

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@kdkoyjfmam)-[/home/kdkoyjfmam]
# 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@kdkoyjfmam)-[/home/kdkoyjfmam]
#
```

Рис.1(nikto установлен)

```
(root@kdkoyjfmam)-[/home/kdkoyjfmam]
# 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)

```
(root@kdkoyjfmn)~[/home/kdkoyjfmn]
# nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

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 (\)
```

Рис.3(сканер исправен и готов к использованию)

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

```
(root@kdkoyjfmn)~[/home/kdkoyjfmn]
# nikto -h https://prostoilinux.ru/
- Nikto v2.5.0

+ Target IP: 116.202.196.92
+ Target Hostname: prostoilinux.ru
+ Target Port: 443

+ SSL Info: Subject: /CN=prostoilinux.ru
            Ciphers: ECDHE-RSA-AES128-GCM-SHA256
            Issuer: /C=US/O=Let's Encrypt/CN=R11
            2024-10-05 20:19:06 (GMT3)

+ Start Time:

+ Server: nginx/1.20.2
+ /: Retrieved x-powered-by header: WP Rocket/3.15.1.
+ /: 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/mis
sing-content-type-header/
+ /wp-json/: Drupal Link header found with value: <https://prostoilinux.ru/wp-json/?; rel="https://api.w.org/". See: https://www.drupal.org/
+ /robots.txt: Entry "/foto/" is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry "/links/" is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry "/wp-content/plugins/" is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 65 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed. at /var/lib/nikto/plugins/LW2.pm line 5254.
+ at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Interrupted system call at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Interrupted system call
+ Scan terminated: 20 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-10-05 20:47:53 (GMT3) (527 seconds)

+ 1 host(s) tested
```

Рис.4

```
(root@kdkoyjfmn)~[/home/kdkoyjfmn]
# nikto -h http://178.72.90.181/cgi-bin/luci
- Nikto v2.5.0

+ 0 host(s) tested

(root@kdkoyjfmn)~[/home/kdkoyjfmn]
```

Рис.5

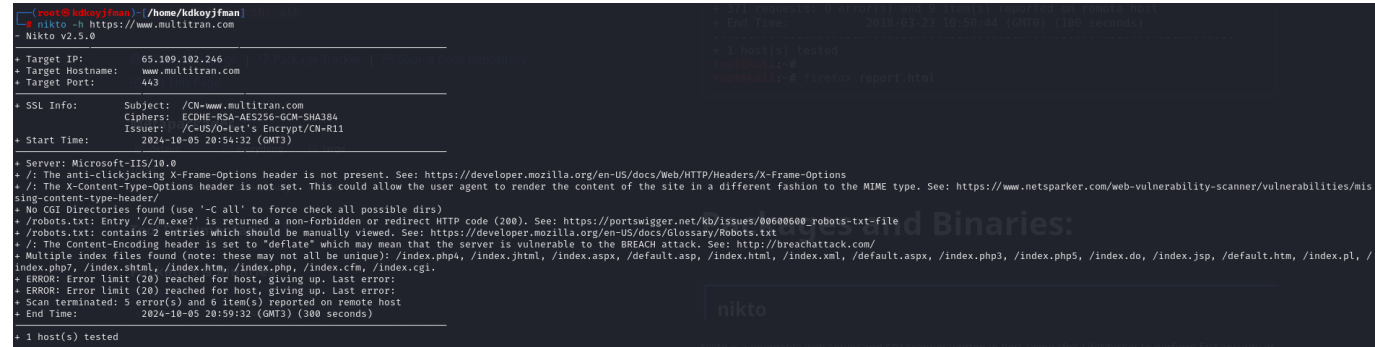


Рис.6

Закключение

В ходе проделанной лабораторной работы основная цель была достигнута.