

Цель работы

Целью данной работы является изучение сканера уязвимостей nikto.

Введение

Nikto: Описание

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности.

Основные задачи Nikto:

- Поиск общих уязвимостей веб-серверов.
- Проверка наличия опасных файлов и конфигураций.
- Выявление устаревших версий веб-серверов и их компонентов.
- Определение серверных технологий и модулей.

Особенности:

- Поддержка множества серверов и протоколов (HTTP, HTTPS, HTTP/2 и другие).
- Возможность добавления собственных правил для обнаружения уязвимостей.
- Регулярные обновления базы данных уязвимостей.

Nikto — это пассивный сканер, и он не пытается активно взламывать систему, а только собирает информацию о потенциальных уязвимостях.

Рекомендуется использовать Nikto в сочетании с другими инструментами безопасности, такими как Nmap и OpenVAS, для более полного анализа безопасности веб-сервера.

Полезные параметры и примеры

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе.

Сканирование веб-сервера

```
perl nikto.pl -h <URL>
```

Сканирование определенного порта

```
perl nikto.pl -h <URL> -p <port>
```

Вывод результатов в файл

```
perl nikto.pl -h <URL> -o output.txt
```

Дополнительные аргументы:

- -ssl — принудительное использование SSL (HTTPS).
- -no_ssl — игнорирование SSL-сертификатов.
- -Tuning — настройка интенсивности сканирования (например, отключение проверки директорий).
- -Plugins — выбор определенных плагинов для сканирования.
- -timeout — установка таймаута для запросов.

Выполнение работы

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию.

Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

```
perl nikto.pl -h http://localhost/dvwa/
```

Сканирование localhost

```

└─$ nikto -h localhost
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:     2024-10-02 12:02:39 (GMT3)

+ Server: Apache/2.4.59 (Debian)
+ /: 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: 29cd, size: 621d5e43cc127, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:      2024-10-02 12:02:58 (GMT3) (19 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.59) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

```

#fig

Сканирование localhost/dvwa/

```

└─$ nikto -h localhost -root /dvwa
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Target Path:    /dvwa
+ Start Time:     2024-10-02 12:03:36 (GMT3)

+ Server: Apache/2.4.59 (Debian)
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: 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)
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2024-10-02 12:03:57 (GMT3) (21 seconds)

+ 1 host(s) tested

```

#fig

Вывод

Мы изучили возможности сканера nikto.