4 этап индивидуального проекта

Основы информационной безопасности

Дьяконова Софья Александровна

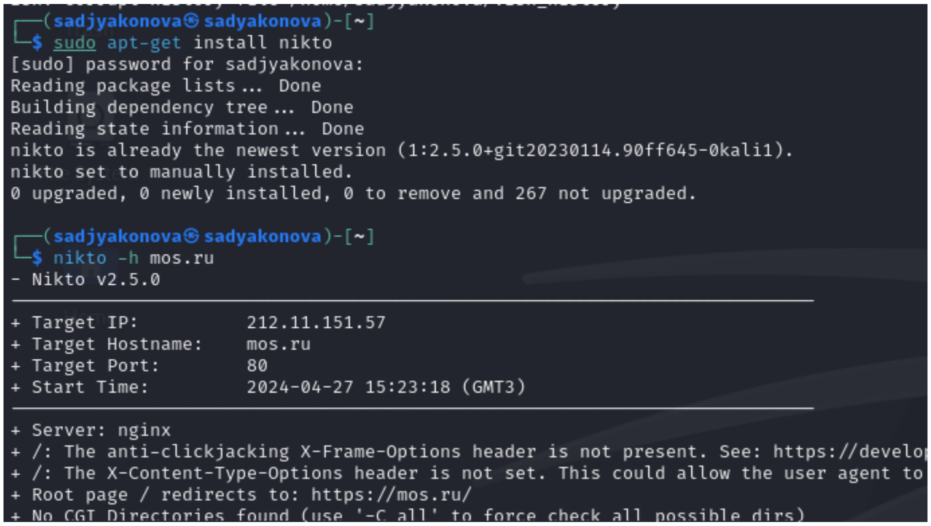
Содержание

Цель работы

Знакомство со сканером безопасности nikto и его применение

Выполнение лабораторной работы

1. Для ознакомления вывожу справку командой nikto -h (рис. [-@fig:001]).

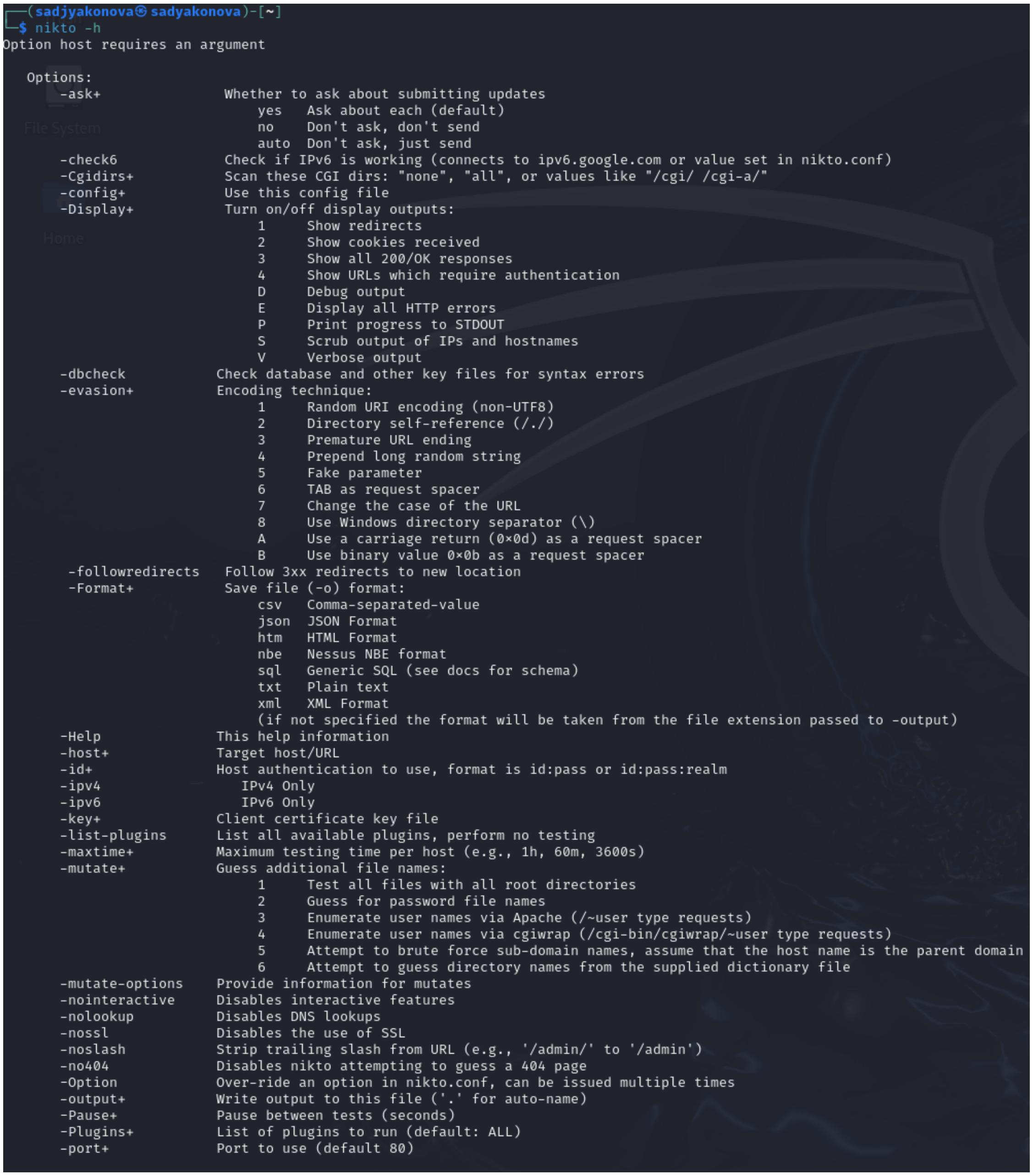


```
┌──(sadjyakonova㉿sadyakonova)-[~]
└─$ sudo apt-get install nikto
[sudo] password for sadjyakonova:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 267 not upgraded.

┌──(sadjyakonova㉿sadyakonova)-[~]
└─$ nikto -h mos.ru
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          212.11.151.57
+ Target Hostname:    mos.ru
+ Target Port:        80
+ Start Time:         2024-04-27 15:23:18 (GMT3)
---------------------------------------------------------------------------
+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develo
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to
+ Root page / redirects to: https://mos.ru/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

справка

2. В качестве примера применения я решила просканировать сайт мэра москвы mos.ru с помощью команды nikto -h mos.ru. (рис. [-@fig:002]).



```
┌──(sadjyakonova㉿sadyakonova)-[~]
└─$ 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 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 spacer
                                  B     Use binary value 0x0b as a request spacer
        -followredirects      Follow 3xx redirects to new location
        -Format+              Save file (-o) format:
                                  csv   Comma-separated-value
                                  json  JSON Format
                                  htm   HTML Format
                                  nbe   Nessus NBE 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)
       -Help                 This help information
       -host+                Target host/URL
       -id+                  Host authentication to use, format is id:pass or id:pass:realm
       -ipv4                    IPv4 Only
       -ipv6                    IPv6 Only
       -key+                 Client certificate key file
       -list-plugins         List all available plugins, perform no testing
       -maxtime+             Maximum testing time per host (e.g., 1h, 60m, 3600s)
       -mutate+              Guess additional file names:
                                  1     Test all files with all root directories
                                  2     Guess for password file names
                                  3     Enumerate user names via Apache (/~user type requests)
                                  4     Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests)
                                  5     Attempt to brute force sub-domain names, assume that the host name is the parent domain
                                  6     Attempt to guess directory names from the supplied dictionary file
       -mutate-options       Provide information for mutates
       -nointeractive        Disables interactive features
       -nolookup             Disables DNS lookups
       -nossl                Disables the use of SSL
       -noslash              Strip trailing slash from URL (e.g., '/admin/' to '/admin')
       -no404                Disables nikto attempting to guess a 404 page
       -Option               Over-ride an option in nikto.conf, can be issued multiple times
       -output+              Write output to this file ('.' for auto-name)
       -Pause+               Pause between tests (seconds)
       -Plugins+             List of plugins to run (default: ALL)
       -port+                Port to use (default 80)
```

проверка веб-сайта

Выводы

Я ознакомилась со сканером безопасности nikto и научилась его применять.

Список литературы