

Отчет по 4 этапу индивидуального проекта

Основы информационной безопасности

Чванова Ангелина Дмитриевна, НПИбд02-21

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Выполнение лабораторной работы	9
Анализ результатов сканирования	11
Выводы	15
Список литературы	16

Список иллюстраций

1	Запуск apache2	9
2	Запуск DVWA	10
3	Запуск nikto	10
4	Проверка веб-приложения	11
5	Сканирование	11

Список таблиц

Цель работы

Изучение сканера nikto и методов тестирования веб-приложений с помощью сканера nikto

Задание

Использование nikto.

Теоретическое введение

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*

По умолчанию, как ранее было показано в других приложениях, при обычном запуске команды отображаются различные доступные параметры. Для сканирования цели введите *nikto -h <цель> -p <порт>*, где — домен или IP-адрес целевого сайта, а — порт, на котором запущен сервис

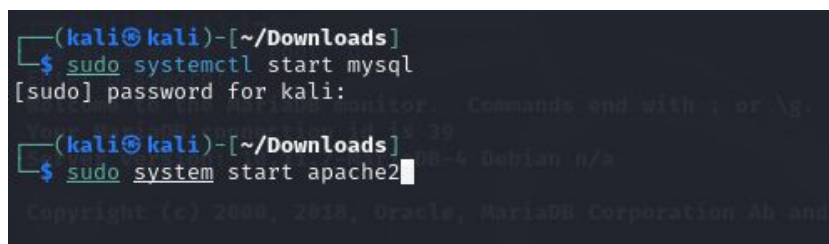
Сканер *nikto* позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения. В дополнение к показанному ранее основному сканированию *nikto* позволяет испытателю на проникновение настроить сканирование конкретной цели. Рассмотрим параметры, которые следует использовать при сканировании. - Указав переключатель командной строки -T с отдельными номерами тестов, можно настроить тестирование конкретных

типов. - Используя при тестировании параметр -t, вы можете установить значение тайм-аута для каждого ответа. - Параметр -D V управляет выводом на экран. - Параметры -o и -F отвечают за выбор формата отчета сканирования.

Существуют и другие параметры, такие как -mutate (угадывать поддомены, файлы, каталоги и имена пользователей), -evasion (обходить фильтр идентификаторов) и -Single (для одиночного тестового режима), которые можно использовать для углубленной оценки цели.

Выполнение лабораторной работы

Для того чтобы работать с nikto, нужно подготовить веб-приложение, которое будем сканировать. В нашем случае было выбрано DVWA, для этого запускаем apache2 (рис. [-@fig:001]).



```
(kali㉿kali)~[~/Downloads]
$ sudo systemctl start mysql
[sudo] password for kali:
(kali㉿kali)~[~/Downloads]
$ sudo system start apache2
```

Рис. 1: Запуск apache2

В адресной строке браузера вводим адрес DVWA, переходим в режим выбора уровня безопасности, ставим минимальный (nikto при обычном сканировании для режима impossible и low выдаст одинаковые потенциальные уязвимости, так как все уязвимости остаются, но изменяется сложность, с которой их можно использовать) (рис. [-@fig:002]).

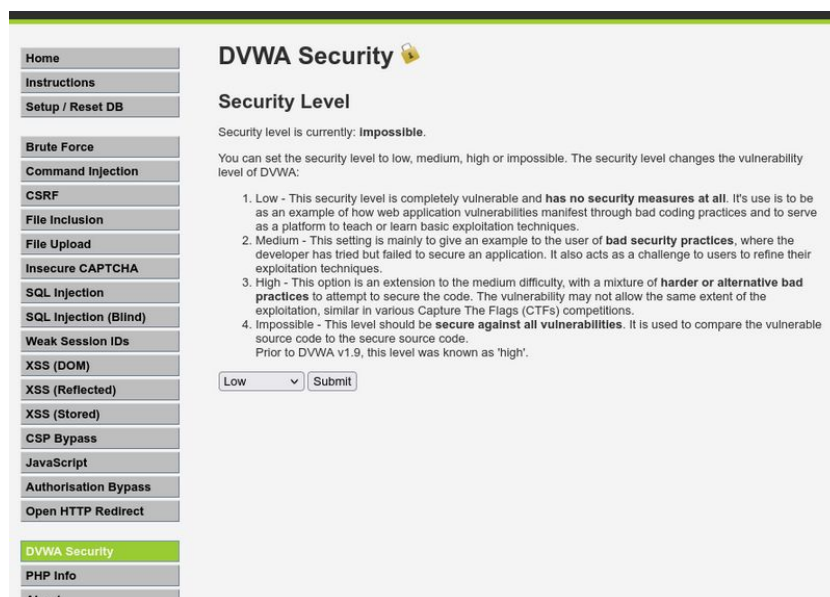


Рис. 2: Запуск DVWA

Запускаем nikto (рис. [-@fig:003]).

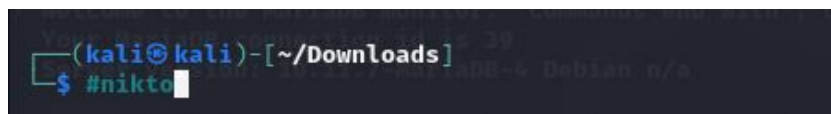


Рис. 3: Запуск nikto

Проверяем веб-приложение, введя его полный URL и не вводя порт (рис. [-@fig:004]).

```
→ nikto -h http://127.0.0.1/DVWA/
Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-04-27 17:34:23 (GMT3)

+ Server: Apache/2.4.58 (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/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /DVWA//etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/.git/index: Git Index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.
+ /DVWA/.gitignore: gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=aa20aa2cat20/etc/hosts: Some D-Link router remote command execution.
+ /DVWA/shellcat/etc/hosts: A backdoor was identified.
+ /DVWA/.dockerignore: dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time:     2024-04-27 17:35:22 (GMT3) (59 seconds)
```

Рис. 4: Проверка веб-приложения

Затем сканируем, введя адрес хоста и адрес порта, результаты отличаются незначительно (рис. [-@fig:005]).

```
Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-04-27 17:38:08 (GMT3)

+ Server: Apache/2.4.58 (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 indices via IfRange header found with file /. Size: 20cd, size: 6126a555d59f, mime: gzip. See: http://cve.nist.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /server-status: This reveals sensitive information. Consider not exposing this to the Apache conf file or restrict access to allowed sources. See: OGN08-361
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /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.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa20aa2cat20/etc/hosts: Some D-Link router remote command execution.
+ /shellcat/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:     2024-04-27 17:38:08 (GMT3) (60 seconds)
```

Рис. 5: Сканирование

Анализ результатов сканирования

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

Сервер: Apache/2.4.58 (Debian) + /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. Смотрите: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

- /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить

пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа. Смотрите: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

- Корневая страница /DVWA перенаправляет на: login.php
- Каталоги CGI не найдены (используйте '-C all', чтобы принудительно проверить все возможные каталоги)
- ОПЦИИ: Разрешенные HTTP-методы: GET, POST, OPTIONS, HEAD .
- /DVWA///etc/hosts: Установка сервера позволяет считывать любой системный файл, добавляя дополнительный "/" к URL-адресу.
- /DVWA/config/: Найдена индексация каталога.
- /DVWA/config/: Информация о конфигурации может быть доступна удаленно.
- /DVWA/tests/: Найдена индексация каталога.
- /DVWA/tests/: Это может быть интересно.
- /DVWA/database/: Найдена индексация каталога.
- /DVWA/база данных/: Найден каталог базы данных.
- /DVWA/документы/: Найдена индексация каталога.
- /DVWA/login.php: Найдена страница входа администратора/раздел.
- /DVWA/.git/index: Индексный файл Git может содержать информацию о списке каталогов.
- /DVWA/.git/HEAD: Найден файл Git HEAD. Может содержаться полная информация о репозитории.
- /DVWA/.git/config: Найден конфигурационный файл Git. Может содержаться информация о деталях репозитория.

- /DVWA/.gitignore: найден файл .gitignore. Можно разобраться в структуре каталогов.
- /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP.
- /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP.
- /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP.
- /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP.
- /DVWA/wp-включает в себя/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: Найден файловый менеджер бэкдора PHP.
- /DVWA/wordpress/wp-включает в себя/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: Найден файловый менеджер бэкдора на PHP.
- /DVWA/assets/mobirise/css/meta.php?filesrc=: Найден файловый менеджер бэкдора на PHP.
- /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Удаленное выполнение какой-либо команды маршрутизатором D-Link.
- /DVWA/shell?cat+/etc/hosts: Обнаружен черный ход.
- /DVWA/.dockerignore: найден файл .dockerignore. Возможно, удастся разобраться в структуре каталогов и узнать больше о сайте.

Бэкдор, тайный вход (от англ. back door — «чёрный ход», «лазейка», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

Также в результатах `nikto` отображает код OSVDB 561 и дает ссылку на CVE-2003-1418. OSVDB — это аббревиатура базы данных уязвимостей с открытым исходным кодом.

CVE-2003-1418 — это уязвимость в Apache HTTP Server 1.3.22–1.3.27 на OpenBSD, которая позволяет удалённым злоумышленникам получать конфиденциальную информацию через:

- Заголовок ETag, который раскрывает номер `inode`.
- Многочастную границу MIME, которая раскрывает идентификаторы дочерних процессов (PID).

В настоящее время эта проблема имеет среднюю степень тяжести.

Выводы

В рамках выполнения этапа индивидуального проекта был изучен и использован сканер nikto для тестирования веб-приложений

Список литературы

[1] Документация по Virtual Box: <https://www.virtualbox.org/wiki/Documentation>