

Nikto Web Vulnerability Scan

This lab demonstrates how to set up and run a vulnerability scan using Nikto against a vulnerable machine (Metasploitable). The goal is to identify insecure configurations, outdated software, and common web vulnerabilities.

Lab Setup: -

Attacker Machine: Kali Linux (Nikto pre-installed)

- Target Machine: Metasploitable 2/3 (vulnerable web services)

- Network: Host-Only or NAT (ensure both VMs are on the same network)

Step 1: Identify IP Addresses

Run the following command on both Kali and Metasploitable to identify IPs: ifconfig

Example:

- Kali: 192.168.56.101

- Metasploitable: 192.168.56.102

Step 2: Verify Target Web Service

On Kali, open a browser and visit:

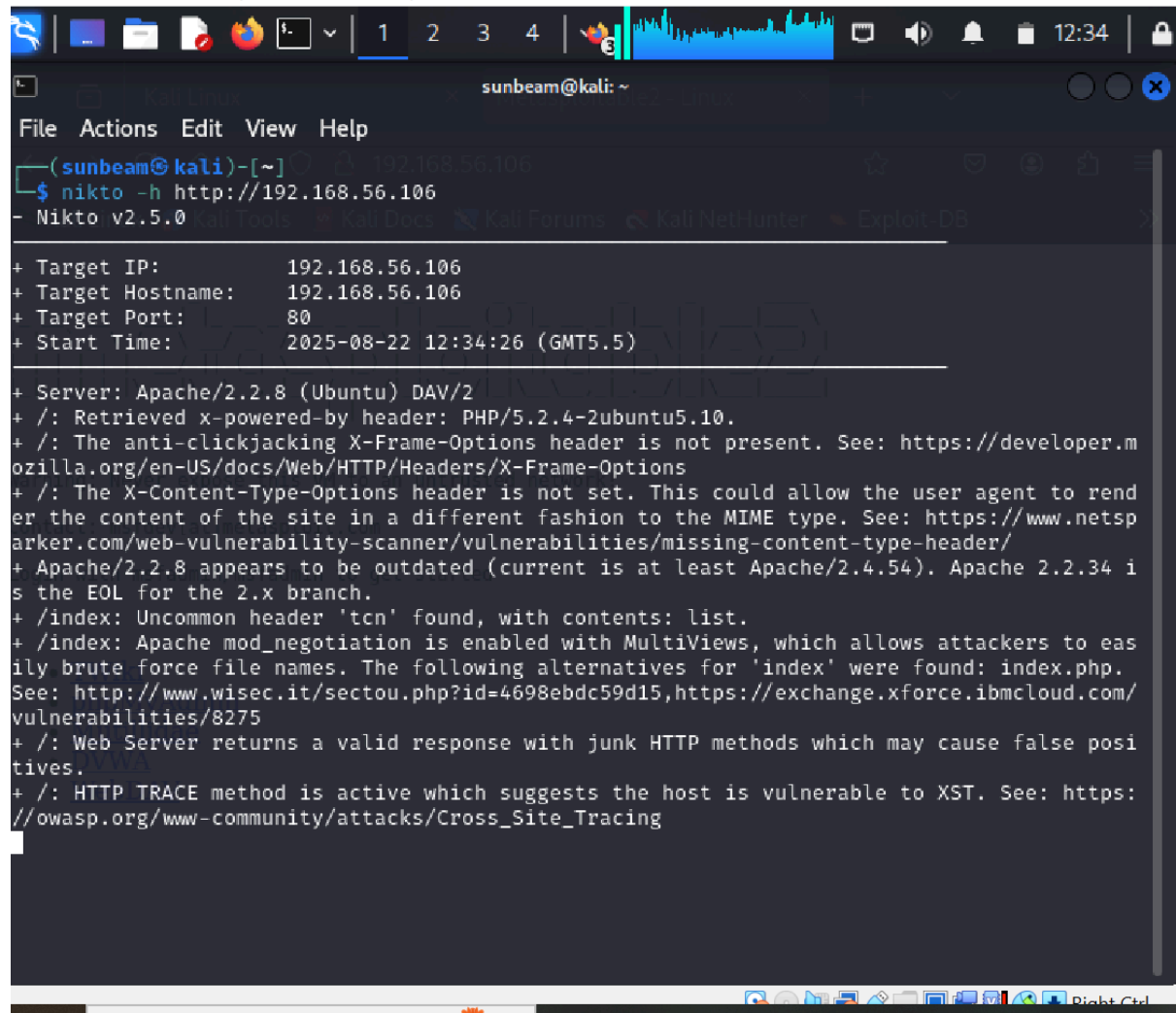
http://192.168.56.102

You should see the Metasploitable default web page.

Step 3: Run Nikto Scan

Basic Scan:

nikto -h http://192.168.56.102



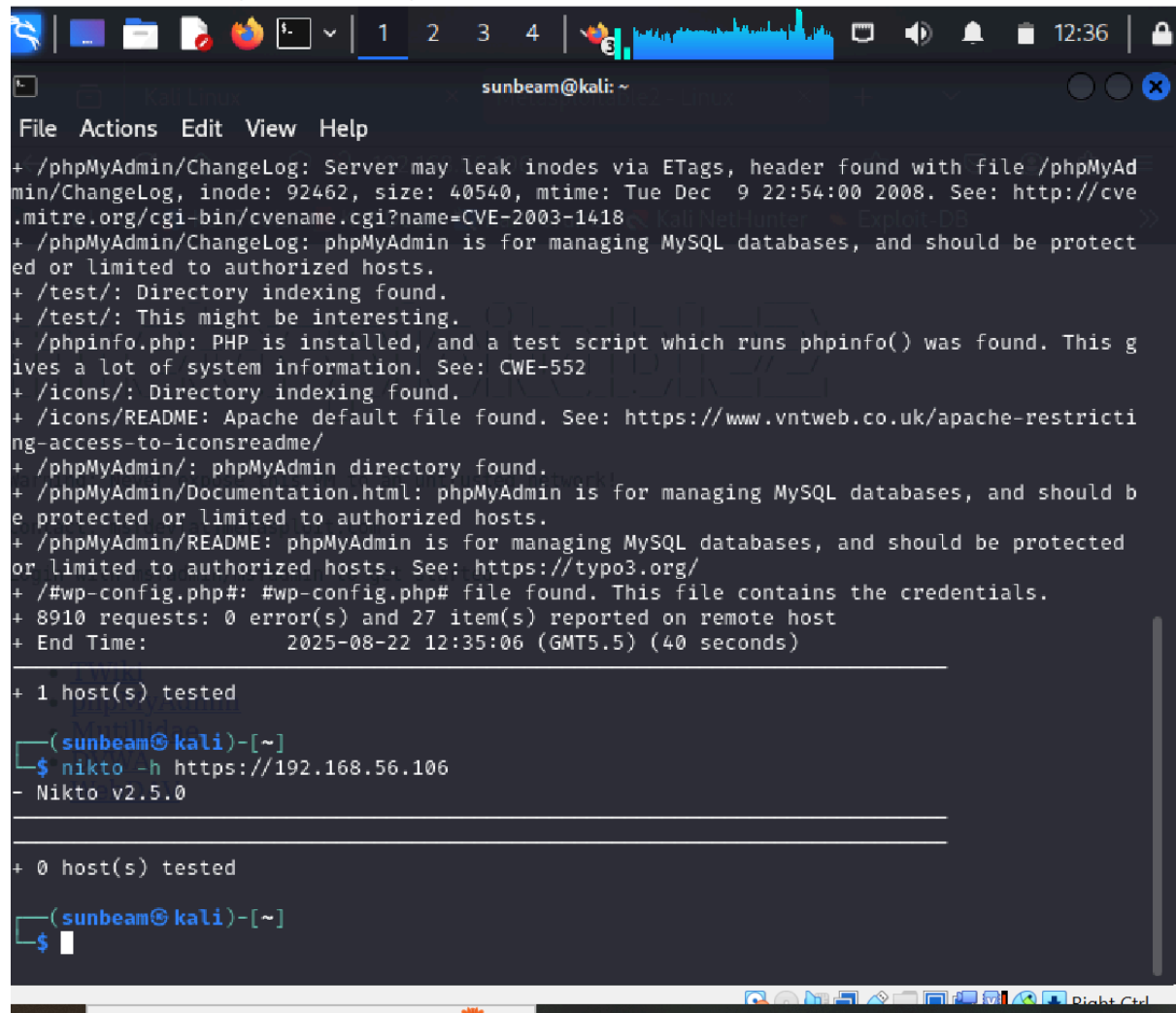
```
(sunbeam@kali)-[~]
$ nikto -h http://192.168.56.106
- Nikto v2.5.0

+ Target IP: 192.168.56.106
+ Target Hostname: 192.168.56.106
+ Target Port: 80
+ Start Time: 2025-08-22 12:34:26 (GMT5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL 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 brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
```

SSL Scan:

nikto -h <https://192.168.56.106>



```
File Actions Edit View Help
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAd
min/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 22:54:00 2008. See: http://cve
.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protect
ed or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This g
ives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricti
ng-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should b
e protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected
or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-08-22 12:35:06 (GMT5.5) (40 seconds)

+ 1 host(s) tested

(sunbeam@kali)-[~]
$ nikto -h https://192.168.56.106
- Nikto v2.5.0

+ 0 host(s) tested

(sunbeam@kali)-[~]
$
```

Specify Port:

nikto -h https://192.168.56.106 -p 8080

```
nikto -h http://192.168.56.102 -o nikto_report.html -Format html
```

```
kali new (freshmachine) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
sunbeam@kali: ~
File Actions Edit View Help
$ nikto -h http://192.168.56.106 -p 8080
- Nikto v2.5.0
- ERROR: The -port option cannot be used with a full URI
(sunbeam@kali)-[~]
$ nikto -h http://192.168.56.106 -o nikto_report.html -Formate html
Unknown option: Formate
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)
```

Step 4: Analyze Results

Nikto will provide details such as:

- Outdated software versions
- Insecure HTTP methods (PUT, DELETE)
- Interesting files (/phpmyadmin, /test, /robots.txt)
- CVE references

Step 5: Reporting

Include in your report:

- Screenshots of Nikto command execution
- Highlight detected CVEs and vulnerabilities
- Suggested remediation (e.g., patch Apache, disable risky methods)

Conclusion: This lab shows how Nikto can be used to quickly identify web application vulnerabilities. The results should always be validated and followed by recommended remediation steps.

