Перезнтация по индивидуальному проект, 5 этап

Неустроева И.Н.

30 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

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

Вводная часть

Цели

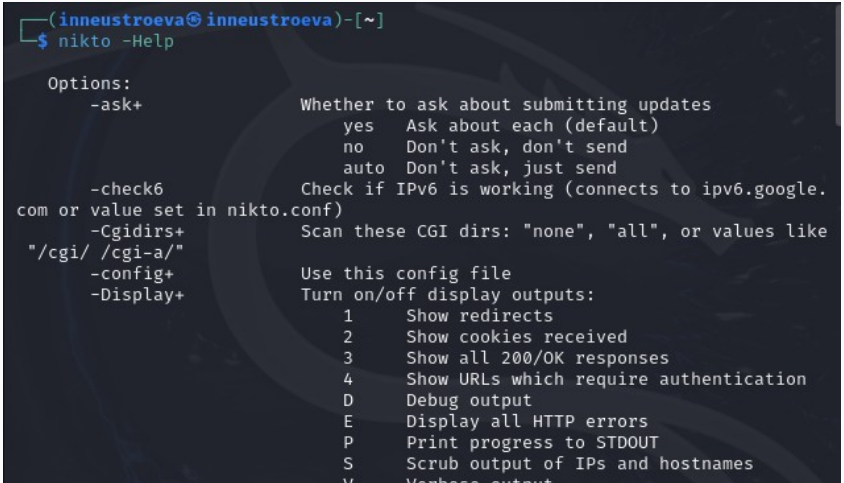
Цели

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

Основная часть

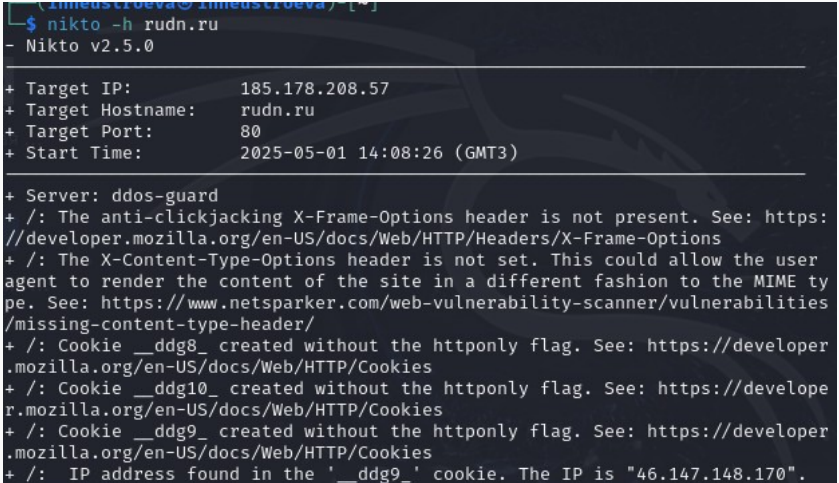
Знакомство с Nikto

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



Базовое сканирование сайта

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



Сканирование сайта pbc.org

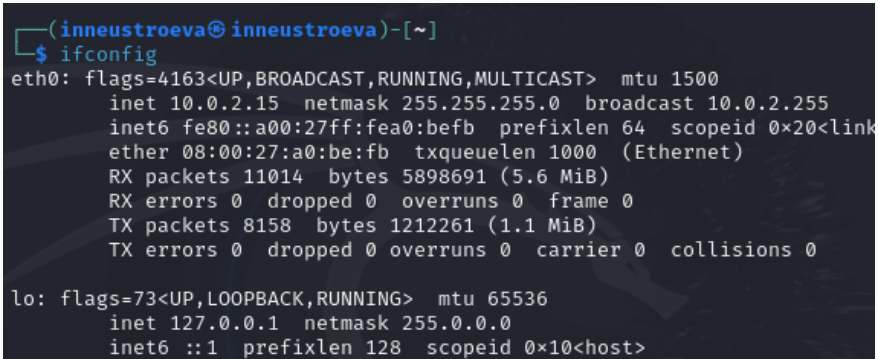
Далее сканирую сайт pbs.org с SSL “nikto -h -ssl”

```
└─$ 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-10-193-194-15
9.ec2.internal.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not d
efined. 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
```

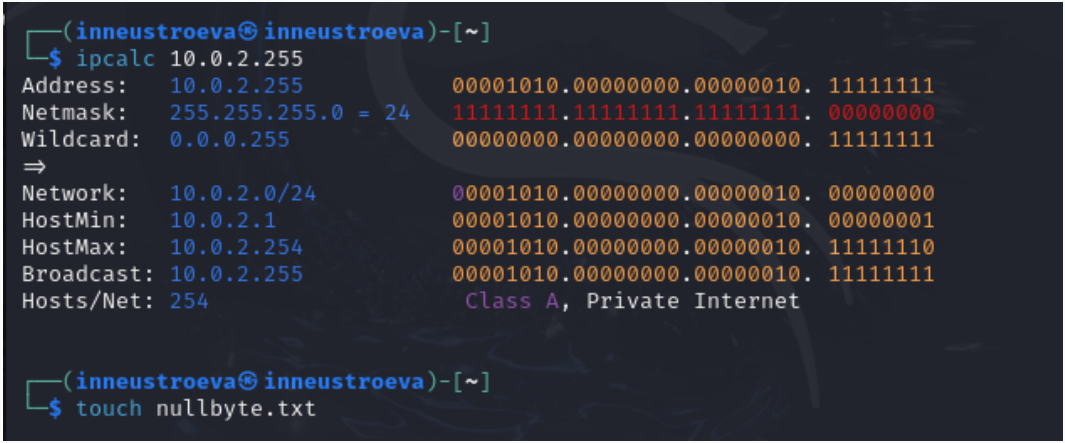
Сканирование IP-адреса с помощью ifconfig

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



Использование IpCalc для IP-адреса

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



Заключительная часть.

Результаты

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