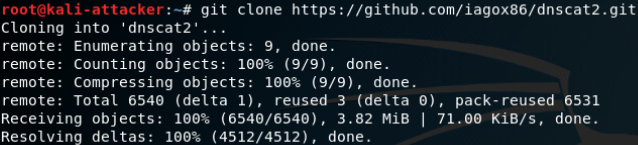
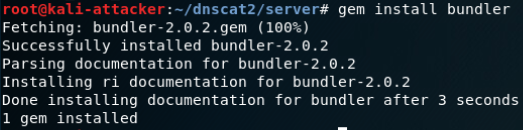
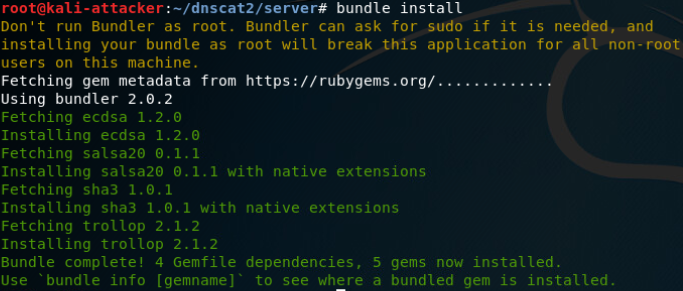
**DNScat2-通过DNS隧道进行C&C通信:**

在限制非常严格的情况下，DNS流量也应该是允许放行的，可以利用DNS隧道技术在目标主机和C&C服务器之间建立连接。命令和信息都包含在DNS查询和识别中，这也是很难检测的原因，即使任意命令就隐藏在非常显眼的地方，但是它们会被认为是合法的流量，也检测不出来。

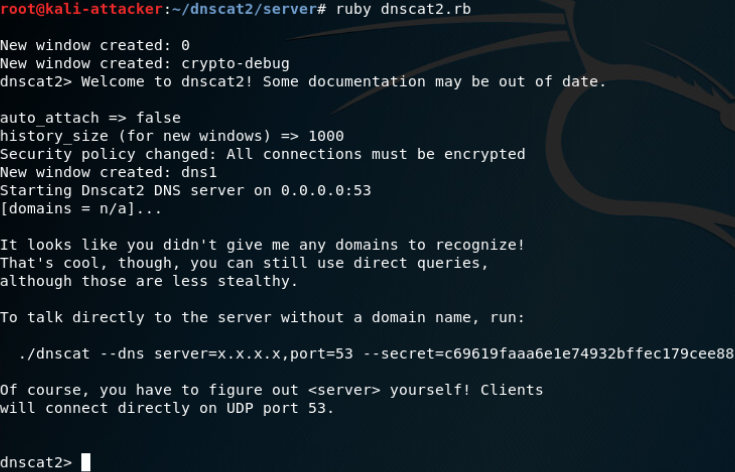
server端安装:



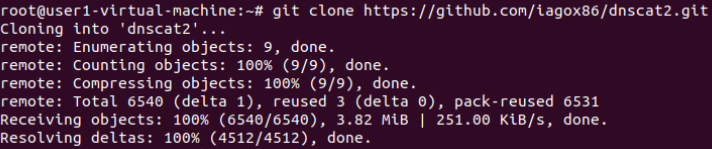




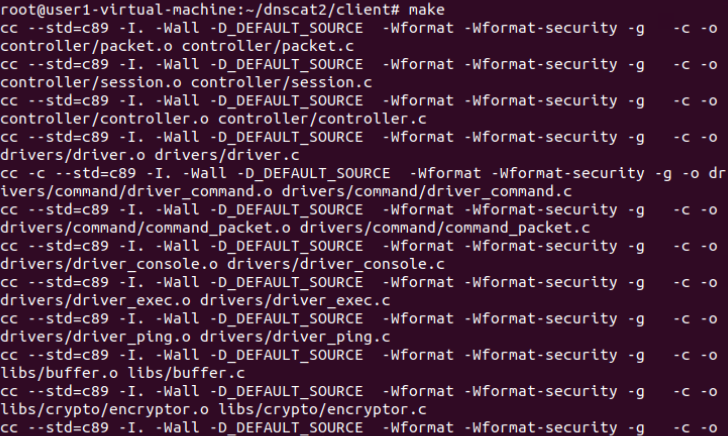
启动服务端



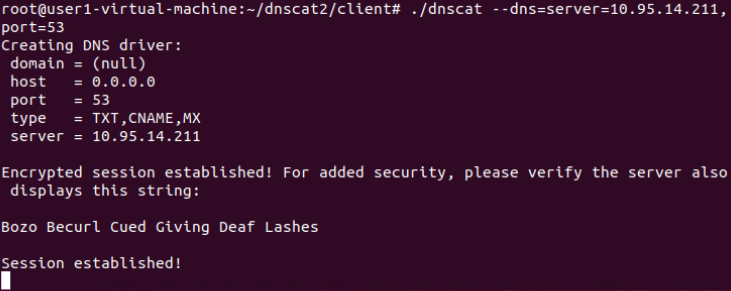
client端安装:

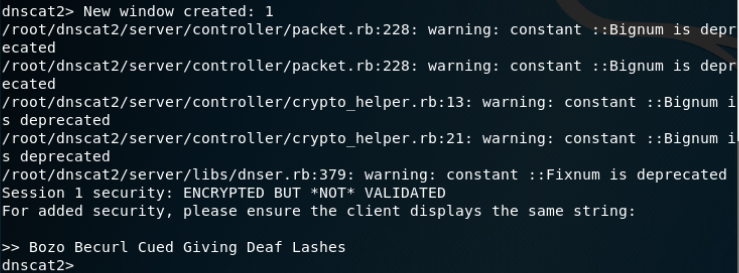


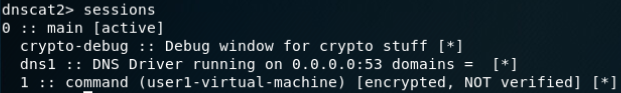
make编译

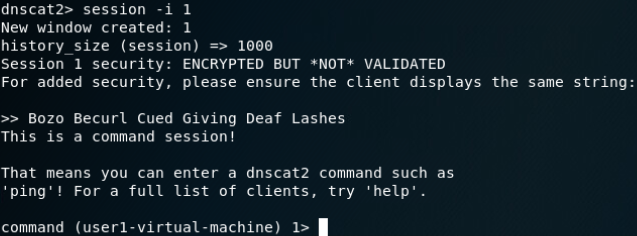


和服务端建立通信:



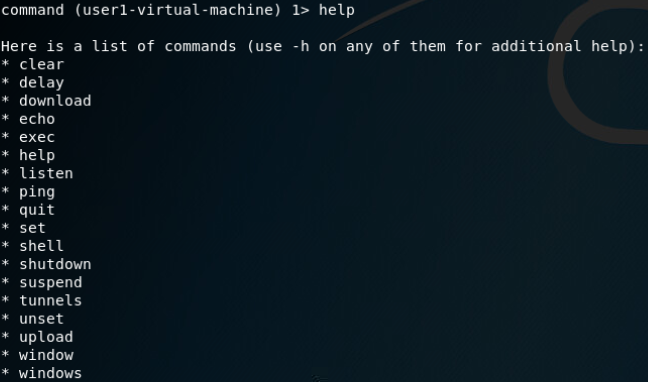


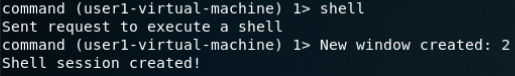


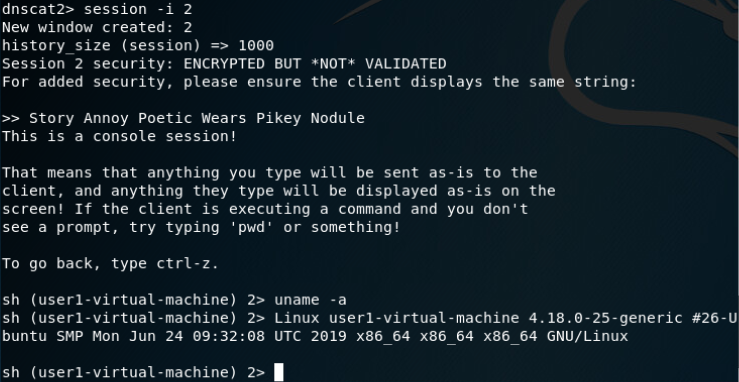


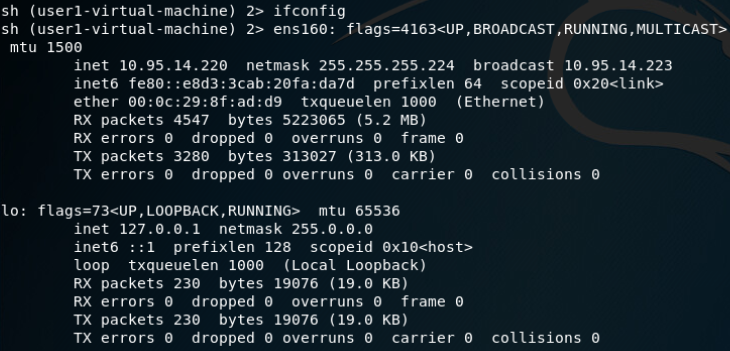












建立DNS隧道转发(SSH连接):



