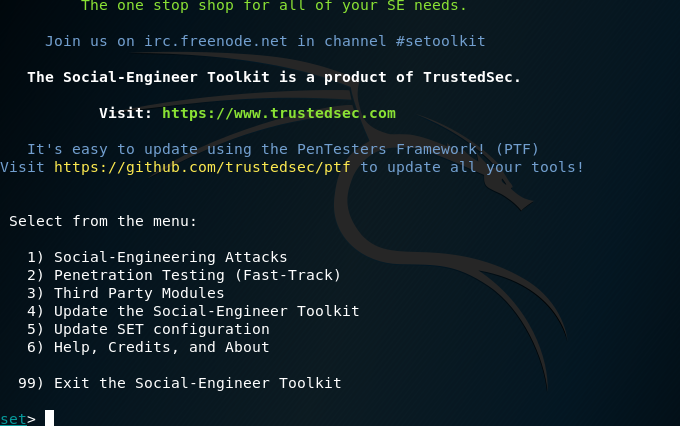
## 工具的启动

命令：setoolkit



## 社会工程学攻击 Social-Engineering Attacks

1) Spear-Phishing Attack Vectors鱼叉式钓鱼攻击

2) Website Attack Vectors网站攻击

3) Infectious Media Generator介质感染攻击

4) Create a Payload and Listener

5) Mass Mailer Attack群发邮件攻击

6) Arduino-Based Attack Vector基于Ardinno的攻击

7) Wireless Access Point Attack Vector无线接入点攻击

8) QRCode Generator Attack Vector二维码攻击

9) Powershell Attack Vectors Powershell攻击

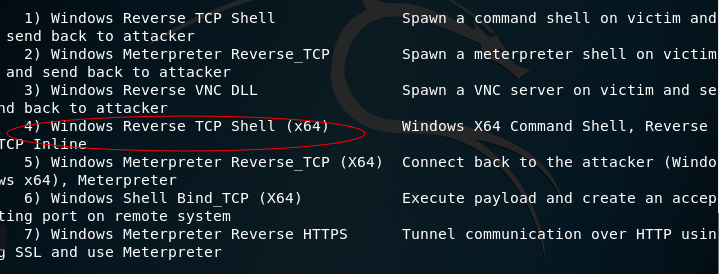
10) SMS Spoofing Attack Vector短信诈骗攻击

11) Third Party Modules

### Spear-Phishing Attack Vectors鱼叉式钓鱼攻击

1. Perform a Mass Email Attack创建一个群发邮件
2. Create a FileFormat Payload文件附件攻击
   1. 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2. 2) SET Custom Written Document UNC LM SMB Capture Attack
   3. 3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4. 4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5. 5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6. 6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7. 7) Adobe Flash Player "Button" Remote Code Execution
   8. 8) Adobe CoolType SING Table "uniqueName" Overflow
   9. 9) Adobe Flash Player "newfunction" Invalid Pointer Use
   10. 10) Adobe Collab.collectEmailInfo Buffer Overflow
   11. 11) Adobe Collab.getIcon Buffer Overflow
   12. 12) Adobe JBIG2Decode Memory Corruption Exploit
   13. 13) Adobe PDF Embedded EXE Social Engineering
   14. 14) Adobe util.printf() Buffer Overflow
   15. 15) Custom EXE to VBA (sent via RAR) (RAR required)
   16. 16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
   17. 17) Adobe PDF Embedded EXE Social Engineering (NOJS)
   18. 18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
   19. 19) Apple QuickTime PICT PnSize Buffer Overflow
   20. 20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
   21. 21) Adobe Reader u3D Memory Corruption Vulnerability
   22. 22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

### 【案例】运用 Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)



选择这个

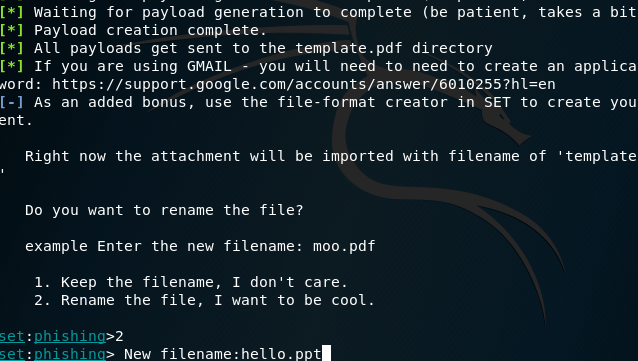


输入反弹到的ip地址，一般输入本kali的公网ip

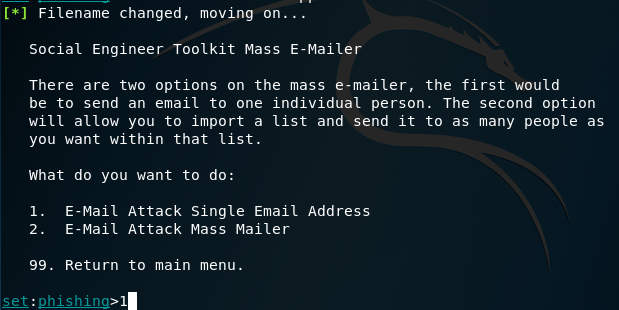


按回车默认443端口

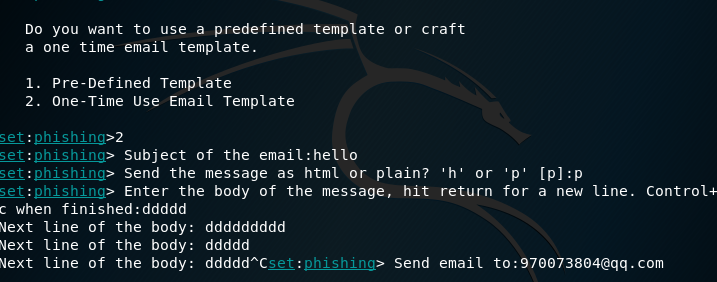
（注意，可能需要退出安装msfconsole）



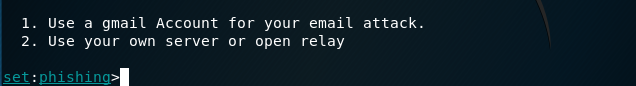
是否重命名，我们重命名为hello.ppt



选择发一篇邮件还是群发邮件，我们选择1



自定义好邮件相关内容



选择配置Gmail邮箱还是其他邮箱



是否标记高级别紧急，我们选yes

3) Create a Social-Engineering Template创建社会工程学模板

### Website Attack Vectors网站攻击

1) Java Applet Attack Method java基于浏览器的小程序攻击

2) Metasploit Browser Exploit Method

3) Credential Harvester Attack Method

4) Tabnabbing Attack Method 浏览器导航标签的攻击

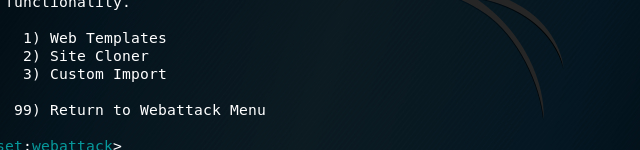
5) Web Jacking Attack Method web劫持攻击

6) Multi-Attack Web Method

7) Full Screen Attack Method

8) HTA Attack Method

# 【案例1】使用 Java Applet Attack Method



1) Web Templates使用模板，一个虚假的页面

2) Site Cloner基于现有的url可克隆一个出来

3) Custom Import自定义导入

我们选择2



是否选择NAT模式，这个需要根据我们虚拟机的网络配置

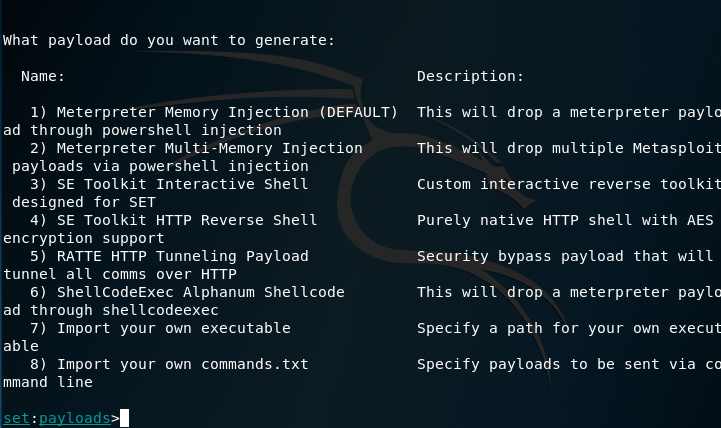
如果虚拟机和主机是同一子网并且有自己的ip地址，我们就选择no



输入监听的ip地址



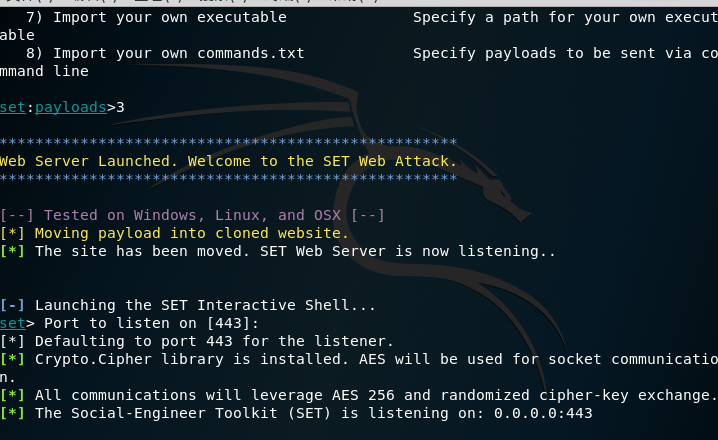
输入监听的url



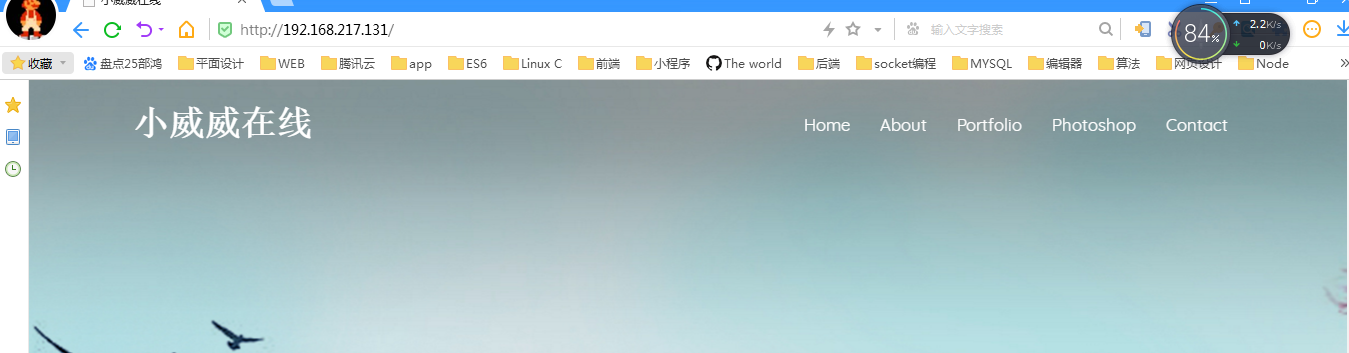
选择shell的交互方式，我们选3

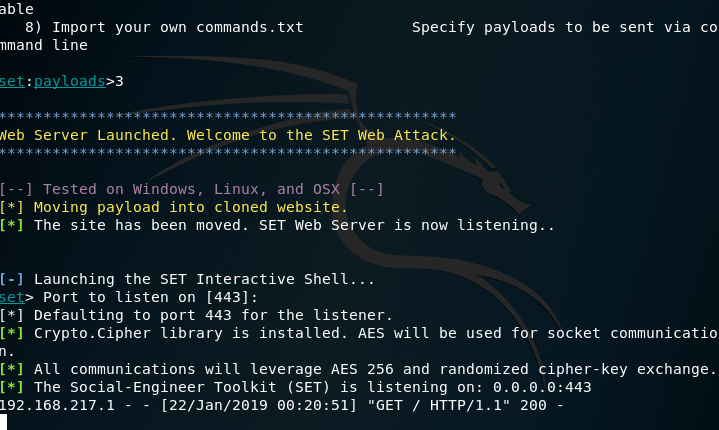


监听端口选择



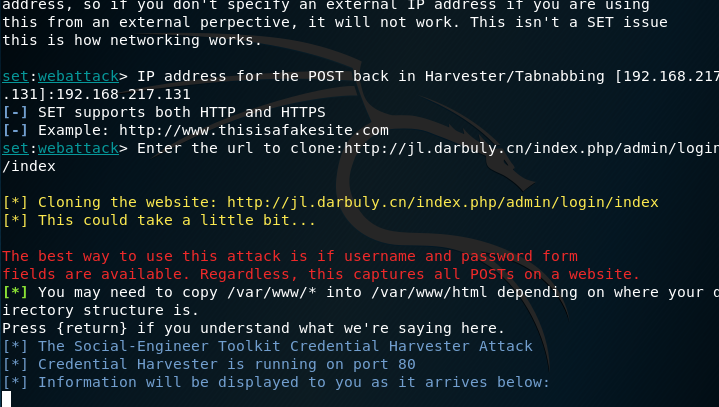
OK，开始监听了！



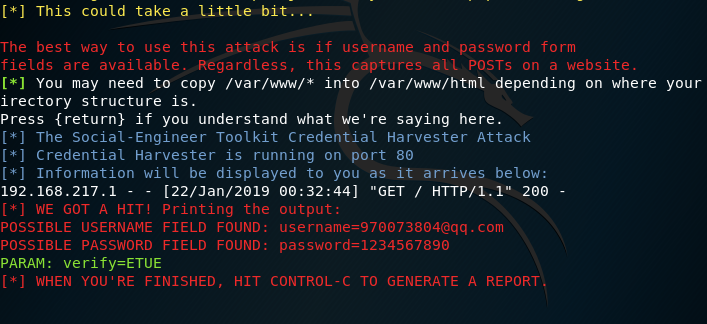


限制条件：对方系统运行java浏览器程序，会跳出警告窗口

【案例2】使用Credential Harvester Attack Method



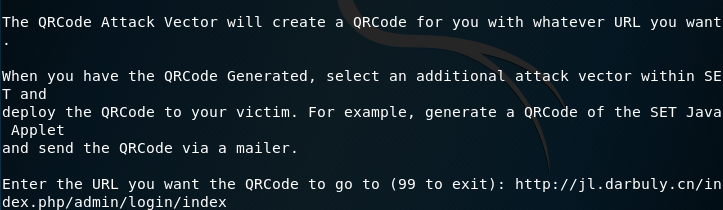
前面都一样



### Wireless Access Point Attack Vector无线接入点攻击

### QRCode Generator Attack Vector二维码攻击

【案例】

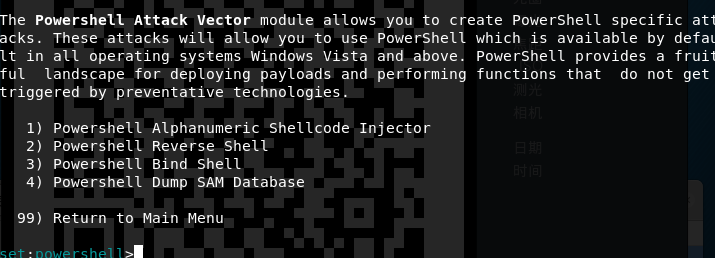


选择要跳入的网址



无非就是将网址转化成一个二维码而已

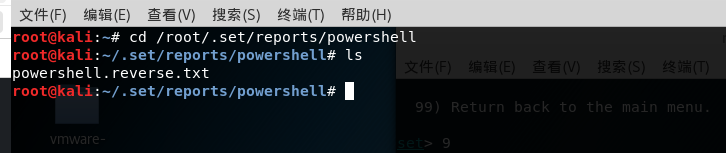
### Powershell Attack Vectors Powershell攻击



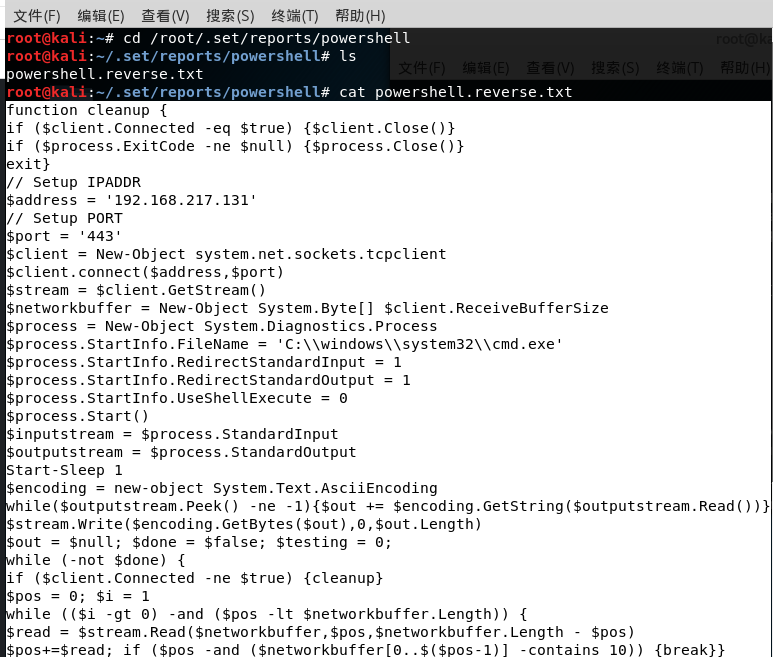
选择2，反弹方式



选择监听ip和默认端口

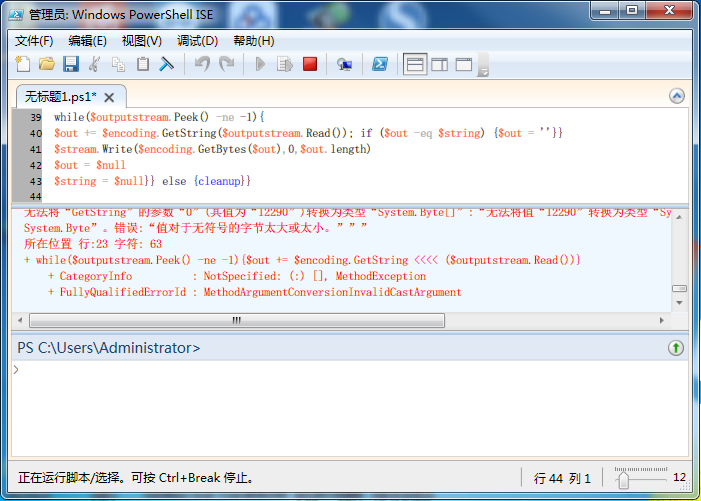


可以看到poweshell脚本文件已经生成了



我们拷贝到windows去运行，并开启监听





到windows去运行



连接上了