РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ Этап проекта №4

Тема: Использование nikto

дисциплина: Информационная безопасность

Студент: Койфман Кирилл Дмитриевич

Группа: НПИбд-01-21

Введение.

Цель работы.

Установить базовый сканер безопасности веб-сервера nikto в гостевую систему к Kali Linux и использовать его для сканирования нескольких веб-приложений.

Ход работы

Для начала, запусти виртуальную машину Kali Linux, установим сканер nikto и ознакомимся со справочной информацией (рис.1 - рис.3):

```
┌──(root㉿kdkoyjfman)-[/home/kdkoyjfman]
└─# apt -y install nikto
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 905

┌──(root㉿kdkoyjfman)-[/home/kdkoyjfman]
└─#
```

РИС.1(nikto установлен)

```
┌──(root㉿kdkoyjfman)-[/home/kdkoyjfman]
└─# 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)
```

РИС.2(справка по сканеру nikto)

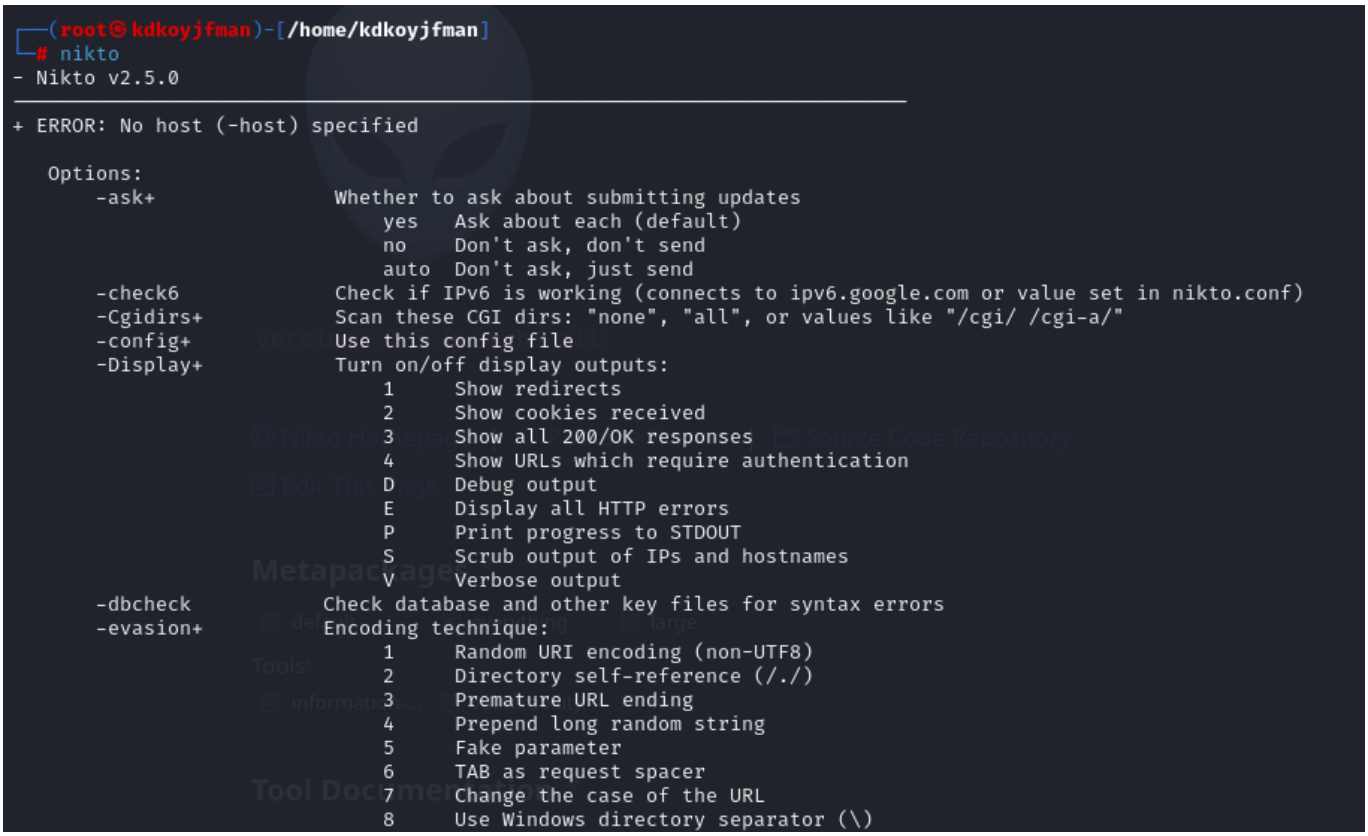

РИС.3(сканер исправен и готов к использованию)

Теперь проведём сканирование нескольких веб-приложений (рис.4 - рис.6):

РИС.4

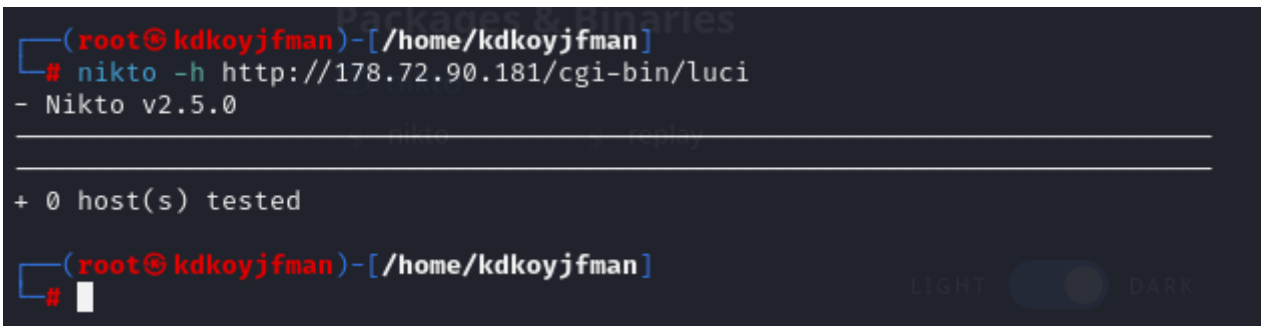

РИС.5

РИС.6

Заключение

В ходе продеданной лабораторной работы основная цель была достигнута.