

Индивидуальный проект

Этап 4

Кармацкий Н. С. Группа НФИбд-01-21

3 Октября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Научиться тестированию веб-приложений с помощью сканера nikto

Задание

1. Использование nikto.

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку nikto построен исключительно на LibWhisker2, он сразу после установки поддерживает кросс-платформенное развертывание, SSL (криптографический протокол, который подразумевает более безопасную связь), методы аутентификации хоста (NTLM/Basic), прокси и несколько методов уклонения от идентификаторов. Он также поддерживает перечисление поддоменов, проверку безопасности приложений (XSS, SQL-инъекции и т. д.) и способен с помощью атаки паролей на основе словаря угадывать учетные данные авторизации.

Для запуска сканера nikto введите в командную строку терминала команду: #
nikto

Выполнение лабораторной работы

Сервер apache

Для работы с nikto, необходимо подготовить веб приложение, которое будем сканировать. В нашем случае это DVWA. Проверим, что сервер apache запущен (рис. 1).

```
(nskarmatskiy㉿kali)-[~]
$ sudo systemctl status apache2
[sudo] password for nskarmatskiy:
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: )
   Active: active (running) since Thu 2024-10-03 12:08:38 MSK; 2h 58min left
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1000 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU
 Main PID: 1111 (apache2)
    Tasks: 7 (limit: 2134)
   Memory: 5.0M (peak: 22.5M swap: 10.2M swap peak: 10.2M)
      CPU: 69ms
     CPU: 69ms
CGroup: /system.slice/apache2.service
        ├─1111 /usr/sbin/apache2 -k start
        ├─1113 /usr/sbin/apache2 -k start
        ├─1114 /usr/sbin/apache2 -k start
        ├─1115 /usr/sbin/apache2 -k start
        ├─1116 /usr/sbin/apache2 -k start
        ├─1117 /usr/sbin/apache2 -k start
        └─1118 /usr/sbin/apache2 -k start

Oct 03 12:08:38 kali systemd[1]: Starting apache2.service - The Apache HTTP Ser
Oct 03 12:08:38 kali apachectl[1036]: AH00558: apache2: Could not reliably dete
Oct 03 12:08:38 kali systemd[1]: Started apache2.service - The Apache HTTP Serv
```

Рис. 1: Сервер apache2

Заходим на наше веб-приложение и в режиме выбора уровня безопасности, ставим минимальный (рис. 2).

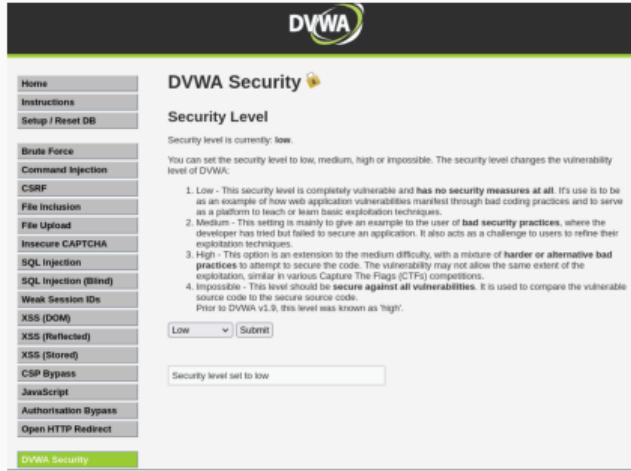


Рис. 2: Изменение уровня безопасности

Запуск nikto

Запускаем nikto (рис. 3).

```
[└(nskarmatskiy㉿kali)-[~]
└$ #nikto
```

Рис. 3: Запуск nikto

Запрос через url

Проверить веб-приложение можно, введя его полный URL и не вводя порт (рис. 4).

```
(makarowskij@kali)-[~]
└─$ nikto -h http://127.0.0.1/DVVA/
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:    2024-10-03 09:11:35 (GMT3)

-----  

+ Server: Apache/2.4.59 (Debian)
+ /DVVA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVVA/: 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: GET, POST, OPTIONS, HEAD
+ /DVVA//etc/passwd: The server is still allowing to read any system file by adding an extra '/' to the URL.
+ /DVVA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/wp-includes/Requests/Utility/content-post.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/wp-includes/Requests/Utility/content-post.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/wp-includes/js/tinymce/themes/modern/Muhy.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/wordpress/wp-includes/js/tinymce/themes/modern/Muhy.php?filesrc/etc/hosts: A PHP backdoor file manager was found.
+ /DVVA/assets/mobirise/css/meta.php?filesrc: A PHP backdoor file manager was found.
+ /DVVA/login.cgi?c1=aaa32aa327cat20/etc/hosts: Some D-Link router remote command execution.
+ /DVVA/shell7cat/etc/hosts: A backdoor was identified.
+ 8073 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:        2024-10-03 09:11:40 (GMT3) (5 seconds)

-----  

+ 1 host(s) tested
```

Рис. 4: Сканирование через url

Запрос через адрес хоста и адрес порта

Затем попробовала просканировать введя адрес хоста и адрес порта, результаты незначительно отличаются (рис. 5).

```
[mskarmatskiy@kali:]-[~]
└─$ nikto -h 127.0.0.1 -p 80
  Nikto v2.5.0

-----[REDACTED]-----
+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:    2024-10-03 09:13:22 (GMT3)

-----[REDACTED]-----
+ 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: 621d8ffff9c642, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ //etc/host: The server install allows reading of any system file by adding an extra '/' to the URL.
+ //server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-361
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Media.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Media.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobile/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /top.cgi?l1=ad2ba007ca730/etc/hosts: Some D-Link router remote command execution.
+ /jshell?cat=/etc/hosts: A backdoor was identified.
80% requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:    2024-10-03 09:13:27 (GMT3) (5 seconds)

-----[REDACTED]-----
+ 1 host(s) tested
```

Рис. 5: Сканирование через адрес хоста и порт

Анализ результатов сканирования 1

Кроме адреса хоста и порта веб-приложения, никто выводит информацию о различных уязвимостях приложения:

Разбор вывода сканирования Nikto:

nikto -h 125.0.0.1 -p 80: Эта команда инициирует сканирование Nikto против локального веб-сервера (IP-адрес 125.0.0.1) на порту 80, который является стандартным портом для HTTP.

Анализ результатов сканирования 2

- Nikto v2.5.0: Указывает версию инструмента Nikto, используемую для сканирования.
- Target IP: 125.0.0.1: Показывает IP-адрес целевого объекта, который сканируется.
- Target Hostname: 125.0.0.1: Отображает имя хоста целевого объекта, которое в данном случае также является адресом обратной связи.
- Target Port: 80: Указывает, что сканирование проводится на порту 80.
- Start Time: 2024-10-03 09:13:22 (GMT3): Записывает время начала сканирования в часовой зоне GMT+3.
- Server: Apache/2.4.59 (Debian): Определяет программное обеспечение веб-сервера и его версию, работающую на целевом объекте, в данном случае это Apache версии 2.4.59 на операционной системе Debian.

Найдены уязвимости:

- /: The anti-clickjacking X-Frame-Options header is not present.: Указывает на отсутствие заголовка X-Frame-Options, который помогает предотвратить атаки clickjacking.
- /: The X-Content-Type-Options header is not set.: Это предупреждение означает, что заголовок X-Content-Type-Options не настроен, что может позволить браузерам интерпретировать файлы неожиданным образом.

- No CGI Directories found (use '-C all' to force check all possible dirs):
Указывает на то, что во время сканирования не были обнаружены директории CGI; использование -C all может помочь найти их, если они существуют.
- /: Server may leak inodes via ETags...: Предупреждает о том, что используются ETags, которые могут привести к утечке информации о инодах файлов и их размерах, потенциально раскрывая структуру сервера или детали файловой системы.

Выводы

Научились тестированию веб-приложений с помощью сканера nikto