# 主机发现

`192.168.247.134`

# 端口扫描

`sudo nmap -sV -O -p- -sC --min-rate=10000 -T5 192.168.247.134`

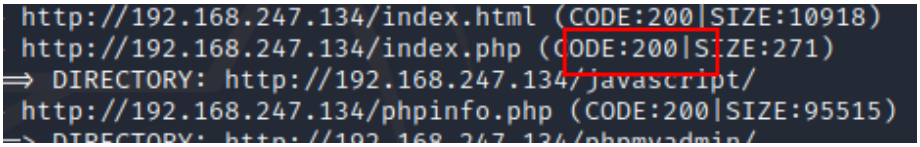
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20d1ed84cc68a5a786f0dab8923fd967 (RSA)
|   256 7889b3a2751276922af98d27c108a7b9 (ECDSA)
|_  256 b8f4d661cf1690c5071899b07c70fdc0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:28:C2:BA (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

# 漏洞扫描

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
| http-enum:
|   /phpinfo.php: Possible information file
|_  /phpmyadmin/: phpMyAdmin
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

发现存在ssh远程登录和http服务开发，且使用phpMyadmin作为数据库管理工具

# web信息收集




访问目标显示是404但是状态码不是，查看源码得到

```
<!--My heart was encrypted, "beelzebub" somehow hacked and
decoded it.-md5-->
```

beelzebub ==>md5==>`d18e1e22becbd915b45e0e655429d487`

得到md5值，在一系列尝试后将它作为网站目录

dirb扫描发现是wordpress的cms

```
dirb
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Mar 12 00:32:06 2023
URL_BASE:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612


---- Scanning URL:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/ -
---
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/in
dex.php (CODE:200|SIZE:57718)
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/
```

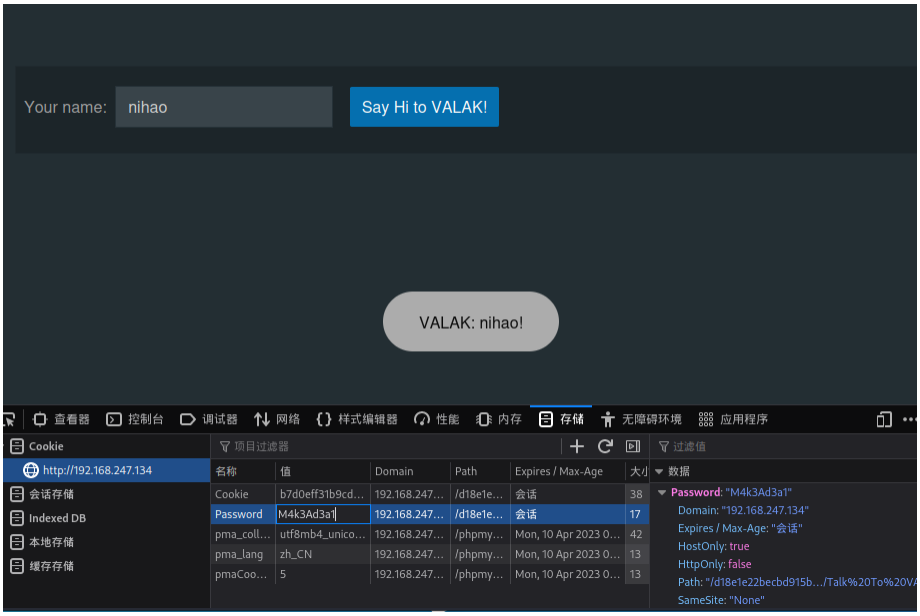
```
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-includes/
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/xm
lrpc.php (CODE:405|SIZE:42)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/css/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/images/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/includes/
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/js/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/maint/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/network/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/user/


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/plugins/
```

```
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/themes/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/upgrade/
==> DIRECTORY:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/uploads/


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/maint/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/network/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/network/admin.php (CODE:302|SIZE:0)
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/network/index.php (CODE:302|SIZE:0)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/user/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/user/admin.php (CODE:302|SIZE:0)
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-admin/user/index.php (CODE:302|SIZE:0)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/plugins/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/plugins/index.php (CODE:200|SIZE:0)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/themes/ ----
+
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/themes/index.php (CODE:200|SIZE:0)


---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/upgrade/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory:
http://192.168.247.134/d18e1e22becbd915b45e0e655429d487/wp
-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

    (Use mode '-w' if you want to scan it anyway)


-----------------
END_TIME: Sun Mar 12 00:32:37 2023
DOWNLOADED: 32284 - FOUND: 11
```

一番搜索在cookie中拿到了密码`M4k3Ad3a1`




```
wpscan --
url=http://192.168.247.134/d18e1e22becbd915b45e0e655429d48
7/ --ignore-main-redirect --force  -e --plugins-detection
aggressive
[i] User(s) Identified:

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

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

```
[!] No WPScan API Token given, as a result vulnerability
data has not been output.
[!] You can get a free API token with 25 daily requests by
registering at https://wpscan.com/register

[+] Finished: Sun Mar 12 00:43:28 2023
[+] Requests Done: 8709
[+] Cached Requests: 11
[+] Data Sent: 2.905 MB
[+] Data Received: 1.33 MB
[+] Memory used: 251.023 MB
[+] Elapsed time: 00:00:54
```

得到两个用户，尝试ssh登录

# SSH登录

---

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

294 packages can be updated.
178 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sat Mar 20 00:38:04 2021 from 192.168.1.7
krampus@beelzebub:~$ whoami
krampus
krampus@beelzebub:~$ sudo -l
Password:
Sorry, user krampus may not run sudo on beelzebub.
krampus@beelzebub:~$
```

登录krampus成功

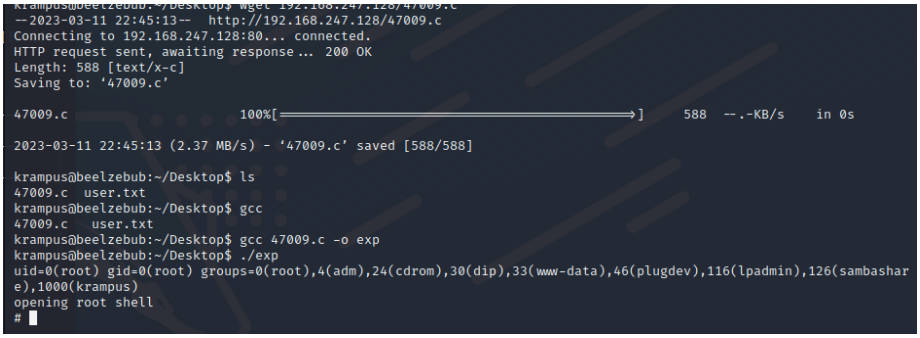
得到用户flag

```
krampus@beelzebub:/$ ls
bin   cdrom  etc   initrd.img      lib    lost
boot  dev    home  initrd.img.old  lib64  medi
krampus@beelzebub:/$ cd /root/
-bash: cd: /root/: Permission denied
krampus@beelzebub:/$ cd /home/
krampus@beelzebub:/home$ ls
krampus
krampus@beelzebub:/home$ cd krampus/
krampus@beelzebub:~$ cd Desktop/
krampus@beelzebub:~/Desktop$ ls
user.txt
krampus@beelzebub:~/Desktop$ cat user.txt
aq12uu909a0q921a2819b05568a992m9
krampus@beelzebub:~/Desktop$
```

# 提权

查看历史命令发现有人使用47009提权


下载上传，gcc编译，执行




本地提权成功

ps:

```
python -m http.server 8080  简单服务器
```