4 этап персонального проекта

Основы информационной безопасности

Ганина Т.С.

27 апреля 2024

Группа НКАбд-01-22

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ганина Таисия
- Студентка 2 курса, НКАбд-01-22
- Направление “Компьютерные и информационные науки”
- Российский университет дружбы народов
- Гитхаб
- https://tsganina.github.io/

Вводная часть

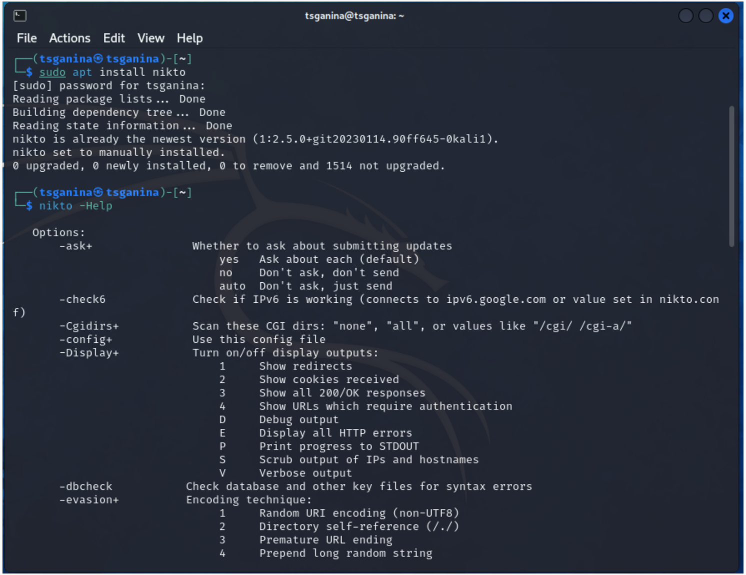
Объект и предмет исследования

- Работа с Nikto

Цели и задачи

Изучение работы сервиса Nikto.

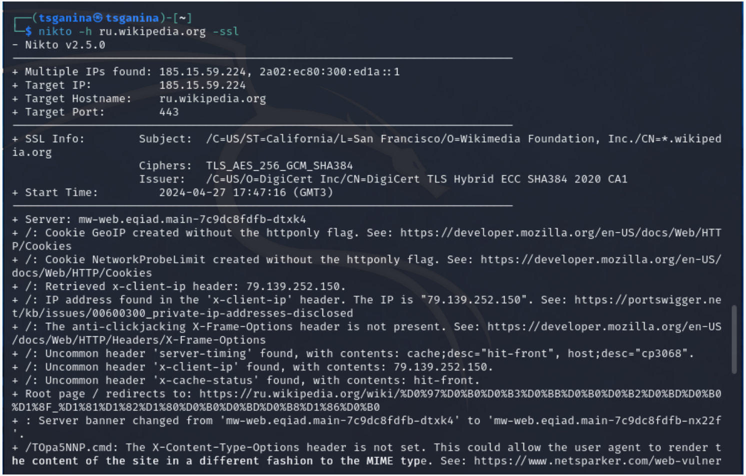
Выполнение лабораторной работы



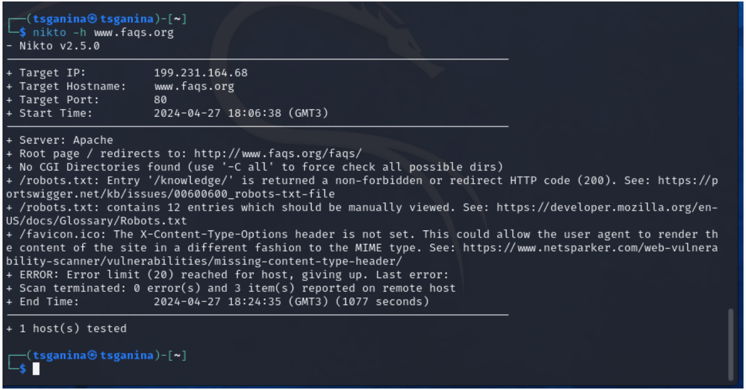
```
┌──(tsganina㉿tsganina)-[~]
└─$ sudo apt install nikto
[sudo] password for tsganina:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1514 not upgraded.

┌──(tsganina㉿tsganina)-[~]
└─$ nikto -Help

   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.con
f)
       -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 errors
       -evasion+          Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
```



```
┌──(tsganina㉿tsganina)-[~]
└─$ nikto -h ru.wikipedia.org -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 185.15.59.224, 2a02:ec80:300:ed1a::1
+ Target IP:          185.15.59.224
+ Target Hostname:    ru.wikipedia.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=Wikimedia Foundation, Inc./CN=*.wikiped
ia.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
+ Start Time:         2024-04-27 17:47:16 (GMT3)
---------------------------------------------------------------------------
+ Server: mw-web.eqiad.main-7c9dc8fdfb-dtxk4
+ /: Cookie GeoIP created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTT
P/Cookies
+ /: Cookie NetworkProbeLimit created without the httponly flag. See: https://developer.mozilla.org/en-US/
docs/Web/HTTP/Cookies
+ /: Retrieved x-client-ip header: 79.139.252.150.
+ /: IP address found in the 'x-client-ip' header. The IP is "79.139.252.150". See: https://portswigger.ne
t/kb/issues/00600300_private-ip-addresses-disclosed
+ /: 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 'server-timing' found, with contents: cache;desc="hit-front", host;desc="cp3068".
+ /: Uncommon header 'x-client-ip' found, with contents: 79.139.252.150.
+ /: Uncommon header 'x-cache-status' found, with contents: hit-front.
+ Root page / redirects to: https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0
%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0
+ : Server banner changed from 'mw-web.eqiad.main-7c9dc8fdfb-dtxk4' to 'mw-web.eqiad.main-7c9dc8fdfb-nx22f
'.
+ /TOpa5NNP.cmd: The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulner
```



```
┌──(tsganina㉿tsganina)-[~]
└─$ nikto -h www.faqs.org
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          199.231.164.68
+ Target Hostname:    www.faqs.org
+ Target Port:        80
+ Start Time:         2024-04-27 18:06:38 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache
+ Root page / redirects to: http://www.faqs.org/faqs/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/knowledge/' is returned a non-forbidden or redirect HTTP code (200). See: https://p
ortswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 12 entries which should be manually viewed. See: https://developer.mozilla.org/en-
US/docs/Glossary/Robots.txt
+ /favicon.ico: The X-Content-Type-Options header is not set. This could allow the user agent to render th
e content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnera
bility-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-04-27 18:24:35 (GMT3) (1077 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(tsganina㉿tsganina)-[~]
└─$ 
```

Результаты

Вывод

Я смогла протестировать несколько сайтов.