

# Четвертый этап индивидуального проекта

Использование nikto

---

Ибатулина Д.Э.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

## Информация

---

- Ибатулина Дарья Эдуардовна
- студентка группы НКАбд-01-22
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- [deibatulina.github.io](https://github.com/deibatulina)
- <https://github.com/deibatulina>



## Вводная часть

---

Навык работы с nikto является очень важным для специалиста по информационной безопасности. К тому же, ОС Kali Linux активно используется хакерами и специалистами по информационной безопасности по всему миру для проведения хакерских атак и защиты системы.

## Цели и задачи

---

Целями работы является: получение знаний о том, для чего используется nikto, сканирование веб-сайта, поиск уязвимостей в нем.

## Основная часть

---

Nikto – это простой открытый сканер веб-серверов, который проверяет веб-сайт и сообщает о найденных уязвимостях, которые могут быть использованы для эксплойта или взлома. Кроме того, это один из наиболее широко используемых инструментов сканирования веб-сайтов на уязвимости во всей отрасли, а во многих кругах он считается отраслевым стандартом.

## Вызов справки по nikto

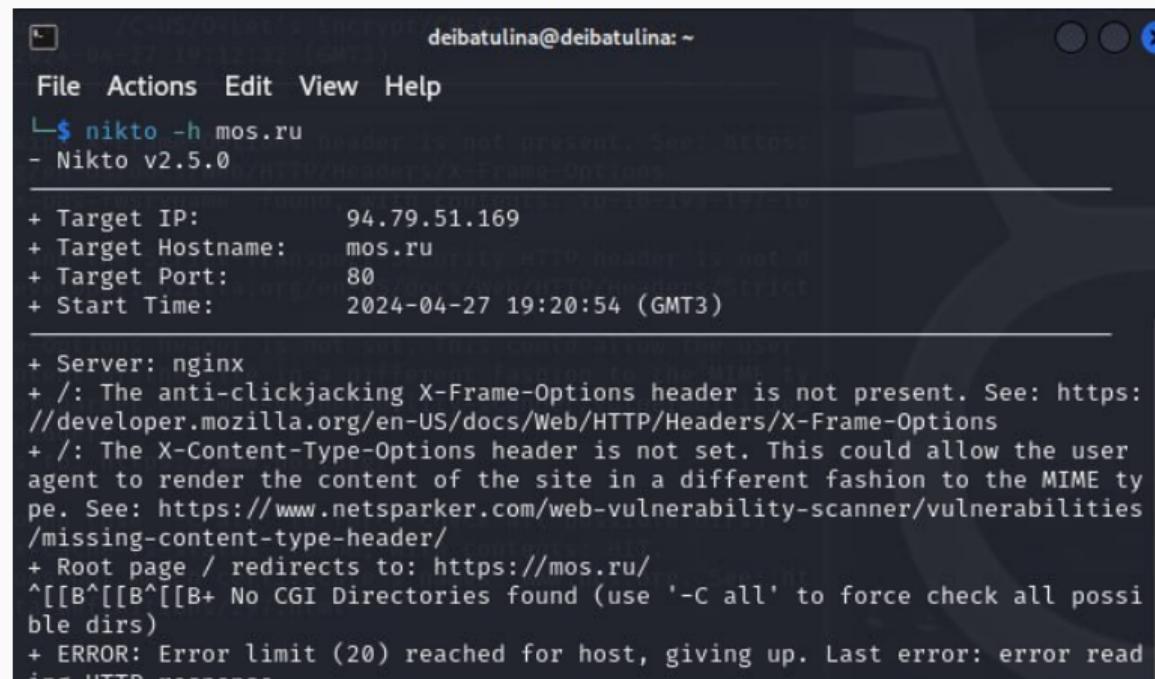
Для начала следует установить nikto. Однако, я использую дистрибутив Kali Linux, а в нем nikto уже предустановлен. Чтобы в этом убедиться, вызову справку командой `nikto -Help`:

```
[root@deibatulina] [/etc/php/8.2/apache2]
# nikto -Help

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
```

## Сканирование сайта мэра Москвы

Затем для классического сканирования сайта буду использовать базовый синтаксис nikto  
-h <IP или hostname> с фактическим IP-адресом или именем хоста без угловых скобок.  
Просканирую таким образом сайт мэра Москвы:



```
deibatulina@deibatulina: ~
File Actions Edit View Help
└$ nikto -h mos.ru
- Nikto v2.5.0

+ Target IP:          94.79.51.169
+ Target Hostname:    mos.ru
+ Target Port:        80
+ Start Time:         2024-04-27 19:20:54 (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/
^[[B^[[B^[[B+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
```

## Сканирование сайта pbs.org с SSL

Далее, сканирую сайт pbs.org с SSL командой nikto -h pbs.org -ssl:

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

+ Multiple IPs found: 54.225.206.152, 54.225.198.196
+ Target IP:          54.225.206.152
+ Target Hostname:    pbs.org
+ Target Port:        443

+ SSL Info:           Subject: /CN=www.pbs.org
                      Ciphers: ECDHE-ECDSA-AES128-GCM-SHA256
                      Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-04-27 19:26:20 (GMT3)

+ Server: openresty
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-148-58.ec2.internal.
+ /: 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
+ /: 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.pbs.org/
```

## Сканирование IP-адреса с помощью ifconfig

Теперь, когда я провела быстрое сканирование веб-сайта, можно попробовать использовать Nikto в локальной сети, чтобы найти embedded-сервера, такие как страница логина роутера или HTTP-сервис на другой машине, который представляет из себя просто сервер без веб-сайта. Чтобы узнать IP-адрес, я буду использовать ifconfig: ifconfig:

```
(deibatulina㉿deibatulina)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe77:c166 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:77:c1:66 txqueuelen 1000 (Ethernet)
            RX packets 55177 bytes 47834718 (45.6 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 27435 bytes 3971524 (3.7 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 3087 bytes 503946 (492.1 KiB)
```

## Использование IpCalc для IP-адреса

IP-адрес, который мне нужен, относится к «inet». На нем можно использовать ipcalc для того, чтобы получить сетевой диапазон. Если у ipcalc не установлен, необходимо установить его с помощью команды `apt install ipcalc`, а затем повторить попытку. Диапазон будет стоять после «Network», в моем случае это 10.0.2.15:

```
(deibatulina㉿deibatulina)-[~]
$ ipcalc 10.0.2.15
Command 'ipcalc' not found, but can be installed with:
sudo apt install ipcalc
Do you want to install it? (N/y)y
sudo apt install ipcalc
[sudo] password for deibatulina:
Sorry, try again.
[sudo] password for deibatulina:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  ipcalc
0 upgraded, 1 newly installed, 0 to remove and 267 not upgraded.
Need to get 26.3 kB of archives.
After this operation, 74.8 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ipcalc all 0.51-1 [26.3 kB]
Fetched 26.3 kB in 0s (53.3 kB/s)
Selecting previously unselected package ipcalc.
```

## Заключительная часть

---

## Результаты

---

В результате выполнения лабораторной работы я получила практические навыки работы с nikto, а также узнала, для чего он используется.