**转发:**

dnscat2: listen 127.0.0.1:9999 <target\_IP>:22

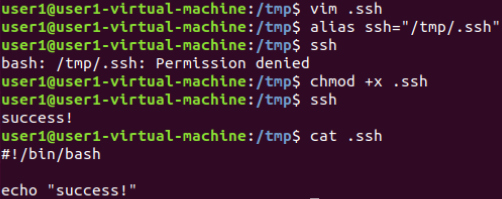
Metasploit: post/windows/manage/autoroute

Metasploit Socks Proxy + Proxychains: use auxiliary/server/socks4a

Meterpreter: portfwd add –l 3389 –p 3389 –r <target\_IP>

VPN over SSH

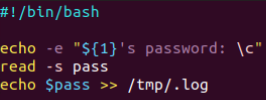
**通过普通用户权限隐形记录SSH登录密码:**



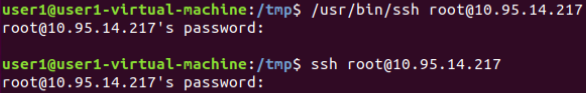
正常SSH连接信息:



修改脚本中的回显，伪装成正常的SSH连接信息:



模仿效果:

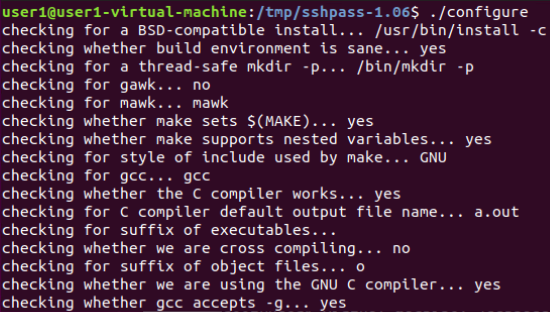


将输入的内容传参给真实的SSH连接(Linux中SSH只接受标准化输入的内容，也就是不能使用的常见的管道符将密码发送给SSH连接):

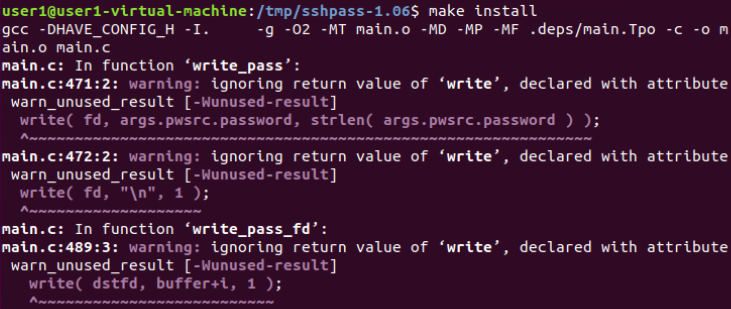
sshpass工具实现传参

https://sourceforge.net/projects/sshpass/

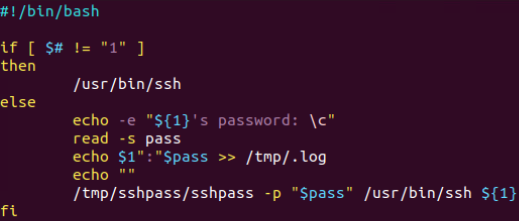
编译:



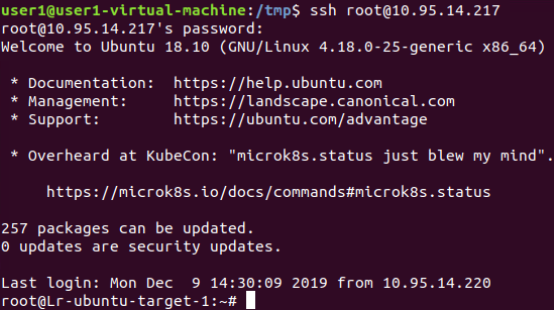
安装:



编辑脚本:



执行:



密码记录结果:



用户持久化生效:



