Nikto

Table of content	
1	*Introduction*
2	*What is Nikto?*
3	*Features of Nikto*
4	*Installation Steps*
5	*Basic Usage*
6	*Common Commands*
7	*Scan and Result Explanation*
8	*Real-World Use Case*
9	*Pros and Cons*
10	*Conclusion*
11	*References*

1.Introduction

In the field of cybersecurity, the reconnaissance phase is critical for gathering information about a target system. One of the most effective tools used for web server vulnerability scanning is Nikto. It is an open-source scanner that identifies known vulnerabilities, insecure files, outdated software, and configuration issues on web servers. Nikto plays a vital role in ethical hacking, penetration testing, and security assessments.

2. What is Nikto?

Nikto is a command-line based web server scanner written in Perl. It is designed to perform comprehensive tests on web servers to find vulnerabilities that could be exploited by attackers.

- *Developer: Sullo from cirt.net*
- *Language: Perl*
- *License: GPL (Open Source)*
- *Type: Web server vulnerability scanner*

It performs more than 6,700 security checks and is regularly updated to include new threats. Unlike general network scanners like Nmap, Nikto focuses entirely on the application layer, especially HTTP and HTTPS services.

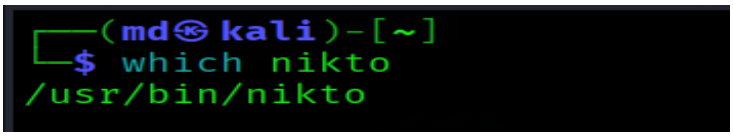
3. Features of Nikto

Nikto offers the following key features:

- *Scans for over 6,700 potentially dangerous files and programs*
- *Checks for outdated versions of over 1,250 servers*
- *Version-specific vulnerability identification*
- *Finds insecure HTTP methods (e.g., PUT, DELETE)*
- *SSL Support to test HTTPS services*
- *Detects directory indexing, open admin panels, and misconfigurations*
- *Proxy support for anonymity*
- *Exports scan results in text, HTML, XML, or CSV format*
- *Integration with Metasploit for further exploitation*

4. Installation Steps

- *If you're using kali linux, Nikto comes preinstall and will be present in "Vulerabilty Analysis" Category*



- *Installing Nikto on Ubuntu*

  $ sudo apt update

  $ sudo apt install nikto

- *Manual Installation from GitHub*

$ git clone https://github.com/sullo/nikto.git

$ cd nikto/program
$ perl nikto.pl -h

** Make sure you have Perl installed, as Nikto is a Perl-based tool.*

5. Basic Usage

Once Nikto is installed, you can use a simple command to scan a target web server for vulnerabilities. The most basic syntax is:
$ nikto -h http://<target-ip-or-domain>

Example :
$ nikto -h http://testphp.vulnweb.com

Explanation:

- *nikto: This is the command-line tool being executed.*
- *-h: Stands for host. This flag specifies the target web server's IP address or domain name.*
- *http://testphp.vulnweb.com: This is the target web server being scanned.*
-

When this command is run, Nikto performs a vulnerability scan on the specified web server. It checks for:

- *Exposed or sensitive files and directories*
- *Insecure HTTP headers*
- *Outdated server software*
- *Known vulnerabilities (CVEs)*
- *Configuration issues*

The scan results are displayed directly in the terminal and help identify potential security weaknesses that could be exploited.

6.Common Command

```
┌──(md㉿kali)-[~]
└─$ nikto -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-a/"
       -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)
```

Some basic command of Nikto are:

-h	***Host or IP address to scan***
-p	***Port to scan (default is 80)***
-Tuning	***Choose types of tests (0–9 or 'a' for all)***
-ssl	***Enable SSL scan (for HTTPS)***
-Format	***Set output format (txt, html, xml, csv)***
-output	***Save output to a file***
-useragent	***Set custom User-Agent string***
-useproxy	***Use a proxy for scanning***

7.Scan and Result Explanation

7.1 Scan a Domain

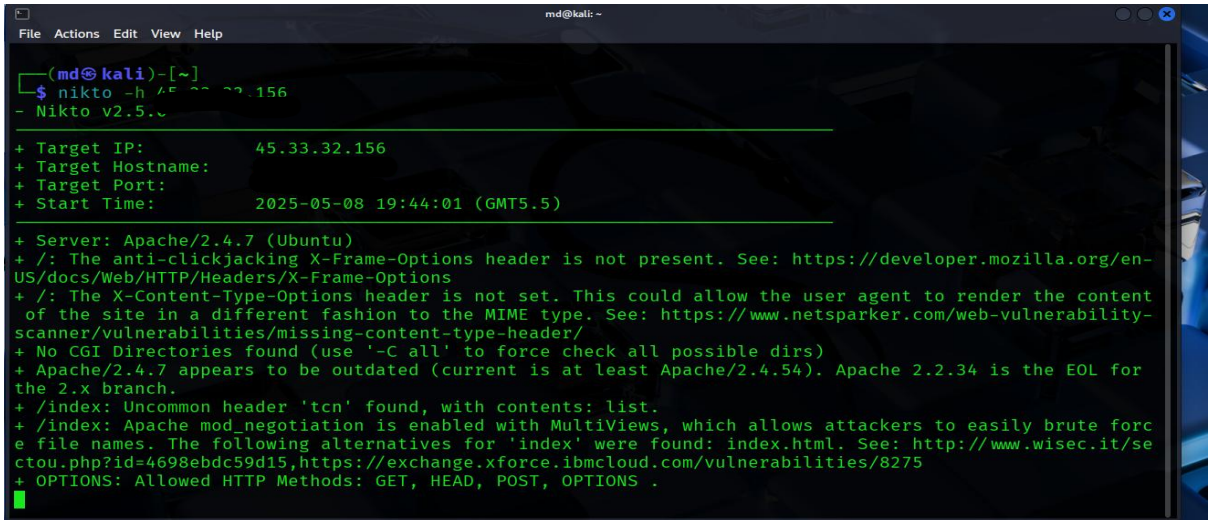
```
md@kali: ~
File  Actions  Edit  View  Help

┌──(md㉿kali)-[~]
└─$ nikto -h http://testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2025-05-08 19:33:39 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: 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 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

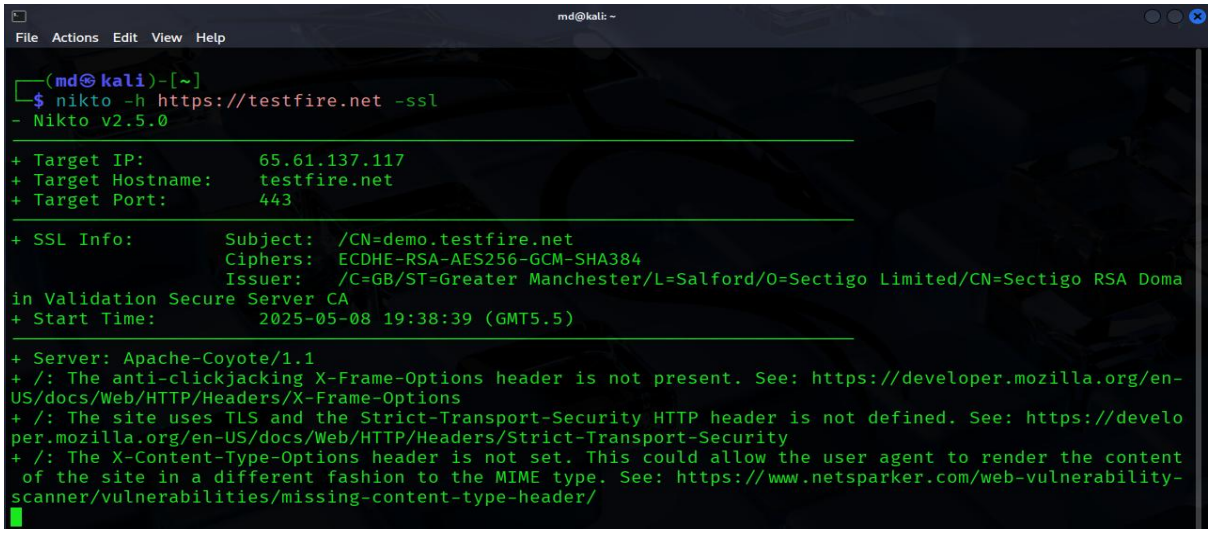
Identified Vulnerabilities/Warnings:

- *Missing X-Frame-Options Header:*
  - *Description: The "X-Frame-Options" HTTP response header is absent.*
  - *Impact: This vulnerability could allow for "clickjacking" attacks, where an attacker embeds the vulnerable site within an <iframe> on their malicious page, potentially tricking users into unintended actions.*
- *Missing X-Content-Type-Options Header:*
  - *Description: The "X-Content-Type-Options" HTTP response header is not set.*
  - *Impact: This issue can lead to MIME-type sniffing vulnerabilities, where browsers might misinterpret content, potentially executing malicious scripts.*

7.2 Scan IP Address



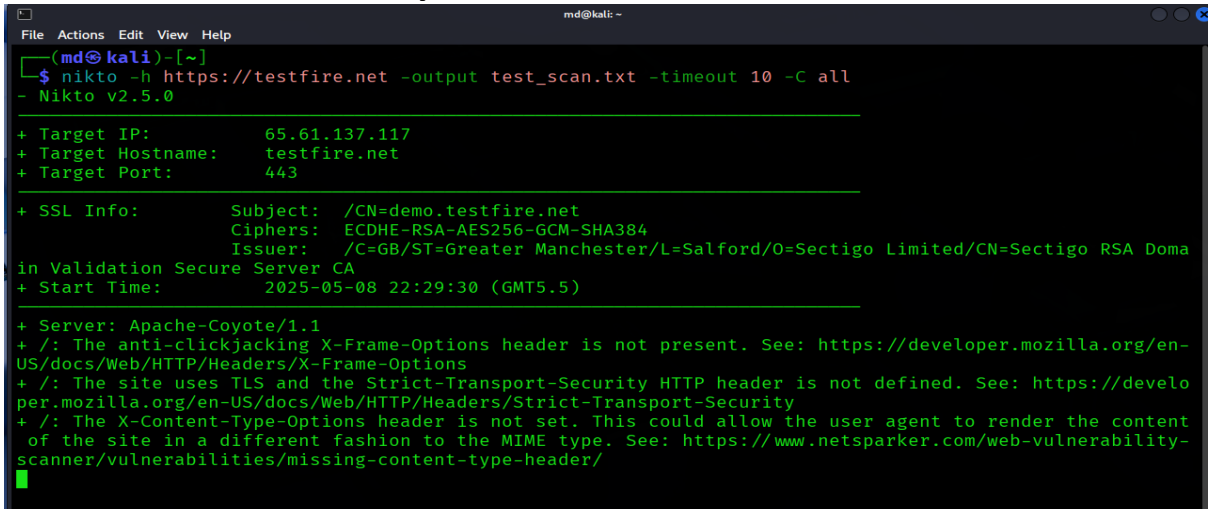
7.3 Scan Domain with SSL Enable



Identified Vulnerabilities/Warnings:

- *Missing X-Frame-Options Header:*
  - *Description: The "X-Frame-Options" HTTP response header is absent.*
  - *Impact: This vulnerability could allow for "clickjacking" attacks, where an attacker embeds the vulnerable site within an <iframe> on their malicious page, potentially tricking users into unintended actions.*
- *Missing Strict-Transport-Security (HSTS) Header:*
  - *Description: The "Strict-Transport-Security" (HSTS) HTTP header is not defined.*
  - *Impact: Without HSTS, browsers might still attempt to connect to the site over insecure HTTP before being redirected to HTTPS, making the initial connection vulnerable to downgrade attacks (e.g., SSL stripping). HSTS forces browsers to always use HTTPS for future connections to the site.*
- *Missing X-Content-Type-Options Header:*
  - *Description: The "X-Content-Type-Options" HTTP response header is not set.*
  - *Impact: This issue can lead to MIME-type sniffing vulnerabilities, where browsers might misinterpret content, potentially executing malicious scripts.*

7.4 Scan with Custom Options



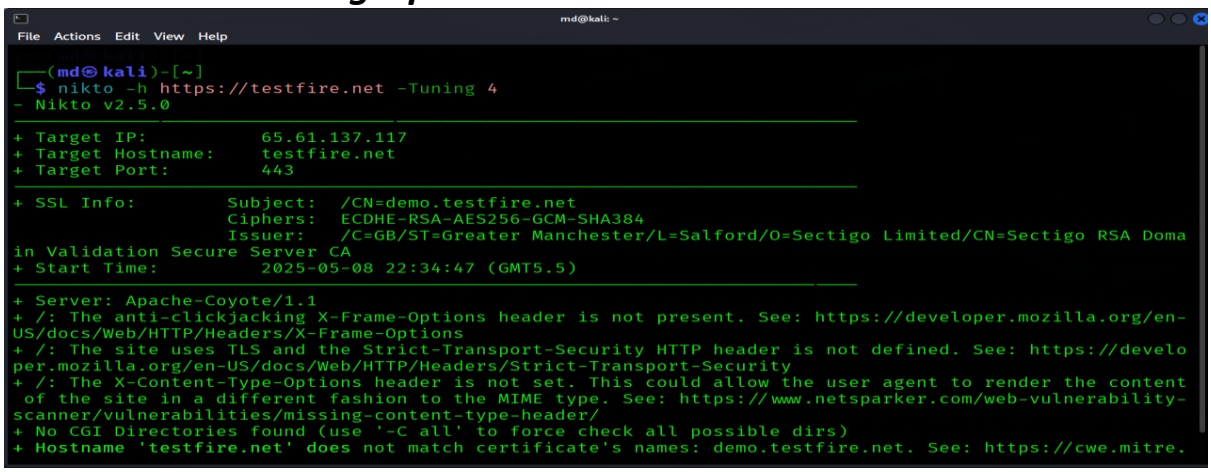
Identified Vulnerabilities/Warnings:

- *Missing X-Frame-Options Header:*
  - *Description: The "X-Frame-Options" HTTP response header is absent.*
  - *Impact: This vulnerability could allow for "clickjacking" attacks,*

where an attacker embeds the vulnerable site within an <iframe> on their malicious page, potentially tricking users into unintended actions.

- *Missing Strict-Transport-Security (HSTS) Header:*
  - *Description: The "Strict-Transport-Security" (HSTS) HTTP header is not defined.*
  - *Impact: Without HSTS, browsers might still attempt to connect to the site over insecure HTTP before being redirected to HTTPS, making the initial connection vulnerable to downgrade attacks (e.g., SSL stripping). HSTS forces browsers to always use HTTPS for future connections to the site.*
- *Missing X-Content-Type-Options Header:*
  - *Description: The "X-Content-Type-Options" HTTP response header is not set.*
  - *Impact: This issue can lead to MIME-type sniffing vulnerabilities, where browsers might misinterpret content, potentially executing malicious scripts.*

7.5 Scan with Tuning Option



Identified Vulnerabilities/Warnings:

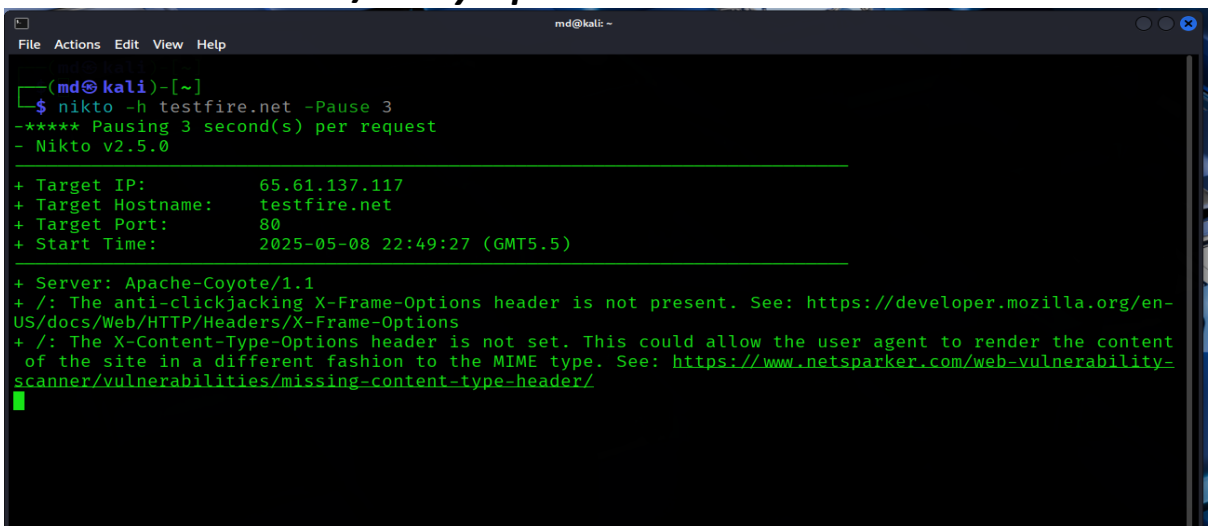
- *Missing X-Frame-Options Header:*
  - *Description: The "X-Frame-Options" HTTP response header is absent.*
  - *Impact: This vulnerability could allow for "clickjacking" attacks, where an attacker embeds the vulnerable site within an <iframe> on their malicious page, potentially tricking users into unintended actions.*
- *Missing Strict-Transport-Security (HSTS) Header:*
  - *Description: The "Strict-Transport-Security" (HSTS) HTTP header is*

not defined.

- *Impact: Without HSTS, browsers might still attempt to connect to the site over insecure HTTP before being redirected to HTTPS, making the initial connection vulnerable to downgrade attacks (e.g., SSL stripping). HSTS forces browsers to always use HTTPS for future connections to the site.*

- *Missing X-Content-Type-Options Header:*
  - *Description: The "X-Content-Type-Options" HTTP response header is not set.*
  - *Impact: This issue can lead to MIME-type sniffing vulnerabilities, where browsers might misinterpret content, potentially executing malicious scripts.*
- *No CGI Directories found:*
  - *Note: This indicates that Nikto did not find any common CGI directories (which might host vulnerable scripts) during the scan. The output suggests using -C all for a more exhaustive check of all possible directories.*
- *Hostname does not match certificate's name:*
  - *Description: The hostname testfire.net used to access the site does not exactly match the Common Name (CN=demo.testfire.net) specified in the SSL certificate.*
  - *Impact: While often benign in test environments, in a production setting, this mismatch can trigger security warnings in browsers and may indicate a misconfiguration or, in some cases, a potential man-in-the-middle attack if the certificate is not genuinely issued for the domain being accessed.*

7.6 Scan with Pause/Delay Option



Identified Vulnerabilities/Warnings:

- *Missing X-Frame-Options Header:*
  - *Description: The "X-Frame-Options" HTTP response header is absent.*
  - *Impact: This vulnerability could allow for "clickjacking" attacks, where an attacker embeds the vulnerable site within an <iframe> on their malicious page, potentially tricking users into unintended actions.*
- *Missing X-Content-Type-Options Header:*
  - *Description: The "X-Content-Type-Options" HTTP response header is not set.*
  - *Impact: This issue can lead to MIME-type sniffing vulnerabilities, where browsers might misinterpret content, potentially executing malicious scripts.*

8. Real-World Use Case

Let's say you're performing a penetration test for a client's e-commerce site. Using Nmap, you find that port 80 and 443 are open. You then use Nikto on those ports:

$ nikto -h https://clientsite.com

Nikto finds that:

- *Apache is outdated*
- *phpinfo.php is publicly accessible*
- *PUT method is enabled (could allow file uploads)*
  - *You include this in your report with remediation steps, helping the client secure their server before a real attacker finds it.*

9. Pros and Cons

Advantages	***Limitations***
Free and open source	*Not stealthy (easily detectable)*
Easy to use for beginners	*Can generate false positives*
Fast and comprehensive	*Limited to known vulnerabilities*

Supports plugins and customization	*Doesn't exploit vulnerabilities – only scans*
Supports multiple output formats	*No advanced scanning like authenticated access*

10. Conclusion

*Nikto is an effective tool for quickly identifying web server vulnerabilities. It's a must-have for beginner and intermediate cybersecurity professionals, especially during the reconnaissance phase. While it's not stealthy or as advanced as tools like **Burp Suite**, it's still a highly respected tool for automated web server analysis. When used alongside tools like **Nmap**, it can significantly improve the efficiency and depth of a security assessment.*

11. References

- 📘 ***Nikto Official GitHub Repository***
- 🌐 ***Nikto Official Website***
- 📖 ***OWASP Web Security Testing Guide***