暴力破解22端口获取meterpreter

孤独的一颗星 关注 IP属地: 广东

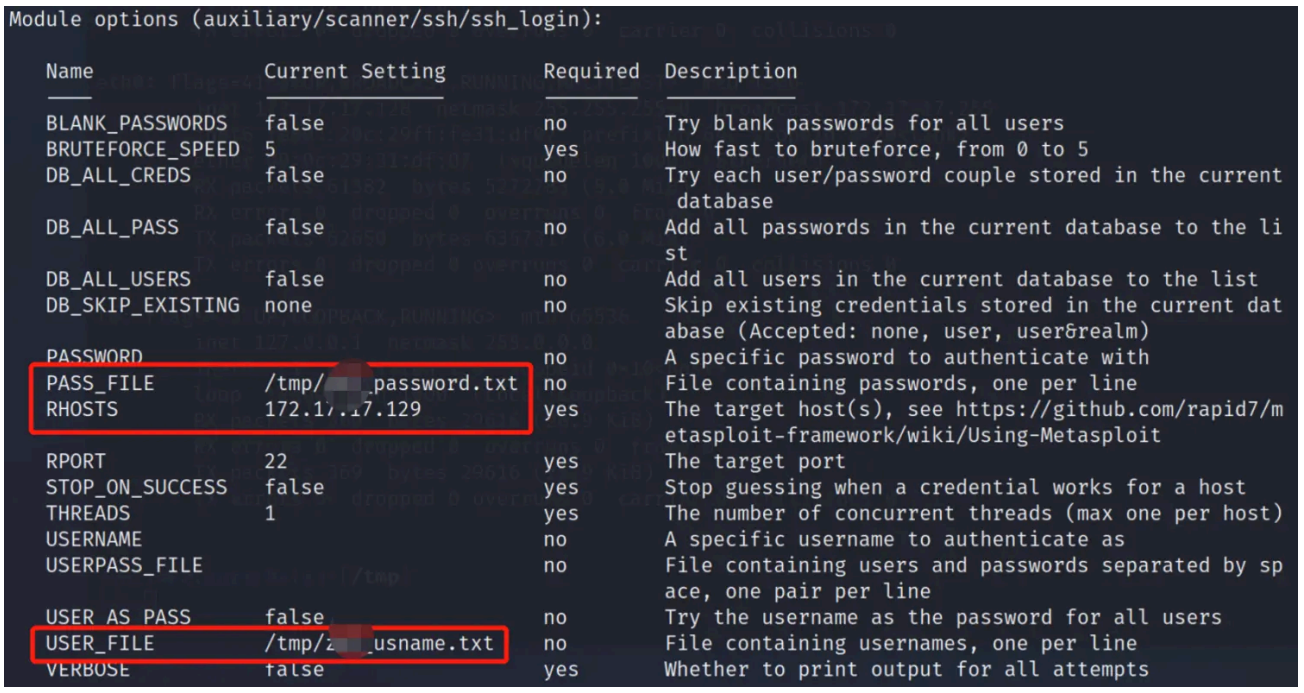
0.097 2022.08.15 22:24:16 字数 173 阅读 1,626

22端口是ssh远程登陆端口，我们常用ssh登陆远程电脑，在Linux中具体操作如：

```
ssh root@172.17.17.129
```

那么，如何利用22端口进行渗透呢？常用的方法是暴力破解。

metasploit中有暴力破解的模块，名为ssh_login，需要设置目标ip、用户字典文件、密码字典文件，爆破成功后会在sessions中保留一个Linux shell会话。



msf中配置情况

此时获取的shell会话不等于meterpreter，但shell会话能转换成meterpreter，只需输入如下命令即可：

```
sessions -u 3
```

注意：此处的 3 是shell会话的编号。