

Индивидуальный проект - этап 4

1

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

```
--(root@kali:~/kali)~
~$ nikt -u localhost
~ Nikto 2.3.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-02 20:06:56 (GMT)

+ Server: Apache/2.4.18 (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 paths via ETags, header found with file /: inode 260d, size: 621094kcc127, mime: gzIp, See http://cve.mitre.org/cgi-bin/cvesame.cgi?name=CVE-2000-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-161
+ 2000 requests: 8 error(s) and 5 (0.0%) responses on remote host
+ End Time: 2024-10-02 20:07:11 (GMT) (17 seconds)

+ 1 host(s) tested
```

Figure 1: Тестирование localhost

Сканирование localhost/dvwa/

```
root@kali:~/# nmap -sS -p 80 localhost --script vuln
Nmap v2.8.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Target Path: /dvwa
+ Start Time: 2024-10-02 20:07:48 (GMT+3)

+ Server: Apache/2.4.18 (Ubuntu)
+ /dvwa/: The 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.wisecoders.com/web-vulnerability-scanner/vulnerabilities/mislog-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP methods: GET, POST, OPTIONS, HEAD
+ 7600 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-10-02 20:07:58 (GMT+3) (10 seconds)

+ 1 host(s) tested
```

Figure 2: Тестирование localhost/dvwa/

Выводы по проделанной работе

Мы изучили возможности сканера nikto.