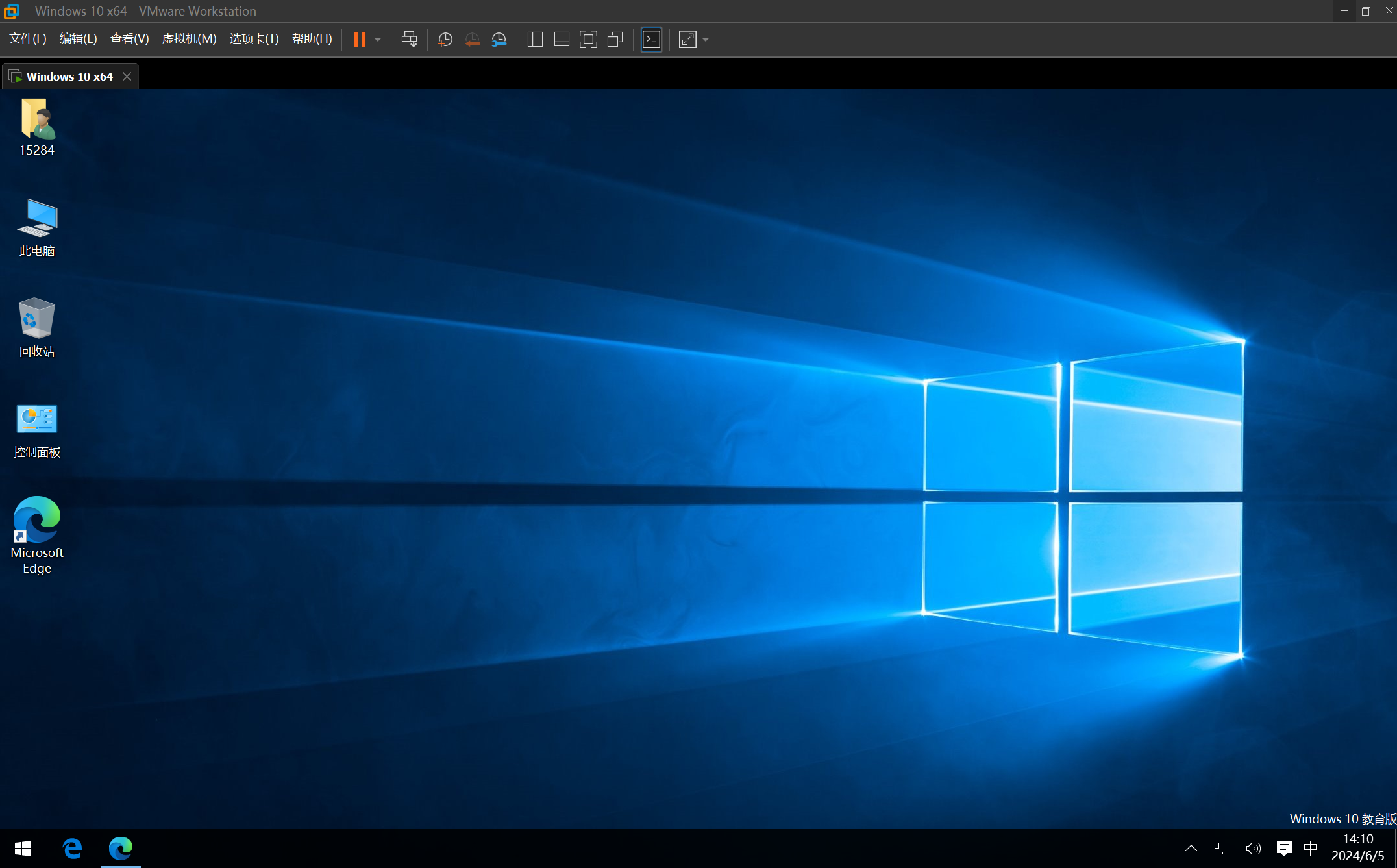
漏洞挖掘环境搭建

1. 搭建windows 内核调试环境，下载虚拟机镜像并使用hyper-v安装虚拟机

windows 10 20H1 X64

ed2k://|file|cn\_windows\_10\_business\_editions\_version\_2004\_updated\_sep\_2020\_x64\_dvd\_7134ba4b.iso|5313628160|7CF0E7C3324B4209663B8B971A5ACEF2|/

下载windows10镜像之后安装到Wmware虚拟机中



1. 宿主机上搭建windbg调试环境，并基于第一个实验中的windows虚拟机搭建内核调试环境

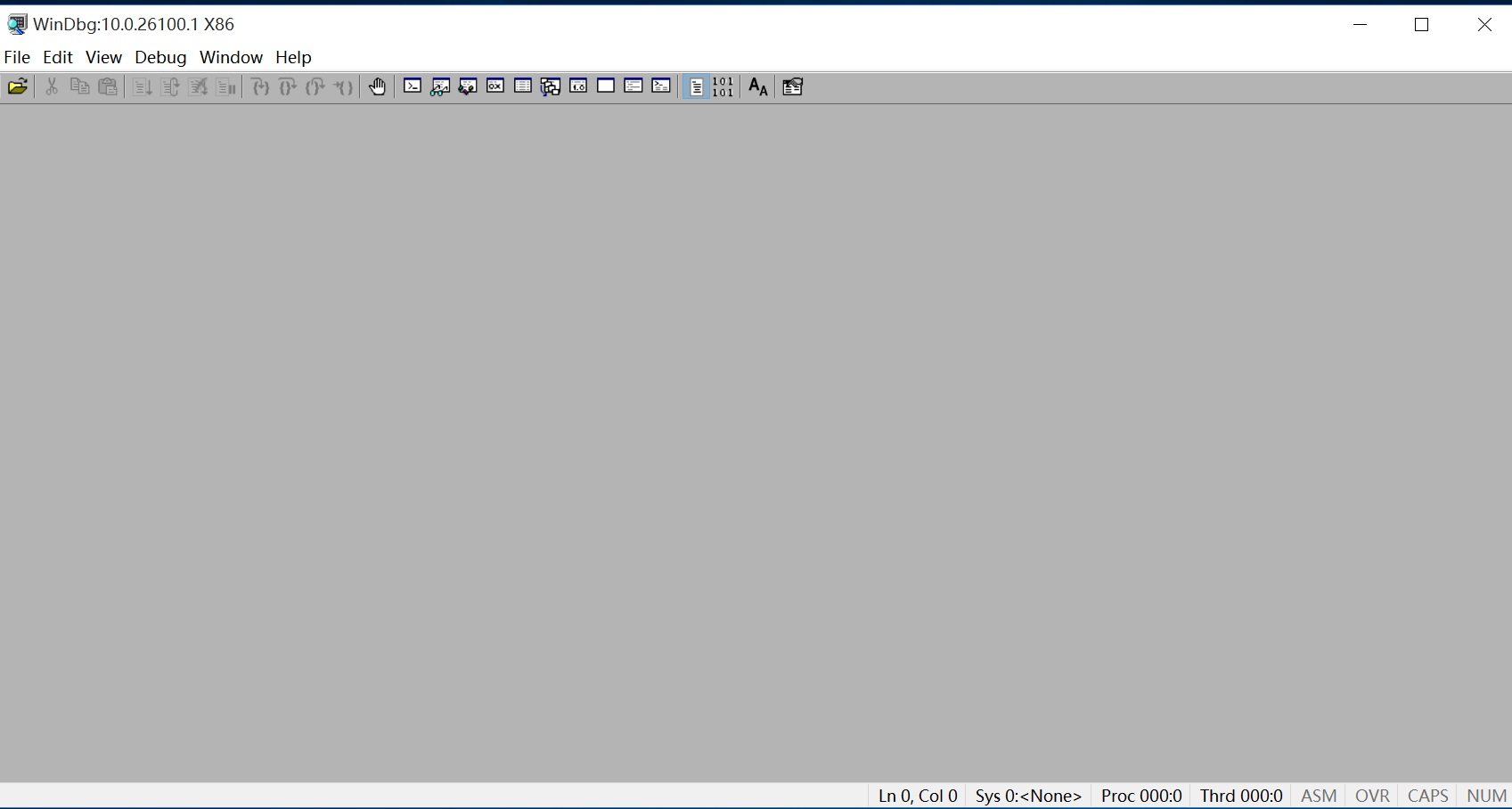
windbg (download from windows sdk)

https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/

在对应的网址下载WDK然后进行安装



安装完成之后如下图所示



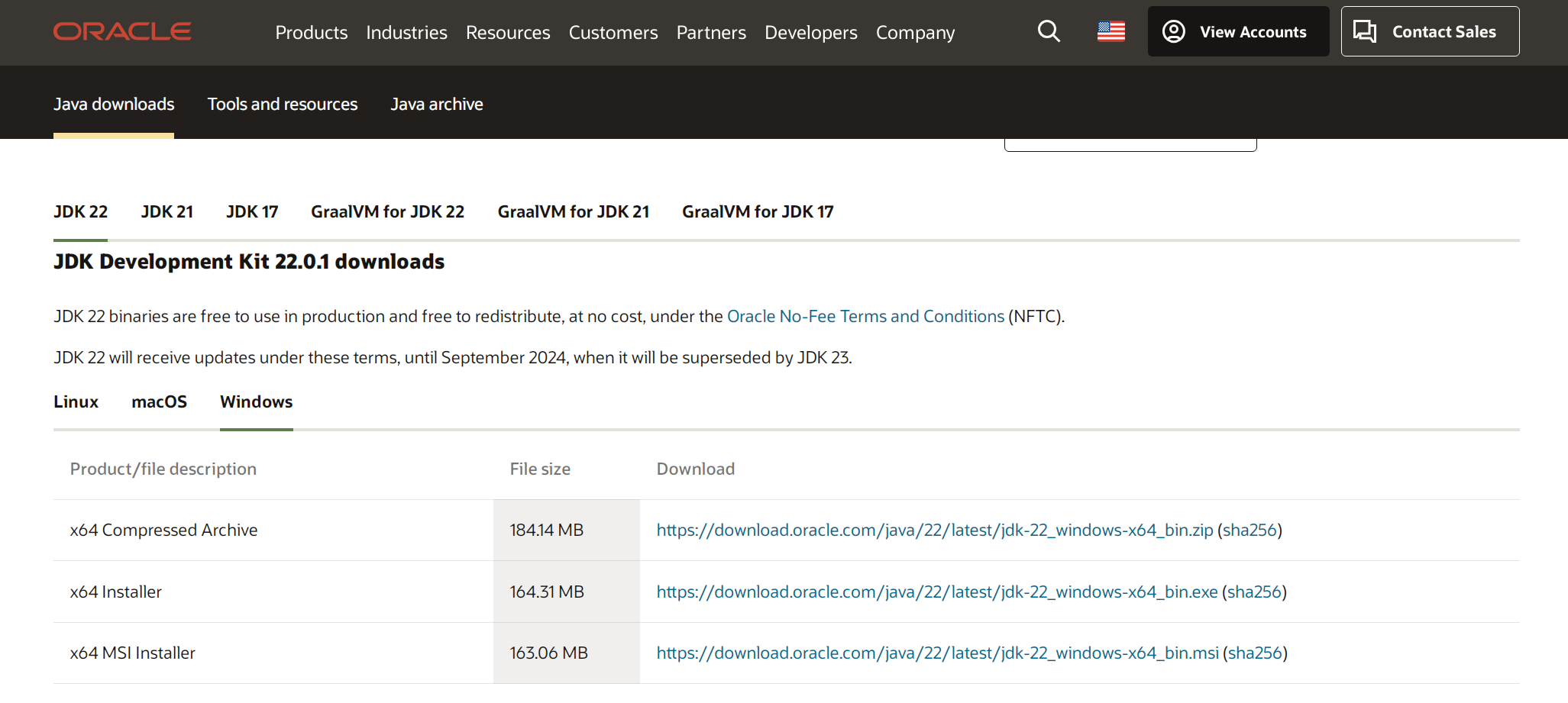
1. 安装Bindiff

Bindiff

<https://github.com/google/bindiff/releases/tag/v8>

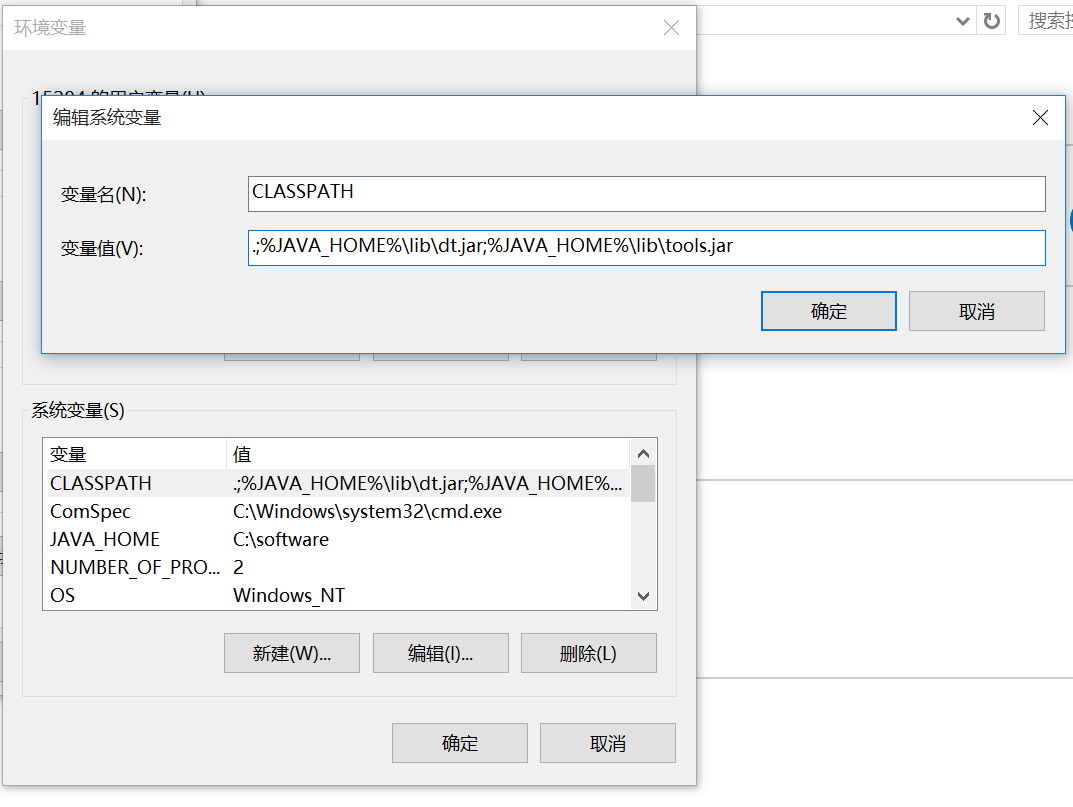
首先安装JDK环境

<https://www.oracle.com/java/technologies/downloads/?er=221886#jdk22-windows>

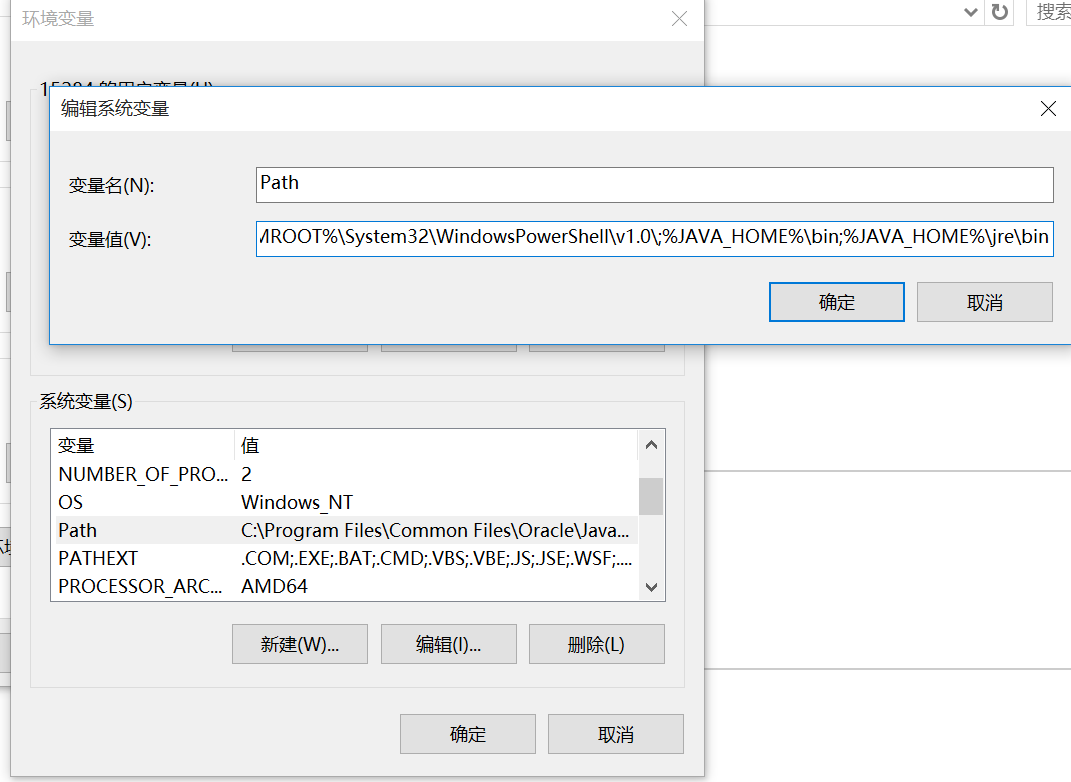


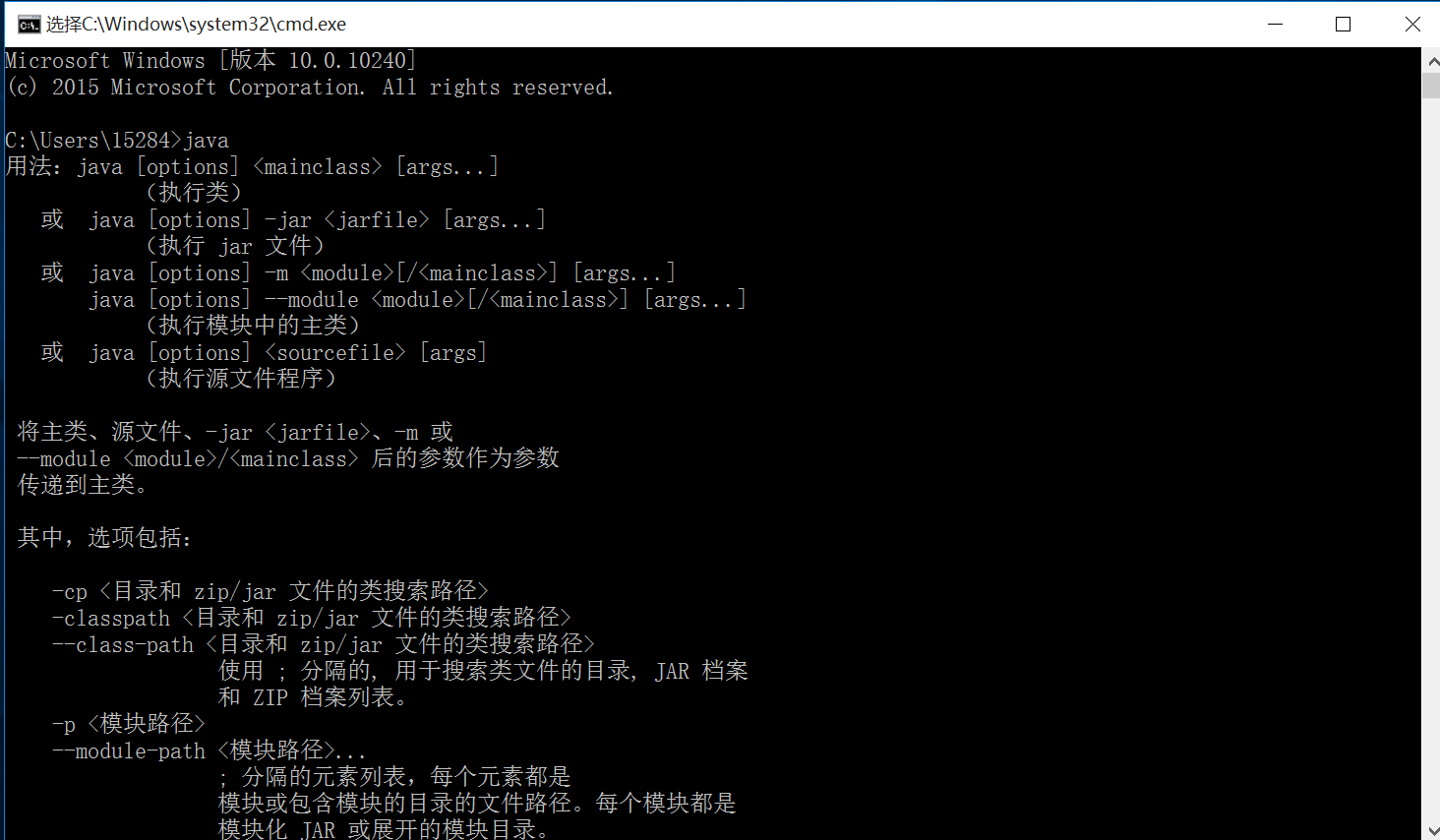
接下来为java配置环境变量

新建CLASSPATH

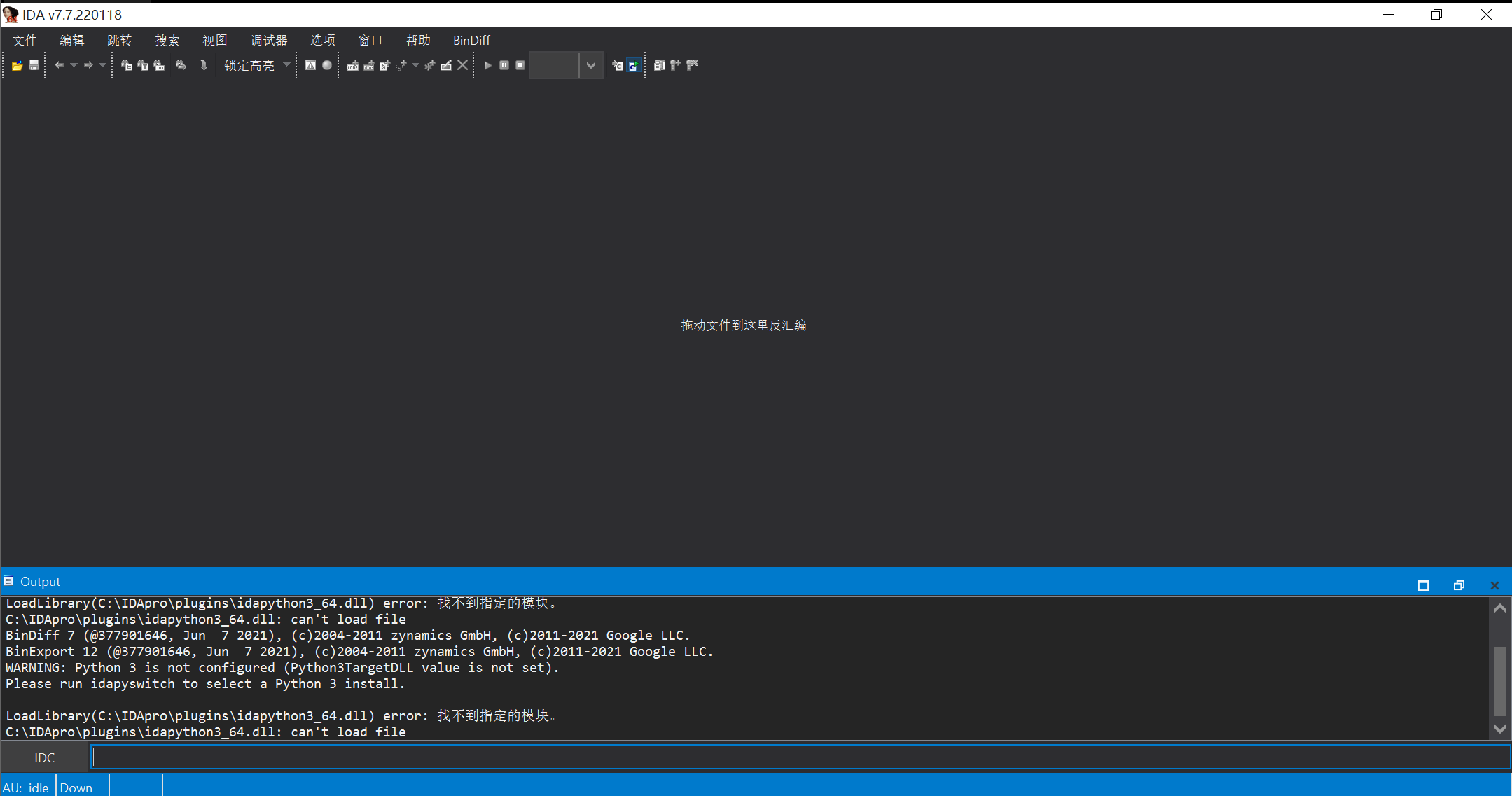


配置Path变量

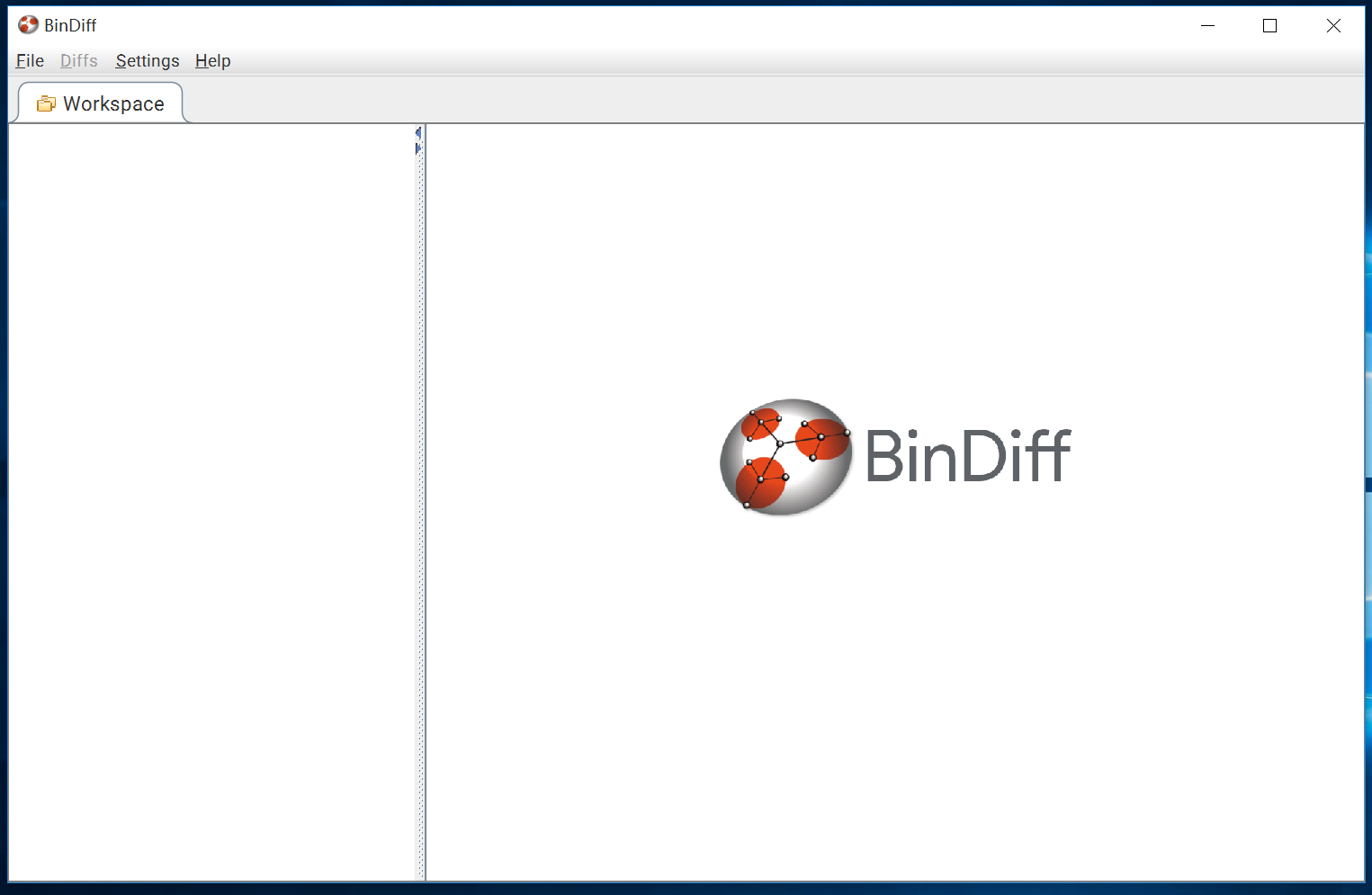
检查JAVA环境



接下来下载IDA pro



接下来安装bindiff

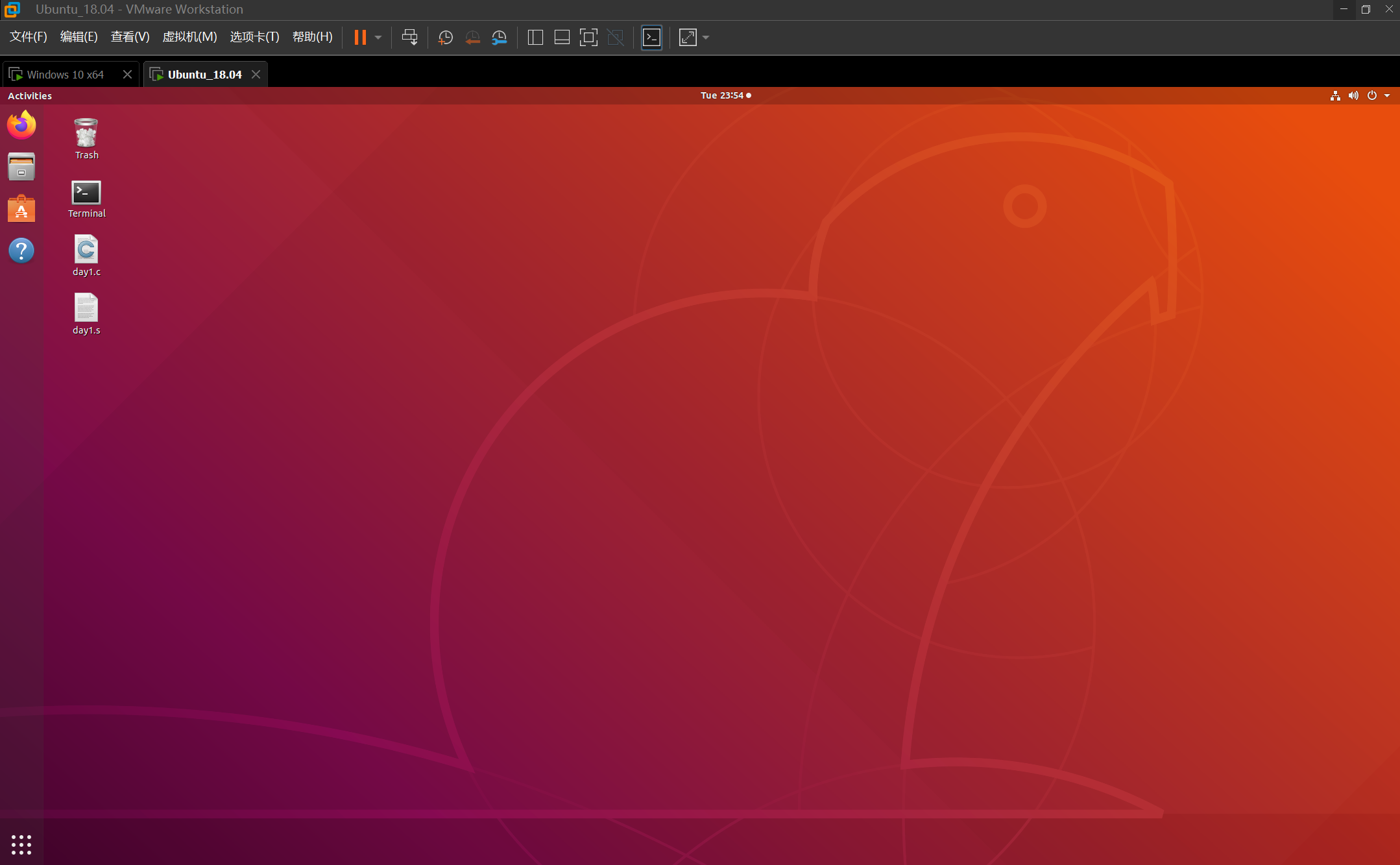


1. 安装Ubuntu fuzz和编译环境

Ubuntu 18.04

<https://releases.ubuntu.com/18.04/ubuntu-18.04.6-desktop-amd64.iso>

安装Ubuntu18.04虚拟机

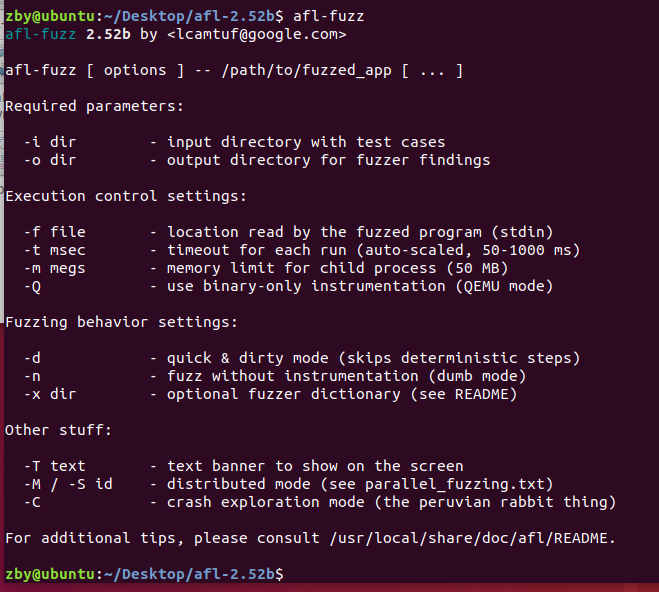


1. 在第四个搭建的环境中安装afl-fuzz工具

afl-fuzz

<https://lcamtuf.coredump.cx/afl/>

在终端中运行该工具afl-fuzz成功出现帮助信息

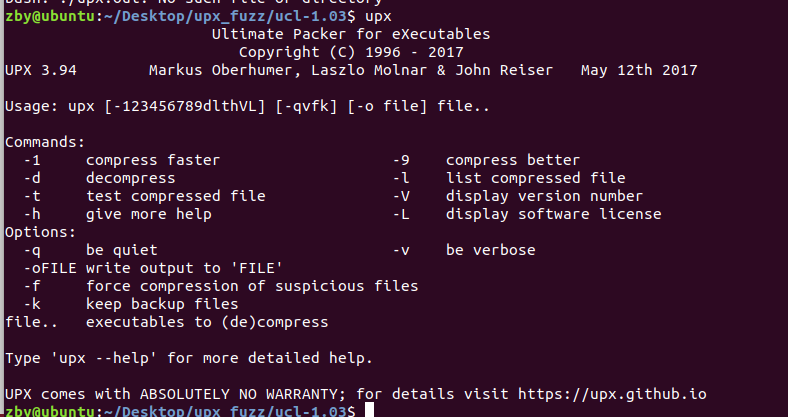


1. 编译upx fuzz目标程序

Upx 请源码编译，对照MakeFile中的安装文档

<https://github.com/upx/upx>

在终端中运行该工具，成功出现帮助信息



1. 宿主机安装Visual Studio 2022 Community版本，并在Visual Studio Installer中安装 C/C++, Windows 10 SDK (10.0.19041.0) 开发环境

<https://visualstudio.microsoft.com/zh-hans/>

下载Visual Studio 2022 Community之后安装如下的开发环境



