扫描发现两个端口 80、8080
访问80 获得private key

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBkV0CJjc
1ZJstvEWXiQObVAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCjaCCHMPZ+
Iq7pJEe1OYrbwlP/ZAczwMqoVBoJp4nLRVmPgeaMJzxVD2c11coTSESgThxrF1U2Jb/7+l
eRmtTSgwQioDyBP5+iCcgeV0FLmAyGZpaGZ1+ww9SR63y0ru/C/IohOrCGZgt1pstCcq8q
K0m/J6+FWufdDWWB4KNpIHI5O9TBYKo2OzFgvNSbI66End+hTxZxK8Qb1xSyizavoRp2z/
VfQ+IpUYSBqTpzhOZYBIEmTE4M5YqEnfCKqtB85c6/9iN+acNNAgkmedc2ypsR+hi7kOjB
nu7AggGSuu+TLldJNJTpKdrti3mEEjAsbpSmwSX6OXmTyHj58jZazMns6Us7ZgNO6XQbvJ
ayYei1nNwy1RsRzbKxiyzufdL7VUXq9EH5RrfBzX42Z28crXGciAN1XjiO2L1+ndvimnW6
iPO3fO8Lgrk+/74TN/aH8CBs3zY2/Mvtg2Tq7eznDyEh8Yy/UZxJOoeRf1c3qaWzLc3k8P
ncuWACZivGch8AAAWAdPgkhhYogu2byWPUYvkaHLByrpq0vdu9ipfpCbHJyYTAx6vJawJO
vD1yekFempyOUNxkQWrprP4wIN1leLmR44YXkvTayRAC/BOJxaBUYyKRgmcHLkWhZuGbpw
e4MiFsquxPVw5ZTPa1Jew0JpdFExNTD8/9CvK99ZBcd24U39N7FWrNmhmm7GvG+Q77eIBS
YdjoiHlBRhLkO2OlH2TGSiJ6mQZC38J12Yp7jaeM7mIuDuUfqHJ9igH/qyKgiY9GZ1jP3M
DXACN+5nuW+jJhkhR/5XrzL4NcCvj6D9rTFksVsqFGdgAV3/aCDlh9WsyxfBgIg2lQs4OU
3FbhWTXaaFRZU7M8l6lF7j2WzmvuexSMTqpDaP9PVALhXZVql9y5jgPIgRct+iXYYOmlvh
oOuxeVVV7FTsPqEipb/AhvxNvzV1Rz1xBG5U1kycTKGFz/DJdDoK+PzhIp+FgtKxOwoEW3
mzFVZr9B9XJmH6aK4PA7WbTnAGW0+ncZG2nkI1nRThy26Qba/y8qDWhW/qoaHsWUxChYs+
6xmjlqmXdNwjBDqPdr0Iv+N+tdoirt41HyPlR98fB/DjFkNey7r8+fWBumaTZ8I2Fci+Rs
zX4FbrhbcPebbC1C0kGjdatNMg5zdzucv1PFGaAUO422ZGCP7iDtMDgrEyhqH7AyIjkMZl
BooOt3ZcwkrQRzyBV148xSKpK16YyNVlVUKw7xqohs3iOEe1R1ARTUrUdUi5tJazos8ItM
Z/f1wYh4PxlDgIDtoZX7oYcvmYhoDM5KVO1JC8oVUVm1vtODyFJni7iPszGdBuxXV+jBn5
v4qNyy3SEcvQbMux2I6dqTP/OddoXtSuPRAOEOiLoumEuMleLpk/hpwaIkW73j9+WBZzAl
Bv6chHlgqOZ9TTo/IpBTaYw7YRSjJxsY3A++sWitiE3OIbj/NKROX/YeIOfdwRjkzyOesx
m+bbayffyOWD8JpHUGCutRKKw8z/8VJmIfWMSHPRihLj47C3XOOnaEILTMCm5kWn2PagGL
+kB97l2NBkScwQlX3d4JWchJI9b3PfGaqOav4FA1evOG1e5xmxjyLVoqSLWIbn9QkUG5xy
2qqQ/fQw9ndVfuRohq9En7vOTkVO75Fw9W8QsV7VMoPxonIlYtOltWkrmlfi1QNGcqxZy3
mwoc4QRbHQ/UGsU/WUkgS3sr3iQtIUAVYuDyCYChSvZOl0A/sAsQerMcifUFCGIJNM8IXL
RGo+5WO2FmORF+gmbkaQKm1FDHqiOBwxWD/M/O+4uDfcA7BgP1oEc9qF/+lwj7gX+ahQ+V
6n+tZmpVrqN55hh6OkXRTxKCoDLCYlju9iglgLJPDTt11PRkNTSvLvshUaDeh9zWYkdPwT
3tPM+jH6a/Bz4e0grFDkC4D3Y8SCLKOYLrf1DWO5RCHARdzD3VoPHiiTmY/s/spQhlpYPb
qguUid3Q1plFCa1gWN6F4agprFa6mcUKNzTOvl2eTCR45dRNJRJ6ZiOiGEfYJoNi34T9ZH
uoi3+yesygci3wkkbAHOvilpVmnbHWF6wLfVOQN2fLuxdayKC7rEtxws+I/QdsaOe7SaCT
YPqw9I4yOkruhHote/gpmoynSxzSzkiAdWUOnHi9jtXU4lNeOP2W1CnUONFMeX78YHI/nD
8XnaeFwaUh92ClLzvvMeItDufoQbXk8r51V5sscLqtNaGSpdAmVvFB6MNQHCkUSBqbJEFW
LIVlDNKRW+ISLxO4BTg+GYUoBCt6pa7+xBktE2A9LNuKLE2WT++fZOPTaRlI2ngMWHY7Vx
ARnMUXO1vXejtrdJZb9znPK1w/2CaFKKFaLufz0ylQwffDm2dwCTgrd279OeRrTzCQtvGJ
lGNbkA==
-----END OPENSSH PRIVATE KEY-----
```

访问8080端口，发现是GMSSH服务 使用上面给的证书发现加密了，那就破解吧

```
python3 /usr/share/john/ssh2john.py id_rsa > id_rsa.hash
```

john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash

john show id_rsa.hash

密码是 cocacola

【ps】一开始没想到监听 127.0.0.1
所以我根据这个私钥获取public key
ssh-keygen -f id_rsa -y > id_rsa.pub
发现用户名 laoye

我直接操作了虚拟机
cat /home/laoye/user.txt
sudo su
cat /root/root.txt