068-漏洞利用渗透测试

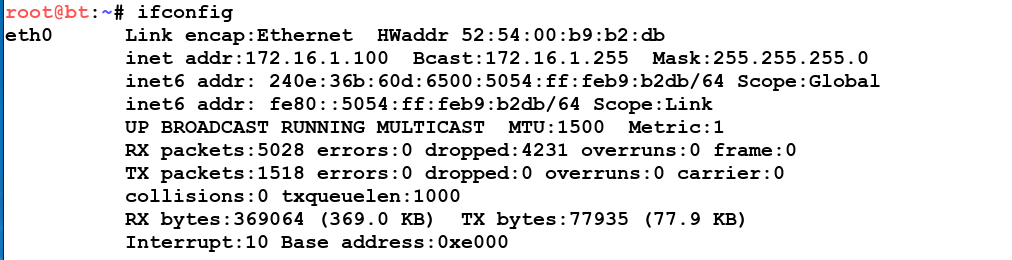
实验环境说明：

渗透机：p100\_bt5-2（BT5） 用户名：root 密码：123456

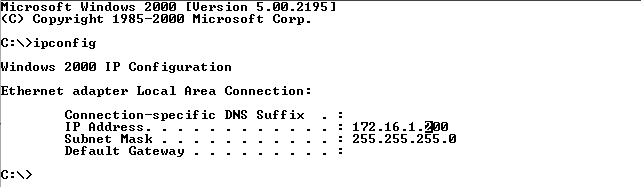
靶机：p100\_win2000-1（Windows 2000） 用户名：administrator 密码：123456

第一步，打开网络拓扑，启动实验虚拟机，分别查看虚拟机IP地址：

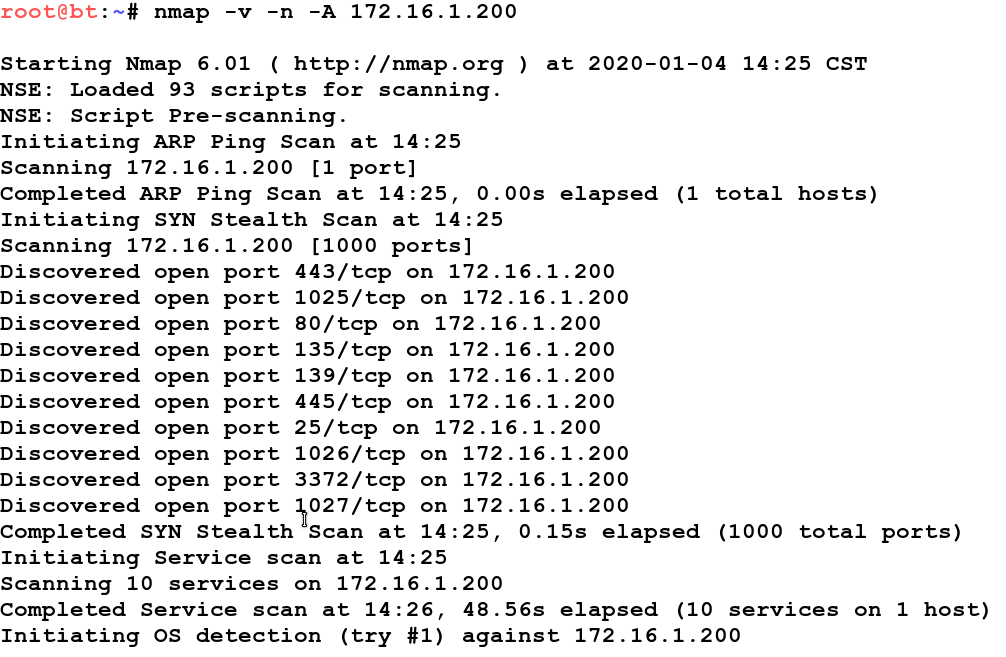
BT5

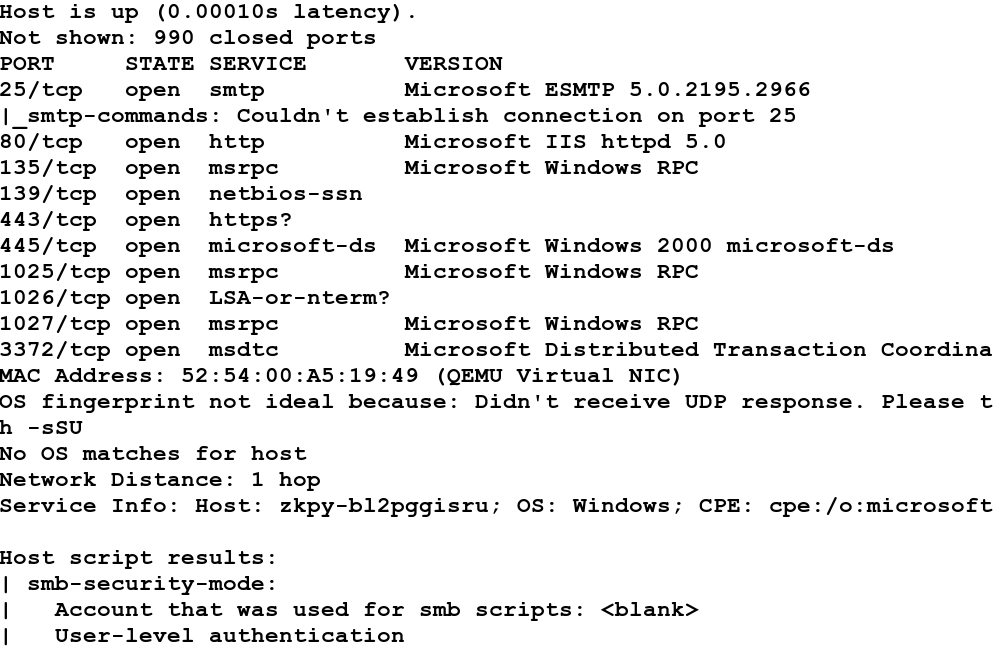


Windows 2000



第二步，对目标靶机进行综合扫描，发现服务器运行的应用程序

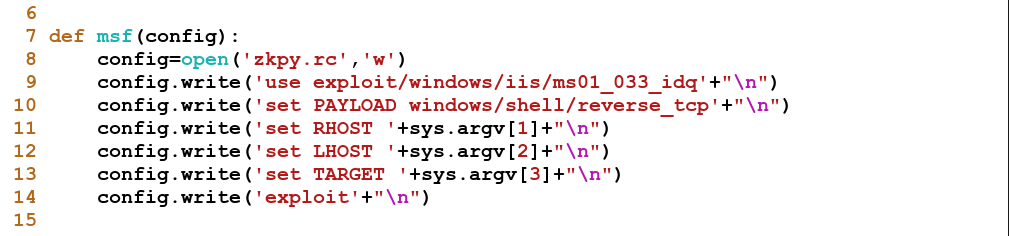




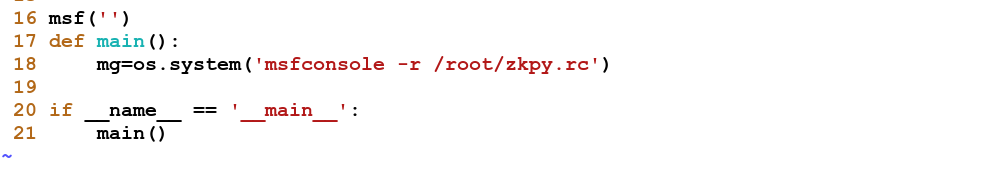
第三步，编写Python脚本针对已发现的漏洞进行渗透测试，首先导入需要用到的模块



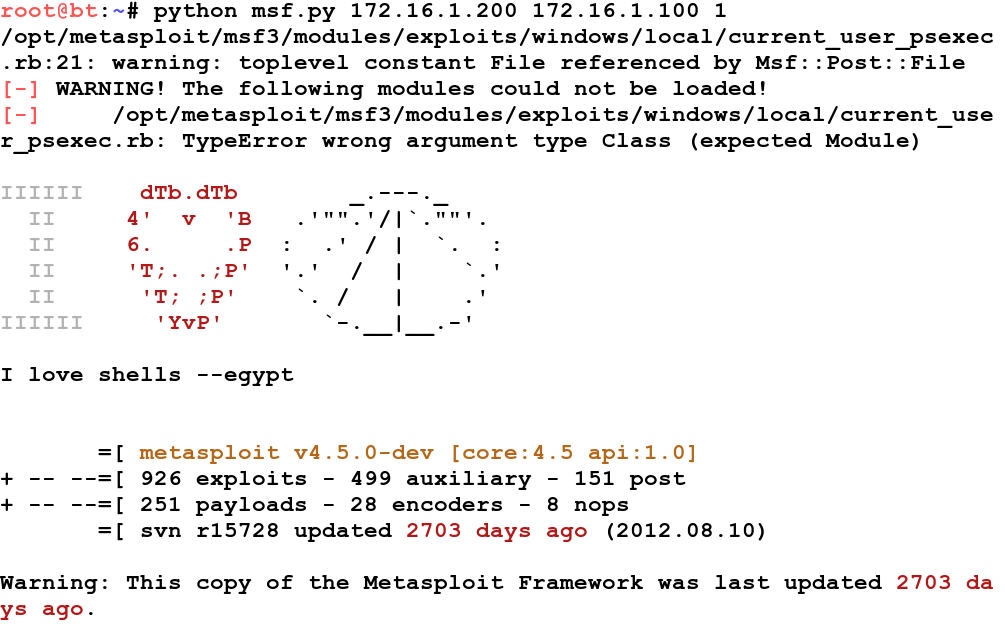
第四步，定义msf函数

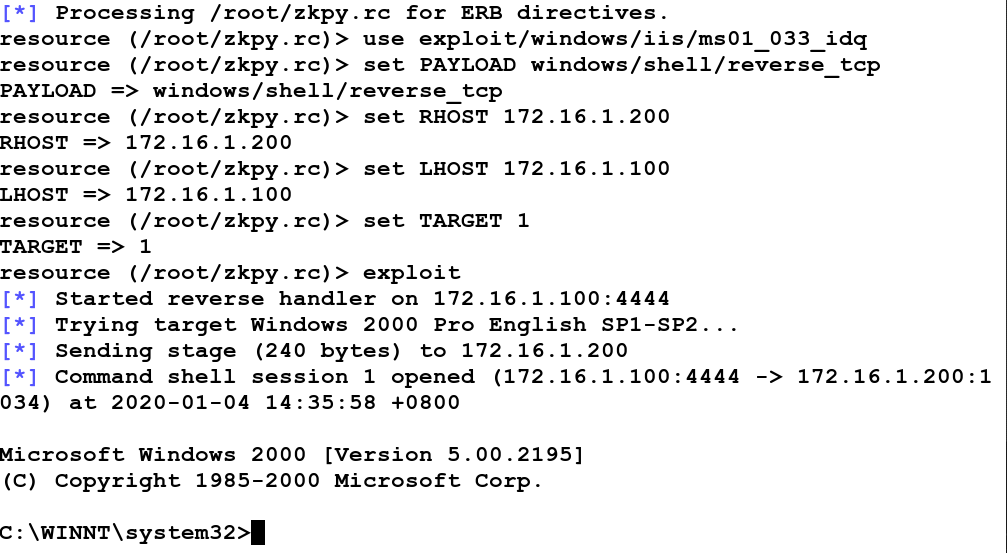


第五步，调用main函数



第六步，验证脚本运行的结果，成功对服务器应用发起渗透测试





实验结束，关闭虚拟机。