Nikto Web Server Scanning – Lab Report

Introduction

Nikto is an open-source **web server vulnerability scanner**. It works by sending thousands of HTTP/HTTPS requests to a web server and comparing the responses against a database of known security issues. These issues include outdated software, insecure files, misconfigured settings, and potentially dangerous scripts.

In this lab, several Nikto commands were used to understand how different options affect scanning behavior and report output

Tool Used

Nikto – an open-source web server vulnerability scanning tool used to detect:

- Web server misconfigurations
- Outdated software and plugins
- Insecure files and directories
- Known vulnerabilities

Commands Used, Explanation, and Screenshots

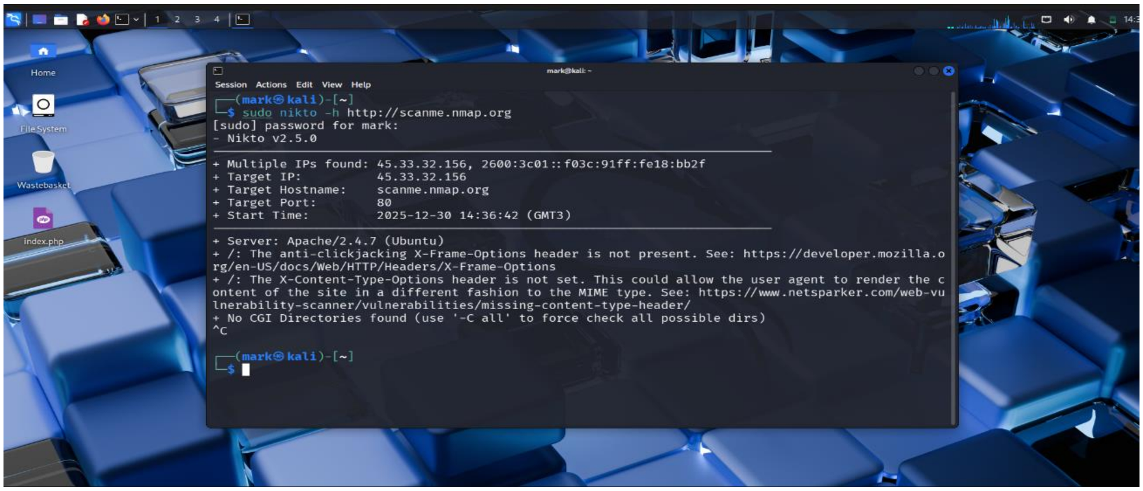
1. Basic Website Scan

sudo nikto -h scanme.nmap.org

This command performs a basic vulnerability scan on the target website. Nikto checks for common vulnerabilities, outdated software, and insecure server configurations.

Screenshot

📷 *Figure 1: Nikto basic scan output for scanme.nmap.org*



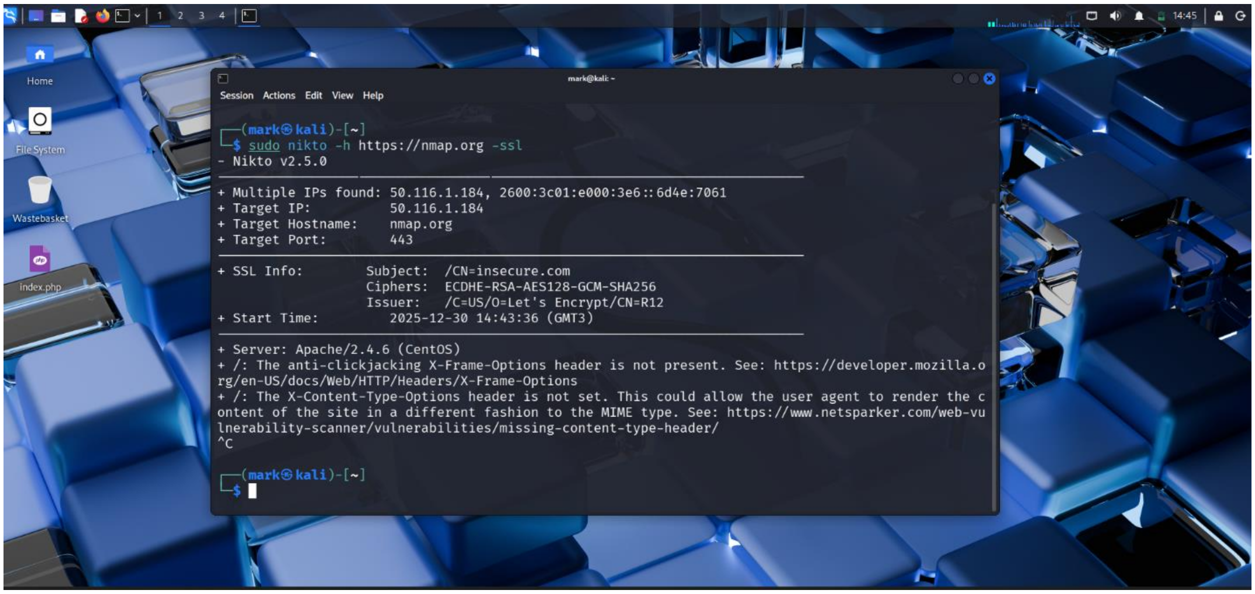
```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org
[sudo] password for mark:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 14:36:42 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
^C

┌──(mark㉿kali)-[~]
└─$ 
```

2. SSL (HTTPS) Scan

sudo nikto -h https://nmap.org -ssl

This command scans a website using HTTPS. The -ssl option forces Nikto to establish a secure connection when scanning SSL-enabled web servers.

Screenshot
📸 *Figure 2: Nikto SSL scan output for https://nmap.org*



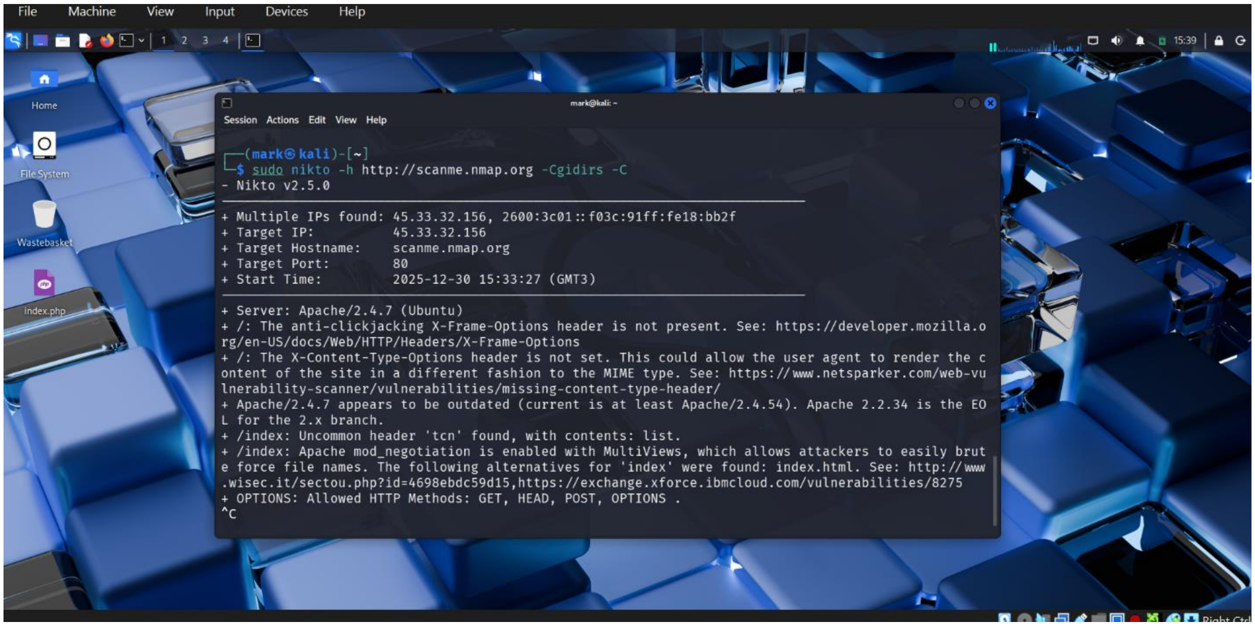
```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h https://nmap.org -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
+ Target IP:          50.116.1.184
+ Target Hostname:    nmap.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=insecure.com
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R12
+ Start Time:         2025-12-30 14:43:36 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ 
```

3. CGI Directory Scan

sudo nikto -h http://scanme.nmap.org -Cgidirs -C

This command checks for vulnerable or misconfigured CGI directories on the target web server. CGI scripts are often targeted by attackers if not properly secured.

Screenshot
📸 *Figure 3: CGI directories scan results*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -Cgidirs -C
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 15:33:27 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EO
L for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brut
e force file names. The following alternatives for 'index' were found: index.html. See: http://www
.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
^C
```

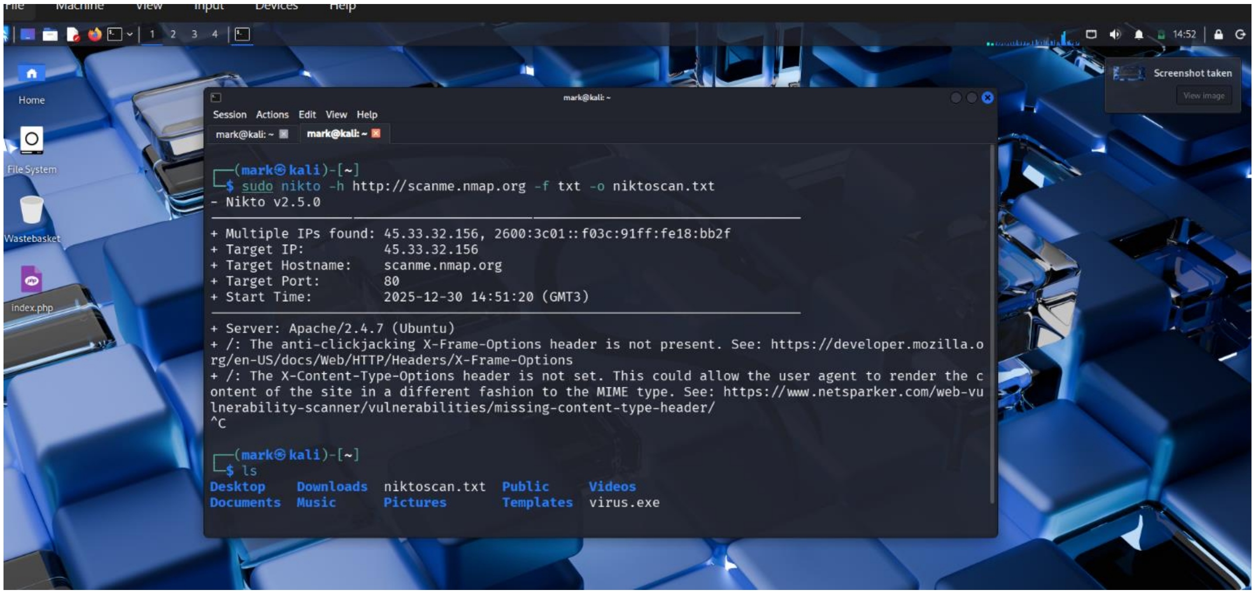
4. Scan Report in Text Format

sudo nikto -h http://scanme.nmap.org txt -o niktoscan.txt

This command saves the scan results in a plain text file, making it easy to review and include in written lab reports.

Screenshot

📸 *Figure 4: Nikto scan saved in TXT format (niktoscan.txt)*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -f txt -o niktoscan.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 14:51:20 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ ls
Desktop    Downloads  niktoscan.txt  Public     Videos
Documents  Music      Pictures       Templates  virus.exe
```

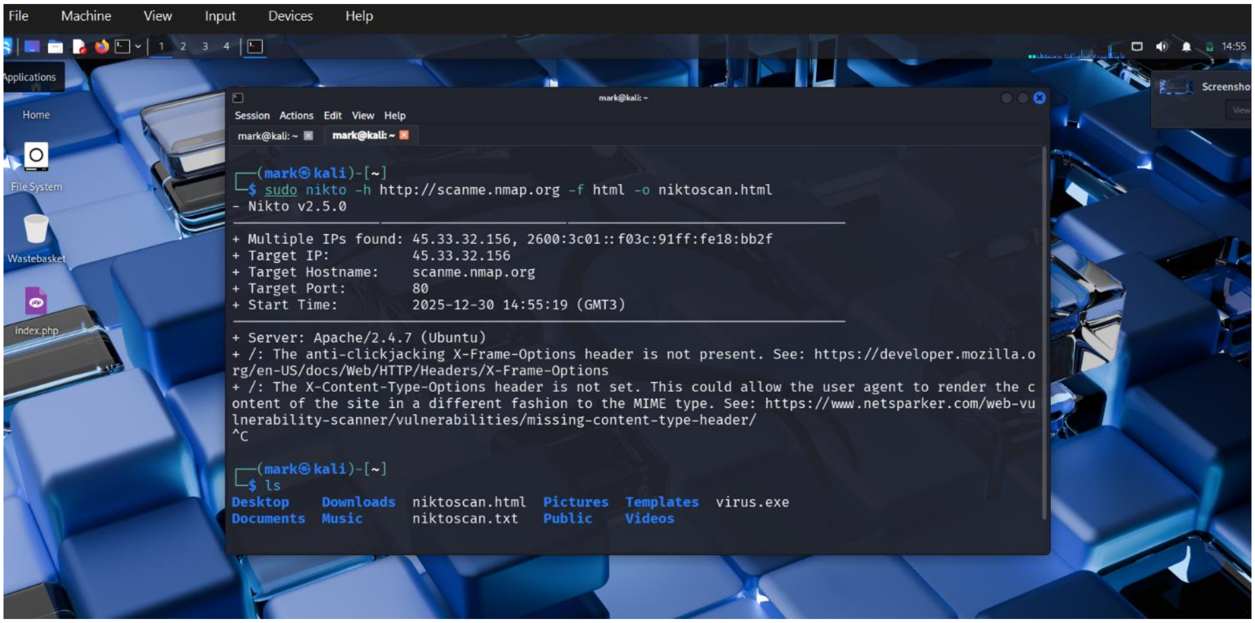
5. Scan Report in HTML Format

sudo nikto -h http://scanme.nmap.org -f html -o niktoscan.html

This command outputs the scan results in HTML format. The report can be opened in a web browser and provides a clean, readable layout.

Screenshot

📷 *Figure 5: Nikto HTML report displayed in a web browser*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -f html -o niktoscan.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 14:55:19 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ ls
Desktop    Downloads  niktoscan.html  Pictures  Templates  virus.exe
Documents  Music      niktoscan.txt   Public    Videos
```

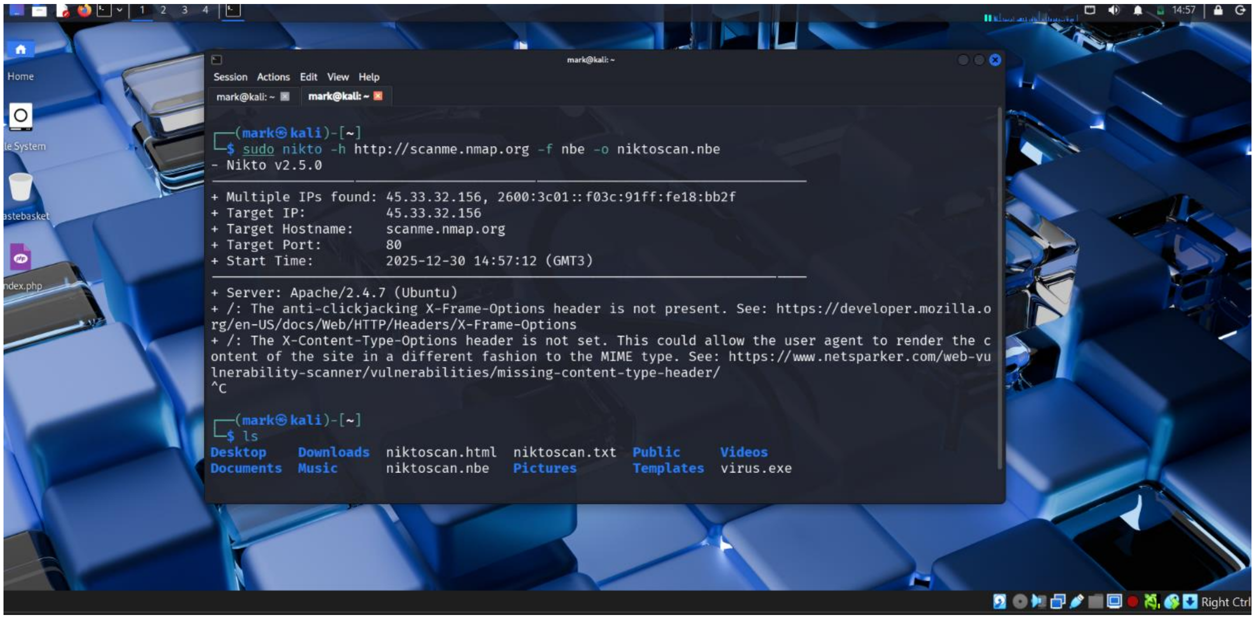
6. Scan Report in Nessus (NBE) Format

sudo nikto -h http://scanme.nmap.org -f nbe -o niktoscan.nbe

This command exports the scan results in Nessus NBE format, which can be imported into vulnerability management tools such as Nessus for further analysis.

Screenshot

📷 *Figure 6: Nikto scan output* saved *in NBE format*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -f nbe -o niktoscan.nbe
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 14:57:12 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ ls
Desktop    Downloads  niktoscan.html  niktoscan.txt  Public     Videos
Documents  Music      niktoscan.nbe   Pictures       Templates  virus.exe
```

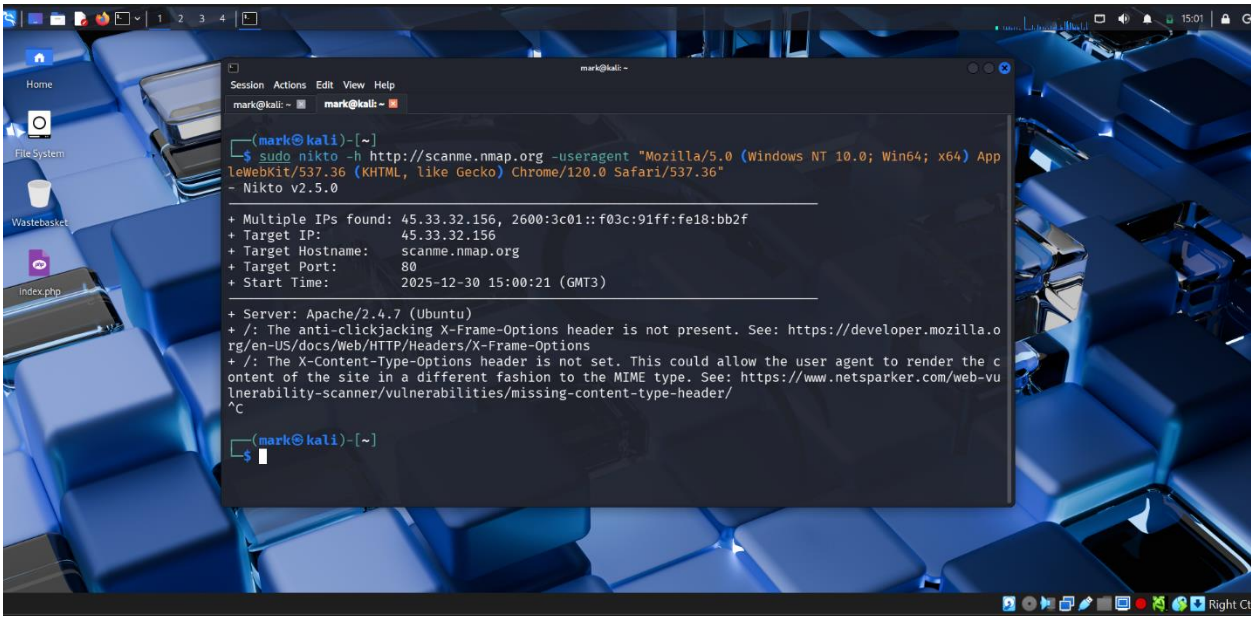
7. User-Agent Control

sudo nikto -h http://scanme.nmap.org -useragent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0 Safari/537.36"

This command runs a Nikto vulnerability scan on a website while making Nikto pretend to be a Google Chrome browser instead of identifying itself as a security scanner.

Screenshot

📷 *Figure 7: Nikto User-Agent configuration output*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -useragent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
leWebKit/537.36 (KHTML, like Gecko) Chrome/120.0 Safari/537.36"
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 15:00:21 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ 
```

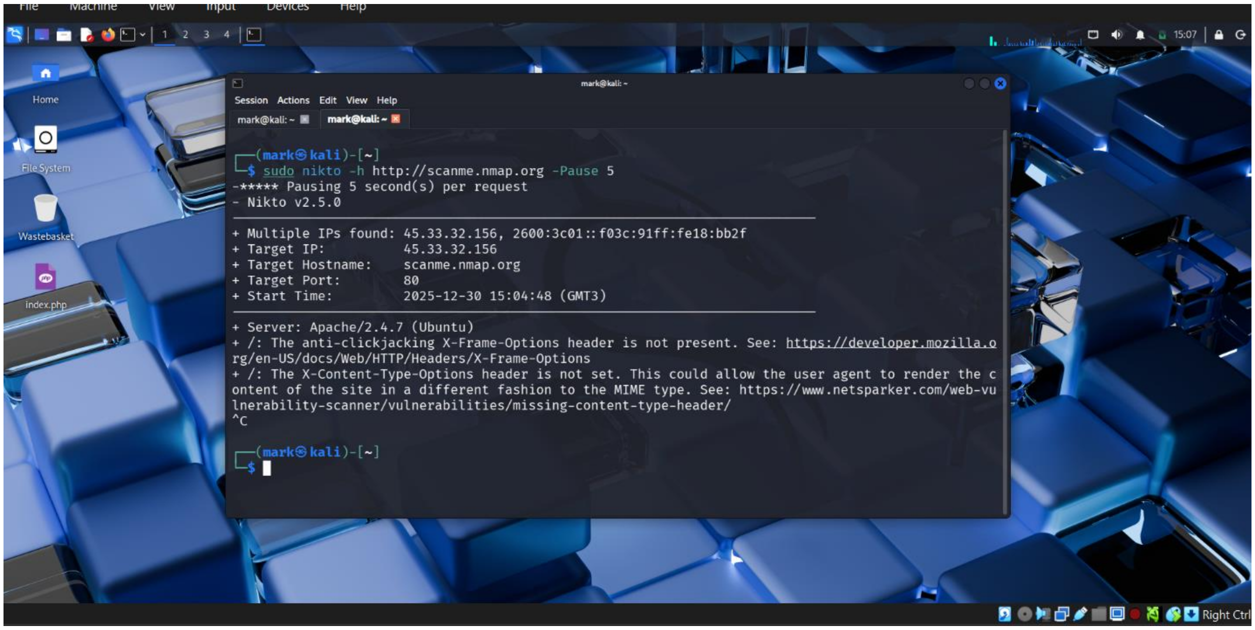
8. Scan Delay (Pause Option)

sudo nikto -h http://scanme.nmap.org -Pause 5

This command introduces a 5-second delay between requests. Slowing down the scan helps reduce server load and avoids triggering intrusion detection systems.

Screenshot

📷 *Figure 8: Nikto scan showing delayed requests*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -Pause 5
-***** Pausing 5 second(s) per request
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 15:04:48 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.o
rg/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 c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vu
lnerability-scanner/vulnerabilities/missing-content-type-header/
^C

┌──(mark㉿kali)-[~]
└─$ 
```

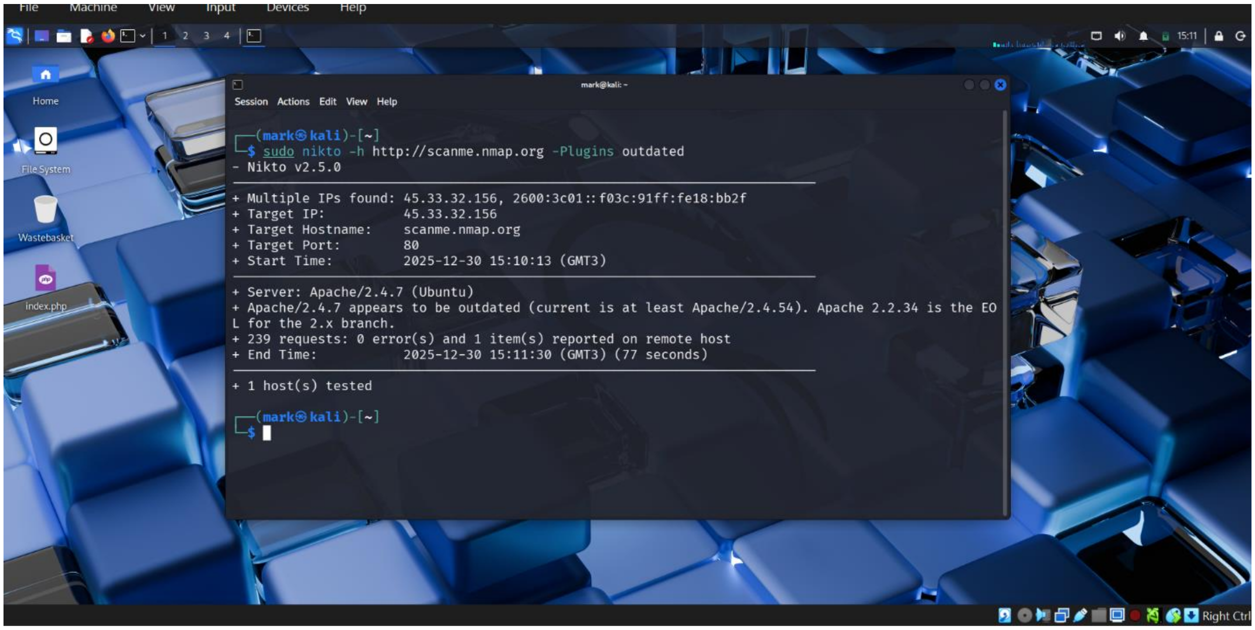
9. Outdated Plugins Scan

sudo nikto -h http://scanme.nmap.org -Plugins outdated

This command checks only for outdated plugins and components running on the web server, which may contain known vulnerabilities.

Screenshot

📷 *Figure 9: Nikto outdated plugins scan results*



```
┌──(mark㉿kali)-[~]
└─$ sudo nikto -h http://scanme.nmap.org -Plugins outdated
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-30 15:10:13 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EO
L for the 2.x branch.
+ 239 requests: 0 error(s) and 1 item(s) reported on remote host
+ End Time:           2025-12-30 15:11:30 (GMT3) (77 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(mark㉿kali)-[~]
└─$ 
```

Conclusion

In this lab, Nikto was used to perform web server vulnerability scanning using different options and output formats. The scans helped identify potential security weaknesses, outdated components, and misconfigurations. Proper use of Nikto is essential for effective web security assessment and penetration testing. The website used was a vulnerable and was designed to be scanned for testing purposes.