ColddBox_THM

Enumuration

We have possible usernames c0ldd,philip and hugo

we bruteforce them

#we get c0ldd password 9876543210

Nmap

```
     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: ColddBox | One more machine
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4e:bf:98:c0:9b:c5:36:80:8c:96:e8:96:95:65:97:3b (RSA)
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_  256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 5.4 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 4512/tcp)
HOP RTT       ADDRESS
1   199.39 ms 10.4.0.1
2   ... 3
4   457.65 ms 10.10.212.248

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 33.54 seconds
```

HTTP:80

gobuster

```
asswd            (Status: 403) [Size: 278]
/.htaccess           (Status: 403) [Size: 278]
/hidden              (Status: 301) [Size: 315] [--> http://10.10.212.248/hidden/]
/index.php           (Status: 301) [Size: 0] [--> http://10.10.212.248/]
/server-status       (Status: 403) [Size: 278]
/wp-admin            (Status: 301) [Size: 317] [--> http://10.10.212.248/wp-admin/]
/wp-content          (Status: 301) [Size: 319] [--> http://10.10.212.248/wp-content/]
/wp-includes         (Status: 301) [Size: 320] [--> http://10.10.212.248/wp-includes/]
/xmlrpc.php          (Status: 200) [Size: 42]
```

SSH:4512

Exploitation

After logging in we abuse the theme edit functionality and add reverse shell code in a thme template file and then access it and get a shell

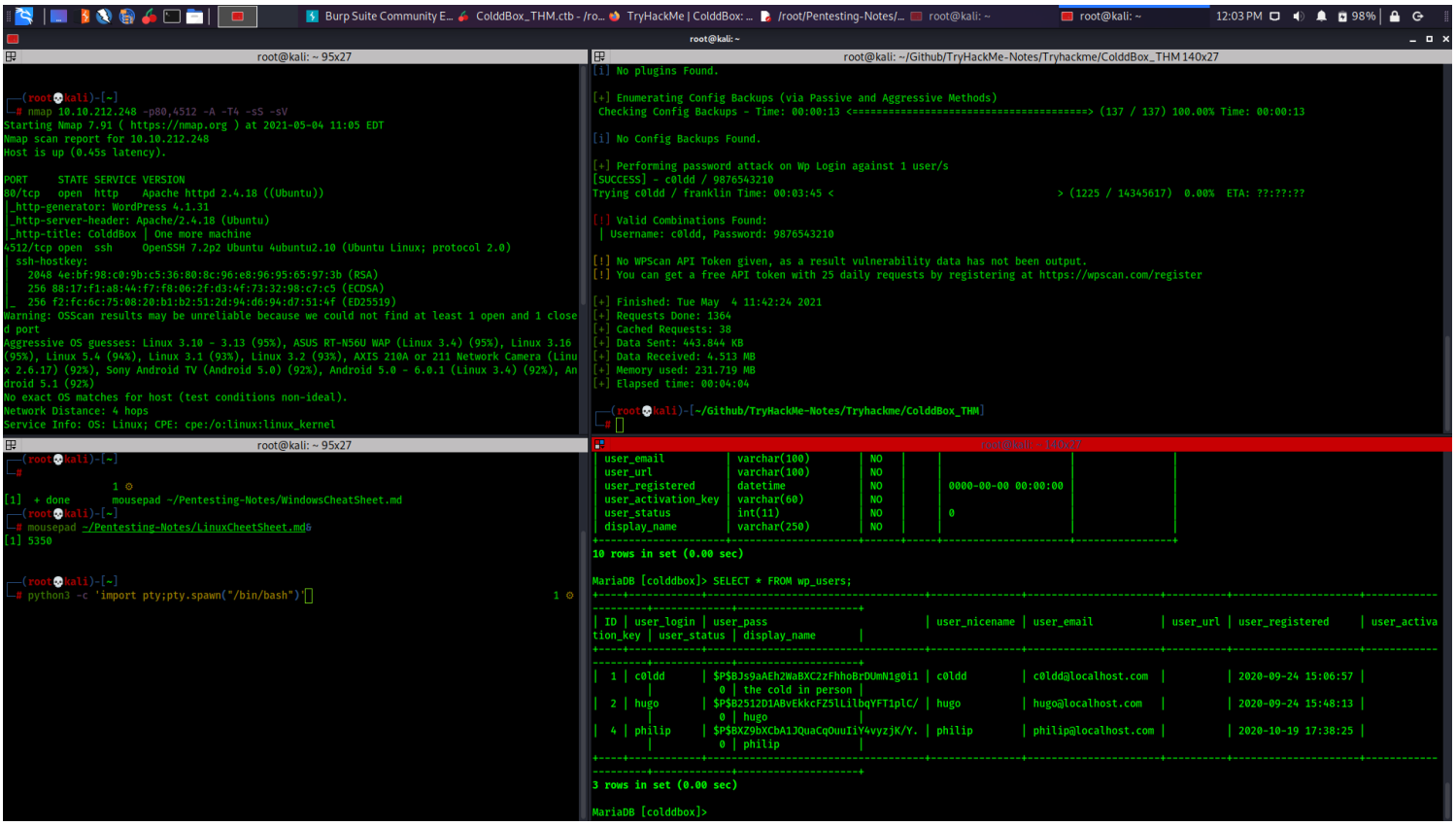
PostExploitation

method 1

we see that find has suid bit set so we direcctly escalated that way

method 2

we read db credentials from database and got the database credentials from wp-config.php file



1 | c0ldd | PBJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 | c0ldd | c0ldd@localhost.com | | 2020-09-24 15:06:57 | 0 | the cold in person |
| 2 | hugo | PB2512D1ABvEkkcFZ5lLilbqYFT1plC/ | hugo | hugo@localhost.com | | 2020-09-24 15:48:13 | 0 | hugo |
| 4 | philip | PBXZ9bXCbA1JQuaCqOuuliY4vyzjK/Y. | philip | philip@localhost.com | | 2020-10-19 17:38:25 | 0 | philip |

#

Loot

Credentials

Possible users

hugo

phillip
c0ldd

wordpress login

c0ldd:9876543210

Flags

User

RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

root flag

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=