Task 7 : Vulnerability Scanning with Nikto

Introduction

This task involves performing a vulnerability scan using **Nikto**, a widely used open-source web server scanner. The goal is to identify common security misconfigurations, insecure headers, outdated software, and directories that expose sensitive information.
The scan was executed on a local Apache server running on Kali Linux.

Objectives

-Install and configure Nikto.
-Scan a local web server (http://localhost).
-Identify security issues.
-Understand and document the vulnerabilities discovered.
-Provide remediation recommendations.

Tools used

-Nikto v2.5
-Apache2
-Kali Linux

Methodology

1. Installing Nikto

Nikto was installed using:

```
sudo apt install nikto
```

2. Starting the Local Web Server :

```
sudo systemctl start apache2
```

3. Running the Nikto Scan

Main scan command:

```
nikto -h http://localhost -o nikto_scan_results.txt
```

4. Reviewing the Output

The output file (nikto_scan_results.txt) was inspected using:

```
cat nikto_scan_results.txt
```

Findings

Based on your scan results, the following vulnerabilities were identified:

1. Missing X-Frame-Options Header
-This header prevents **clickjacking attacks**.
-Its absence means attackers can load your page inside an iframe.

2.Missing X-Content-Type-Options Header
-Without this header, browsers may MIME-sniff content incorrectly.
-This can lead to **XSS or malicious content rendering**.

3.Server Version Disclosure
-The server reveals:

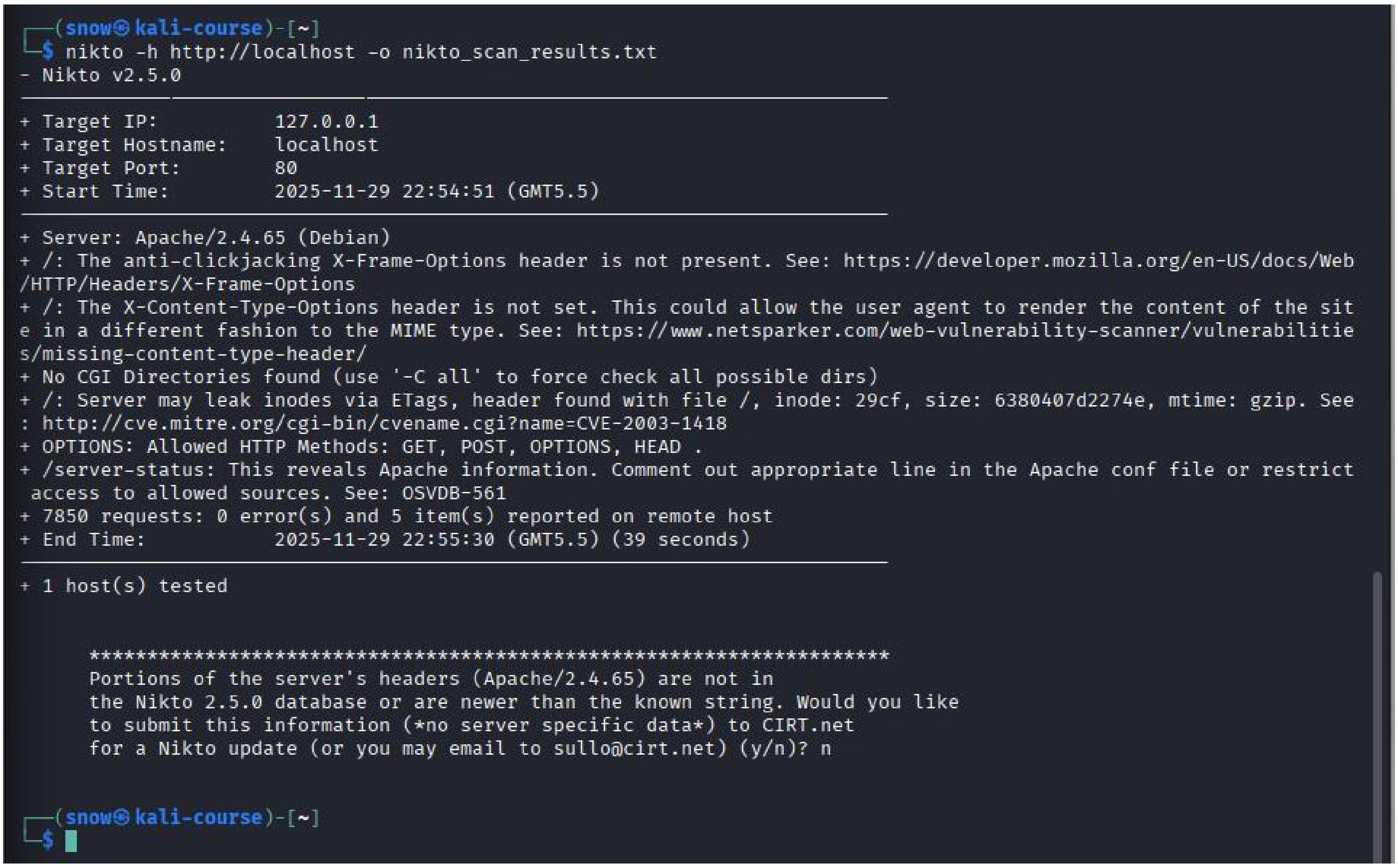
```
Apache/2.4.65 (Debian)
```

Exposing version info helps attackers match known exploits to your server.

4.ETag Leakage
-ETags enable fingerprinting and cache manipulation.
-Should be disabled on secure servers.
5.OPTIONS Method Enabled
-Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
-While not extremely dangerous, OPTIONS exposes server capabilities.

6. /server-status Page Exposed
/server-status: This reveals Apache information.
This page exposes:
-Active connections
-Server uptime
-IP addresses
-Running requests
-This is highly sensitive information and should not be publicly accessible.

Screenshots



```
┌──(snow㉿kali-course)-[~]
└─$ nikto -h http://localhost -o nikto_scan_results.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2025-11-29 22:54:51 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.65 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 6380407d2274e, mtime: gzip. See
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict
 access to allowed sources. See: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-11-29 22:55:30 (GMT5.5) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.65) are not in
      the Nikto 2.5.0 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n


┌──(snow㉿kali-course)-[~]
└─$ 
```

Remediation Recommendations

-Add Security Headers
Header always append X-Frame-Options SAMEORIGIN.
Header set X-Content-Type-Options nosniff.

-Hide Server Version
ServerTokens Prod.
ServerSignature Off.

-Disable ETags

```
FileETag None.
```

-Restrict or Disable /server-status

Option 1 (restrict):

```
<Directory "/server-status">
   Require local
</Directory>
```

Option 2 (disable):

```
sudo a2dismod status
```

Conclusion

The Nikto scan revealed multiple misconfigurations, missing security headers, and information disclosure weaknesses. These vulnerabilities could be exploited for reconnaissance, fingerprinting, clickjacking, and other attacks. Proper server hardening is strongly recommended.

This task helped develop a practical understanding of web server security assessment and the importance of secure configurations.