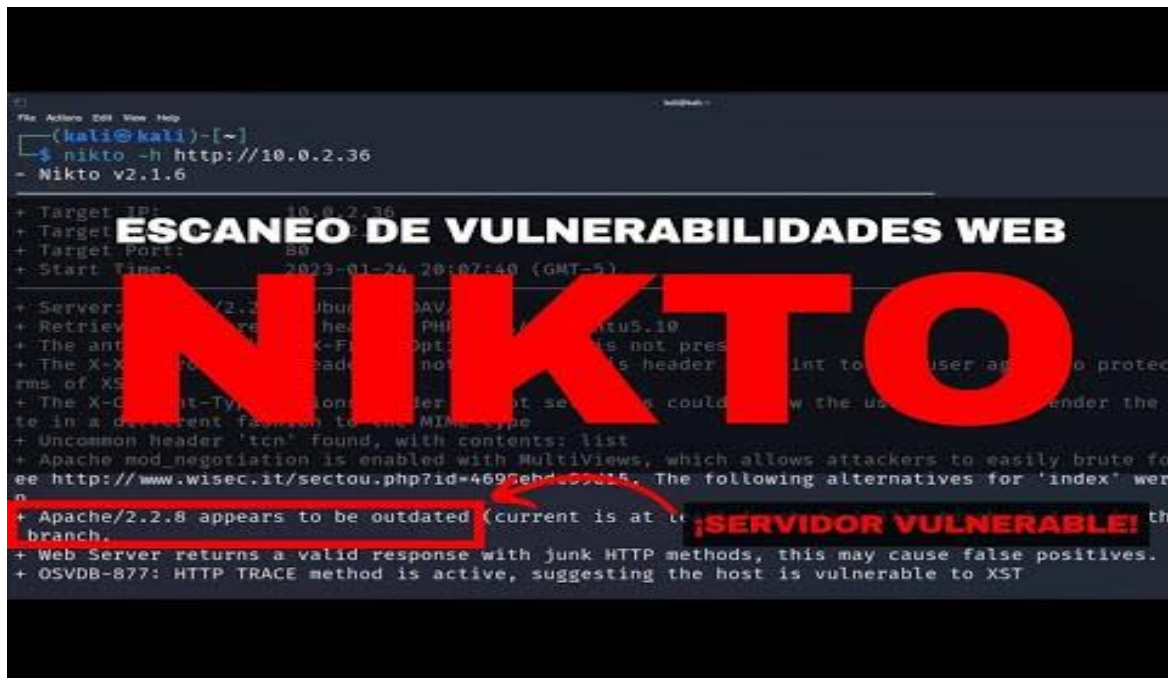


Nikto: un práctico escáner de vulnerabilidades de sitios web

[Nikto | Escaneo de vulnerabilidades web - YouTube](#)



Nikto, también conocido como Nikto2, es un escáner de servidor web de código abierto (GPL) y de uso gratuito que realiza un escaneo de vulnerabilidades en servidores web en busca de múltiples elementos: incluidos archivos/programas peligrosos y busca versiones desactualizadas del software del servidor web. También comprueba si hay errores de configuración del servidor y las posibles vulnerabilidades que puedan haber introducido.

Principales características:

- Nikto es de uso gratuito, de código abierto y se actualiza con frecuencia.
- Se puede utilizar para escanear cualquier servidor web (Apache, Nginx, Lighttpd, Litespeed, etc.)
- Escanea frente a más de 6700 vulnerabilidades conocidas y verificaciones de versión para más de 1250 servidores web (y sigue creciendo)
- Analiza en busca de problemas relacionados con la configuración, como directorios de índice abiertos
- Escaneo de certificados SSL
- Capacidad para escanear varios puertos en un servidor con varios servidores web en ejecución
- Opción de escanear a través de un proxy y con autenticación http
- Capacidad para especificar el tiempo máximo de escaneo, excluir ciertos tipos de escaneos y también se ven encabezados de informes inusuales.

Instalación de Nikto sobre Windows


Para usar esta aplicación en Windows, tenemos previamente que instalar perl (que es un lenguaje de programación) y Git.

Las instalaciones no requieren nada en especial y son bastante sencillas (en Windows, hay que tener en cuenta desactivar el antivirus).

[Git - Downloading Package \(git-scm.com\)](https://git-scm.com/)

https://git-scm.com/download/win

ASUS Software Port... MyASUS Software ... McAfee LiveSafe

 **git** --fast-version-control

Search entire site...

About
Documentation
Downloads
GUI Clients
Logos
Community

The entire [Pro Git book](#) written by Scott Chacon and Ben Straub is available to [read online](#) for free. Dead tree versions are available on [Amazon.com](#).

Download for Windows

[Click here to download](#) the latest (2.40.1) 64-bit version of Git for Windows. This is the most recent [maintained build](#). It was released 1 day ago, on 2023-04-25.

Other Git for Windows downloads

Standalone Installer
[32-bit Git for Windows Setup](#).
[64-bit Git for Windows Setup](#).

Portable ("thumbdrive edition")
[32-bit Git for Windows Portable](#).
[64-bit Git for Windows Portable](#).

Using winget tool
Install [winget tool](#) if you don't already have it, then type this command in command prompt or Powershell.

```
winget install --id Git.Git -e --source winget
```

The current source code release is version 2.40.1. If you want the newer version, you can build it from [the source code](#).

Now What?

Now that you have downloaded Git, it's time to start using it.




Perl Download - www.perl.org

https://www.perl.org/get.html

Importar favoritos ASUS Software Port... MyASUS Software ... McAfee LiveSafe

Perl runs on over 100 platforms!

We recommend that you always run the latest stable version, currently 5.36.1. If you're running a version older than 5.8.3, you may find that the latest version of CPAN modules will not work.

Unix/Linux	macOS	Windows
 Included (may not be latest)	 Included (may not be latest)	 Strawberry Perl & ActiveState Perl
GET STARTED	GET STARTED	GET STARTED

Unix
Running Linux, Solaris, AIX, HPUX, or any other UNIX-like system?

Binaries
✓ Already Installed
You probably already have perl installed. Type `perl -v` on a command line to find out which version.
ActiveState Perl has binary distributions of Perl for many platforms. This is the simplest way to install the latest version of Perl.

[DOWNLOAD ACTIVEPERL](#)

Source
Consider looking at App::perlbrew to help compile and manage Perl from source.
Find out more about the source code, development versions as well as current releases of the Perl source code.
Latest under development source code

[DOWNLOAD LATEST STABLE SOURCE \(5.36.1\)](#)

https://www.perl.org/get.html#win32

Una vez instalado Perl y Git, nos descargamos Nikto, usando github desde consola.

```
Git CMD
C:\Users\padil>git clone https://github.com/sullo/nikto.git
Cloning into 'nikto'...
remote: Enumerating objects: 7138, done.
remote: Counting objects: 100% (1149/1149), done.
remote: Compressing objects: 100% (350/350), done.
remote: Total 7138 (delta 864), reused 1051 (delta 798), pack-reused 5989
Receiving objects: 100% (7138/7138), 4.70 MiB | 812.00 KiB/s, done.
Resolving deltas: 100% (5181/5181), done.

C:\Users\padil>
```

Entramos en el directorio del programa.

```
Git CMD
C:\Users\padil>cd nikto

C:\Users\padil\nikto>dir
El volumen de la unidad C es OS
El número de serie del volumen es: 3CC7-DCF3

Directorio de C:\Users\padil\nikto

27/04/2023  10:59    <DIR>          .
27/04/2023  10:58    <DIR>          ..
27/04/2023  10:59                93 .dockerignore
27/04/2023  10:59               217 .editorconfig
27/04/2023  10:59                21 .gitattributes
27/04/2023  10:59    <DIR>          .github
27/04/2023  10:59               100 .gitignore
27/04/2023  10:59            18.092 COPYING
27/04/2023  10:59    <DIR>          devdocs
27/04/2023  10:59               902 Dockerfile
27/04/2023  10:59    <DIR>          documentation
27/04/2023  10:59    <DIR>          program
27/04/2023  10:59             7.454 README.md
                   7 archivos                26.879 bytes
                   6 dirs  156.004.204.544 bytes libres

C:\Users\padil\nikto>
```

Dentro de Program, ejecutamos ejecutamos nikto.pl llamando a perl

```
C:\Users\tarde\nikto\program>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 38D2-37A9

Directorio de C:\Users\tarde\nikto\program

07/04/2023  16:19    <DIR>          .
07/04/2023  16:19    <DIR>          ..
07/04/2023  16:19    <DIR>          databases
07/04/2023  16:19    <DIR>          docs
07/04/2023  16:19                3.394 nikto.conf.default
07/04/2023  16:19            12.600 nikto.pl
07/04/2023  16:19    <DIR>          plugins
07/04/2023  16:19            3.280 replay.pl
07/04/2023  16:19    <DIR>          templates
                3 archivos             19.274 bytes
                6 dirs  648.888.864.768 bytes libres

C:\Users\tarde\nikto\program>_
```

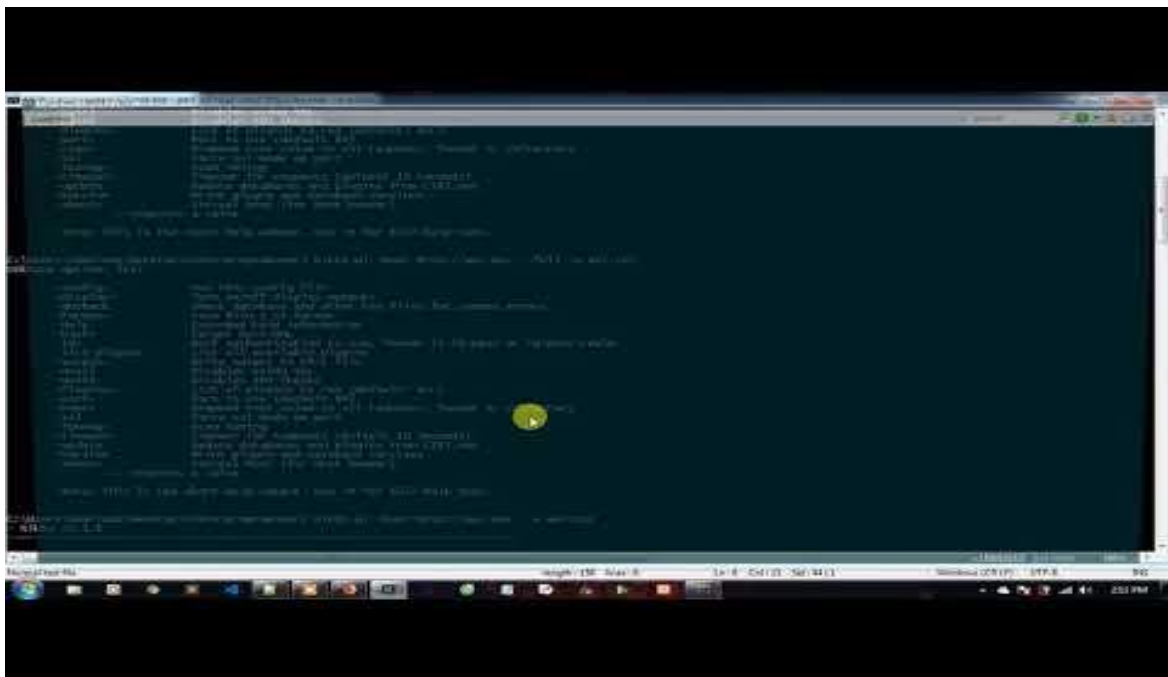
```

C:\Users\tarde\nikto\program>perl nikto.pl
Nikto v2.1.6
-----
ERROR: No host (-host) specified

Options:
-ask+           Whether to ask about submitting updates
                  yes   Ask about each (default)
                  no    Don't ask, don't send
                  auto  Don't ask, just send
-Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
-config+        Use this config file
-Display+       Turn on/off display outputs:
                  1     Show redirects
                  2     Show cookies received
                  3     Show all 200/OK responses
                  4     Show URLs which require authentication
                  D     Debug output
                  E     Display all HTTP errors
                  P     Print progress to STDOUT
                  S     Scrub output of IPs and hostnames
                  V     Verbose output
-dbcheck        Check database and other key files for syntax errors
-evasion+       Encoding technique:
                  1     Random URI encoding (non-UTF8)
                  2     Directory self-reference (/./)
                  3     Premature URL ending
                  4     Prepend long random string
                  5     Fake parameter
                  6     TAB as request spacer
                  7     Change the case of the URL
                  8     Use Windows directory separator (\)
                  A     Use a carriage return (0x0d) as a request spacer
                  B     Use binary value 0x0b as a request spacer

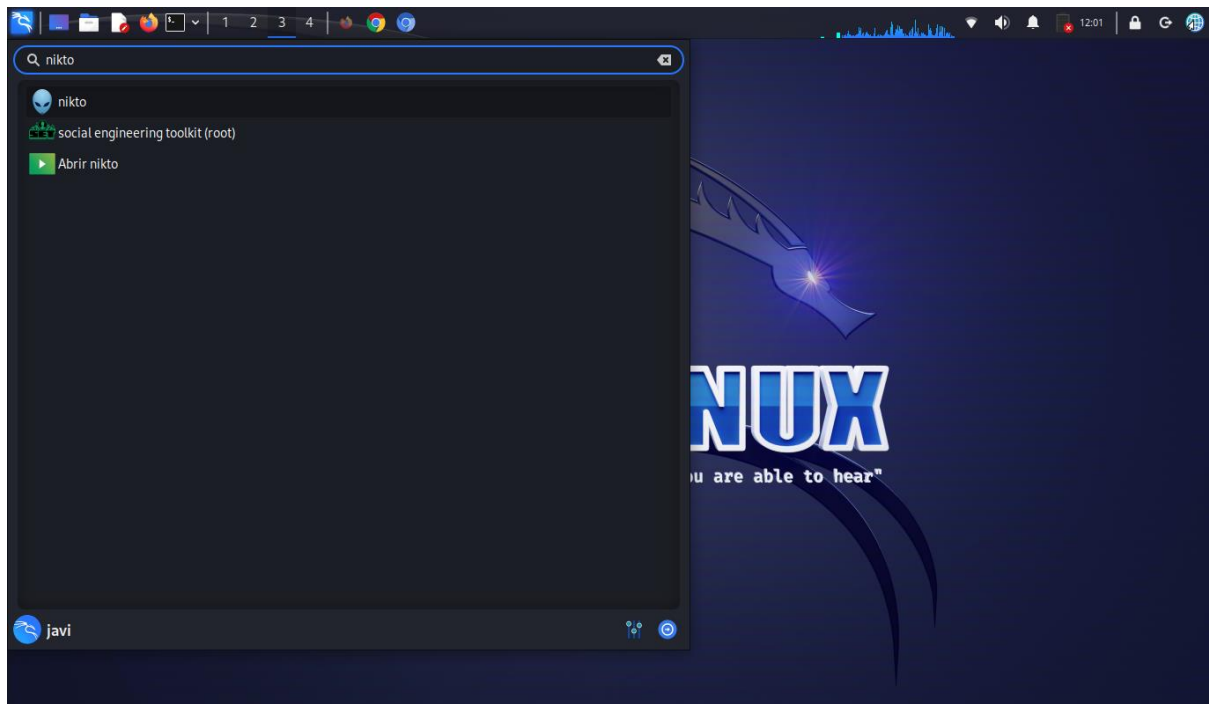
```

[NIKTO web server scanner installation in WINDOWS - YouTube](#)



Instalación de Nikto sobre Kali linux

Nikto es una aplicación nativa de Kali Linux, simplemente hay que buscarla en el menú como muestra la imagen.



Ejemplo de Escaneo sobre un Servidor Web (máquina Metaesplotable 192.168.1.87)

192.168.1.87 / 192.168.1.87 port 80

Target IP	192.168.1.87
Target hostname	192.168.1.87
Target Port	80
HTTP Server	Apache/2.2.8 (Ubuntu) DAV/2
Site Link (Name)	http://192.168.1.87:80/
Site Link (IP)	http://192.168.1.87:80/
URI	/
HTTP Method	GET
Description	/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/index
HTTP Method	GET
Description	/index: Uncommon header 'tcn' found, with contents: list.
Test Links	http://192.168.1.87:80/index http://192.168.1.87:80/index
References	

URI	/index
HTTP Method	GET
Description	/index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php.
Test Links	http://192.168.1.87:80/index http://192.168.1.87:80/index
References	http://www.wisec.it/sectou.php?id=4698ebdc59d15 , https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
URI	/
HTTP Method	HEAD
Description	Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	
URI	/
HTTP Method	AGULVYCG
Description	/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	
URI	/
HTTP Method	TRACE
Description	/: HTTP TRACE method is active which suggests the host is vulnerable to XST.
Test Links	http://192.168.1.87:80/ http://192.168.1.87:80/
References	https://owasp.org/www-community/attacks/Cross_Site_Tracing
URI	/phpinfo.php?VARIABLE=<script>alert("Vulnerable")</script>
HTTP Method	GET
Description	/phpinfo.php: Output from the phpinfo() function was found.
Test Links	<a href="http://192.168.1.87:80/phpinfo.php?VARIABLE=<script>alert(" script>"="" vulnerable")<="">http://192.168.1.87:80/phpinfo.php?VARIABLE=<script>alert("Vulnerable")</script> <a href="http://192.168.1.87:80/phpinfo.php?VARIABLE=<script>alert(" script>"="" vulnerable")<="">http://192.168.1.87:80/phpinfo.php?VARIABLE=<script>alert("Vulnerable")</script>
References	

URI	/phpMyAdmin/Documentation.html
HTTP Method	GET
Description	/phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
Test Links	http://192.168.1.87:80/phpMyAdmin/Documentation.html http://192.168.1.87:80/phpMyAdmin/Documentation.html
References	
URI	/phpMyAdmin/README
HTTP Method	GET
Description	/phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
Test Links	http://192.168.1.87:80/phpMyAdmin/README http://192.168.1.87:80/phpMyAdmin/README
References	https://typo3.org/
URI	/#wp-config.php#
HTTP Method	GET
Description	/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
Test Links	http://192.168.1.87:80/#wp-config.php# http://192.168.1.87:80/#wp-config.php#
References	

Host Summary

Start Time	2023-04-24 11:00:51
End Time	2023-04-24 11:02:02
Elapsed Time	71 seconds
Statistics	8910 requests, 0 errors, 27 findings

Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-h 192.168.1.87 -o scan.html -Format htm
Hosts Tested	1
Start Time	Mon Apr 24 11:00:50 2023
End Time	Mon Apr 24 11:02:02 2023
Elapsed Time	72 seconds