信息安全的艺术　实验一

PB23010356 张竞一
学院：数学科学学院

2025 年 10 月 17 日

1　第一部分　虚拟机环境的搭建

1.1　实验环境

1.1.1　硬件条件

主机操作系统：Windows11
内存：16GB
硬盘空间：512GB

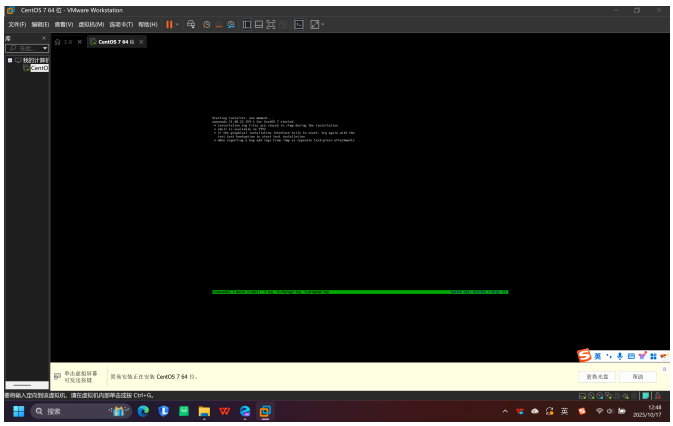
1.1.2　软件条件

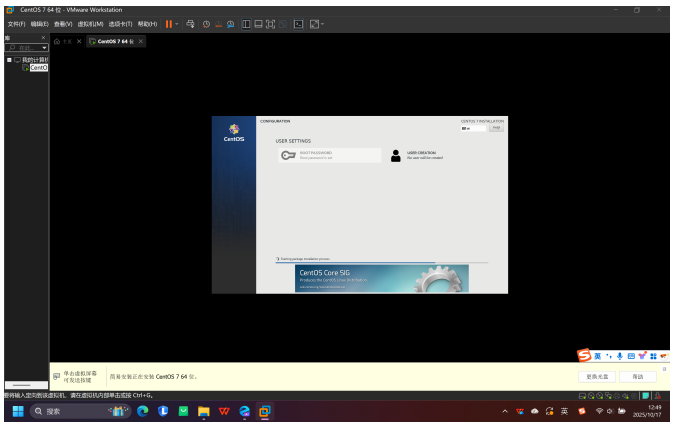
虚拟机软件：VMware Workstation Pro
安装的操作系统：CentOS 7
网络模式：桥接模式

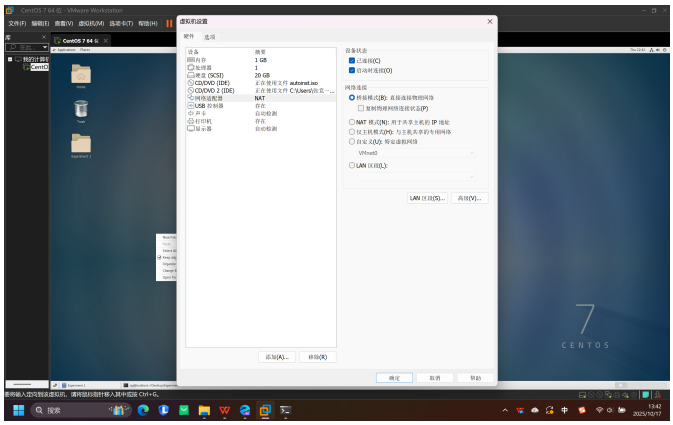
1.2　实验结果

1.2.1　虚拟机环境搭建

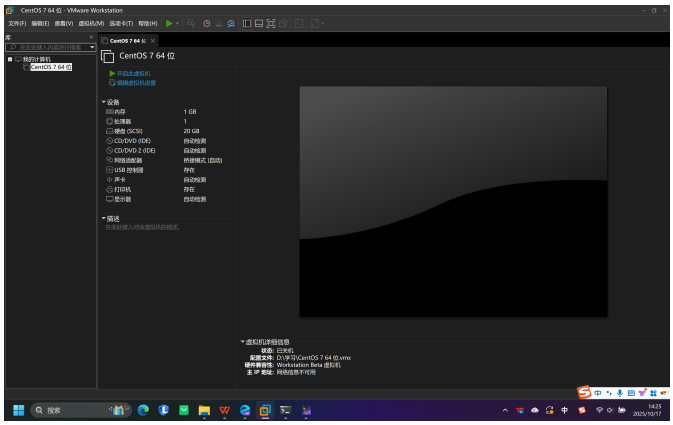
下载 VMware Workstation Pro 作为虚拟机载体，然后将下载的 CentOS-7-x86_64-DVD-2009.iso 文件导入进行虚拟机的安装，在创建账户后登录账户即可进入 CentOS 7 系统页面。页面中可以进行文件夹创建，终端打开输入指令等操作。







虚拟机属性如下：



2 第二部分 网格命令的使用

2.1 ping 命令

2.1.1 指令说明

ping 命令用于测试主机之间的网络连接是否畅通，通过发送 ICMP 回显请求报文来检测目标主机是否可达。

2.1.2 常用指令

- 基本用法：`ping [目标 IP 或域名]`
- 指定发送次数：`ping -n [次数] [目标]`（Windows）或 `ping -c [次数] [目标]`（Linux）
- 指定超时时间：`ping -w [超时时间（ms）] [目标]`（Windows）或 `ping -W [超时时间（s）] [目标]`（Linux）
- 连续 ping 直到手动停止：`ping -t [目标]`（Windows）或 `ping [目标]`（Linux，默认连续 ping）

附上 Windows 执行 `ping` 命令的终端截图:

```
C:\Users\张竞一>ping ustc.edu.cn

正在 Ping ustc.edu.cn [2001:da8:d800:642::248] 具有 32 字节的数据:
来自 2001:da8:d800:642::248 的回复: 时间=4ms
来自 2001:da8:d800:642::248 的回复: 时间=5ms
来自 2001:da8:d800:642::248 的回复: 时间=4ms
来自 2001:da8:d800:642::248 的回复: 时间=2ms

2001:da8:d800:642::248 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 5ms, 平均 = 3ms

C:\Users\张竞一>ping -n 3 ustc.edu.cn

正在 Ping ustc.edu.cn [2001:da8:d800:642::248] 具有 32 字节的数据:
来自 2001:da8:d800:642::248 的回复: 时间=2ms
来自 2001:da8:d800:642::248 的回复: 时间=4ms
来自 2001:da8:d800:642::248 的回复: 时间=4ms

2001:da8:d800:642::248 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 4ms, 平均 = 3ms
```

2.2 `tracert/traceroute` 命令

2.2.1 指令说明

`tracert`（Windows）和 `traceroute`（Linux）用于跟踪数据包从源主机到目标主机所经过的路由路径，显示每个跃点的延迟时间。

2.2.2 常用指令

- 基本用法：`tracert [目标]`（Windows）或 `traceroute [目标]`（Linux）
- 指定最大跃点数:`tracert -h [跃点数] [目标]`（Windows）或 `traceroute -m [跃点数] [目标]`（Linux）
- 不解析 IP 对应的主机名：`tracert -d [目标]`（Windows）或 `traceroute -n [目标]`（Linux）

附上 Windows 执行 `tracert` 命令的终端截图:

```
C:\Users\张竞一>tracert ustc.edu.cn

通过最多 30 个跃点跟踪
到 ustc.edu.cn [2001:da8:d800:642::248] 的路由:

  1     4 ms     4 ms     7 ms  2001:da8:d800:310::2
  2     9 ms     8 ms     6 ms  2001:da8:d800:310::1
  3     5 ms     2 ms     4 ms  2001:da8:d800:ffff::158
  4     3 ms     4 ms     6 ms  2001:da8:d800:642::248

跟踪完成。

C:\Users\张竞一>tracert -h 50 ustc.edu.cn

通过最多 50 个跃点跟踪
到 ustc.edu.cn [2001:da8:d800:642::248] 的路由:

  1    31 ms    15 ms    12 ms  2001:da8:d800:310::2
  2    23 ms    14 ms    30 ms  2001:da8:d800:310::1
  3    17 ms    12 ms    15 ms  2001:da8:d800:ffff::158
  4    27 ms    15 ms    13 ms  2001:da8:d800:642::248

跟踪完成。
```

2.3 nslookup 命令

2.3.1 指令说明

nslookup 命令用于查询域名系统（DNS）以获取域名对应的 IP 地址，或 IP 地址对应的域名。

2.3.2 常用指令

- 基本用法：`nslookup [域名]`
- 指定 DNS 服务器查询：`nslookup [域名] [DNS 服务器 IP]`
- 交互模式：直接输入 nslookup 进入交互模式，然后输入 `set type=mx` 查询邮件交换记录

附上执行 nslookup 命令的终端截图

```
C:\Users\张竞一>nslookup ustc.edu.cn
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

名称:    ustc.edu.cn
Addresses:  2001:da8:d800:642::248
          202.38.64.246
```

2.4 ipconfig/ifconfig 命令

2.4.1 指令说明

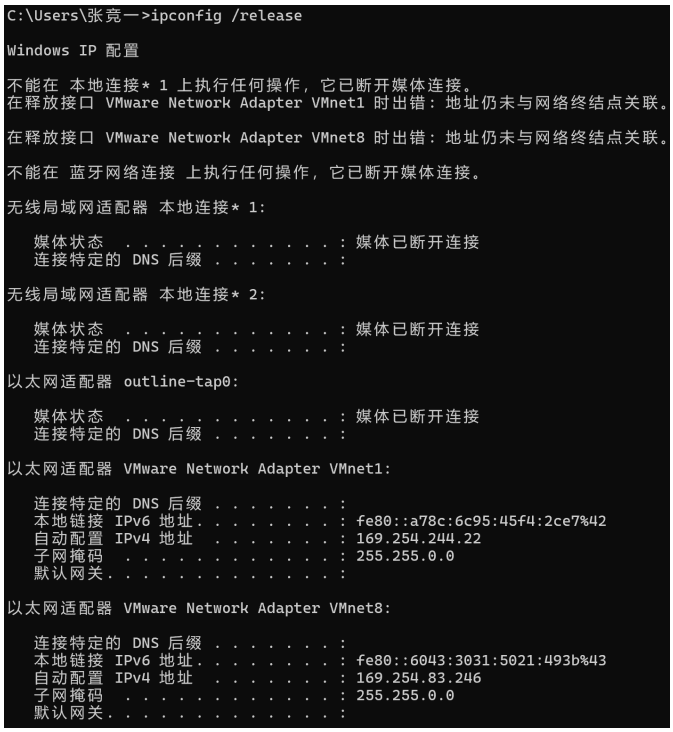
- ipconfig（Windows）：用于显示、修改和刷新本机的网络配置信息。

- `ifconfig` / `ip`（Linux）：用于配置和显示网络接口信息。

2.4.2 常用指令

- Windows：
  - 显示所有网络配置信息：`ipconfig /all`
  - 刷新 DNS 缓存：`ipconfig /flushdns`
  - 释放 IP 地址：`ipconfig /release`
  - 重新获取 IP 地址：`ipconfig /renew`
- Linux：
  - 显示网络接口信息：`ifconfig`（需安装 net-tools）或 `ip addr show`
  - 启用/禁用网络接口：`ifconfig [接口名] up/down` 或 `ip link set [接口名] up/down`

附上 Windows 执行 `ipconfig` 命令的终端截图



2.5 arp 命令

2.5.1 指令说明

arp 命令用于显示和修改本机的 ARP（地址解析协议）缓存表，将 IP 地址映射为 MAC 地址。

2.5.2 常用指令

- 显示 ARP 缓存表：`arp -a`
- 添加静态 ARP 映射：`arp -s [IP 地址] [MAC 地址]`
- 删除 ARP 映射：`arp -d [IP 地址]`

附上 Windows 执行 arp 命令的终端截图

```
C:\Users\张竞一>arp -a

接口: 100.65.18.27 --- 0xc
  Internet 地址         物理地址              类型
  100.65.0.1            c8-33-e5-8a-5d-45     动态
  100.65.57.128         c8-33-e5-8a-5d-45     动态
  100.65.63.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  224.55.10.221         01-00-5e-37-0a-dd     静态
  225.93.17.27          01-00-5e-5d-11-1b     静态
  230.129.136.119       01-00-5e-01-88-77     静态
  231.189.122.112       01-00-5e-3d-7a-70     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 169.254.244.22 --- 0x2a
  Internet 地址         物理地址              类型
  169.254.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 169.254.83.246 --- 0x2b
  Internet 地址         物理地址              类型
  169.254.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

2.6 route 命令

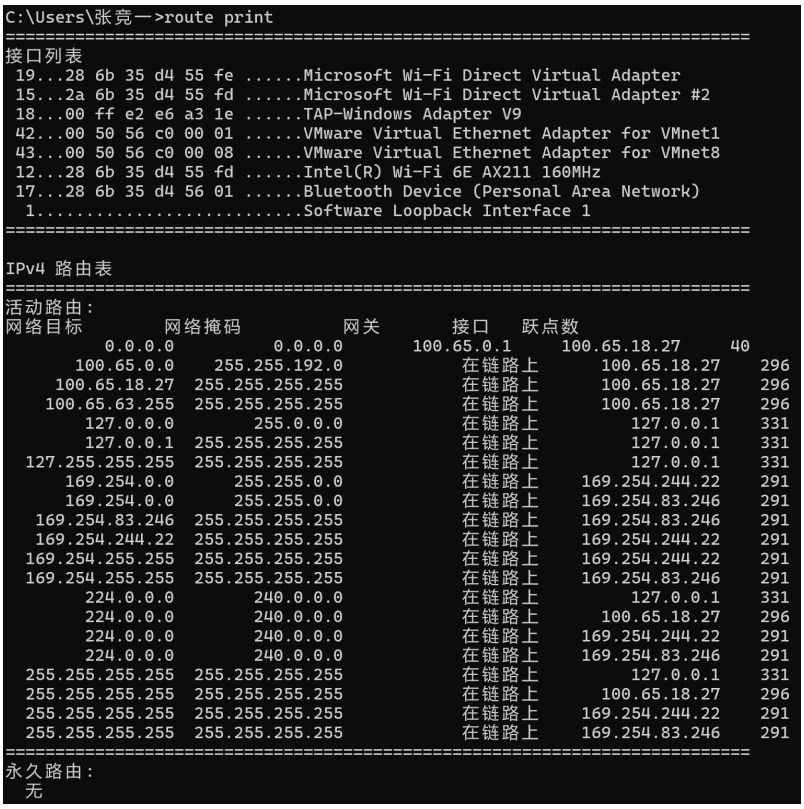
2.6.1 指令说明

route 命令用于显示和修改本机的路由表，管理数据包的转发路径。

2.6.2 常用指令

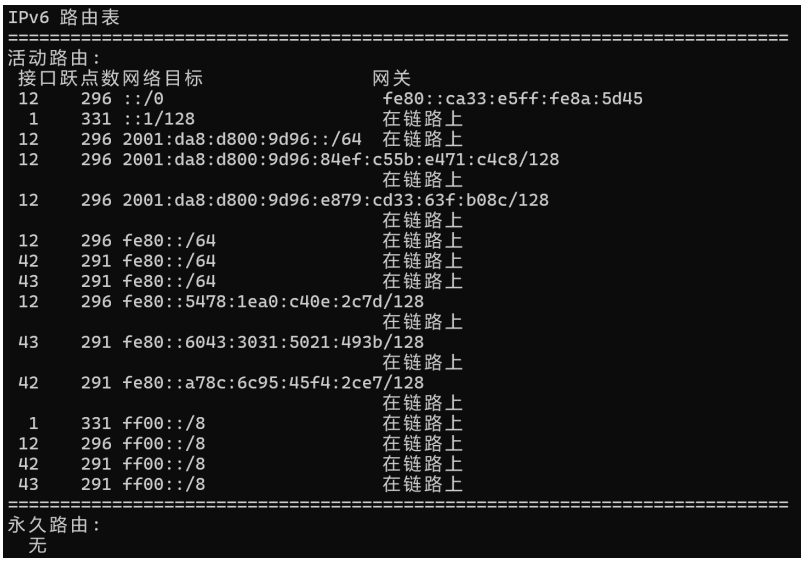
- 显示路由表：`route print`（Windows）或 `route -n`（Linux）
- 添加路由：`route add [目标网络] mask [子网掩码] [网关]`（Windows）或 `route add -net [目标网络] netmask [子网掩码] gw [网关]`（Linux）
- 删除路由：`route delete [目标网络]`

附上 Windows 执行 `route` 命令的终端截图



```
C:\Users\张竞一>route print
===========================================================================
接口列表
 19...28 6b 35 d4 55 fe ......Microsoft Wi-Fi Direct Virtual Adapter
 15...2a 6b 35 d4 55 fd ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...00 ff e2 e6 a3 1e ......TAP-Windows Adapter V9
 42...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 43...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 12...28 6b 35 d4 55 fd ......Intel(R) Wi-Fi 6E AX211 160MHz
 17...28 6b 35 d4 56 01 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      100.65.0.1     100.65.18.27     40
       100.65.0.0    255.255.192.0            在链路上       100.65.18.27    296
     100.65.18.27  255.255.255.255            在链路上       100.65.18.27    296
    100.65.63.255  255.255.255.255            在链路上       100.65.18.27    296
        127.0.0.0        255.0.0.0            在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上          127.0.0.1    331
      169.254.0.0      255.255.0.0            在链路上     169.254.244.22    291
      169.254.0.0      255.255.0.0            在链路上     169.254.83.246    291
   169.254.83.246  255.255.255.255            在链路上     169.254.83.246    291
   169.254.244.22  255.255.255.255            在链路上     169.254.244.22    291
  169.254.255.255  255.255.255.255            在链路上     169.254.244.22    291
  169.254.255.255  255.255.255.255            在链路上     169.254.83.246    291
        224.0.0.0        240.0.0.0            在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0            在链路上       100.65.18.27    296
        224.0.0.0        240.0.0.0            在链路上     169.254.244.22    291
        224.0.0.0        240.0.0.0            在链路上     169.254.83.246    291
  255.255.255.255  255.255.255.255            在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255            在链路上       100.65.18.27    296
  255.255.255.255  255.255.255.255            在链路上     169.254.244.22    291
  255.255.255.255  255.255.255.255            在链路上     169.254.83.246    291
===========================================================================
永久路由:
  无
```



```
IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                网关
 12    296 ::/0                    fe80::ca33:e5ff:fe8a:5d45
  1    331 ::1/128                 在链路上
 12    296 2001:da8:d800:9d96::/64 在链路上
 12    296 2001:da8:d800:9d96:84ef:c55b:e471:c4c8/128
                                   在链路上
 12    296 2001:da8:d800:9d96:e879:cd33:63f:b08c/128
                                   在链路上
 12    296 fe80::/64               在链路上
 42    291 fe80::/64               在链路上
 43    291 fe80::/64               在链路上
 12    296 fe80::5478:1ea0:c40e:2c7d/128
                                   在链路上
 43    291 fe80::6043:3031:5021:493b/128
                                   在链路上
 42    291 fe80::a78c:6c95:45f4:2ce7/128
                                   在链路上
  1    331 ff00::/8                在链路上
 12    296 ff00::/8                在链路上
 42    291 ff00::/8                在链路上
 43    291 ff00::/8                在链路上
===========================================================================
永久路由:
  无
```

2.7 netstat/ss 命令

2.7.1 指令说明

netstat（Windows/Linux）和 ss（Linux）用于显示网络连接、路由表、接口统计等信息。

2.7.2 常用指令

- 显示所有连接：netstat -a（Windows/Linux）或 ss -a（Linux）
- 显示进程使用的端口：netstat -anp（Windows）显示按当前使用的 TCP 或 UDP 端口数排序的进程列表：netstat -c（Windows）

附上 Windows 执行 netstat 命令的终端截图

```
C:\Users\张竞一>netstat -c

端口消耗

 协议  PID NumberOfPorts
  TCP    14168      35
  TCP    7452       12
  TCP    30432      11
  TCP    0          11
  TCP    34984      5
  TCP    14964      4
  TCP    38744      4
  TCP    40360      4
  TCP    4080       3
  TCP    5552       3
  TCP    10088      3
  TCP    22764      3
  TCP    9204       2
  TCP    4          2
  TCP    22656      2
  TCP    5892       2
  TCP    9040       2
  TCP    22100      2
  TCP    11476      2
  TCP    5456       2
  TCP    6352       1
  TCP    22876      1
  TCP    23056      1
  TCP    4860       1
  TCP    19880      1
  TCP    1576       1
  TCP    10112      1
  TCP    29032      1
  TCP    9224       1
  TCP    5744       1
  TCP    2016       1
  TCP    13544      1
  TCP    1760       1
  TCP    32520      1
  TCP    2548       1
  TCP    1708       1
  TCP    28248      1
  TCP    3164       1
  TCP    5688       1
  TCP    35204      1
  UDP    10736      9
  UDP    2376       6
  UDP    4080       3
  UDP    4          2
  UDP    5572       1
  UDP    40360      1
  UDP    34984      1
  UDP    13544      1
  UDP    10088      1
  UDP    21116      1
  UDP    30432      1
```