Internal_THM

Enumuration

1- found website onoport 80
2- wordpress site
3- /blog and /wordpress
4- found username admin using wp-scan and a login page at /blog/wp-login.php
5- add the website to etc host with hostname internal.thm

Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%),
ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%),
Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   200.26 ms 10.4.0.1
2   ... 3
4   455.59 ms 10.10.137.33

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.02 seconds
```

SSH:22

HTTP:80

Gobuster

```
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/blog                 (Status: 301) [Size: 311] [--> http://10.10.137.33/blog/]
/index.html           (Status: 200) [Size: 10918]
/javascript           (Status: 301) [Size: 317] [--> http://10.10.137.33/javascript/]
```

```
/phpmyadmin          (Status: 301) [Size: 317] [--> http://10.10.137.33/phpmyadmin/]
/server-status       (Status: 403) [Size: 277]
/wordpress
```

```
/.hta                (Status: 403) [Size: 277]
/.htaccess           (Status: 403) [Size: 277]
/.htpasswd           (Status: 403) [Size: 277]
/index.php           (Status: 301) [Size: 0] [--> http://10.10.137.33/blog/]
/wp-admin            (Status: 301) [Size: 320] [--> http://10.10.137.33/blog/wp-admin/]
/wp-content          (Status: 301) [Size: 322] [--> http://10.10.137.33/blog/wp-content/]
/wp-includes         (Status: 301) [Size: 323] [--> http://10.10.137.33/blog/wp-includes/]
/xmlrpc.php          (Status: 405) [Size: 42]
```

Wordpress

```
+] URL: http://internal.thm/blog/ [10.10.137.33]
[+] Started: Mon May 24 09:25:04 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://internal.thm/blog/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://internal.thm/blog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://internal.thm/blog/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 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://internal.thm/blog/index.php/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>
 |  - http://internal.thm/blog/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://internal.thm/blog/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-04-27T00:00:00.000Z
 | Readme: http://internal.thm/blog/wp-content/themes/twentyseventeen/readme.txt
 | [!] The version is out of date, the latest version is 2.7
 | Style URL: http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'Version: 2.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:15 <=========================================> (137 / 137) 100.00% Time: 00:00:15

[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: Mon May 24 09:25:44 2021
[+] Requests Done: 171
[+] Cached Requests: 5
[+] Data Sent: 43.929 KB
[+] Data Received: 364.163 KB
[+] Memory used: 206.371 MB
[+] Elapsed time: 00:00:39


#user found

  +] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Login Error Messages (Aggressive Detection)
```

hydra Login

```
 hydra -l admin -P WordLists/rockyou.txt internal.thm http-post-form  "/blog/wp-login.php:log=^USER^&pwd=^PASS^:The password you entered "
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-24 09:46:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://internal.thm:80/blog/wp-login.php:log=^USER^&pwd=^PASS^:The password you entered
[STATUS] 438.00 tries/min, 438 tries in 00:01h, 14343961 to do in 545:49h, 16 active
[STATUS] 436.33 tries/min, 1309 tries in 00:03h, 14343090 to do in 547:52h, 16 active
[STATUS] 444.00 tries/min, 3108 tries in 00:07h, 14341291 to do in 538:21h, 16 active
[80][http-post-form] host: internal.thm   login: admin   password: my2boys
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-24 09:55:35
```

Exploitation

1. Go to appearance and edit current theme and paste a reverse shell in 404.php
2. Now access it using http://internal.thm/blog/wp-content/themes/twentyseventeen/404.php url and get a shell back

Post-Exploitation

1- we get user password from a note in opt directory

2- Now we ssh into it and we have to get root3

3-we see that a note says that we have to get to a internal server running at 172.17.0.2:8080

4- we do local port forwarding by ssh -L 7777:172.17.0.2:8080 aubreanna@ip
5- now we can access the internal webserver at 127.0.0.1:7777
6- we get a login and we bruteforce it and get a passowrd for user admin:spongebob
7- Now we are isnide jenkins dashboard and we can execute scripts using the geoovy scripting engine in jenkins
8- we use a groovy payload and get a reverse shell back which is basically docker contianer
9- here we manually enumurate and get the root user credentials in opt direcotry
10- NOw we simply ssh into the root

wp-config.php

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'wordpress123' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
```

```
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'No9]-c] _7M5ae[&|ow)97dfBLUV1G8AakB)?#XIN:W`y4?tgN,DOoC8 mD/)8vh' );
define( 'SECURE_AUTH_KEY',  'xs.zSjNj^a: zpzBLb@r[u65WA9uNd:vLXtLs^>@q38*x.kVxr g,yoGlOpd%Xde' );
define( 'LOGGED_IN_KEY',    'rZU=>v+8g,ey/*Q;c**79^K14&M@2-IDB)DknMf7<a/;hviCw?kRv=MW5lk.vSoG' );
define( 'NONCE_KEY',        '8v={}7jgkSu|D[Nfy]y}>MX}60oSjSMn^qC2rW%V,3|Fg0TJrB6m4}Mb>V@[pZ<w' );
define( 'AUTH_SALT',        'ASOB>S,c3MiYiYSh!;My@BaY7MYRQRI}/~ZC6k?9^e7/jCB00r@Z0)Oe@gQ8Trk*' );
define( 'SECURE_AUTH_SALT', 'd(=umc=!qOCnjIvr~_T_(Ia5.mG6VGF~ktdtt1uzj6A$KJsEAAA5k7.(zFgLa96[' );
define( 'LOGGED_IN_SALT',   '~A,!e|5RGqu!KB=/1R4TN_tcGuK}+]]I_p`FZ[(~L0rv_OY#EItD)tC [hM|l|0z' );
define( 'NONCE_SALT',       'H+T|fK,+u K}_qDTs,ob{,h0TLbd}#pwksNuBzu9~Kw<GcDnJiMYm}[AvPQVTr_,' );

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
	define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
```

Loot

Flags

# User Flag

THM{int3rna1_fl4g_1}

# Root Flag

THM{d0ck3r_d3str0y3r}

Credentials

wordpress login

admin:my2boys

## Mysql database credentials

wordpress:wordpress123

## Hash dump from databse

admin: $P$BOFWK.UcwNR/tV/nZZvSA6j3bz/WIp/

william:arnold147

## SSH credentials

aubreanna:bubb13guM!@#123

### INternal jenkins webserver login

admin:spongebob

### Root credentials

root:tr0ub13guM!@#123