

4 этап индивидуального проекта

Основы информационной безопасности

Серёгина Ирина Андреевна

Содержание

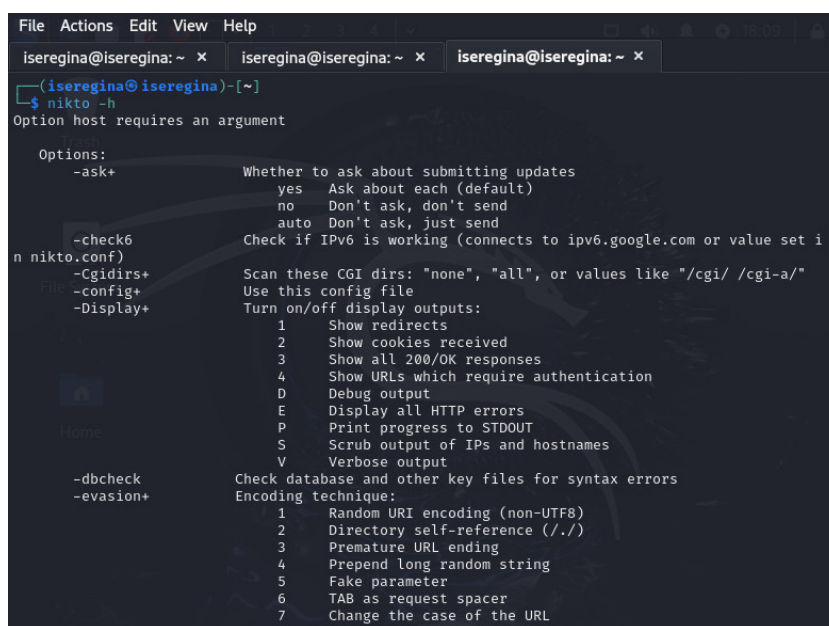
1	Цель работы	3
2	Выполнение лабораторной работы	4
3	Выводы	6
	Список литературы	7

1 Цель работы

Знакомство со сканером безопасности nikto и его применение

2 Выполнение лабораторной работы

1. Для ознакомления вывожу справку командой `nikto -h` (рис. [2.1]).



```
File Actions Edit View Help
iseregina@iseregina: ~ x iseregina@iseregina: ~ x iseregina@iseregina: ~ x
(iseregina@iseregina)-[~]
$ 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 i
n 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 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
```

Рис. 2.1: справка

2. В качестве примера применения я решила просканировать сайт мэра моск-
вы `mos.ru` с помощью команды `nikto -h mos.ru`. (рис. [2.2]).

```
File Actions Edit View Help
iseregina@iseregina: ~ x iseregina@iseregina: ~ x iseregina@iseregina: ~ x

+ 0 host(s) tested

(iseregina@iseregina)-[~]
$ nikto -h mos.ru.
- Nikto v2.5.0

+ Target IP: 94.79.51.169
+ Target Hostname: mos.ru.
+ Target Port: 80
+ Start Time: 2024-04-26 18:04:43 (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
+ /: 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://mos.ru/
+ No CGI Directories found (use '-C all' to force check all possible dirs)

-C all
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-04-26 18:09:07 (GMT3) (264 seconds)

+ 1 host(s) tested

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

Рис. 2.2: проверка веб-сайта

3 Выводы

Я ознакомилась со сканером безопасности nikto и научилась его применять.

Список литературы