

Перезентация по индивидуальному проекту, 4 этап

Неустроева И.Н.

30 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов
- <https://inneustroeva.github.io/ru/>

Вводная часть

Цели

Приобретение практических навыков по использованию инструмента Nikto для сканирования веб-сайтов и поиска уязвимости в нем

Основная часть

Знакомство с Nikto

Перед сканированием веб-серверов использовали параметр -Help, чтобы увидеть, что можно делать с этим инструментом

```
(inneustroeva@inneustroeva)-[~]
$ 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
                   P     Print progress to STDOUT
                   S     Scrub output of IPs and hostnames
                   V     Verbose output
```


Базовое сканирование сайта

Затем используем базовый синтаксис `nikto -h` для классического сканирования сайта. Таким образом мы просканировали сайт `rudn.ru`

```
(immedstroevea@immedstroevea) [~]  
$ nikto -h rudn.ru  
- Nikto v2.5.0  
  
+ Target IP: 185.178.208.57  
+ Target Hostname: rudn.ru  
+ Target Port: 80  
+ Start Time: 2025-05-01 14:08:26 (GMT3)  
  
+ Server: ddos-guard  
+ /: 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/  
+ /: Cookie __ddg8_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: Cookie __ddg10_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: Cookie __ddg9_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: IP address found in the '__ddg9_' cookie. The IP is "46.147.148.170".
```

Сканирование сайта pbs.org

Далее сканирую сайт pbs.org с SSL “nikto -h -ssl”

```
L$ 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=E6

+ Start Time: 2025-05-01 14:12:44 (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-kids-map' found, with contents: nousername.
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-194-159.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 ty
```

Сканирование IP-адреса с помощью ifconfig

Теперь, когда мы провели 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 сервис без веб-сайта, Чтобы узнать IP-адрес, я буду использовать ifconfig

```
(inneustroeva@inneustroeva)-[~]  
$ 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:fea0:befb  prefixlen 64  scopeid 0x20<link>  
    ether 08:00:27:a0:be:fb  txqueuelen 1000  (Ethernet)  
    RX packets 11014  bytes 5898691 (5.6 MiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 8158  bytes 1212261 (1.1 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>
```

Использование IpCalc для IP-адреса

IP-адрес, который нам нужен относиться к inet. На нем мы можем использовать ipcalc. Диапазон будет стоять после Network, в нашем случае это 10.0.2.255

```
(inneustroeva@inneustroeva)-[~]
$ ipcalc 10.0.2.255
Address:    10.0.2.255          00001010.00000000.00000010. 11111111
Netmask:    255.255.255.0 = 24  11111111.11111111.11111111. 00000000
Wildcard:   0.0.0.255          00000000.00000000.00000000. 11111111
⇒
Network:    10.0.2.0/24         00001010.00000000.00000010. 00000000
HostMin:    10.0.2.1           00001010.00000000.00000010. 00000001
HostMax:    10.0.2.254         00001010.00000000.00000010. 11111110
Broadcast:  10.0.2.255         00001010.00000000.00000010. 11111111
Hosts/Net:  254                Class A, Private Internet
```

```
(inneustroeva@inneustroeva)-[~]
$ touch nullbyte.txt
```

Заключительная часть.

В ходе нашей работы, приобрела практические навыки по использованию инструмента Nikto для сканирования веб-сайтов и поиска уязвимости в нем.