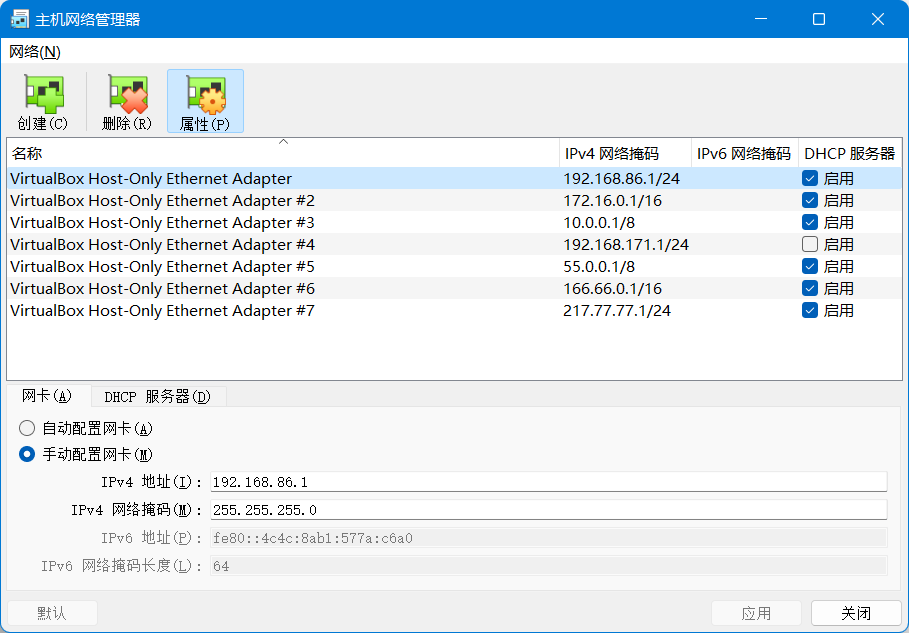
**实验 1 网络信息安全基础实验**

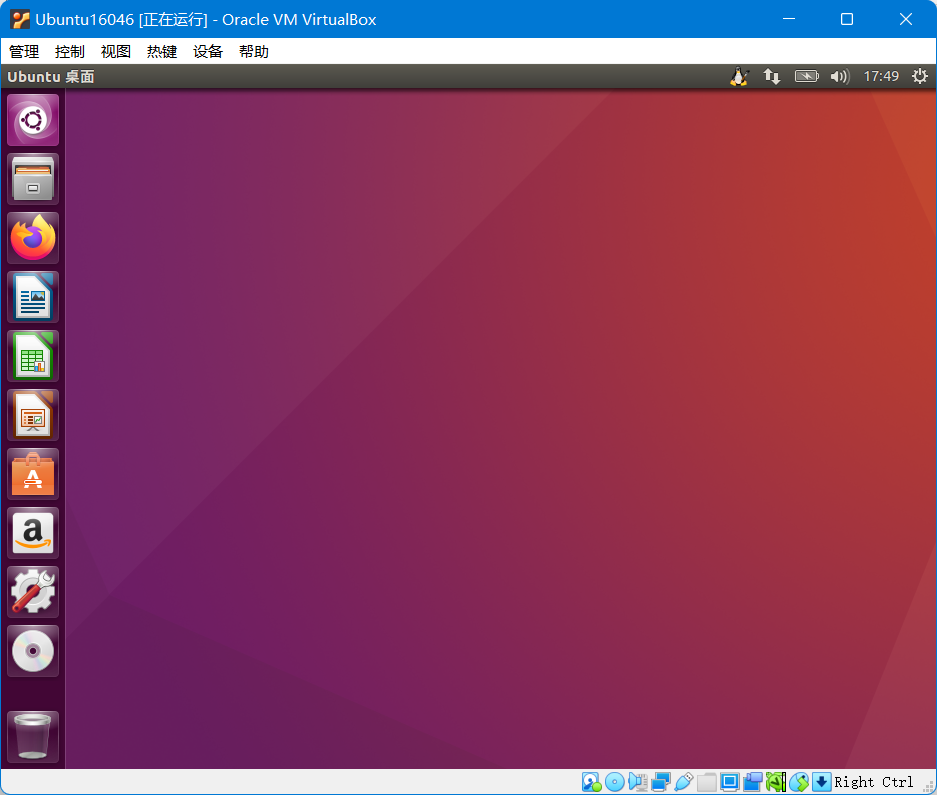
李远航 PB20000137

1. **实验目的**
2. 使用 VirtualBox 虚拟机建立网络信息安全实验环境；
3. 配置虚拟网卡，虚拟机使用多个虚拟网卡进行通信；
4. 安装及配置新的虚拟机；
5. 使用已经安装好的虚拟机；
6. 在 Windows 和 Linux 虚拟机上运行常用的信息安全相关的命令行程序，用 CSocket 编写 C 语言程序实现两台计算机之间的网络通信；
7. 用网络侦察工具探测远程主机的安全漏洞等信息；
8. 用经典的网络安全工具 netcat 在本机开启一个监听端口，实现远程木马的功能。
9. **实验内容**
10. 选择一种较新的 Windows 版本 VirtualBox，安装 VirtualBox 虚拟机。
11. 配置多个虚拟网卡，在一台主机上模拟多个网络交换机，实现多个子网的互联。
12. 安装和配置新的 ubuntu Linux。
13. 配置和使用已安装好的虚拟机，设置虚拟机操作系统的 IP 地址，使用 Ping 命令测试 其能否与主机(或其它虚拟机)进行网络通信。
14. 在虚拟机上运行常用的命令行程序。
15. **实验步骤**
16. 安装 VirtualBox 虚拟机

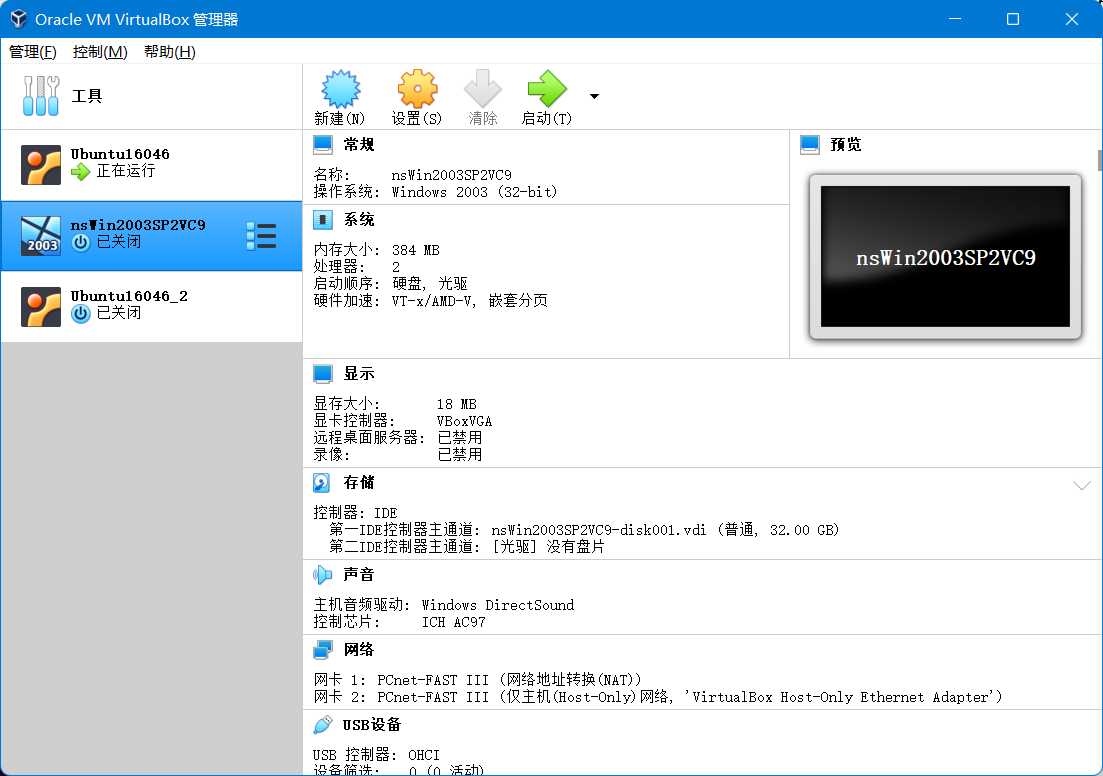


1. 配置多个虚拟网卡，模拟多个网络

1. 安装和配置新的虚拟机系统

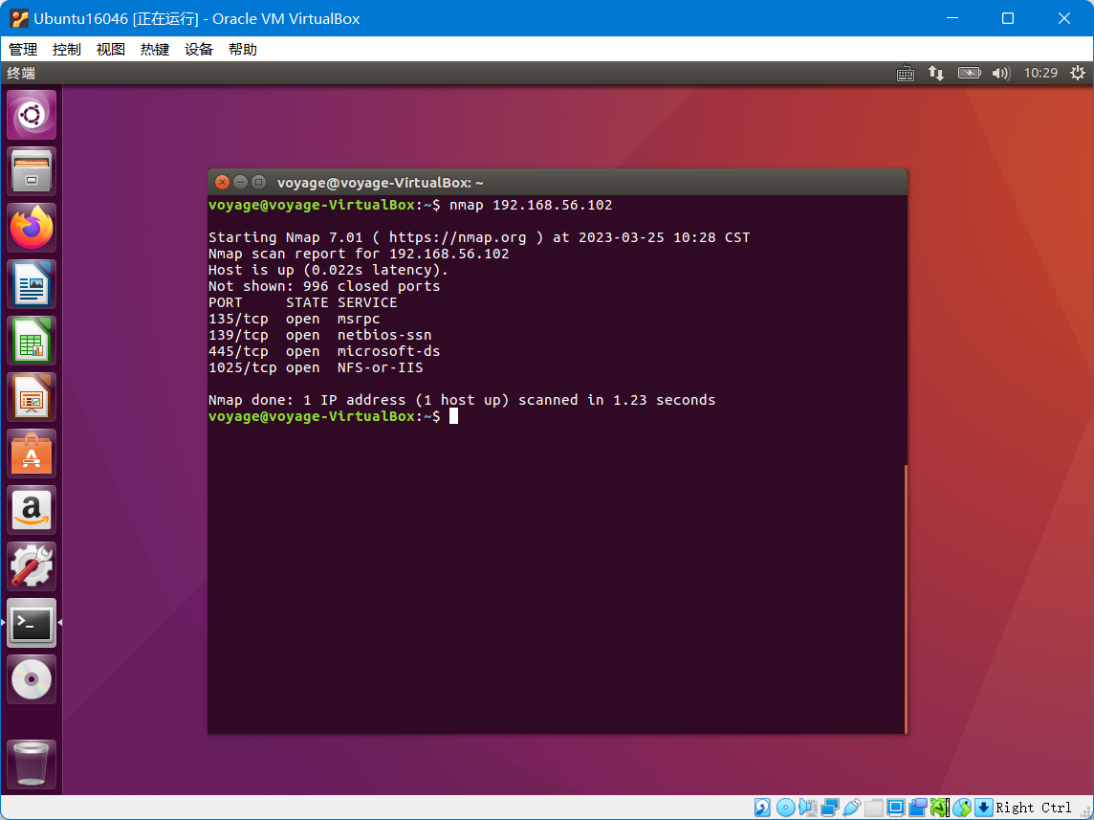


1. 导入和导出安装好的虚拟机

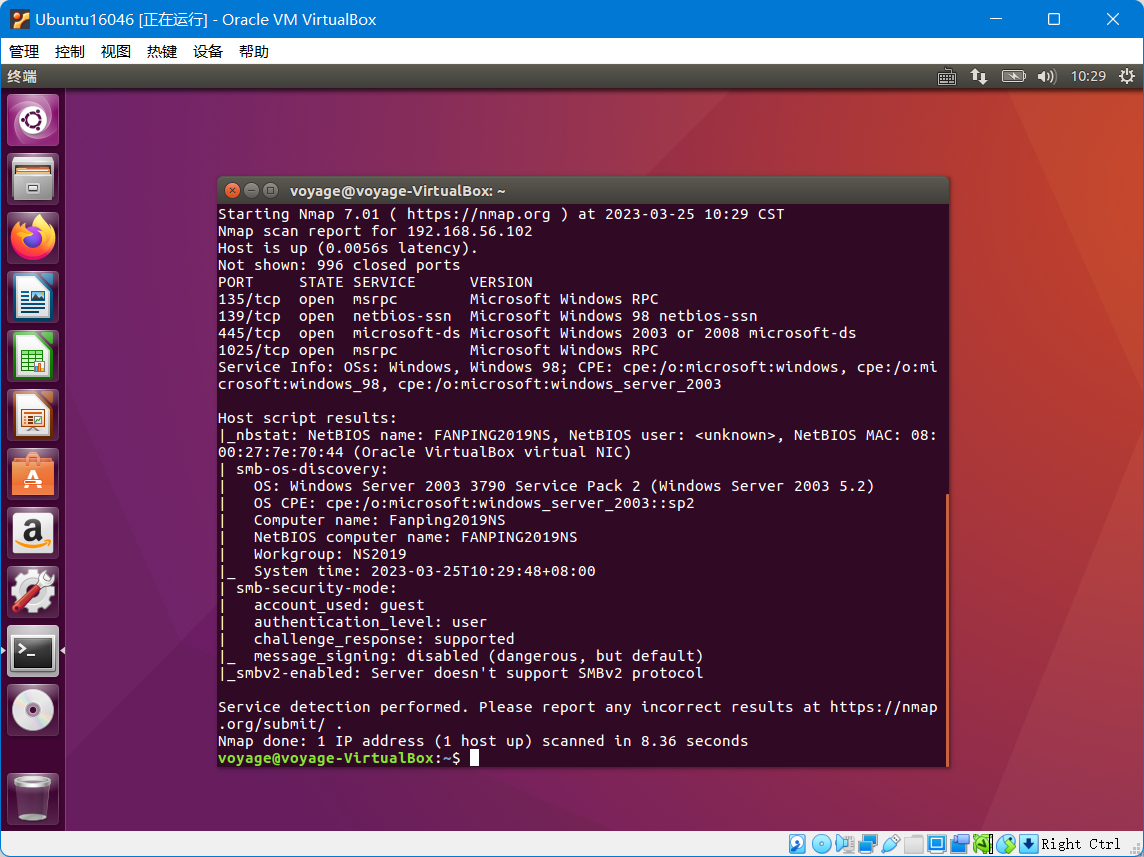


1. **上机实验**
2. 用 ubuntu 虚拟机中的网络侦察工具 nmap（如果没有，安装一个）查看并记录已下 载的 Windows 2003 虚拟机中开放了哪些网络端口，用 nmap 探测 Windows 2003 虚拟机的操 作系统类型。

开放的端口：使用nmap 192.168.56.102

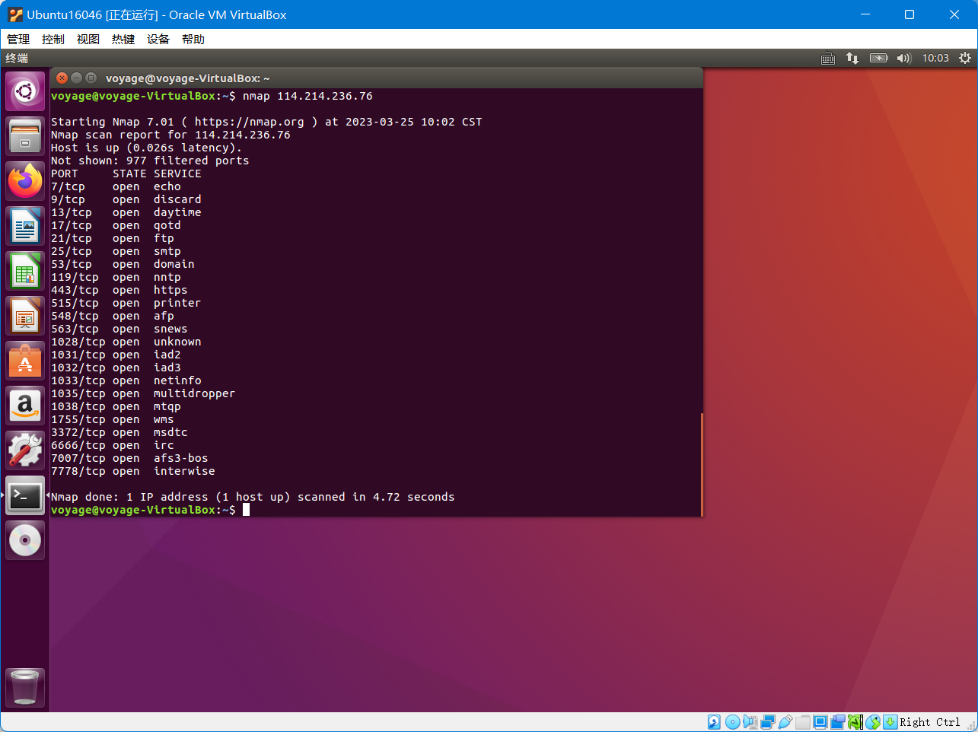


探测操作系统：使用 nmap -A 192.168.56.102



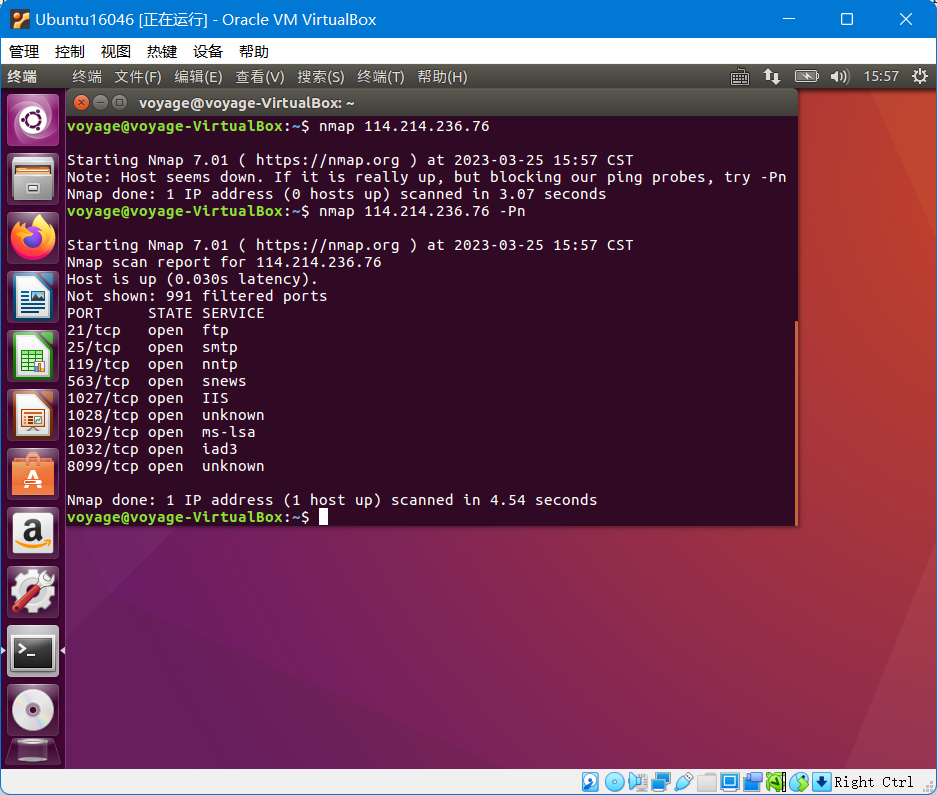
1. 在以下时间段用 nmap 扫描 114.214.236.76，查看并记录该 IP 地址开放了哪些端口。

* 2023 年 3 月 25 日星期六，上午 8:00 至 12:00



* 2023 年 3 月 25 日星期六，上午 14:00 至 18:00

第一次出现错误的情况，根据提示，添加了相关参数，顺利完成实验

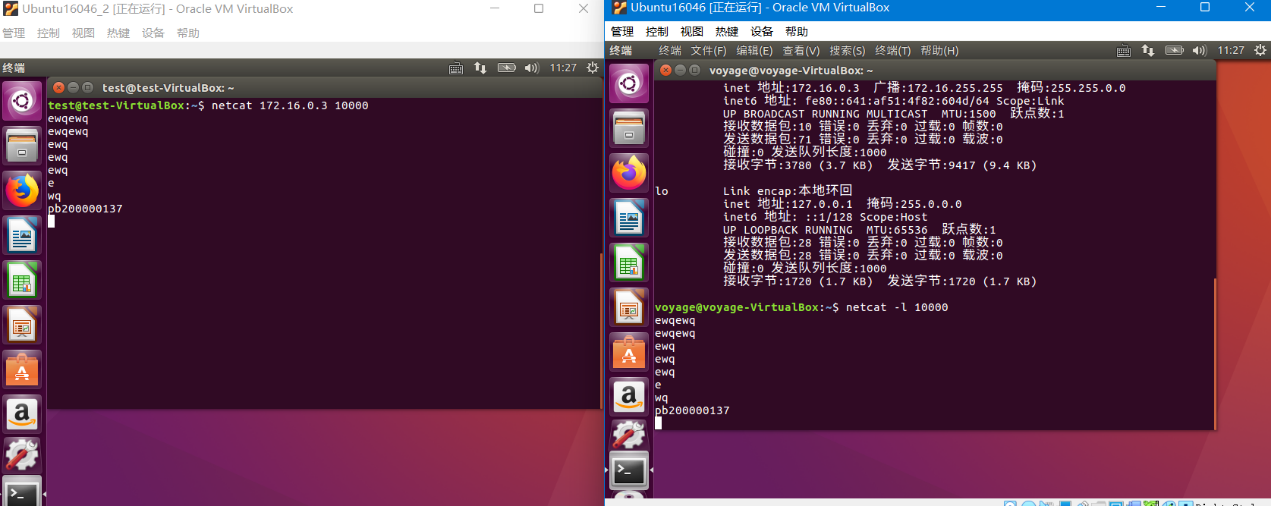


1. 在 ubuntu 虚拟机中用经典的网络安全工具 netcat 在本机开启一个监听端口，实现远程木马的功能

如图所示，先查询获得右图中系统的ip为172.16.0.3

右图使用 netcat -l 10000 命令，监听10000端口

左图中命令行使用 netcat 172.16.0.3 10000 命令，输入字符，可以在右图监听端口呈现同样的输出



1. **实验收获**
2. 熟悉了linux操作系统相关命令行指令
3. 对网络安全实验有初步的了解
4. 认识到信息安全的重要性