

Индивидуальный проект - этап 4

Алёна Лебедева¹

2 октября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение сканера уязвимостей nikto.

Процесс выполнения лабораторной работы

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.

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

Сканирование веб-сервера

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

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

```
user@kali:~$ sudo nikto -h localhost
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-02 11:52:39 (GMT+3)

+ Server: Apache/2.4.29 (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.wisecoders.com/web-vulnerabilities-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ / : Server may leak inode via flag, header found with file /, inode: 294, size: 621614112, mtime: gfp. See: http://cve.mitre.org/cgi-bin/cvesum.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: CVE-2018-161
+ 7456 requests: 8 error(s) and 1 item(s) reported on remote host
+ End Time: 2024-10-02 11:52:39 (GMT+3) (29 seconds)

+ 1 host(s) tested
```

Figure 1: Тестирование localhost

Сканирование localhost/dvwa/

```
root@kali:~# nmap -sS -p 80 -u http://localhost/dvwa/
Nmap 2.8.0

```

Host	IP Address	OS	Service	Version	Device Type	OS Class	OS CPE	Service CPE
10.10.10.10	10.10.10.10	Linux 3.2-5.8	Apache/2.4.18 (Ubuntu)	2.4.18	Web Server	Linux 3.2-5.8	cpe:/o:linux:3.2-5.8	cpe:/a:apache:2.4.18

```

# Host: 10.10.10.10
# OS: Linux 3.2-5.8
# Service: Apache/2.4.18 (Ubuntu)
# Version: 2.4.18
# Device Type: Web Server
# OS Class: Linux 3.2-5.8
# OS CPE: cpe:/o:linux:3.2-5.8
# Service CPE: cpe:/a:apache:2.4.18
# X-Content-Type-Options: not set
# X-Frame-Options: not set
# X-XSS-Protection: 1; mode=block
# Warnings: 0
# Errors: 0
# Hosts: 1
# Targets: 1
# Total: 1
# Time: 0.00s
# Exit: 0
```

Figure 2: Тестирование localhost/dvwa/

Выводы по проделанной работе

Мы изучили возможности сканера nikto.