- Российский университет дружбы народов
- Github

Цели работы

- Получить начальные практические навыки работы с `nikto`

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:

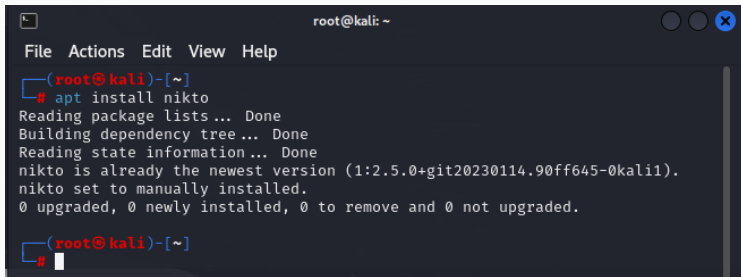
```
nikto -h [доменное_имя или IP_адрес]
```

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

Выполнение



1. От имени суперпользователя установим необходимую программу:



```
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. 1: Установка nikto

2. Изучим справку по команде:

```
root@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
  -checks       Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgiext       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-bin/"
  -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
  -discheck     Check database and other key files for syntax errors
  - evasion     Increasing techniques:
                 1    Random URL 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 0x00 as a request spacer
  -followredirects Follow 3xx redirects to new location
  -format       Save file (-o) format:
                 csv  Comma-separated-value
                 json JSON Format
                 html HTML Format
                 osw  Nessus NSE 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. 2: nikto -h

3. Протестируем сайт ТУИС:

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

+ Target IP: 37.230.195.241
+ Target Hostname: esystem.rudn.ru
+ Target Port: 80
+ Start Time: 2024-04-27 10:57:46 (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).
+ 8046 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-04-27 10:59:19 (GMT-4) (93 seconds)

+ 1 host(s) tested

(kali@kali)-[~]
$
```

Рис. 3: nikto -h esystem.rudn.ru

4. Протестируем сайт московской школы №1366:

```
[kali@kali]~$ nikto -h school1366.ru
- Nikto v2.5.0
```

```
+ Multiple IPs found: 31.31.198.199, 2a08:f940::2:2:1:4:0:95
+ Target IP:      31.31.198.199
+ Target Hostname: school1366.ru
+ Target Port:    80
+ Start Time:     2024-04-27 10:59:31 (GMT+4)
```

```
+ 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
+/ 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/
/[A][A][A][A][A][A][A][A][A][A][A][A][A][A][A][A]: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+/ administrator/gallery/uploadimage.php: Mamba PHP Portal/Server 4.0.12 BETA and below may allow upload of any file type simply putting '.jpg' before the real file extension.
+/ admin/config.php: PHP Config file may contain database IDs and passwords.
+/ administrator/config.php: PHP Config file may contain database IDs and passwords.
+/ admin-serv/config/admwp/: This contains the encrypted Netscape admin password. It should not be accessible via the web.
+/ administrator/upLoad.php?newBanner=1&choice=c%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).
+/ administrator/popups/sections/window.php?type=web&link=c%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+/ administrator/gallery/view.php?path=a%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+/ administrator/gallery/downloadImage.php?idDirectory=a%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+/ administrator/gallery/navigation.php?idDirectory=a%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+/ administrator/gallery/gallery.php?idDirectory=a%<script>alert(document.cookie)</script>: Mamba PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+/ admin/sh_taskframes.aspTitleFieldContentID=CS3BMS2Qdnc22regrostr2WebURLMasterSettings\Web_LogSettings.aspTab1-TabsWebViewer2Gtatbz2Tabs WebLogSettingsKbc_SAPageKey=5742D5874AD85934AI3CDBF5FG9C32AGeReturnURL=a%<script>alert(document.cookie)</script>; IE 8 on Windows 2003 is vulnerable to Cross Site Scripting (XSS) in certain error messages.
+/ phpinfo.phpVARS[a-z]*=<script>alert('vulnerable')</script>; Retrieved x-powered-by header: PHP/5.3.29.
+/ phpinfo.php Output from the phpinfo() function was found.
+/ admin/cplgfile.log: DevBB 1.0 Final log file is readable remotely. Upgrade to the latest version. See: http://www.nybbboard.com
+/ admin/system_footer.php: myphpnuke version 1.8.8-final_7 reveals detailed system information.
+/ /JdkWeb/10.10.10.10: The remote DBW/WEB server may allow you to connect to arbitrary machines and ports. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1454
+/ admin/php7en_log_id=ObAction-function: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-5412
+/ admin/php7en_log_id=ObAction-functions: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-5412
+/ admin/php7reg_login.html: Mon Album version 0.6.2d allows remote admin access. This should be protected.
+/ admin/admin_phpinfo.php4: Non Album version 0.6.2d allows remote admin access. This should be protected.
```

Рис. 4: nikto -h school1366.ru

```
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /cgi-bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1607
+ //admin/admin.shtml: Axis network camera may allow admin bypass by using double-slashes before URLs. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0240
+ /admin/database/webForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein. See: OSVDB-2813
+ //admin/index.htm: FlexWATCH firmware 2.2 is vulnerable to authentication bypass by prepending an extra '/s. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-3606
+ /admin/wg_user-info.wl: WebGate Web Eye exposes user names and passwords. See: OSVDB-2922
+ /admin.htm: This might be interesting.
+ /admin.html: This might be interesting.
+ /admin.php: This might be interesting.
+ /admin.php3: This might be interesting.
+ /admin.shtml: This might be interesting.
+ /admin/: This might be interesting.
+ /administration/: This might be interesting.
+ /administrator: This might be interesting.
+ /files/: Directory indexing found.
+ /files/: This might be interesting.
+ /mail/: Directory indexing found.
+ /mail/: This might be interesting.
+ /pix/: Directory indexing found.
+ /pix/: This might be interesting.
+ /img-sys/: Default image directory should not allow directory listing.
+ /admin/auth.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/cfg/configscreen.inc.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/cfg/configsite.inc.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/cfg/configsql.inc.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/cfg/configtache.inc.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/cms/htmltags.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/credit_card_info.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/exec.php3: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/index.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/modules/cache.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/objects.inc.php4: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/script.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/settings.inc.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/templates/header.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin/upload.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /admin_t/include/off_liste_langue.php: This might be interesting; has been seen in web logs from an unknown scanner.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CVE-552
+ /images/: Directory indexing found.
+ /admin/adminproc.asp: Xpede administration page may be available. The /admin directory should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0579
+ /admin/datasource.asp: Xpede page reveals SQL account name. The /admin directory should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0579
+ /admin/admin.phpadminpy-l: PY-Membres 4.2 may allow administrator access. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1198
```

Рис. 5: nikto -h school1366.ru

```

File Actions Edit View Help
+ /administr8.php: Admin login page/section found.
+ /administr8/: Admin login page/section found.
+ /administracao.php: Admin login page/section found.
+ /administracao/: 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.
+ /adminisratora.php: Admin login page/section found.
+ /adminisratora: 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.
+ /adminprv/: 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-4) (2214 seconds)

+ 1 host(s) tested

```

Рис. 6: nikto -h school1366.ru

Спасибо за внимание!
