# Cyber Security Intern

**Mohammad Nishar Ansari**

**Cyber Security Intern**

# Nikto

Nikto, also known as Nikto2, is an open source (GPL) and free-to-use web server scanner which performs vulnerability scanning against web servers for multiple items including dangerous files and programs, and checks for outdated versions of web server software. It also checks for server configuration errors and any possible vulnerabilities they might have introduced.

The Nikto vulnerability scanner project is a fast-moving effort, frequently updated with the latest known vulnerabilities. This allows you to scan your web servers with confidence as you search for any possible issues.

Nikto is a perl based security testing tool and this means it will run on most operating systems with the necessary Perl interpreter installed. We will guide you through using it on Ubuntu Linux, basically because it is our operating system of choice and it just works. Perl comes already installed in Ubuntu. So it is a matter of downloading the tool, unpacking it and running the command with the necessary options. For Windows users running Nikto will involve installing a perl environment (activestate perl) or loading up a Linux virtual machine using Virtualbox or VMware.

## Features: -

- Nikto is free to use, open source and frequently updated.
- It can be used to scan any web server (Apache, Nginx, Lighttpd, Litespeed, etc.)
- It is used to scans against 6,700+ known vulnerabilities and version checks for 1,250+ web servers (and growing)
- It scans for configuration-related issues such as open index directories.
- It is used for SSL certificate scanning.
- It has ability to scan multiple ports on a server with multiple web servers running.
- It is also capable to scan through a proxy and with http authentication.
- It has ability to specify maximum scan time, exclude certain types of scans and unusual report headers seen as well.

# Commands: -

1. Nikto is a pre installed tool in Linux but you can also clone it from the github.

```
┌──(root㉿kali)-[/home/kali/nikto/program]
└─# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto' ...
remote: Enumerating objects: 7286, done.
remote: Counting objects: 100% (1307/1307), done.
remote: Compressing objects: 100% (458/458), done.
remote: Total 7286 (delta 979), reused 1119 (delta 848), pack-reused 5979
Receiving objects: 100% (7286/7286), 4.61 MiB | 2.82 MiB/s, done.
Resolving deltas: 100% (5288/5288), done.
```

2. Now move towards nikto/program/ to use the tool.

```
┌──(root㉿kali)-[/home/kali/nikto/program]
└─# cd nikto/program
```

3. If you want to have a basic scan use flag h.

```
┌──(root㉿kali)-[/home/…/nikto/program/nikto/program]
└─# nikto -h google.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 142.250.194.110, 2404:6800:4002:821::200e
+ Target IP:          142.250.194.110
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2024-05-21 17:56:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: gws
+ /: 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 / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'gws' to 'sffe'.
+ /: Cookie 1P_JAR created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /news/news.mdb: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64,
 Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version.
```

4. We can use -ssl flag to have a ssl certificate scan.

```
┌──(root㉿kali)-[/home/…/nikto/program/nikto/program]
└─# nikto -h google.com -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 142.250.194.110, 2404:6800:4002:821::200e
+ Target IP:          142.250.194.110
+ Target Hostname:    google.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.google.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services LLC/CN=GTS CA 1C3
+ Start Time:         2024-05-21 18:05:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: gws
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt
-svc
+ /: 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 / redirects to: https://www.google.com/
```

5. Here we use -port in order to have scan of a particular port.