

Этап 4

Nikto

Хамдамова Айжана Нфибд-04-22

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	13

Список иллюстраций

Список таблиц

1 Цель работы

Работа с nikto.

2 Теоретическое введение

Nikto – это сканер с открытым исходным кодом (GPL) для веб-серверов, он выполняет комплексные тесты в отношении серверов по нескольким направлениям, включая более 6700 потенциально опасных файлов/программ, проверка на устаревшие версии более 1250 серверов и проблемы, специфичные для версий более чем 270 серверов. Сканер также проверяет элементы конфигурации сервера, такие как присутствие нескольких индексных файлов, серверные опции HTTP и пытается определить имя и версии веб-сервера и программного обеспечения.

На официальном сайте изменения замерли на 2.1.5 версии аж в 2012 году. Тем не менее, под руководством автора проект живёт на GitHub'е, пользователи регулярно добавляют в базу данных и плагины изменения для сканирования новых уязвимостей, новых версий и т.д.

Nikto не создавался быть незаметным. Он будет тестировать веб-сервер за самое быстрое возможное время, очевидно, что его активность попадёт в логи веб-сервера и в поле зрения IPS/IDS (систем обнаружения/предотвращения вторжений). Тем не менее, имеется поддержка для анти-IDS методов из LibWhisker – на случай, если вы захотите их попробовать (или протестировать вашу систему IDS).

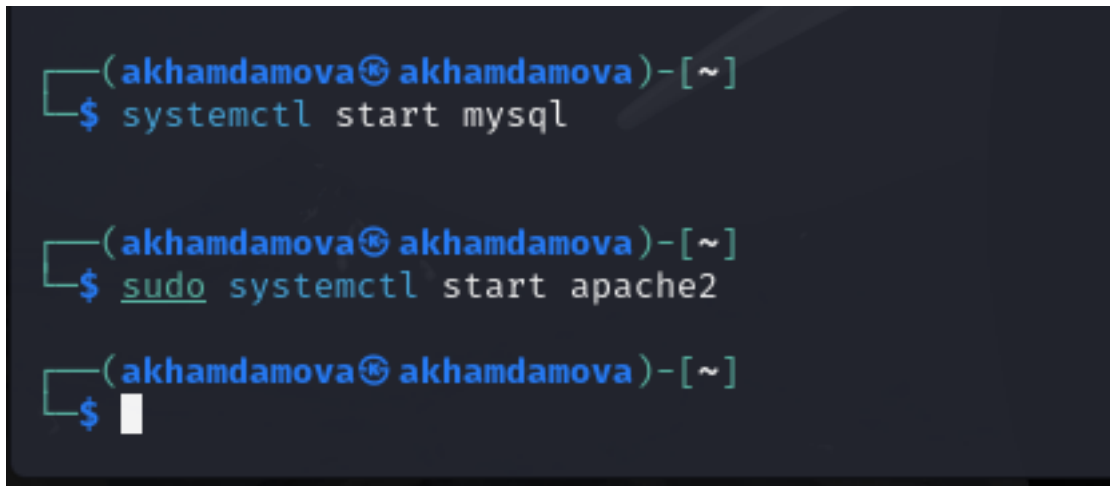
Не каждая проверка относится к проблеме безопасности, хотя большинство относятся. Некоторые пункты являются проверками типа «только для информации», которые ищут вещи, может быть не имеющие брешей безопасности, но веб-мастер или инженер по безопасности могут не знать, что

это присутствует на сервере. Обычно в выводимой информации эти элементы помечены соответствующим образом. Есть также некоторые проверки на неизвестные элементы, которые были замечены в файлах журналов.

Особенности и возможности Nikto Вот некоторые из основных особенностей Nikto:

Поддержка SSL (Unix с OpenSSL или может быть Windows с Perl/NetSSL в ActiveState) Полная поддержка HTTP прокси Проверка на устаревшие компоненты сервера Сохранение отчёта в виде простого текста, XML, HTML, NBE или CSV Движок шаблонов для простой настройки отчётов Сканирование нескольких портов на сервере или несколько серверов полученных из файла ввода (включая вывод nmap) Техники кодирования LibWhisker IDS Идентификация установленного программного обеспечения по заголовкам, иконкам (favicon) и файлам Аутентификация на хосте с Basic и NTLM Угадывание поддоменов Перечисление имён пользователей Apache и cgiwrap Техники мутации для «рыбалки» за контентом веб-серверов Подстройка сканирования, для включения или исключения целых классов проверок на уязвимости Предположение учётных данных для области авторизации (включая множество стандартных комбинаций логинов/паролей) Угадывание авторизации работает с любой директорией, а не только с корневой Улучшенное подавление ложных срабатываний посредством нескольких методов: заголовки, содержимое страницы и вычисления хеша содержимого Сообщение о «необычных» увиденных заголовках Интерактивный статус, можно поставить на паузу и изменить настройки вербальности Сохранение полных запросов/ответов для тестов, давших положительные результаты Повторное воспроизведение положительных запросов Максимальное время выполнения на одну цель Автоматическая постанова на паузу в определённое время Проверки на распространённые «парковочные» сайты Вход в Metasploit

3 Выполнение лабораторной работы



```
(akhamdamova@akhamdamova)-[~]  
$ systemctl start mysql  
  
(akhamdamova@akhamdamova)-[~]  
$ sudo systemctl start apache2  
  
(akhamdamova@akhamdamova)-[~]  
$
```


127.0.0.1/DVWA/security.php

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

DVWA

HomeInstructionsSetup / Reset DBBrute ForceCommand InjectionCSRFFile InclusionFile UploadInsecure CAPTCHASQL InjectionSQL Injection (Blind)Weak Session IDsXSS (DOM)XSS (Reflected)XSS (Stored)CSP BypassJavaScriptAuthorisation BypassOpen HTTP RedirectDVWA SecurityPHP InfoAbout

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**, as an example of how web application vulnerabilities manifest through bad coding practices as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practice** developer has tried but failed to secure an application. It also acts as a challenge to use exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or advanced practices** to attempt to secure the code. The vulnerability may not allow the same external exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

```
(akhamdamova@akhamdamova)-[~]
$ #nikto

(akhamdamova@akhamdamova)-[~]
$ 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 15:09:12 (GMT-4)

+ 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: GET, POST, OPTIONS, HEAD .
+ /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/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
```

```
(akhamdamova@akhamdamova)-[~]
$ 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 15:09:12 (GMT-4)

+ 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: GET, POST, OPTIONS, HEAD .
+ /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/: 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/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=: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /DVWA/shell?cat+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 15:09:22 (GMT-4) (10 seconds)
```

```

(akhamdamova@akhamdamova)-[~]
$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-04-27 15:11:08 (GMT-4)

+ 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 inodes via ETags, header found with file /, inode: 29cd, size: 612b10274676c, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ ///etc/hosts: 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-561
+ /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/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat=/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-04-27 15:11:17 (GMT-4) (9 seconds)

+ 1 host(s) tested

```

4 Выводы

Научилась использовать сканер nikto для тестирования веб-приложений