

# Отчёт по 4 этапу индивидуального проекта

Применение программы Nikto

---

Городянский Ф.Н.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Городянский Фёдор Николаевич
- студент фФМиЕН
- Российский университет дружбы народов
- <https://yamadharma.github.io/ru/>

## Элементы презентации

---

Nikto – бесплатный (open source) сканер для поиска уязвимостей в веб-серверах. Утилита относится к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения.

Среди функций Nikto можно выделить следующие:

- поддержка SSL,
- поддержка HTTP прокси;
- создание отчетов в текстовом формате, XML, HTML, NBE или CSV;
- возможность сканирования портов;
- поиск поддоменов;
- поддержка плагинов для расширения функционала сканирования.

Изучить программу Nikto.

```
(kali㉿kali)-[~]  
└─$ sudo apt -y install nikto программа  
[sudo] password for kali:  
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 1550 not upgraded.
```

Рис. 1: Установка программы

## Проверка корректной установки.

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

Рис. 2: Проверка



```
(kali@kali)-[~]
$ nikto -h school1366.ru
- Nikto v2.5.0

+ Multiple IPs found: 31.31.198.199, 2a00:f940:2:2:1:4:0:95
+ Target IP: 31.31.198.199
+ Target Hostname: school1366.ru
+ Target Port: 80
+ Start Time: 2024-04-27 13:06:48 (GMT+4)

+ 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 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabilities/missing-content-type-header/
```

Рис. 3: Сканирование сайта

## Сканирую заданные порты сайта.

```
(kali@kali)-[~]
$ nikto -h school1366.ru -p 22,25,2096,3306
- Nikto v2.5.0

+ Multiple IPs found: 31.31.198.199, 2a00:f940:2:2:1:4:0:95
+ Multiple IPs found: 31.31.198.199, 2a00:f940:2:2:1:4:0:95
+ Multiple IPs found: 31.31.198.199, 2a00:f940:2:2:1:4:0:95
+ Multiple IPs found: 31.31.198.199, 2a00:f940:2:2:1:4:0:95

+ Target IP: 31.31.198.199
+ Target Hostname: school1366.ru
+ Target Port: 2096
+ Start Time: 2024-04-27 13:09:58 (GMT-4)

+ Server: No banner retrieved
+ /: 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://scp95.hosting.reg.ru:2096
^[[B^[[B^[[B+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-04-27 13:10:29 (GMT-4) (31 seconds)

+ 1 host(s) tested
```

Рис. 4: Сканирование портов сайта

## Сканирование информации связанной с протоколом HTTPS сайта.

```
(kali@kali)-[~]
$ nikto -h freecodecamp.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 188.114.99.233, 188.114.98.233, 2a06:98c1:3122:e000::9, 2a06:98c1:3123:e000::9
+ Target IP: 188.114.99.233
+ Target Hostname: freecodecamp.org
+ Target Port: 443

+ SSL Info: Subject: /CN=freecodecamp.org
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=Let's Encrypt/CN=E1
+ Start Time: 2024-04-27 13:11:25 (GMT-4)

+ Server: cloudflare
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: 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://www.freecodecamp.org/
```

Рис. 5: Получение информации протокола сайта

Получил навыки пользования программой-сканером Nikto.