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an open-source web server scanner that performs comprehensive tests against web servers for multiple vulnerabilities, outdated server versions, dangerous files, and configurations.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Nikto is a widely used web server scanner that performs extensive tests against web servers for vulnerabilities, outdated server versions, dangerous files, and configurations.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- Scans for outdated versions on over 1,250 servers.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).

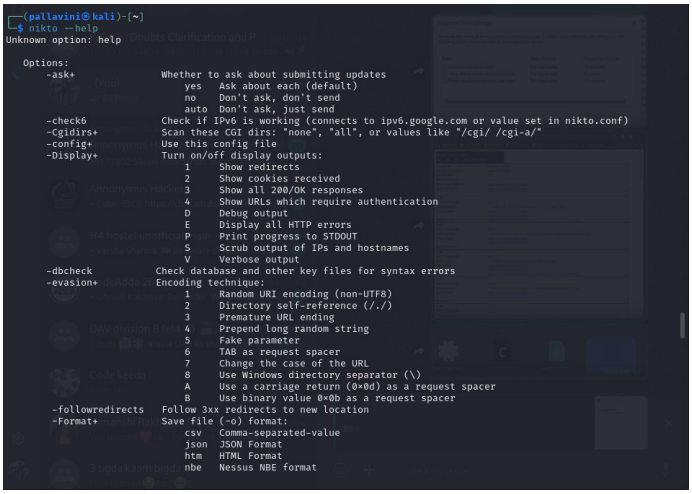

Fig. 1. Nikto installation process on Linux

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.

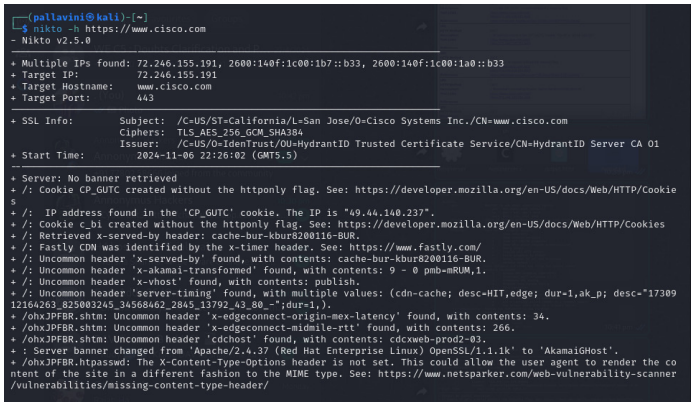

Fig. 2. Basic scan command example

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.

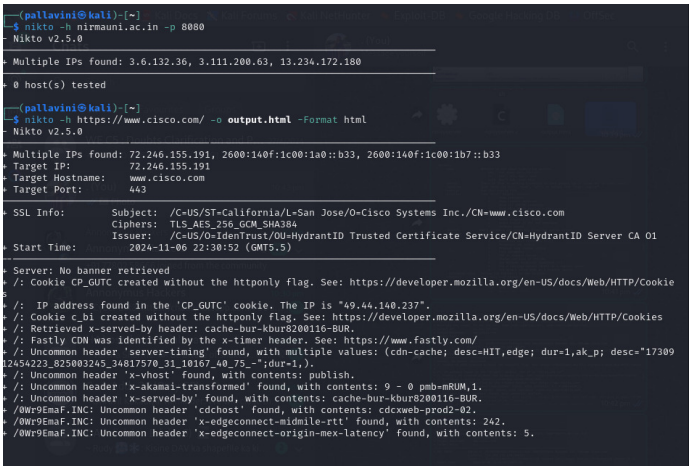

Fig. 3. SSL/TLS scanning example

4) **Verbose Mode**:

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

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.

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 -For
```

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

Fig. 5. HTML output report example

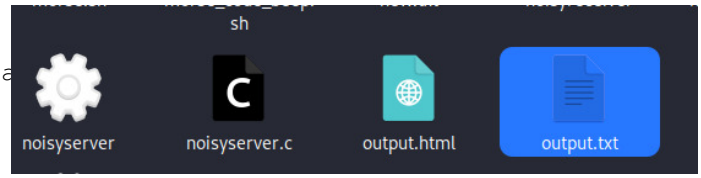

Fig. 6. Saving output to an HTML file

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.

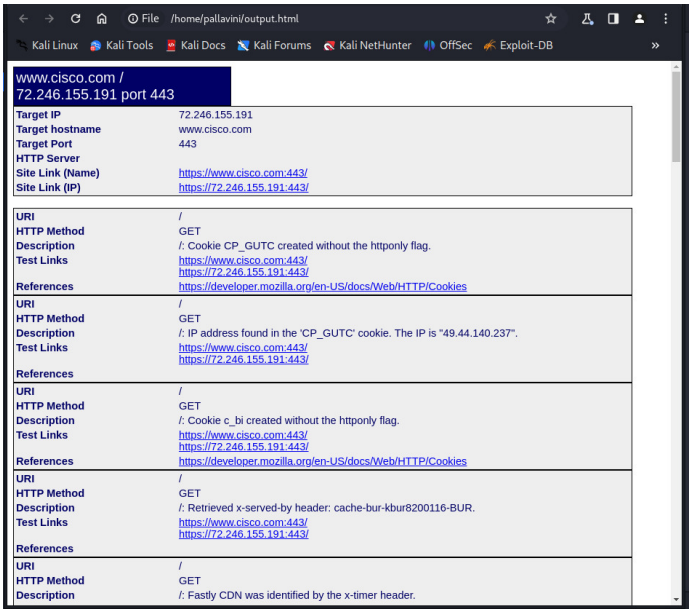

Fig. 7. HTML output report example

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.