

Индивидуальный проект - этап 4

Использование nikto

Сморчков Дмитрий

Содержание

1	Цель работы	4
2	Введение	5
2.1	Nikto: Описание	5
2.2	Полезные параметры и примеры	6
3	Выполнение лабораторной работы	7
3.1	Сканирование localhost	7
3.2	Сканирование localhost/dvwa/	9
4	Вывод	11

List of Figures

3.1	Тестирование localhost	7
3.2	Тестирование localhost/dvwa/	9

1 Цель работы

Целью данной работы является изучение сканера уязвимостей nikto.

2 Введение

2.1 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.

2.2 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.

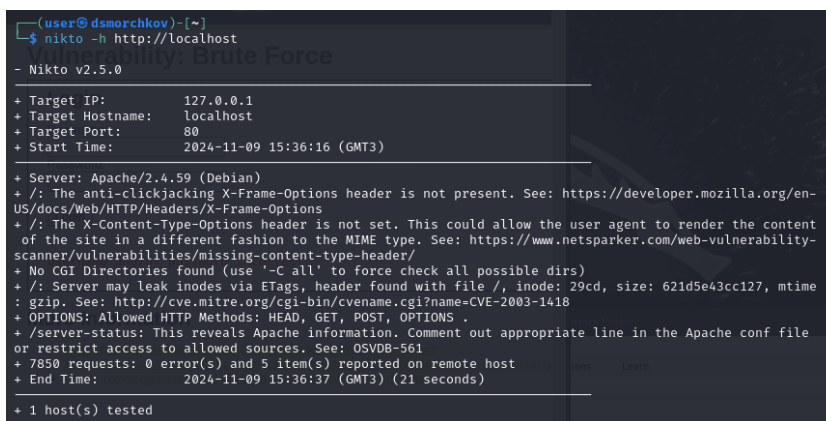
3 Выполнение лабораторной работы

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/
```

3.1 Сканирование localhost



```
(user@dsrnorkov)-[~]
$ nikto -h http://localhost

- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-11-09 15:36:16 (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: 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: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2024-11-09 15:36:37 (GMT3) (21 seconds)

+ 1 host(s) tested
```

Figure 3.1: Тестирование localhost

Отчет сканирования:

- IP-адрес цели: 127.0.0.1
- Имя хоста: localhost

- Порт: 80
- Путь: /dvwa
- Сервер: Apache/2.4.59 (Debian)
- Количество запросов: 7849
- Ошибок: 0
- Количество обнаруженных проблем: 3

Детализация обнаруженных проблем:

- Отсутствие заголовка X-Frame-Options: На странице / отсутствует заголовок X-Frame-Options. Это делает сайт уязвимым к атакам Clickjacking, позволяющим злоумышленникам внедрять сайт в iframe на другой странице.
- Отсутствие заголовка X-Content-Type-Options: На странице / отсутствует заголовок X-Content-Type-Options. Это может позволить браузеру отображать содержимое не в соответствии с его MIME-типом, что повышает риск XSS-атак.
- Утечка inode через заголовок ETag: Сервер может утекать идентификаторы inode через заголовки ETag. Это может быть использовано для определения версий файлов и атак типа кэш-поиска.
- Разрешенные HTTP-методы: Разрешены HTTP-методы OPTIONS, HEAD, GET, POST. Хотя эти методы могут быть необходимы для работы сайта, их наличие открывает возможность для злоумышленников собирать информацию о поддерживаемых сервером методах.
- Открытый доступ к /server-status: Путь /server-status открыт для всех, что раскрывает информацию о сервере Apache (включая информацию о процессах и клиентах).

3.2 Сканирование localhost/dvwa/

```
(user@dsorchkov)~$ nikto -h http://localhost/DVWA
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-11-09 15:37:41 (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/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/login.php: Admin login page/section 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/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2024-11-09 15:38:03 (GMT3) (22 seconds)

+ 1 host(s) tested
```

Figure 3.2: Тестирование localhost/dvwa/

Отчет сканирования:

- IP-адрес цели: 127.0.0.1
- Имя хоста: localhost
- Порт: 80
- Путь: /dvwa
- Сервер: Apache/2.4.59 (Debian)
- Количество запросов: 7849
- Ошибок: 0
- Количество обнаруженных проблем: 3

Детализация обнаруженных проблем:

- Отсутствие заголовка X-Frame-Options: На странице /dvwa/ отсутствует заголовок X-Frame-Options. Это позволяет злоумышленникам внедрять сайт в iframe на других сайтах, что может привести к атакам Clickjacking.
- Отсутствие заголовка X-Content-Type-Options: На странице /dvwa/ отсутствует заголовок X-Content-Type-Options. Это может позволить браузеру обработать файл не в соответствии с его MIME-типом, что может привести к неправильной интерпретации содержимого.
- Разрешенные HTTP-методы: Разрешены методы OPTIONS, HEAD, GET, POST. Хотя сами по себе эти методы не уязвимы, наличие метода OPTIONS может предоставить злоумышленникам дополнительную информацию о поддерживаемых сервером HTTP-методах.

4 Вывод

Мы изучили возможности сканера nikto.