Nikto, nuclei ? ??.

Коммерческие:

- acunetix
- netsparker
- IBM AppScan
- WebInspect

Бесплатные:

- OWASP Zap
- W3af
- arachni
- Iron Wasp
- Nexpose (совместим с MSF)
- Nessus (совместим с MSF)

Nikto

```
nikto -host 172.16.10.11 -port 80


+ Server: Apache/2.4.58 (Ubuntu)
+ /: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af, size:
63d6cf46a153e, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /backup/: Directory indexing found.
+ /backup/: This might be interesting.
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-08-30 20:12:35 (GMT8) (40 seconds)
```

Nuclei

Адрес проекта

Отправляет DNS, HTTP, сокеты. Общая база с возможностью расширения. Можно использовать для поиска данных авторизации в локальных файлах.

Основан на YAML шаблонах. Структура шаблона:

ID	Уникальный идентификатор шаблона
Metadata	Описание шаблона (автор, ...
Protocol	Протокол
Operators	Паттерны и получаемые данные

Простой шаблон:

```
id: detect-apache-welcome-page
info:
  name: Apache2 Ubuntu Default Page
  author: Dolev Farhi and Nick Aleks
  severity: info
  tags: apache
http:
  - method: GET
    path:
      - '{{BaseURL}}'
    matchers:
      - type: word
        words:
          - "Apache2 Ubuntu Default Page: It works"
        part: body
```

wmap

Сканер web уязвимостей, встроенный в MSF. Почему-то предлагается сначала создать новую базу для хранения результатов.

```
msf > workspace -a for_wmap
msf > workspace
  default
* for_wmap
```

Загружаем в MSF модуль

```
msf > load wmap
```

После этого появятся команды сканера. Команда wmap_sites управляет списком сайтов.

wmap_sites -a http://172.16.194.172	Добавить сайт для сканирования
wmap_sites -l	Список сайтов
wmap_sites -d [id]	Удаляет цели из списка по id

wmap_targets управляет endpoint сайта

Добавляем сайт для сканирования

wmap_targets -t https://172.16.194.172	Добавить endpoint для сканирования
wmap_targets -l	Список endpoint
wmap_sites -d [id]	Удаляет endpoint из списка по id

wmap_run управляет запуском сканирования

wmap_run -t	Список модулей, используемых для сканирования
wmap_run -e	Выполнить модули

wmap_vulns выводит информацию об уязвимостях.

wmap_vulns -l	Список уязвимостей

Однако в выводе сканера можно увидеть дополнительную информацию, которая не попала в данный список, например предположительную версию web сервера или сертификаты.

В таблице vulns также уязвимости.

Cariddi

Сканер endpoint. Git проекта. Сначала установить go.

Если не ограничить - сначала просматривает все страницы.

Опции	
-e	Поиск уязвимостей в endpoint -ef string Use an external file (txt, one per line) to use custom parameters for endpoints hunting.

-info	Ищет полезную информацию. Например, быстрый поиск email ip Используется самостоятельно.
-s	Hunt for secrets. -sf string Use an external file (txt, one per line) to use custom regexes for secrets hunting.
-err	Hunt for errors in websites.
-ext int	Hunt for juicy file extensions. Integer from 1(juicy) to 7(not juicy).
Настройки формата запроса	
-proxy string	Set a Proxy to be used (http and socks5 supported).
-headers string	Use custom headers for each request E.g. -headers "Cookie: auth=yes;;Client: type=2".
-headersfile string	Read from an external file custom headers (same format of headers flag).
-rua	Use a random browser user agent on every request.
-ua	Use a custom User Agent.
Настройки поиска	
-i string	Ignore the URL containing at least one of the elements of this array.
-ie value	Comma-separated list of extensions to ignore while scanning. `cat urls.txt | cariddi -ie pdf,png,jpg`
-it string	Ignore the URL containing at least one of the lines of this file.
-md int	Maximum level the crawler will follow from the initial target URL.
-intensive	Crawl searching for resources matching 2nd level domain.
Скорость работы	
-c int	Concurrency level. (default 20)
-d int	Delay between a page crawled and another.
-t int	Set timeout for the requests. (default 10)
Выходной формат	

-json	Print the output as JSON in stdout.
-oh string	Write the output into an HTML file.
-ot string	Write the output into a TXT file.
-plain	Print only the results.
Дополнительно	
-debug	Print debug information while crawling.
-examples	Print the examples.
-sr	Store HTTP responses.
-cache	Use the .cariddi_cache folder as cache.

Revision #9
Created 2 October 2025 07:18:21 by Admin
Updated 18 October 2025 12:26:47 by Admin