

# **Индивидуальный проект**

**Этап 4. Использование nikto**

Хватов Максим Григорьевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоритическое введение</b>	<b>6</b>
<b>3</b>	<b>Выполнение этапа проекта</b>	<b>7</b>
<b>4</b>	<b>Сканирование сайта с SSL</b>	<b>8</b>
<b>5</b>	<b>Сканирование IP-адреса</b>	<b>9</b>
<b>6</b>	<b>Сканирование HTTP-сайта</b>	<b>11</b>
<b>7</b>	<b>Вывод</b>	<b>12</b>

# Список иллюстраций

4.1	Рис. 1	8
5.1	Рис. 2	9
5.2	Рис. 3	10
5.3	Рис. 4	10
6.1	Рис. 5	11

## **Список таблиц**

# 1 Цель работы

Научиться использовать nikto для сканирования сайтов на уязвимости

## 2 Теоритическое введение

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Несмотря на то, что этот инструмент чрезвычайно эффективен, он не действует скрытно. Любой сайт с системой обнаружения вторжений или иными мерами безопасности поймет, что его сканируют. Nikto был разработан для тестирования безопасности и о скрытности его работы никто не задумывался.

### 3 Выполнение этапа проекта

Сначала проверяю установку nikto командой `nikto -HELP` и получаю справку всех имеющихся команд, что говорит о наличии nikto на машине.

## 4 Сканирование сайта с SSL

Я пробую сканировать сайт pbs.org. Использую команду `nikto -h pbs.org -ssl`. Получаю результат:

```
File Actions Edit View Help
(kali@kali)~$ 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: 2024-04-22 23:36:12 (GMT-4)

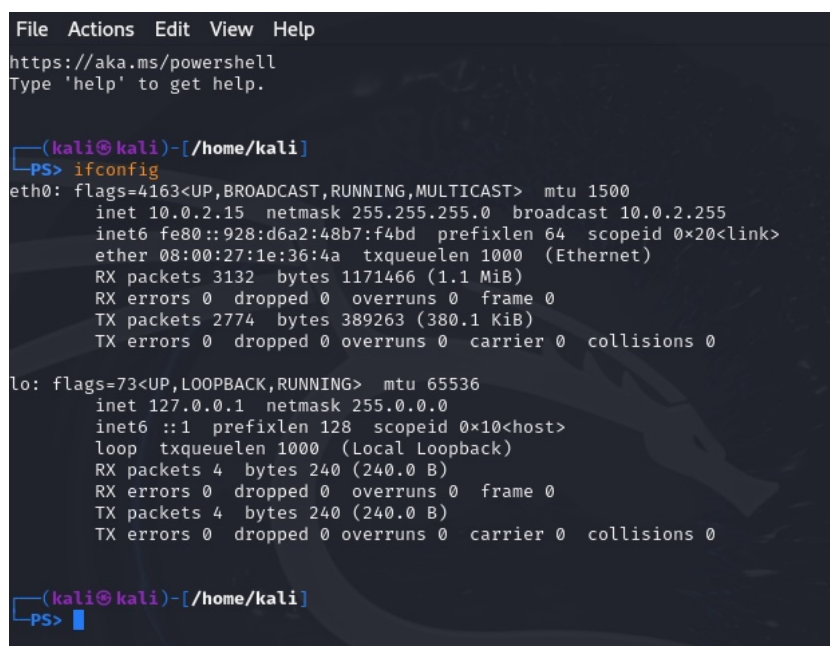
+ Server: openresty
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-148-58.ec2.internal.
+ /: The site uses TLS and the Strict-Transport-Security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

Рис. 4.1: Рис. 1



## 5 Сканирование IP-адреса

Теперь, когда мы провели быстрое сканирование веб-сайта, мы можем 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 мы будем использовать ifconfig.



```
File Actions Edit View Help
https://aka.ms/powershell
Type 'help' to get help.

(kali@kali)-[/home/kali]
PS> 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::928:d6a2:48b7:f4bd prefixlen 64 scopeid 0<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 3132 bytes 1171466 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2774 bytes 389263 (380.1 KiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[/home/kali]
PS>
```

Рис. 5.1: Рис. 2

Создаю файл targetIP.txt командой touch и просматриваю его содержимое через cat

```
File Actions Edit View Help
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package ipcalc is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Package 'ipcalc' has no installation candidate

(kali@kali)-[/home/kali]
PS> touch targetIP.txt

(kali@kali)-[/home/kali]
PS> cat ./targetIP.txt
192.168.0.1
192.168.0.2
192.168.0.4
192.168.0.5
192.168.0.11
192.168.0.24
192.168.0.31
192.168.0.48
192.168.0.60

(kali@kali)-[/home/kali]
PS> █
```

Рис. 5.2: Рис. 3

Начинаю сканировать список IP-адресов с помощью команды `nikto -h targetIP.txt` Результатов никаких не получено почему-то. Скорее всего из-за того, что не использовал `ipcalc`, а его установить нельзя.

```
(kali@kali)-[/home/kali]
PS> nikto -h ./targetIP.txt
- Nikto v2.5.0

+ 0 host(s) tested (es found (use -t all to force check all possible dirs)
Unknown header x-cache-status found, with contents: HIT.
[...]
```

Рис. 5.3: Рис. 4

## 6 Сканирование HTTP-сайта

До этого мы сканировали защищенный сайт, а теперь просканируем незащищенны, который работает на 80-м порту. Используем команду `nikto -h www.afl.com.au`. И через какое-то время получаем результат.

```
+ Multiple IPs found: 128.75.237.170, 128.75.237.128, 2a02:26f0:d0::214:fed9,  
2a02:26f0:d0::214:feb8  
+ Target IP: 128.75.237.170  
+ Target Hostname: www.afl.com.au  
+ Target Port: 80  
+ Start Time: 2024-04-22 23:45:10 (GMT-4)  


---

+ Server: AkamaiGHost  
+ /: Uncommon header 'akamai-grn' found, with contents: 0.a6ed4b80.1713843897.  
.4600e8c.  
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache;  
desc=HIT,edge; dur=1,ak_p; desc='1713843897281_2152459686_73404044_179_11698  
_4_0_-';dur=1).  
+ /: Uncommon header 'x-instart-country-code' found, with contents: RU.  
+ Root page / redirects to: https://www.afl.com.au/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: 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  
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities  
/missing-content-type-header/  
^[^A][^A][^A][^A][^A][^A][^A][^A][^A][^B][^B][^B][^B][^B][^B][^B][^B][^B]  
[[^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B][^B]  
uests: 0 error(s) and 4 item(s) reported on remote host  
+ End Time: 2024-04-22 23:48:57 (GMT-4) (227 seconds)  


---

+ 1 host(s) tested
```

Рис. 6.1: Рис. 5

## 7 Вывод

Я научился использовать nikto для сканирования защищенных и незащищенных сайтов на уязвимости, и научился также получать дополнительную информацию из nikto.