mrRobot

└─\$ nmap -T4 -p- -A 192.168.103.150

130 ×

Starting Nmap 7.91 (https://nmap.org) at 2021-03-09 10:38 EST

Nmap scan report for 192.168.103.150

Host is up (0.0014s latency). Not shown: 65532 filtered ports PORT STATE SERVICE VERSION

22/tcp closed ssh

80/tcp open http Apache httpd |_http-server-header: Apache

| http-title: Site doesn't have a title (text/html).

443/tcp open ssl/http Apache httpd

| http-server-header: Apache

| http-title: Site doesn't have a title (text/html).

| ssl-cert: Subject: commonName=<u>www.example.com</u>

| Not valid before: 2015-09-16T10:45:03 | Not valid after: 2025-09-13T10:45:03

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.

Nmap done: 1 IP address (1 host up) scanned in 103.03 seconds

22/tcp

80/tcp

Nikto

-\$ nikto -h 'http://192.168.103.150'

- Nikto v2.1.6

+ Target IP: 192.168.103.150 + Target Hostname: 192.168.103.150

+ Target Port: 80

+ Start Time: 2021-03-09 10:46:32 (GMT-5)

- + Server: Apache
- + 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
- + Retrieved x-powered-by header: PHP/5.5.29
- + No CGI Directories found (use '-C all' to force check all possible dirs)
- + Uncommon header 'tcn' found, with contents: list

- + Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.php
- + OSVDB-3092: /admin/: This might be interesting...
- + Uncommon header 'link' found, with contents: http://192.168.103.150/?p=23; rel=shortlink
- + /wp-links-opml.php: This WordPress script reveals the installed version.
- + OSVDB-3092: /license.txt: License file found may identify site software.
- + /admin/index.html: Admin login page/section found.
- + Cookie wordpress test cookie created without the httponly flag
- + /wp-login/: Admin login page/section found.
- + /wordpress: A Wordpress installation was found.
- + /wp-admin/wp-login.php: Wordpress login found
- + /wordpresswp-admin/wp-login.php: Wordpress login found
- + /blog/wp-login.php: Wordpress login found
- + /wp-login.php: Wordpress login found
- + /wordpresswp-login.php: Wordpress login found
- + 7915 requests: 0 error(s) and 18 item(s) reported on remote host
- + End Time: 2021-03-09 10:48:47 (GMT-5) (135 seconds)

PHP/5.5.29

Dirbuster

admin

audio

bloa

comments

feed

image

Image

images

login

video

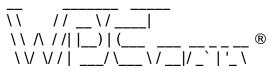
wp-content

wp-login

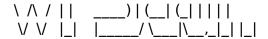
cat dirs| grep -E '^Dir'| grep 200| cut -d '/' -f 2 | sort|uniq

Wpscan

\$\text{L-\$ wpscan --url \(\text{http://192.168.103.150/} \)







WordPress Security Scanner by the WPScan Team Version 3.8.15

Sponsored by Automattic - https://automattic.com/ @ WPScan , @ethicalhack3r, @erwan Ir, @firefart

[+] URL: http://192.168.103.150/ [192.168.103.150]

[+] Started: Tue Mar 9 11:37:53 2021

Interesting Finding(s):

[+] Headers

| Interesting Entries: | - Server: Apache

| - X-Mod-Pagespeed: 1.9.32.3-4523 | Found By: Headers (Passive Detection)

I Confidence: 100%

[+] robots.txt found: http://192.168.103.150/robots.txt

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.103.150/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

I References:

- | http://codex.wordpress.org/XML-RPC Pingback API
- | https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
- I https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
- | https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
- I https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.103.150/readme.html

| Found By: Direct Access (Aggressive Detection)

I Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.103.150/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

- | https://www.iplocation.net/defend-wordpress-from-ddos
- | https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.25 identified (Latest, released on 2020-10-29).

| Found By: Emoji Settings (Passive Detection)

- http://192.168.103.150/7adcb59.html, Match: '-release.min.js?ver=4.3.25'

| Confirmed By: Meta Generator (Passive Detection)

- http://192.168.103.150/7adcb59.html, Match: 'WordPress 4.3.25'

[+] WordPress theme in use: twentyfifteen

| Location: http://192.168.103.150/wp-content/themes/twentyfifteen/

| Last Updated: 2020-12-09T00:00:00.000Z

| Readme: http://192.168.103.150/wp-content/themes/twentyfifteen/readme.txt

[!] The version is out of date, the latest version is 2.8

| Style URL: http://192.168.103.150/wp-content/themes/twentyfifteen/style.css?ver=4.3.25 | Style Name: Twenty Fifteen | Style URI: https://wordpress.org/themes/twentyfifteen/ | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st... Author: the WordPress team | Author URI: https://wordpress.org/ | Found By: Css Style In 404 Page (Passive Detection) | Version: 1.3 (80% confidence) | Found By: Style (Passive Detection) | - http://192.168.103.150/wp-content/themes/twentyfifteen/style.css?ver=4.3.25, Match: 'Version: 1.31 [+] Enumerating All Plugins (via Passive Methods) [i] No plugins Found. [+] Enumerating Config Backups (via Passive and Aggressive Methods) Checking Config Backups - Time: 00:00:00 (22 / 22) 100.00% Time: 00:00:00 [i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Mar 9 11:37:57 2021

[+] Requests Done: 52 [+] Cached Requests: 6 [+] Data Sent: 12.882 KB

[+] Data Received: 235.375 KB [+] Memory used: 245.809 MB [+] Elapsed time: 00:00:04

WordPress version 4.3.25

WordPress theme: twentyfifteen 1.3

443/tcp