4 этап индивидуального проекта

Использование Nikto

Гисматуллин А.В.

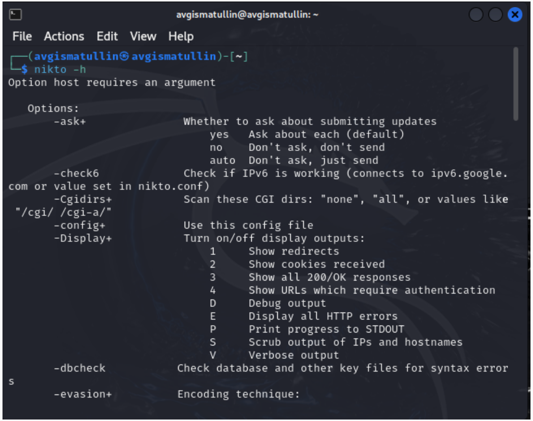
Российский университет дружбы народов, Москва, Россия

Цели и задачи

- Получение практических навыков работы с Nikto и нахождению уязвимостей.

Процесс выполнения лабораторной работы

Справочная информация

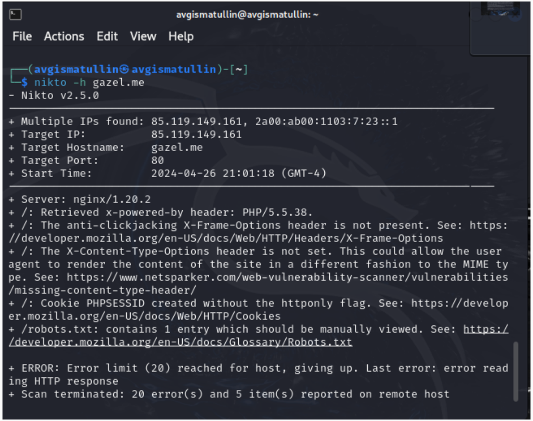


```
┌──(avgismatullin㉿avgismatullin)-[~]
└─$ nikto -h
Option host requires an argument

   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
s
       -evasion+          Encoding technique:
```

Рис. 1: Просмотр справочной информации

Проверка сайта

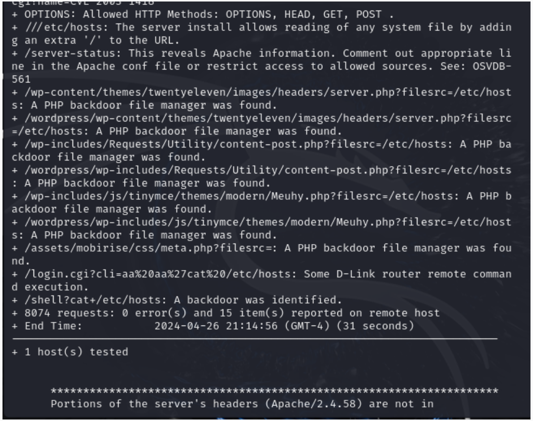


```
┌──(avgismatullin㉿avgismatullin)-[~]
└─$ nikto -h gazel.me
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 85.119.149.161, 2a00:ab00:1103:7:23::1
+ Target IP:          85.119.149.161
+ Target Hostname:    gazel.me
+ Target Port:        80
+ Start Time:         2024-04-26 21:01:18 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.20.2
+ /: Retrieved x-powered-by header: PHP/5.5.38.
+ /: 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 ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: contains 1 entry which should be manually viewed. See: https:/
/developer.mozilla.org/en-US/docs/Glossary/Robots.txt

+ ERROR: Error limit (20) reached for host, giving up. Last error: error read
ing HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
```

Рис. 2: Проверка gazel.me

Локальный сервер

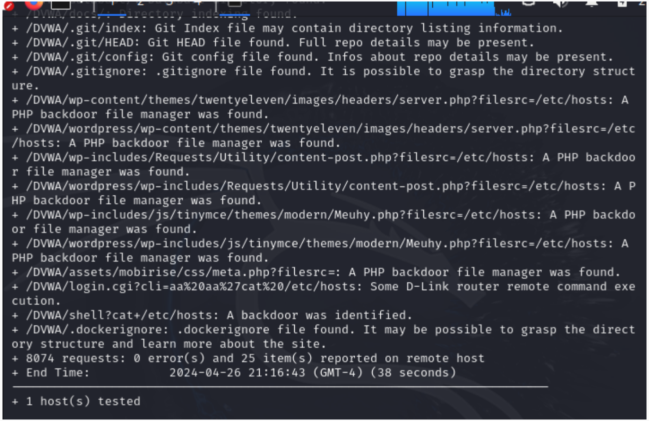


```
cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ///etc/hosts: The server install allows reading of any system file by addin
g an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate li
ne in the Apache conf file or restrict access to allowed sources. See: OSVDB-
561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/host
s: 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 ba
ckdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts
: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP b
ackdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was fou
nd.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote comman
d execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2024-04-26 21:14:56 (GMT-4) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.58) are not in
```

Рис. 3: Поиск уязвимостей на локальном сервере

DVWA



```
+ /DVWA/docs/: Directory indexing 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 struct
ure.
+ /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 backdoo
r file manager was found.
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A P
HP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdo
or file manager was found.
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A
PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command exe
cution.
+ /DVWA/shell?cat+/etc/hosts: A backdoor was identified.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the direct
ory structure and learn more about the site.
+ 8074 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time:           2024-04-26 21:16:43 (GMT-4) (38 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Рис. 4: Проверка DVWA

Выводы по проделанной работе

Выводы по проделанной работе

В ходе выполнения данного этапа были получены практические навыки работы с Nikto и поиском уязвимостей