Nikto

Nikto is an open-source web server scanner designed to identify vulnerabilities, misconfigurations, and security issues on web servers. It helps penetration testers and security professionals analyze and assess the security of web applications and servers efficiently.

Before scanning a web server, it is essential to understand Nikto's available features and commands. You can list all options using:

```
nikto -h
```

This command provides an overview of Nikto's capabilities, including scanning options, output formats, and tuning parameters.

1. Scanning a Specific Port

Nikto allows you to specify a particular port to scan. By default, it scans port 80, but you can define a different port as needed.

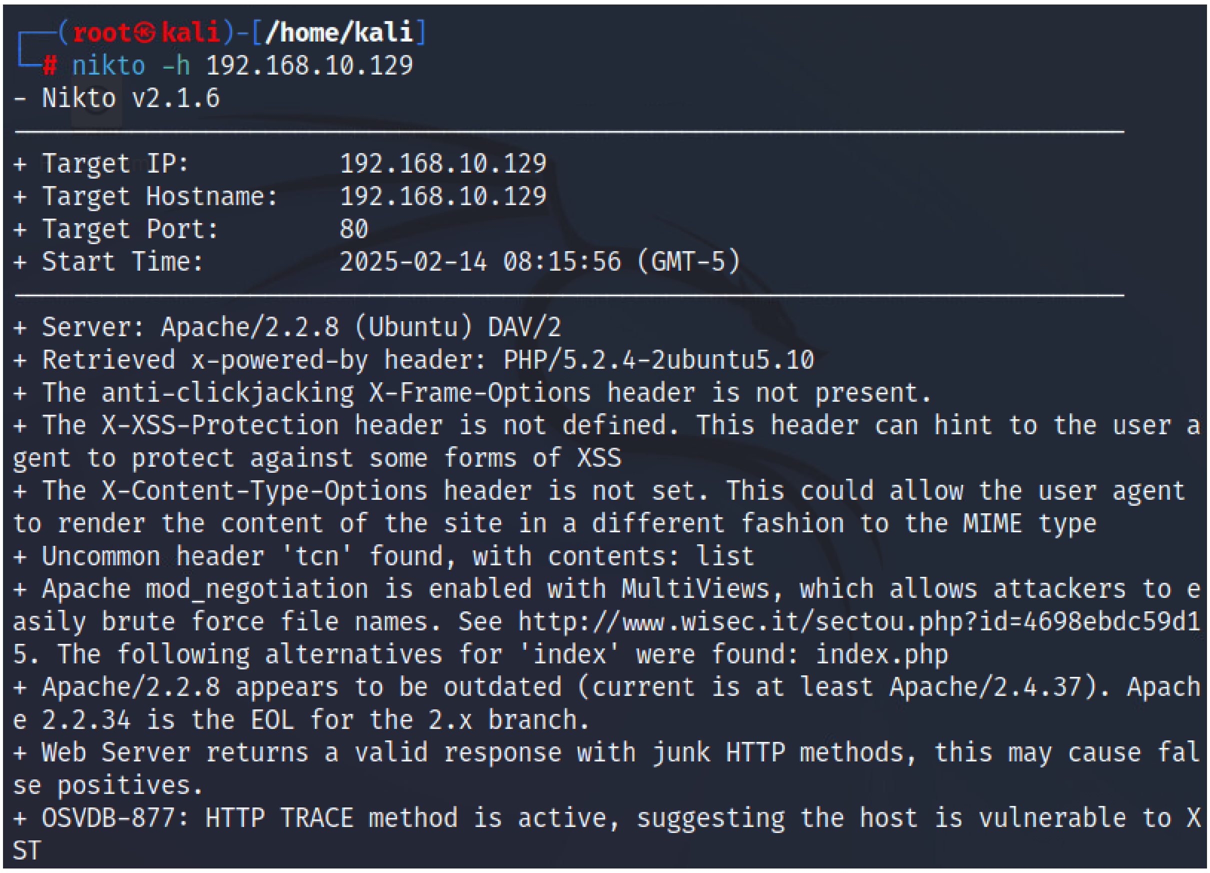
Command:

```
nikto -h <target-IP> -p 80
```

Explanation:

- -h <target-IP> specifies the target's IP address.
- -p 80 instructs Nikto to scan port 80 for vulnerabilities.

To scan a different port, replace 80 with the desired port number.



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h 192.168.10.129
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.10.129
+ Target Hostname:    192.168.10.129
+ Target Port:        80
+ Start Time:         2025-02-14 08:15:56 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ 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
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apach
e 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
```

2. Scanning an IP Address or Hostname

Nikto can perform a complete vulnerability scan on a web server using its IP address or hostname.

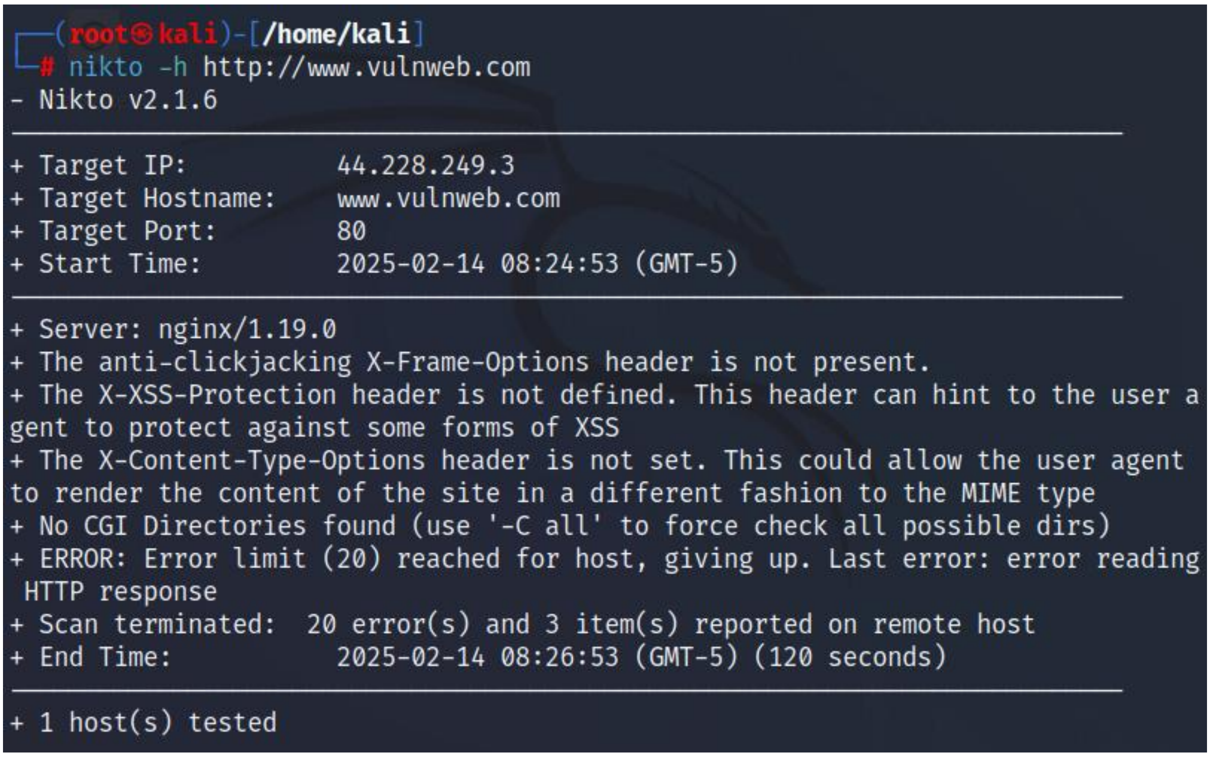
Command:

# nikto -h <URL>

Explanation:

- -h <URL> targets the specified website or web server for analysis.

This command helps identify outdated software, security flaws, and misconfigurations.



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h http://www.vulnweb.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    www.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-02-14 08:24:53 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading
 HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-02-14 08:26:53 (GMT-5) (120 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto is scanning the web server www.vulnweb.com (a test site for security research), and the report details various security issues.

1. Basic Information

- **Nikto v2.1.6** → Version of Nikto being used.
- **Target IP** → The resolved IP address of the target website.
- **Target Hostname** → The domain name of the target.
- **Target Port: 80** → The scan is performed on port 80 (default HTTP port).
- **Start Time** → The timestamp when the scan started.

2. Identified Security Issues

The web server is running **nginx version 1.19.0**. Knowing the exact version can help attackers determine if the server has known vulnerabilities.

X-Frame-Options header missing → This means the website is vulnerable to **clickjacking attacks**, where an attacker can trick users into clicking on hidden buttons or links.

X-XSS-Protection header missing → The website lacks built-in browser protection against **cross-site scripting (XSS) attacks**.

X-Content-Type-Options missing → Could lead to **MIME-type sniffing attacks**, where a browser incorrectly interprets files, leading to potential security risks.

3. Errors and Termination

Error limit reached (20 errors) → Nikto stopped scanning because it encountered too many errors while reading HTTP responses.

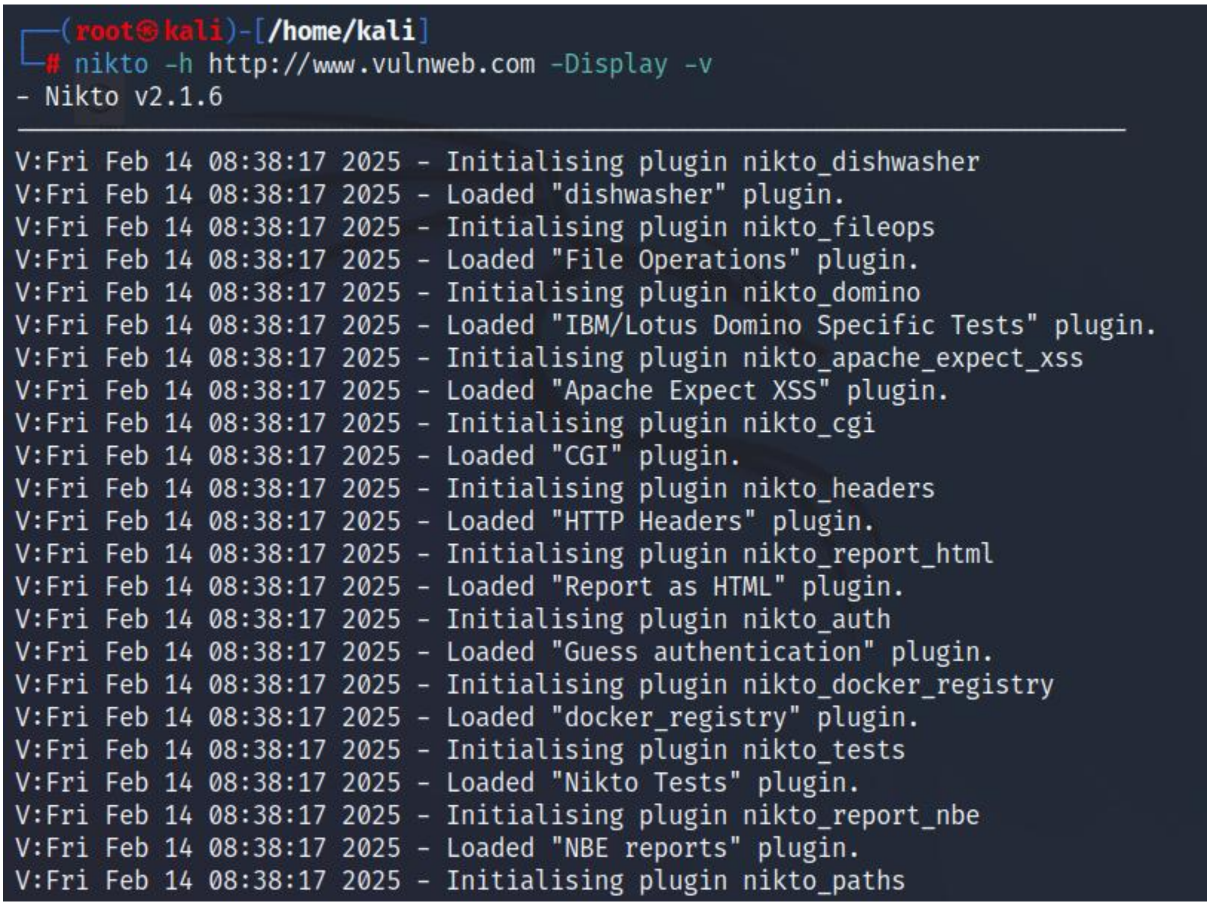
Possible causes:

- The website blocked Nikto’s scan (firewall, rate limiting, or intrusion prevention system).
- Network issues or server timeouts.
- The scan found **several missing security headers**, making the site vulnerable to **clickjacking, XSS, and MIME-type sniffing attacks**.
- The **server version (nginx 1.19.0)** was revealed, which could be used for further research on vulnerabilities.
- The scan was **incomplete due to error limits**, meaning some vulnerabilities might not have been detected.

To improve results:

1. **Use verbose mode** to get more details

```
nikto -h http://www.vulnweb.com -Display -v
```



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h http://www.vulnweb.com -Display -v
- Nikto v2.1.6
---------------------------------------------------------------------------
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_dishwasher
V:Fri Feb 14 08:38:17 2025 - Loaded "dishwasher" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_fileops
V:Fri Feb 14 08:38:17 2025 - Loaded "File Operations" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_domino
V:Fri Feb 14 08:38:17 2025 - Loaded "IBM/Lotus Domino Specific Tests" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_apache_expect_xss
V:Fri Feb 14 08:38:17 2025 - Loaded "Apache Expect XSS" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_cgi
V:Fri Feb 14 08:38:17 2025 - Loaded "CGI" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_headers
V:Fri Feb 14 08:38:17 2025 - Loaded "HTTP Headers" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_report_html
V:Fri Feb 14 08:38:17 2025 - Loaded "Report as HTML" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_auth
V:Fri Feb 14 08:38:17 2025 - Loaded "Guess authentication" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_docker_registry
V:Fri Feb 14 08:38:17 2025 - Loaded "docker_registry" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_tests
V:Fri Feb 14 08:38:17 2025 - Loaded "Nikto Tests" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_report_nbe
V:Fri Feb 14 08:38:17 2025 - Loaded "NBE reports" plugin.
V:Fri Feb 14 08:38:17 2025 - Initialising plugin nikto_paths
```

3. Scanning an SSL-Enabled Website

Web servers using HTTPS require a slightly different approach to ensure proper scanning.

Command:

nikto -h <URL> ssl

Explanation:

- The ssl flag forces Nikto to use SSL/TLS when connecting to the web server.
- This is crucial when scanning HTTPS-enabled sites.

4. Customizing Scans with Tuning Options

Nikto provides tuning options that allow you to focus on specific types of vulnerabilities. This feature helps tailor scans based on particular areas of interest.

Tuning Categories:

- 0 – File Upload
- 1 – Interesting Files/Seen in Logs
- 2 – Misconfiguration/Default Files
- 3 – Information Disclosure
- 4 – Injection (XSS/Script/HTML)
- 5 – Remote File Retrieval (Inside Web Root)
- 6 – Denial of Service
- 7 – Remote File Retrieval (Server-Wide)
- 8 – Command Execution / Remote Shell
- 9 – SQL Injection

Command Example:

```
nikto -h <target-IP> -Tuning 123
```

Explanation:

- -Tuning 123 selects tests for interesting files, misconfigurations, and information disclosure.
- This improves scan efficiency by focusing on relevant vulnerabilities.

5. Advanced Scan Options

Scanning Multiple Hosts

Nikto can scan multiple targets listed in a text file.

Command:

```
nikto -h hosts.txt
```

Explanation:

- hosts.txt contains a list of IP addresses or domain names to scan.

Verbose Mode

For more detailed output during scans, use verbose mode.

Command:

```
nikto -h <target-IP> -Display -v
```

Explanation:

- -Display -v provides detailed scan progress and findings.

Conclusion

Nikto is a valuable tool for web security assessments, providing detailed insights into potential vulnerabilities. By leveraging its scanning, tuning, and advanced options, penetration testers can efficiently evaluate web server security.

For more details, visit the official Nikto documentation at https://cirt.net/Nikto2.