

实验报告

课程名称： 网络攻防技术

实验项目： 实验七：权限提升实验

学 生 姓 名：

学 号：

二级学院名称：

专 业：

指 导 教 师：

# 1实验目的和要求

1）清楚模拟令牌的概念和工作原理；

2）掌握用模拟令牌提升Windows用户权限的方法。

# 2实验设备及材料

1）VMware虚拟机：VMware-workstation-full-14.1.3.zip

2）Kali虚拟机系统：Kali-linux-2018.1-vm-amd64.ova

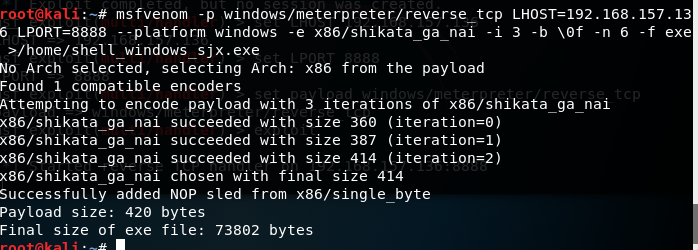
3）Windows靶机系统：Windows 2003 Server虚拟机

# 3实验内容

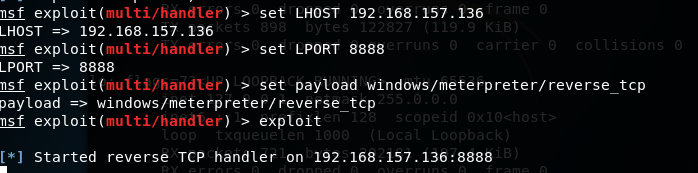
利用模拟令牌来提升Windows用户权限。

## 3.1 建立Meterpreter会话连接

1）生成后门程序文件；



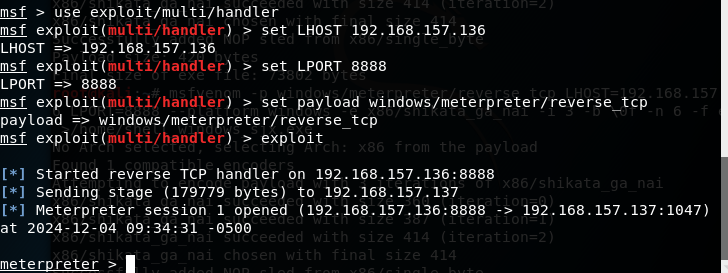
2）MSFConsole启动Reverse\_TCP反向连接监听；



3）在Windows上启动shell\_windows\_zbj.exe程序；

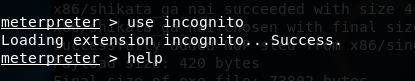


4）建立Meterpreter会话。

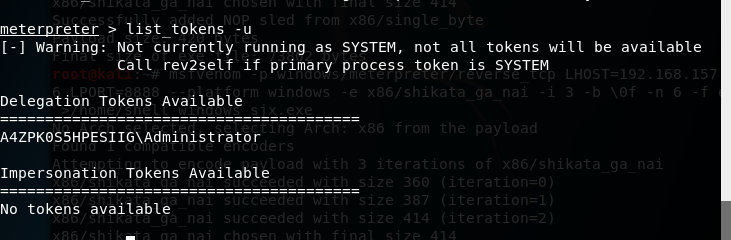


## 3.2 提升权限

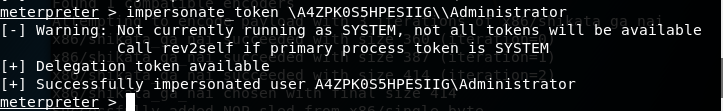
1）使用incognito模块；



2）列出Windows虚拟机当前可用的令牌；

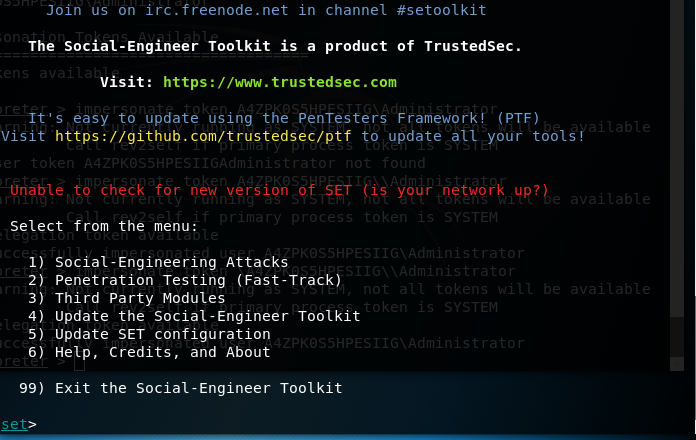


3）模拟Windows虚拟机用户令牌。

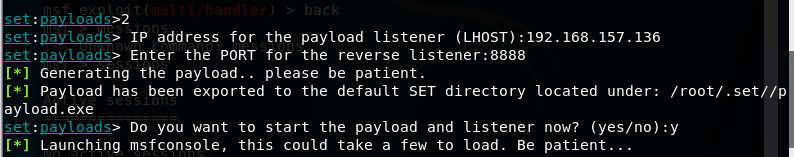


## 3.3使用社会工程工具包SET来提升Windows用户权限，步骤如下：

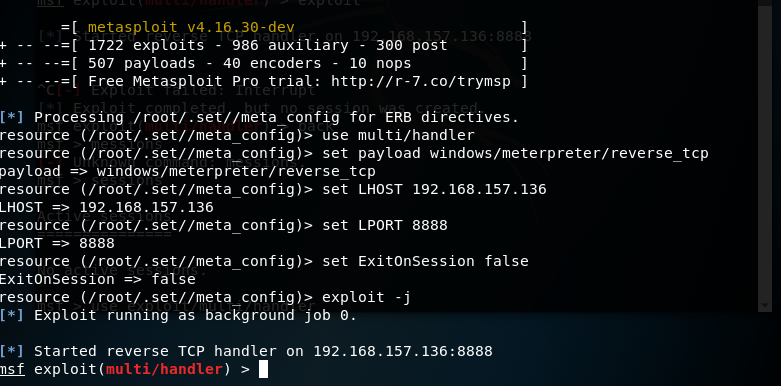
1. 在终端输入命令“setoolkit”可以启动SET；



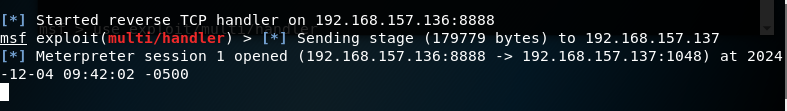
1. 创建一个攻击载荷和监听器；
2. 设置Reverse\_TCP攻击载荷；



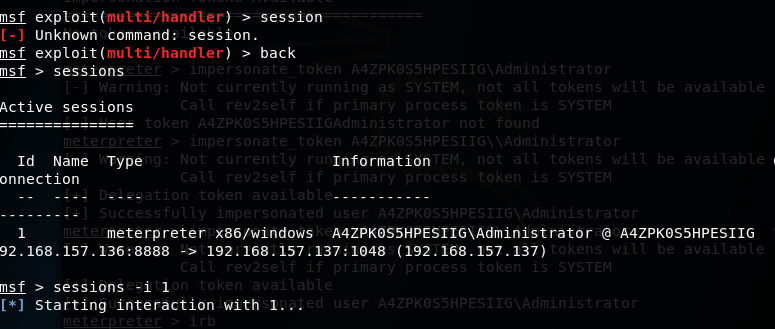
1. 启动MSFConsole的multi/handler渗透攻击模块；



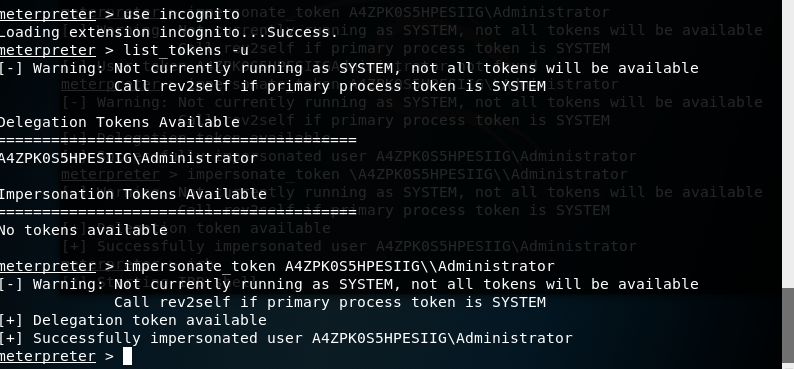
1. 反向连接MSFConsole启动的监听模块；



1. 建立Meterpreter会话连接；



1. 利用前面的手段提升权限。



# 4实验总结

模拟令牌是windows系统提供的一种访问控制机制，利用这种机制攻击者可以假冒网络中的用户进行各种操作。本次实验通过模拟令牌模仿用户以及setool社工工具包来提升权限，我认为从主机到靶机之间建立连接通道是关键。