Assignment no. 5

Name: Yashashree Nimbalkar (CSEAI)
Roll no: 381040
PRN no: 22311423

- **Title**

Network Scanning Using Nikto: A Practical Approach to Perform Network Discovery and Scanning Using Nikto.

1. Introduction & Objective

This document serves as a comprehensive guide to using **Nikto**, a powerful open-source web server scanner. The primary objective is to equip network administrators, penetration testers, and security enthusiasts with the practical skills needed to perform network discovery and web vulnerability scanning.

By the end of this guide, you will be able to:

- Install and configure Nikto on both Windows and Linux systems.
- Execute common and advanced scanning commands.
- Interpret the output to identify potential vulnerabilities.
- Document and report findings in a structured manner.

Nikto is an essential tool for security assessments, helping to identify misconfigurations, outdated software, and other common security weaknesses before malicious actors can exploit them.

2. Prerequisites

To follow this guide, you will need the following tools, software, and permissions.

Required Tools & Software:

- A Target Machine: A virtual machine or a server that you have explicit permission to scan. Never run Nikto against a target you do not own or have permission to test.
- Operating System: A Windows (10/11) or Linux (e.g., Ubuntu, Kali Linux) machine to run the scan from.
- Perl Interpreter: Nikto is a Perl script, so the Perl interpreter is a mandatory dependency.
    - For Windows: Strawberry Perl is highly recommended as it

includes many essential modules out-of-the-box.
  - For Linux: Perl is typically pre-installed.
- Nikto: The latest version downloaded from the official CIRT.net GitHub repository.
- Permissions: Administrative or root-level access on your scanning machine to install software and run commands from the terminal or command prompt.

3. Theory: Understanding Nikto

Nikto is an Open Source (GPL) web server scanner that performs thousands of tests against web servers to identify potential security vulnerabilities. It is not designed to be a stealthy tool; instead, it is built to be fast and comprehensive, making it an ideal choice for internal security audits and penetration tests.

How It Works

Nikto operates by sending a barrage of HTTP requests to a target web server, checking for known security flaws. Its functionality is driven by a set of databases (.db files) and plugins that contain signatures for thousands of known issues.

Key Items Nikto Checks For:

- **Over 6700 Potentially Dangerous Files/CGIs:** Checks for known insecure scripts, shells, and default files.
- **Outdated Server Software:** Identifies outdated versions of web servers like Apache, Nginx, and Microsoft IIS. It reports the specific version, allowing you to check for public exploits.
- **Version-Specific Problems:** Looks for vulnerabilities that are specific to the detected software versions.
- **Server Configuration Issues:** Detects misconfigurations such as open directory listings, insecure HTTP methods (e.g., PUT, DELETE), and revealing HTTP headers.
- **Insecure Cookies and Headers:** Checks for missing security headers like X-Frame-Options or cookies without the HttpOnly and Secure flags.

Important Note: Nikto can generate a significant amount of network traffic, which is easily detectable by Intrusion Detection Systems (IDS) and firewalls. It can also generate false positives, so all findings must be manually verified.

4. Setup & Installation

Follow these steps to get Nikto up and running on your system.

Step 1—Install Perl

On Windows:

1. Navigate to the Strawberry Perl website and download the latest recommended 64-bit version.
2. Run the installer executable and follow the on-screen instructions. The default settings are usually sufficient.

Once installed, open a new Command Prompt (cmd.exe) or PowerShell window and verify the installation by typing:

Bash

```
perl -v
```

3. You should see output indicating the version of Perl installed.

On Linux (Debian/Ubuntu): Perl is usually pre-installed. If not, you can install it easily:

Bash

```
sudo apt-get update
sudo apt-get install perl
```

Step 2 — Download and Set Up Nikto

1. Go to the official Nikto GitHub repository and download the latest version as a .zip file.
2. Extract the archive to a convenient location, for example:
   - **Windows:** C:\tools\nikto-master
   - **Linux:** /opt/nikto
3. Navigate into the program directory within the extracted folder. This is where the main nikto.pl script is located.

Windows:

PowerShell

```
cd C:\tools\nikto-master\program
```

○

Linux:

Bash

```
cd /opt/nikto/program
```

○

Step 3—Verify Nikto Installation

You can test if Nikto is working correctly by running it with the -Help flag.

Bash
```
perl nikto.pl -Help
```

This command should display the full list of available options, confirming that Perl can execute the script.

Step 4—Update Nikto (Recommended)

Nikto's effectiveness depends on its databases. To ensure you have the latest vulnerability checks, run the update command:

Bash
```
perl nikto.pl -update
```

5. Performing Scans: Common Commands

All commands should be run from within the program directory.

Basic Scans

Scan a website using its domain name (HTTP): This is the most basic scan, targeting the standard web port 80.
Bash
```
perl nikto.pl -h http://example.com
```

- **Scan a specific IP address:** Useful when you don't have a domain name or want to test the server directly.
  Bash
  ```
  perl nikto.pl -h 192.168.1.100
  ```
- **Scan an HTTPS target:** Use the https protocol and optionally specify the SSL port.
  Bash
  ```
  perl nikto.pl -h https://example.com -p 443
  ```
- Advanced Scanning Techniques

Scan a target behind a proxy (SNI): When scanning an IP address that hosts multiple websites (common in cloud environments), you must specify the hostname using -vhost.
Bash
```
perl nikto.pl -h https://104.26.9.237 -vhost example.com
```

Save output to a file: It is crucial to save your results. The -output (-o) flag is used for this. Nikto supports multiple formats (.txt, .html, .csv, .xml).
Bash

```
perl nikto.pl -h example.com -o scan_results.html -Format html
```

Scan a non-standard port: If a web service is running on a port other than 80 or 443, specify it with the `-port` (`-p`) flag.
Bash

```
perl nikto.pl -h 192.168.1.100 -p 8080
```

Tune your scan for speed: The `-Tuning` (`-T`) option allows you to control which tests are run. `Tuning 1` (Interesting Files) is one of the fastest.
Bash

```
# Quick scan for interesting files and misconfigurations

  perl nikto.pl -h example.com -Tuning 1x
```

*T*he `x` reverses the logic, excluding options instead of including them, which can be useful for targeted scans.

6. Interpreting Results & Documentation

Once a scan is complete, Nikto provides a summary of its findings. Understanding this output is key.

Example Output Snippet:

```
+ Server: Apache/2.4.29 (Ubuntu)
+ 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 agent 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
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting.
```

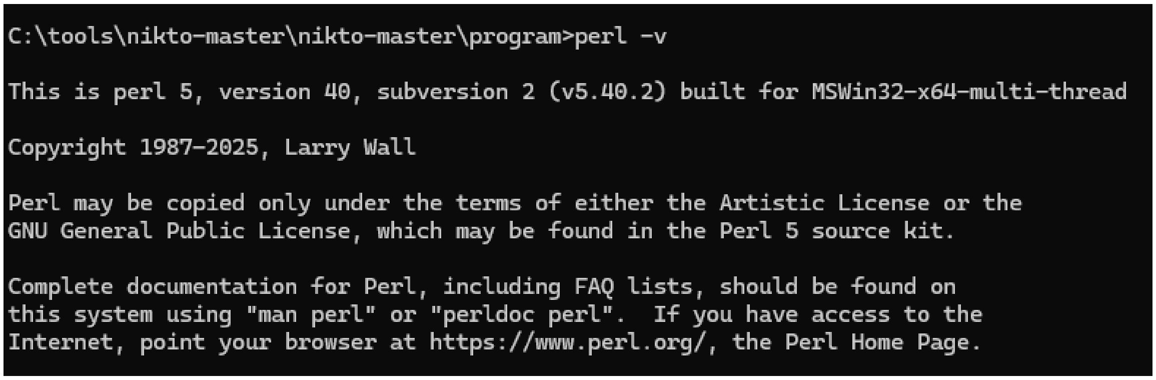
Breakdown:

Server Banner: `Server: Apache/2.4.29 (Ubuntu)` tells you the web server software and version. You can immediately search for known vulnerabilities affecting this version.

Missing Security Headers: Lines like `The anti-clickjacking X-Frame-Options header is not present.` point to missing security configurations that should be implemented.

OSVDB References: `OSVDB-3233` is a reference to the Open Source Vulnerability Database (now defunct, but the codes are still widely used). These indicate specific findings, such as default files (`/icons/README`) or potentially interesting pages (/test.php) that should be investigated further.

Output:



```
C:\tools\nikto-master\nikto-master\program>perl -v

This is perl 5, version 40, subversion 2 (v5.40.2) built for MSWin32-x64-multi-thread

Copyright 1987-2025, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the
GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on
this system using "man perl" or "perldoc perl".  If you have access to the
Internet, point your browser at https://www.perl.org/, the Perl Home Page.
```

# Check Perl version (after install) perl -v

# Navigate to Nikto directory

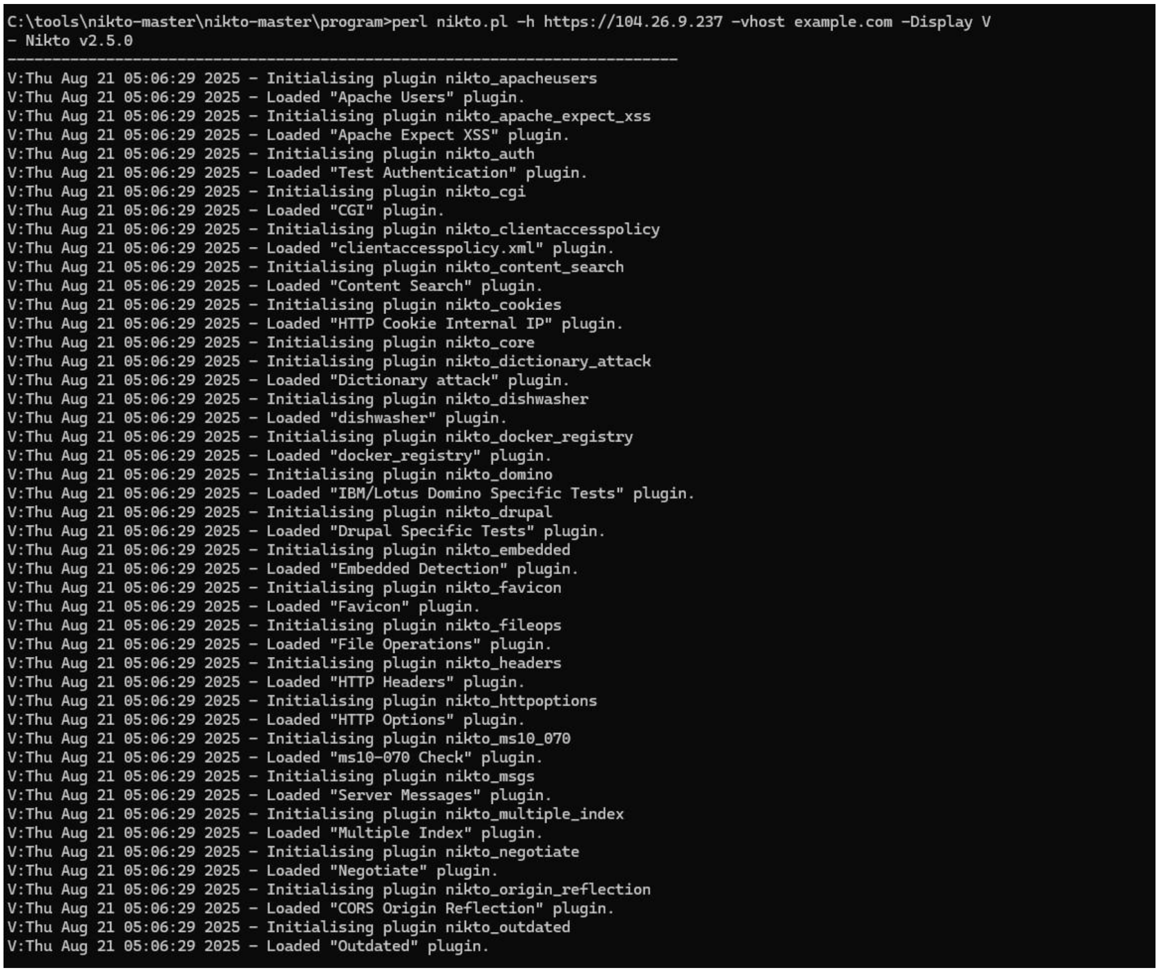
cd C:\tools\nikto-master\nikto-master\program # Run a

basic HTTP scan on a hostname

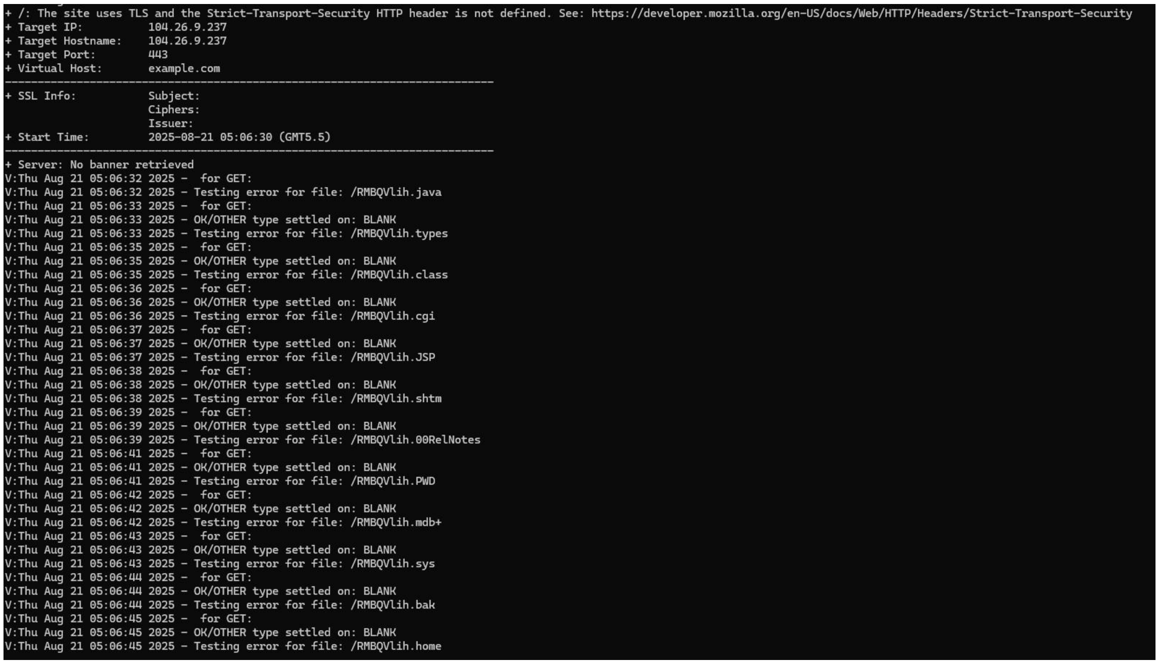
perl nikto.pl -h http://example.com # Run

HTTP scan on IP

perl nikto.pl -h http://104.26.9.237



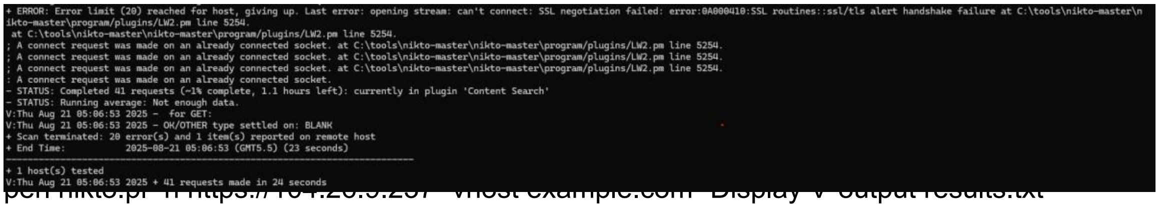
```
C:\tools\nikto-master\nikto-master\program>perl nikto.pl -h https://104.26.9.237 -vhost example.com -Display V
- Nikto v2.5.0
---------------------------------------------------------------------------
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_apacheusers
V:Thu Aug 21 05:06:29 2025 - Loaded "Apache Users" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_apache_expect_xss
V:Thu Aug 21 05:06:29 2025 - Loaded "Apache Expect XSS" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_auth
V:Thu Aug 21 05:06:29 2025 - Loaded "Test Authentication" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_cgi
V:Thu Aug 21 05:06:29 2025 - Loaded "CGI" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_clientaccesspolicy
V:Thu Aug 21 05:06:29 2025 - Loaded "clientaccesspolicy.xml" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_content_search
V:Thu Aug 21 05:06:29 2025 - Loaded "Content Search" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_cookies
V:Thu Aug 21 05:06:29 2025 - Loaded "HTTP Cookie Internal IP" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_core
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_dictionary_attack
V:Thu Aug 21 05:06:29 2025 - Loaded "Dictionary attack" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_dishwasher
V:Thu Aug 21 05:06:29 2025 - Loaded "dishwasher" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_docker_registry
V:Thu Aug 21 05:06:29 2025 - Loaded "docker_registry" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_domino
V:Thu Aug 21 05:06:29 2025 - Loaded "IBM/Lotus Domino Specific Tests" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_drupal
V:Thu Aug 21 05:06:29 2025 - Loaded "Drupal Specific Tests" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_embedded
V:Thu Aug 21 05:06:29 2025 - Loaded "Embedded Detection" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_favicon
V:Thu Aug 21 05:06:29 2025 - Loaded "Favicon" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_fileops
V:Thu Aug 21 05:06:29 2025 - Loaded "File Operations" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_headers
V:Thu Aug 21 05:06:29 2025 - Loaded "HTTP Headers" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_httpoptions
V:Thu Aug 21 05:06:29 2025 - Loaded "HTTP Options" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_ms10_070
V:Thu Aug 21 05:06:29 2025 - Loaded "ms10-070 Check" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_msgs
V:Thu Aug 21 05:06:29 2025 - Loaded "Server Messages" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_multiple_index
V:Thu Aug 21 05:06:29 2025 - Loaded "Multiple Index" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_negotiate
V:Thu Aug 21 05:06:29 2025 - Loaded "Negotiate" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_origin_reflection
V:Thu Aug 21 05:06:29 2025 - Loaded "CORS Origin Reflection" plugin.
V:Thu Aug 21 05:06:29 2025 - Initialising plugin nikto_outdated
V:Thu Aug 21 05:06:29 2025 - Loaded "Outdated" plugin.
```



```
+ /: 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
+ Target IP:          104.26.9.237
+ Target Hostname:    104.26.9.237
+ Target Port:        443
+ Virtual Host:       example.com
---------------------------------------------------------------------------
+ SSL Info:           Subject:
                      Ciphers:
                      Issuer:
+ Start Time:         2025-08-21 05:06:30 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
V:Thu Aug 21 05:06:32 2025 -  for GET:
V:Thu Aug 21 05:06:32 2025 - Testing error for file: /RMBQVlih.java
V:Thu Aug 21 05:06:33 2025 -  for GET:
V:Thu Aug 21 05:06:33 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:33 2025 - Testing error for file: /RMBQVlih.types
V:Thu Aug 21 05:06:35 2025 -  for GET:
V:Thu Aug 21 05:06:35 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:35 2025 - Testing error for file: /RMBQVlih.class
V:Thu Aug 21 05:06:36 2025 -  for GET:
V:Thu Aug 21 05:06:36 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:36 2025 - Testing error for file: /RMBQVlih.cgi
V:Thu Aug 21 05:06:37 2025 -  for GET:
V:Thu Aug 21 05:06:37 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:37 2025 - Testing error for file: /RMBQVlih.JSP
V:Thu Aug 21 05:06:38 2025 -  for GET:
V:Thu Aug 21 05:06:38 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:38 2025 - Testing error for file: /RMBQVlih.shtm
V:Thu Aug 21 05:06:39 2025 -  for GET:
V:Thu Aug 21 05:06:39 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:39 2025 - Testing error for file: /RMBQVlih.00RelNotes
V:Thu Aug 21 05:06:41 2025 -  for GET:
V:Thu Aug 21 05:06:41 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:41 2025 - Testing error for file: /RMBQVlih.PWD
V:Thu Aug 21 05:06:42 2025 -  for GET:
V:Thu Aug 21 05:06:42 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:42 2025 - Testing error for file: /RMBQVlih.mdb+
V:Thu Aug 21 05:06:43 2025 -  for GET:
V:Thu Aug 21 05:06:43 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:43 2025 - Testing error for file: /RMBQVlih.sys
V:Thu Aug 21 05:06:44 2025 -  for GET:
V:Thu Aug 21 05:06:44 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:44 2025 - Testing error for file: /RMBQVlih.bak
V:Thu Aug 21 05:06:45 2025 -  for GET:
V:Thu Aug 21 05:06:45 2025 - OK/OTHER type settled on: BLANK
V:Thu Aug 21 05:06:45 2025 - Testing error for file: /RMBQVlih.home
```

```
# Run HTTPS scan on IP with hostname (SNI)

perl nikto.pl -h https://104.26.9.237 -vhost example.com -Display V
```



```
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at C:\tools\nikto-master\n
ikto-master\program/plugins/LW2.pm line 5254.
 at C:\tools\nikto-master\nikto-master\program/plugins/LW2.pm line 5254.
; A connect request was made on an already connected socket. at C:\tools\nikto-master\nikto-master\program/plugins/LW2.pm line 5254.
; A connect request was made on an already connected socket. at C:\tools\nikto-master\nikto-master\program/plugins/LW2.pm line 5254.
; A connect request was made on an already connected socket. at C:\tools\nikto-master\nikto-master\program/plugins/LW2.pm line 5254.
: A connect request was made on an already connected socket.
- STATUS: Completed 41 requests (~1% complete, 1.1 hours left): currently in plugin 'Content Search'
- STATUS: Running average: Not enough data.
V:Thu Aug 21 05:06:53 2025 -  for GET:
V:Thu Aug 21 05:06:53 2025 - OK/OTHER type settled on: BLANK
+ Scan terminated: 20 error(s) and 1 item(s) reported on remote host
+ End Time:           2025-08-21 05:06:53 (GMT5.5) (23 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
V:Thu Aug 21 05:06:53 2025 + 41 requests made in 24 seconds
```

```
perl nikto.pl -h https://104.26.9.237 -vhost example.com -Display V -output results.txt
```

Conclusion:

This assignment demonstrates how to install and run Nikto for web server scanning.