

Nikto Web Server Scanner: Features, Commands, and Vulnerability Assessment

Abstract—Nikto is an open-source web server scanner that performs comprehensive tests against web servers for multiple vulnerabilities, outdated server versions, dangerous files, and configurations. It is commonly used in cybersecurity for vulnerability assessment due to its ease of use and effectiveness.

I. INTRODUCTION

Nikto is a widely used web server scanner that performs extensive tests against web servers for vulnerabilities, outdated server versions, dangerous files, and configurations. Due to its user-friendly interface and thorough testing capabilities, Nikto is an effective tool in cybersecurity for vulnerability assessment.

A. Key Features

- Checks for over 6,700 potentially dangerous files/programs.
- Scans for outdated versions on over 1,250 servers.
- Identifies version-specific problems on more than 270 servers.
- Detects server configuration issues.

II. INSTALLATION

Nikto can be installed on various operating systems, such as Kali Linux, Ubuntu, and Windows (using a compatible environment like WSL or Cygwin).

```
[pallavi@kali:~]$ nikto -help
Unknown option: help

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
  -check6        Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-bin/"
  -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 0x00 as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+       Save file (-o) format:
                  csv Comma-separated-value
                  json JSON Format
                  htm HTML Format
                  nbe Nessus NBE format
```

Fig. 1. Nikto installation process on Linux

A. On Linux (Ubuntu/Kali)

```
sudo apt update
sudo apt install nikto -y
```

B. On macOS (using Homebrew)

```
brew install nikto
```

C. On Windows

- Install a compatible environment (e.g., Cygwin or Windows Subsystem for Linux).
- Install Nikto as in Linux.

III. USING NIKTO: COMMANDS AND EXAMPLES

Nikto provides a variety of commands for different purposes, from scanning a single target to configuring custom scan options. Below are some essential commands along with their descriptions.

A. Basic Syntax

```
nikto -h <target>
```

This is the basic command syntax where <target> is the URL of the website you want to scan.

B. Examples and Key Options

1) Simple Scan: Scan a target by specifying its URL.

```
nikto -h http://www.cisco.com
```

Description: This command performs a basic scan of the specified target for known vulnerabilities.

```
[pallavi@kali:~]$ nikto -h https://www.cisco.com
- Nikto v2.5.0

+ Multiple IPs found: 72.246.155.191, 2600:140f:1c00:1b7::b33, 2600:140f:1c00:1a0::b33
+ Target IP: 72.246.155.191
+ Target Hostname: www.cisco.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=DigiNotus/CN=HydrantID Trusted Certificate Service/CN=HydrantID Server CA 01
+ Start Time: 2024-11-06 22:26:02 (GMT+5)

+ Server: No banner retrieved
+ /: Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: IP address found in the 'CP_GUTC' cookie. The IP is '49.44.140.237'.
+ /: Cookie c_b1 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-served-by header: cache-bur-kbure280116-BUR.
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-bur-kbure280116-BUR.
+ /: Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb-mRUM,1.
+ /: Uncommon header 'x-ghost' found, with contents: publish.
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="17309
12164263_825082245_34568462_2845_13792_42_86_-";dur=1,).
+ /ohxJPfBR.shtm: Uncommon header 'x-edgeconnect-mid-mile-rtt' found, with contents: 266.
+ /ohxJPfBR.shtm: Uncommon header 'cdchost' found, with contents: cdcweb-prod2-03.
+ : Server banner changed from 'Apache/2.4.27 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'AkamaiGHost'.
+ /ohxJPfBR.htpasswd: The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner
/vulnerabilities/missing-content-type-header/
```

Fig. 2. Basic scan command example

2) Scan Specific Port:

```
nikto -h http://www.cisco.com -p 8080
```

Description: This command scans the target on port 8080 instead of the default port 80.

3) Use SSL/TLS:

```
nikto -h https://www.cisco.com
```

Description: This command enables the scanner to connect to the target using HTTPS, allowing it to scan secure web applications.

```
--(pallavini@kali)-[~]
$ nikto -h https://www.cisco.com -o output.html -Format html
Nikto v2.5.0

+ Multiple IPs found: 72.246.155.191, 2600:140f:1c00:1a0::b33, 2600:140f:1c00:1b7::b33
+ Target IP: 72.246.155.191
+ Target Hostname: www.cisco.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=IdenTrust/OU=HydrantID Trusted Certificate Service/CN=HydrantID Server CA 01
2024-11-06 22:30:52 (GMT+5)

+ Start Time:

Server: No banner retrieved
+ Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ IP address found in the 'CP_GUTC' cookie. The IP is "49.44.140.237".
+ Cookie c-bi created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Retrieved x-served-by header: cache-bur-kbur200116-BUR.
+ Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak,p; desc="17309
245+223.92590245.1481770.31.18107.40.75"-dur=1),.
+ Uncommon header 'x-vhost' found, with contents: publish.
+ Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=MRUM,1.
+ Uncommon header 'x-served-by' found, with contents: cache-bur-kbur200116-BUR.
+ /Rw9EmaF.INC: Uncommon header 'cdcho' found, with contents: cdcweb-prod2-02.
+ /Rw9EmaF.INC: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 242.
+ /Rw9EmaF.INC: Uncommon header 'x-edgeconnect-origin-mex-latency' found, with contents: 5.
```

Fig. 3. SSL/TLS scanning example

4) Verbose Mode:

```
nikto -h http://www.cisco.com -Display
```

Description: This command enables verbose output, providing detailed information during the scan process.

5) Tuning Options:

To scan only specific vulnerability categories (e.g., file uploads, SQL injection), use the `-Tuning` flag.

```
nikto -h http://www.cisco.com -Tuning 1,2,3
```

Description: This command allows you to customize the scan by specifying which types of vulnerabilities to test for, making it more efficient.

```
--(pallavini@kali)-[~]
$ nikto -h https://www.cisco.com -Tuning 1,2,3
Nikto v2.5.0

+ Multiple IPs found: 72.246.155.191, 2600:140f:1c00:1b7::b33, 2600:140f:1c00:1a0::b33
+ Target IP: 72.246.155.191
+ Target Hostname: www.cisco.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=IdenTrust/OU=HydrantID Trusted Certificate Service/CN=HydrantID Server CA 01
2024-11-06 22:32:00 (GMT+5)

+ Start Time:

Server: No banner retrieved
+ Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ IP address found in the 'CP_GUTC' cookie. The IP is "49.44.140.237".
+ Cookie c-bi created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Retrieved x-served-by header: cache-bur-kbur200116-BUR.
+ Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=MRUM,1.
+ Uncommon header 'x-served-by' found, with contents: cache-bur-kbur200116-BUR.
+ Uncommon header 'x-vhost' found, with contents: publish.
+ Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak,p; desc="17309
232155.925900245.14808057.42.11452.28.57"-dur=1),.
+ /RfRh7Z.cobalt: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 250.
+ /RfRh7Z.cobalt: Uncommon header 'cdcho' found, with contents: cdcweb-prod1-03.
+ /RfRh7Z.cobalt: Uncommon header 'x-edgeconnect-origin-mex-latency' found, with contents: 5.
```

Fig. 4. Tuning options example

IV. MANAGING OUTPUT FILES

After completing a scan, Nikto saves the scan results in various formats, including HTML, CSV, and TXT, which are easy to analyze and share.

To save the output to a specific file:

```
nikto -h http://www.cisco.com -o results.html -Format html
```

Description: This command executes a scan and saves the results in an HTML file named `results.html`.

```
--(pallavini@kali)-[~]
$ nikto -h https://www.cisco.com/ -o output.html -Format html
Nikto v2.5.0

+ Multiple IPs found: 72.246.155.191, 2600:140f:1c00:1a0::b33, 2600:140f:1c00:1b7::b33
+ Target IP: 72.246.155.191
+ Target Hostname: www.cisco.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=IdenTrust/OU=HydrantID Trusted Certificate Service/CN=HydrantID Server CA 01
2024-11-06 22:24:38 (GMT+5)

+ Start Time:

Server: No banner retrieved
+ Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ IP address found in the 'CP_GUTC' cookie. The IP is "49.44.140.237".
+ Cookie c-bi created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Retrieved x-served-by header: cache-bur-kbur200116-BUR.
+ Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=MRUM,1.
+ Uncommon header 'x-served-by' found, with contents: cache-bur-kbur200116-BUR.
+ Uncommon header 'x-vhost' found, with contents: publish.
+ Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak,p; desc="17309
1207943.825903245.34402864.35.8340.39.80"-dur=1),.
+ /y2cQK0Yf.10:100: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 237.
```

Fig. 5. HTML output report example

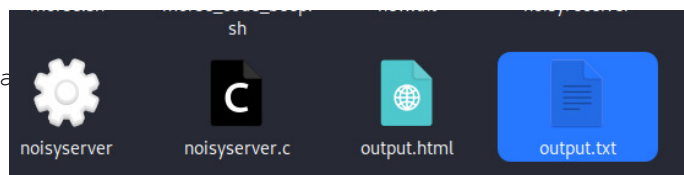


Fig. 6. Saving output to an HTML file

A. Output Format Options

- `html`: Generates a well-structured report for quick access.
- `csv`: Provides a tabular format useful for integrating with other tools.
- `txt`: Creates a plaintext report for basic documentation.

V. GENERATING A VULNERABILITY ASSESSMENT REPORT

A typical vulnerability assessment report using Nikto should include the following sections:

- 1) **Executive Summary:** High-level overview of the assessment, vulnerabilities found, and potential impacts.
- 2) **Scan Details:** Information on target, scan date, Nikto version, and command options used.
- 3) **Vulnerability Findings:**
 - List of detected vulnerabilities, including file paths, descriptions, severity ratings, and recommended actions.
- 4) **Conclusion and Recommendations:**
 - Summary of findings with actionable recommendations to mitigate the identified risks.

www.cisco.com / 72.246.155.191 port 443	
Target IP	72.246.155.191
Target hostname	www.cisco.com
Target Port	443
HTTP Server	
Site Link (Name)	https://www.cisco.com/443/
Site Link (IP)	https://72.246.155.191.443/
URI	/
HTTP Method	GET
Description	/: Cookie CP_GUTC created without the httponly flag.
Test Links	https://www.cisco.com/443/ https://72.246.155.191.443/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/
HTTP Method	GET
Description	/: IP address found in the 'CP_GUTC' cookie. The IP is '49.44.140.237'.
Test Links	https://www.cisco.com/443/ https://72.246.155.191.443/
References	
URI	/
HTTP Method	GET
Description	/: Cookie c_bi created without the httponly flag.
Test Links	https://www.cisco.com/443/ https://72.246.155.191.443/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/
HTTP Method	GET
Description	/: Retrieved x-served-by header: cache-bur-kbur8200116-BUR.
Test Links	https://www.cisco.com/443/ https://72.246.155.191.443/
References	
URI	/
HTTP Method	GET
Description	/: Fastly CDN was identified by the x-timer header.

Fig. 7. HTML output report example

VI. CONCLUSION

Nikto is a powerful, easy-to-use tool for assessing web server vulnerabilities, providing a wide range of scanning options and customizable output formats. While Nikto is efficient in detecting common vulnerabilities, it should ideally be used alongside other tools, as it is limited to known vulnerabilities and does not conduct deep analysis on modern web applications. Using Nikto can significantly enhance web security assessments by identifying potential risks before they are exploited.