

# nc(NETCAT)

NETCAT是一种特色的网络实用工具，使用TCP/IP协议读取和写入网络连接的数据。它被设计成一个可靠的“后端”工具，它可以直接或容易地被其他程序和脚本驱动。同时，它是一个功能丰富的网络调试和探索工具，因为它可以创建几乎任何类型的连接。

## 下载教程

### 一、Linux环境

无需下载，系统自带，只需要打开终端（命令行），即可直接使用。

```
ubuntu@LAPTOP-TCFTP77V: $ nc
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
        [-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
```

linux进入终端的方法：

方法一：

使用快捷键：Ctrl+Alt+T。

方法二：搜索框内搜索“终端”。

### 二、Windows环境

个人建议最好使用法三，简单方便。然后是法一，不太建议法二。法四其实是最好的，但是要求有点高。

#### 法一：安装Powercat

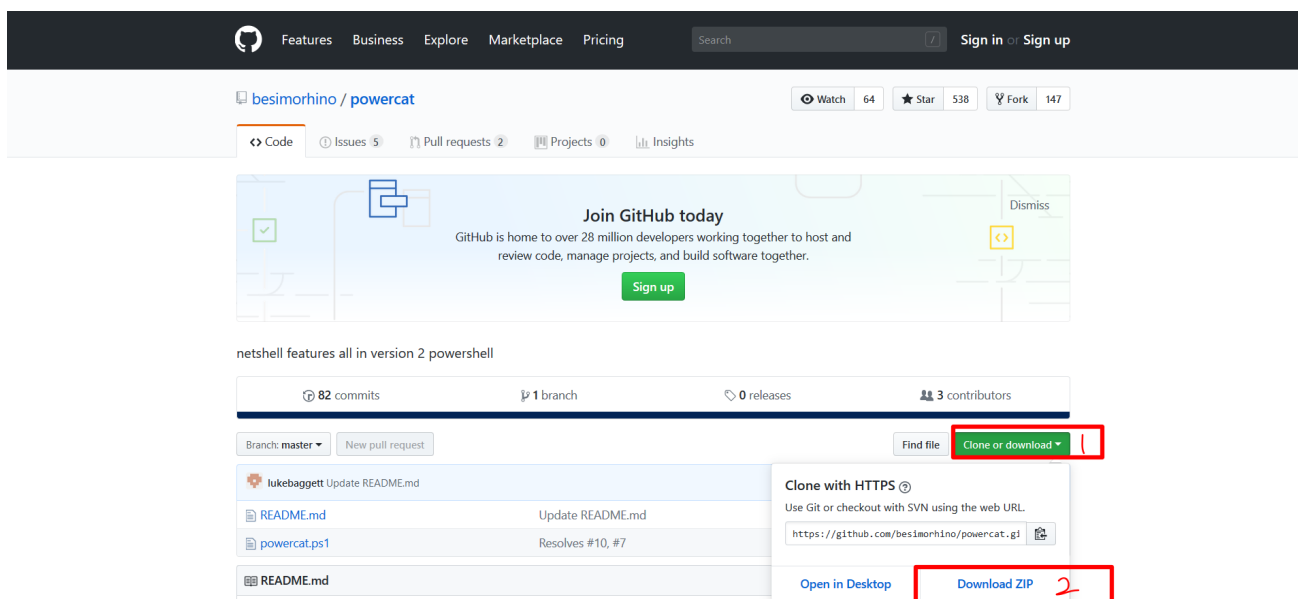
powercat简介

是 NetCat 的 Powershell 版本。注意：使用此方法指令会有所不同

下载地址：

<http://www.4hou.com/info/news/5205.html>

打开后点击 Clone or download，然后再弹出来的窗口中点击 Download ZIP。



下载到本地后进行解压，解压出来的是这两个文件。

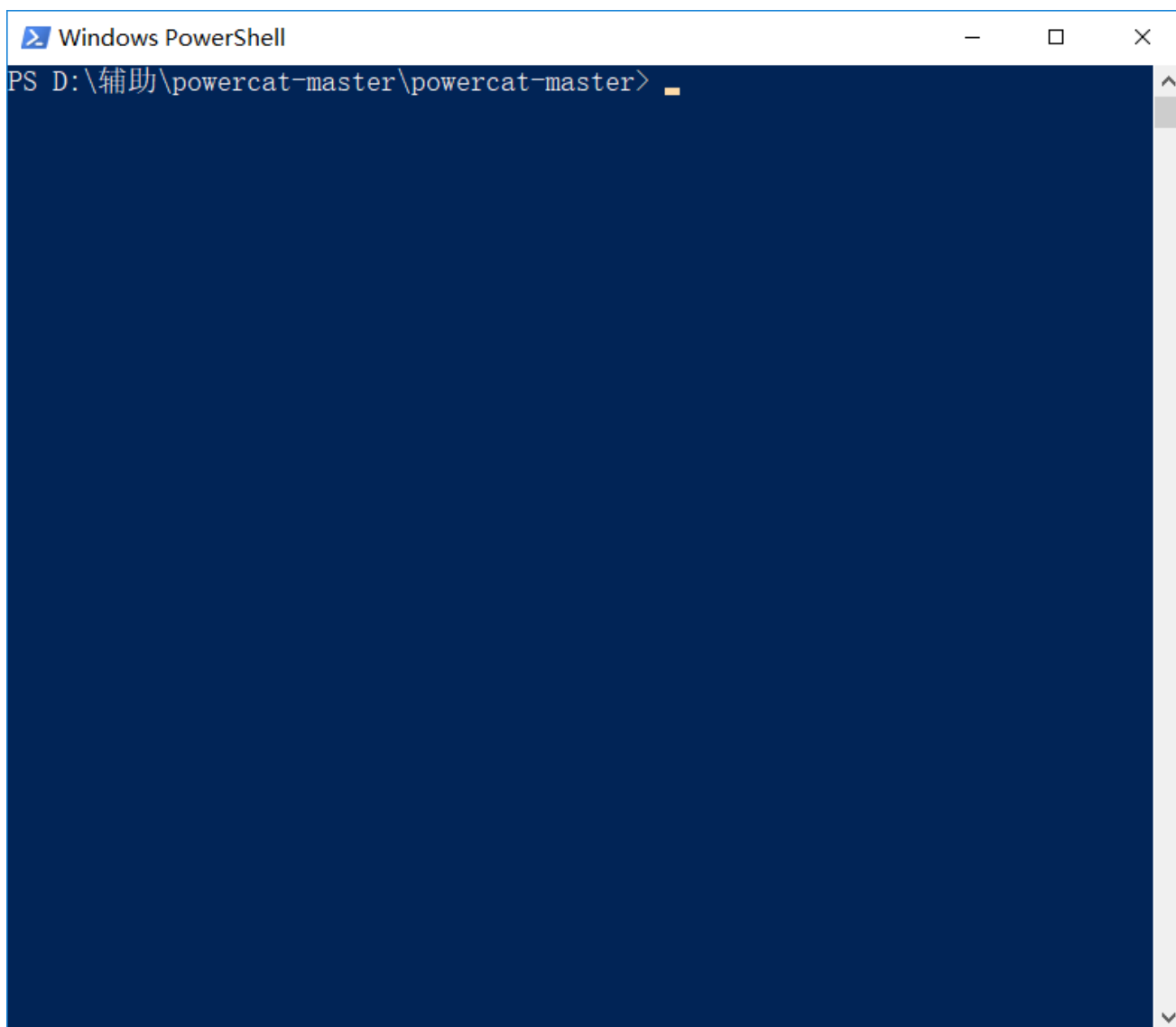
 powercat.ps1	2017/8/5 12:19	Windows Power...	37 KB
 README.md	2017/8/5 12:19	Markdown File	6 KB

然后在当前文件夹下，按住 **shift** 键的同时点击右键。菜单里会多出一个 **在此处打开Powershell窗口**。然后点击 **在此处打开Powershell窗口**。

名称	修改日期	类型	大小
 powercat.ps1	2017/8/5 12:19	Windows Power...	37 KB
 README.md	2017/8/5 12:19	Markdown File	6 KB



会出现窗口。

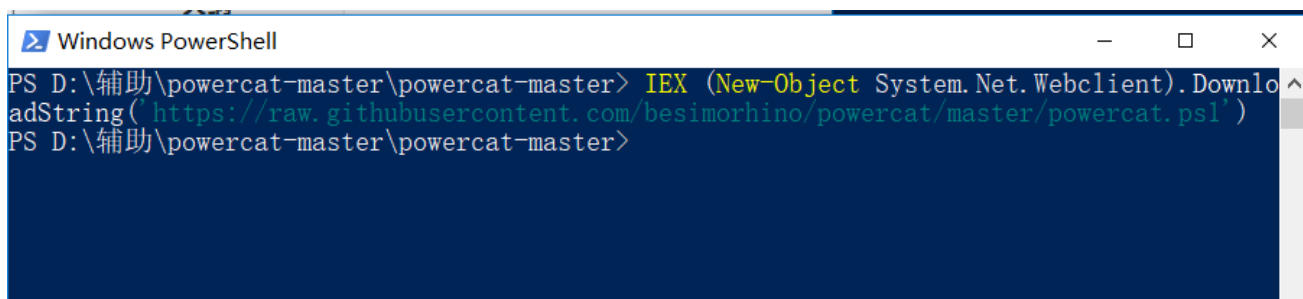


```
Windows PowerShell
PS D:\辅助\powercat-master\powercat-master>
```

然后输入

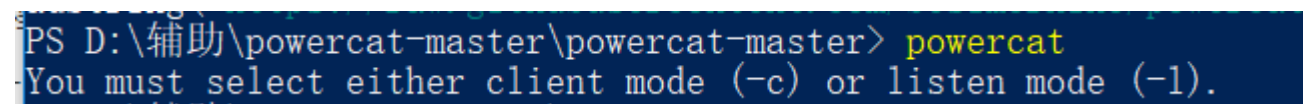
```
IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1')
```

若无报错则进行下一步。注：以后每一次重新打开PowerShell来使用powercat，都要重新输入一次该语句



```
Windows PowerShell
PS D:\辅助\powercat-master\powercat-master> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1')
PS D:\辅助\powercat-master\powercat-master>
```

输入 `powercat`，若显示以下内容则说明安装成功。



```
PS D:\辅助\powercat-master\powercat-master> powercat
You must select either client mode (-c) or listen mode (-l).
```

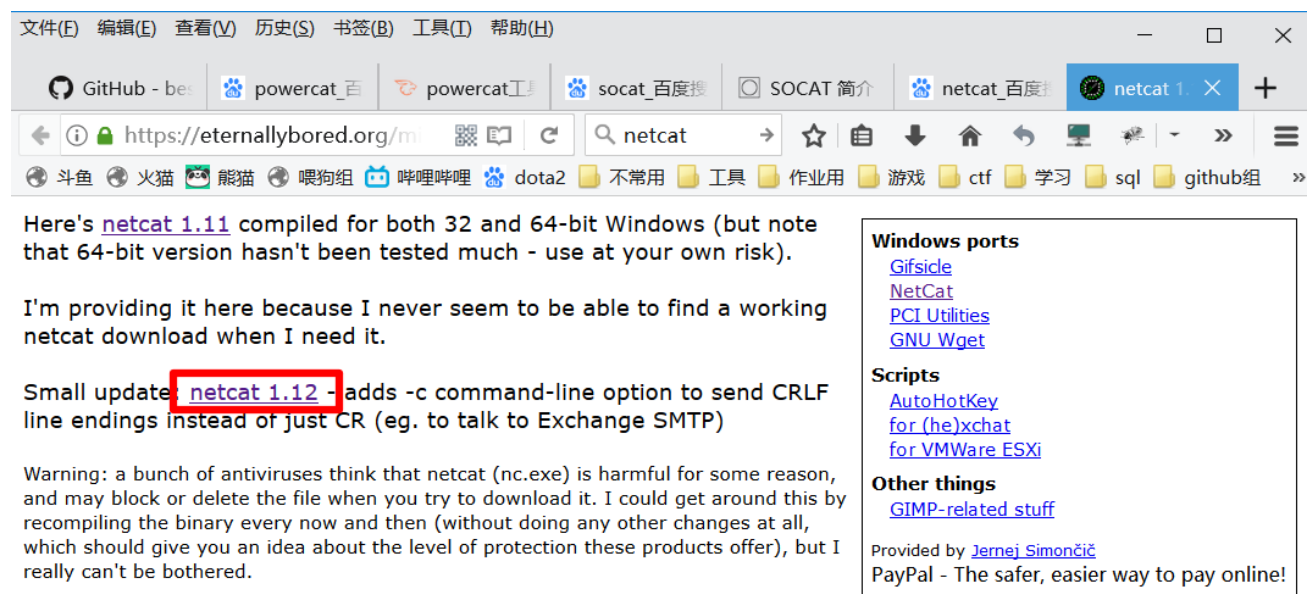
## 法二：安装netcat

此法需要关闭电脑的各种安全软件。例如360，腾讯管家，火绒等等。

下载地址：

<https://eternallybored.org/misc/netcat/>

访问后，点击 netcat 1.12 进行下载。



Here's [netcat 1.11](#) compiled for both 32 and 64-bit Windows (but note that 64-bit version hasn't been tested much - use at your own risk).

I'm providing it here because I never seem to be able to find a working netcat download when I need it.

Small update: **netcat 1.12** - adds -c command-line option to send CRLF line endings instead of just CR (eg. to talk to Exchange SMTP)

Warning: a bunch of antiviruses think that netcat (nc.exe) is harmful for some reason, and may block or delete the file when you try to download it. I could get around this by recompiling the binary every now and then (without doing any other changes at all, which should give you an idea about the level of protection these products offer), but I really can't be bothered.

**Windows ports**

- [Gifsicle](#)
- [NetCat](#)
- [PCI Utilities](#)
- [GNU Wget](#)

**Scripts**

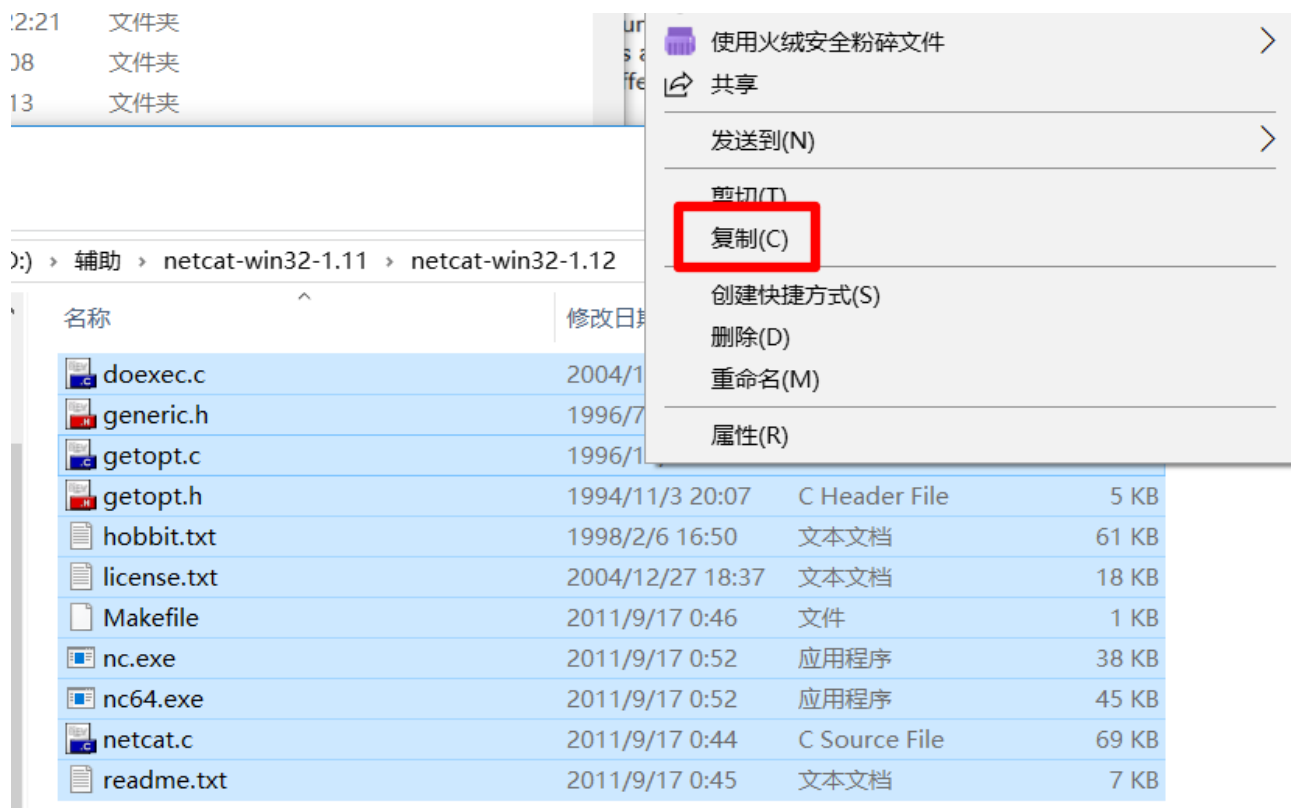
- [AutoHotKey for \(he\)xchat](#)
- [for VMWare ESXi](#)

**Other things**

- [GIMP-related stuff](#)

Provided by [Jernej Simončič](#)  
PayPal - The safer, easier way to pay online!

下载完成后，进行解压，然后将解压下来的所有程序都复制到 c:\windows\System32 中。



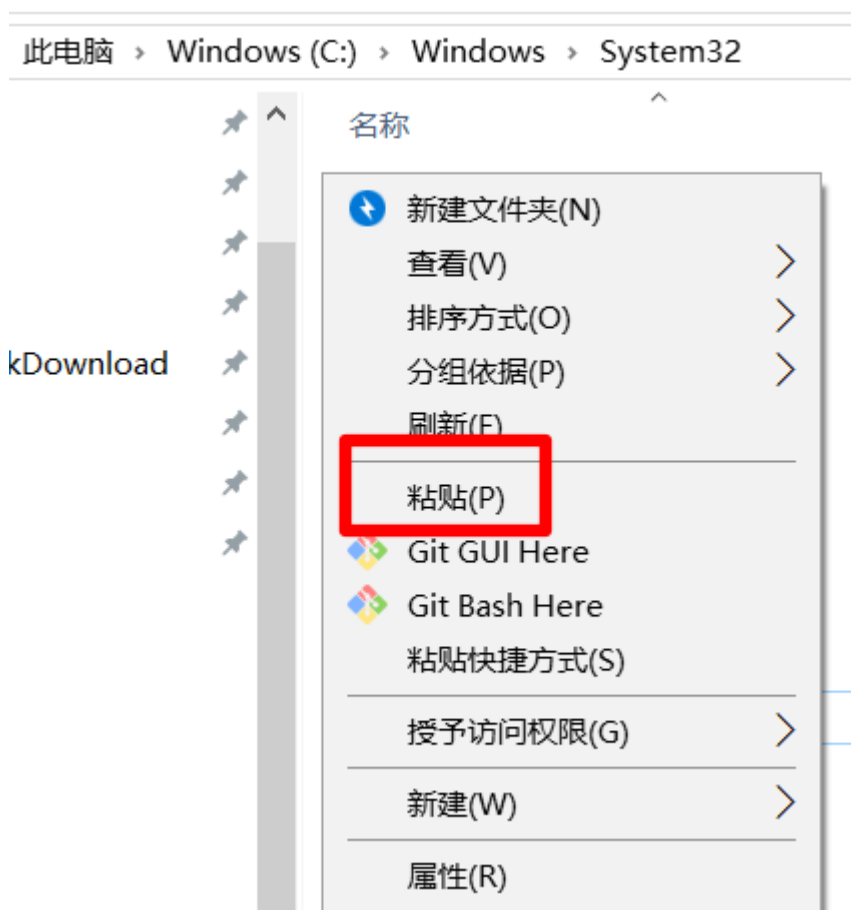
2:21 文件夹  
08 文件夹  
13 文件夹

ur  
s a  
fe

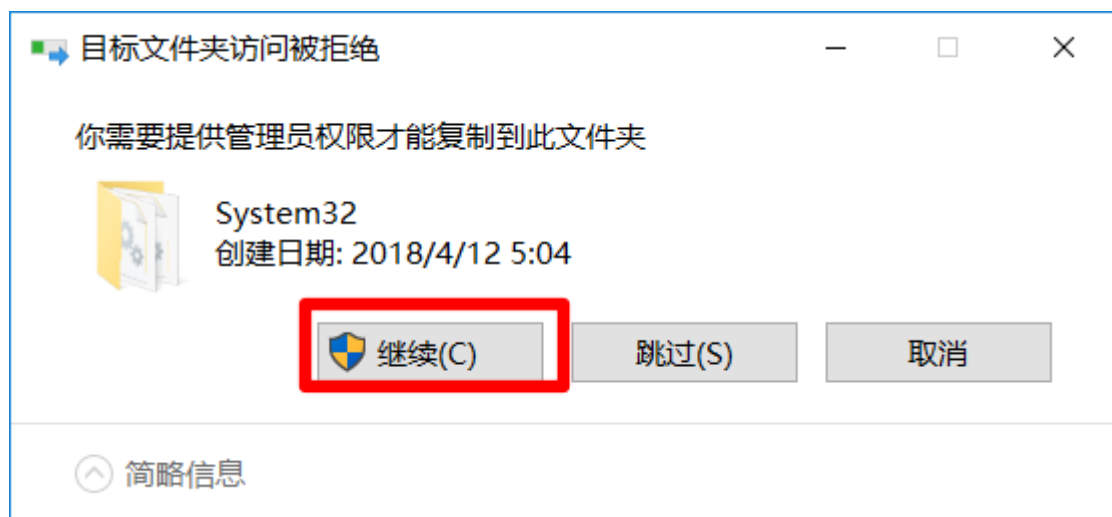
使用火绒安全粉碎文件  
共享  
发送到(N)  
剪切(T)  
**复制(C)**  
创建快捷方式(S)  
删除(D)  
重命名(M)  
属性(R)


名称 修改日期 类型 大小

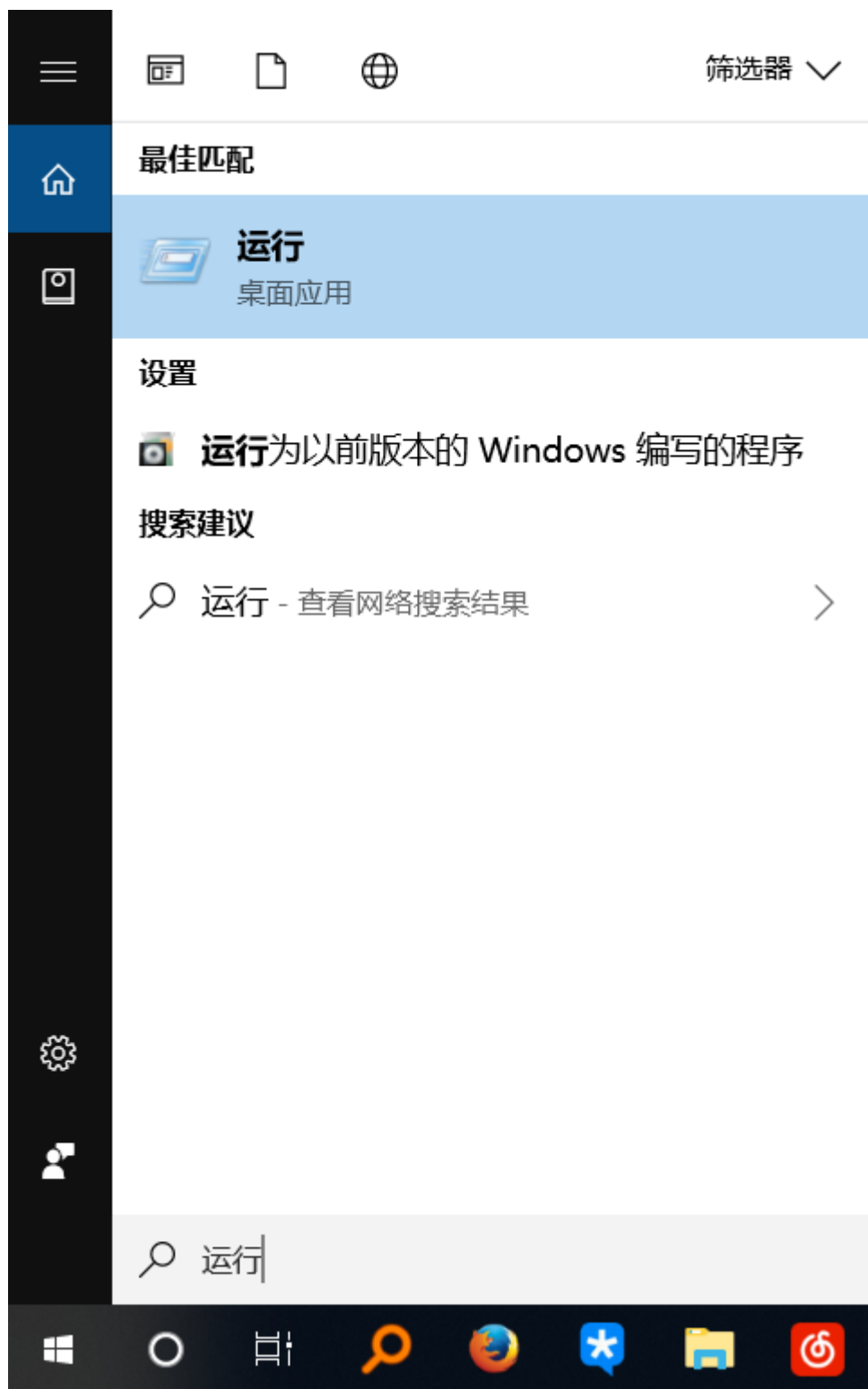
名称	修改日期	类型	大小
doexec.c	2004/1/1	C Source File	5 KB
generic.h	1996/7/1	C Header File	61 KB
getopt.c	1996/1/1	C Source File	18 KB
getopt.h	1994/11/3 20:07	C Header File	5 KB
hobbit.txt	1998/2/6 16:50	文本文档	61 KB
license.txt	2004/12/27 18:37	文本文档	18 KB
Makefile	2011/9/17 0:46	文件	1 KB
nc.exe	2011/9/17 0:52	应用程序	38 KB
nc64.exe	2011/9/17 0:52	应用程序	45 KB
netcat.c	2011/9/17 0:44	C Source File	69 KB
readme.txt	2011/9/17 0:45	文本文档	7 KB



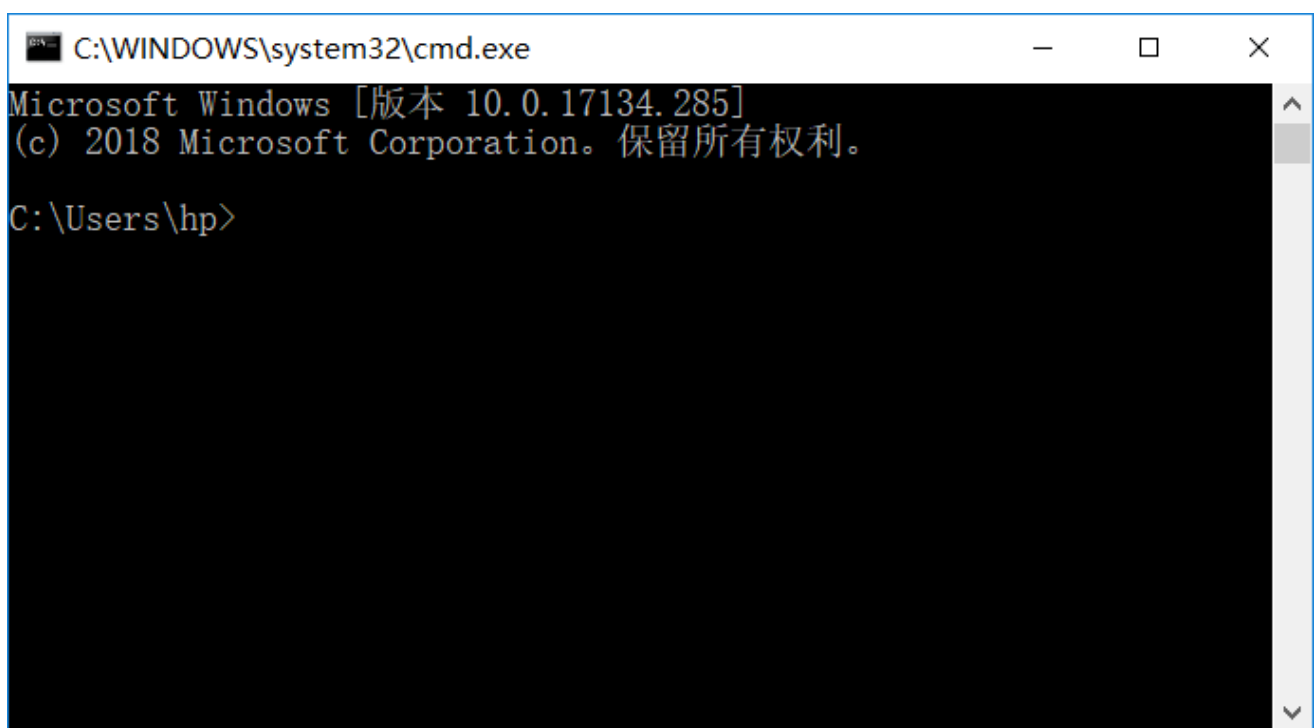
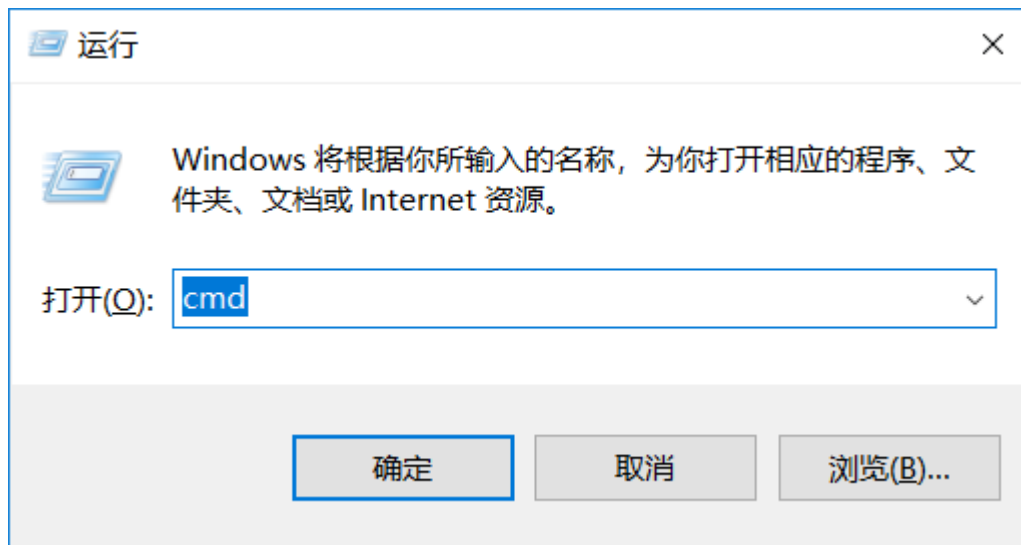
提示说要管理员权限，点解继续即可。



完成后按着 win 键和 r 键，快速打开 运行。或者是在左下角（任务栏）里找到小娜 ，然后打开，搜索 运行，然后打开 运行。



打开后 `cmd` 打开命令行,



然后键入 `nc` , 要是出现 发现病毒或是木马





而且nc后没有任何的显示（如下），则说明没有关闭杀毒软件。

```
Microsoft Windows [版本 10.0.17134.285]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\hp>nc

C:\Users\hp>_
```

在关闭后，重新输入nc，若是获得回显则说明安装成功。

```
C:\WINDOWS\system32\cmd.exe - nc
Microsoft Windows [版本 10.0.17134.285]
(c) 2018 Microsoft Corporation。保留所有权利。

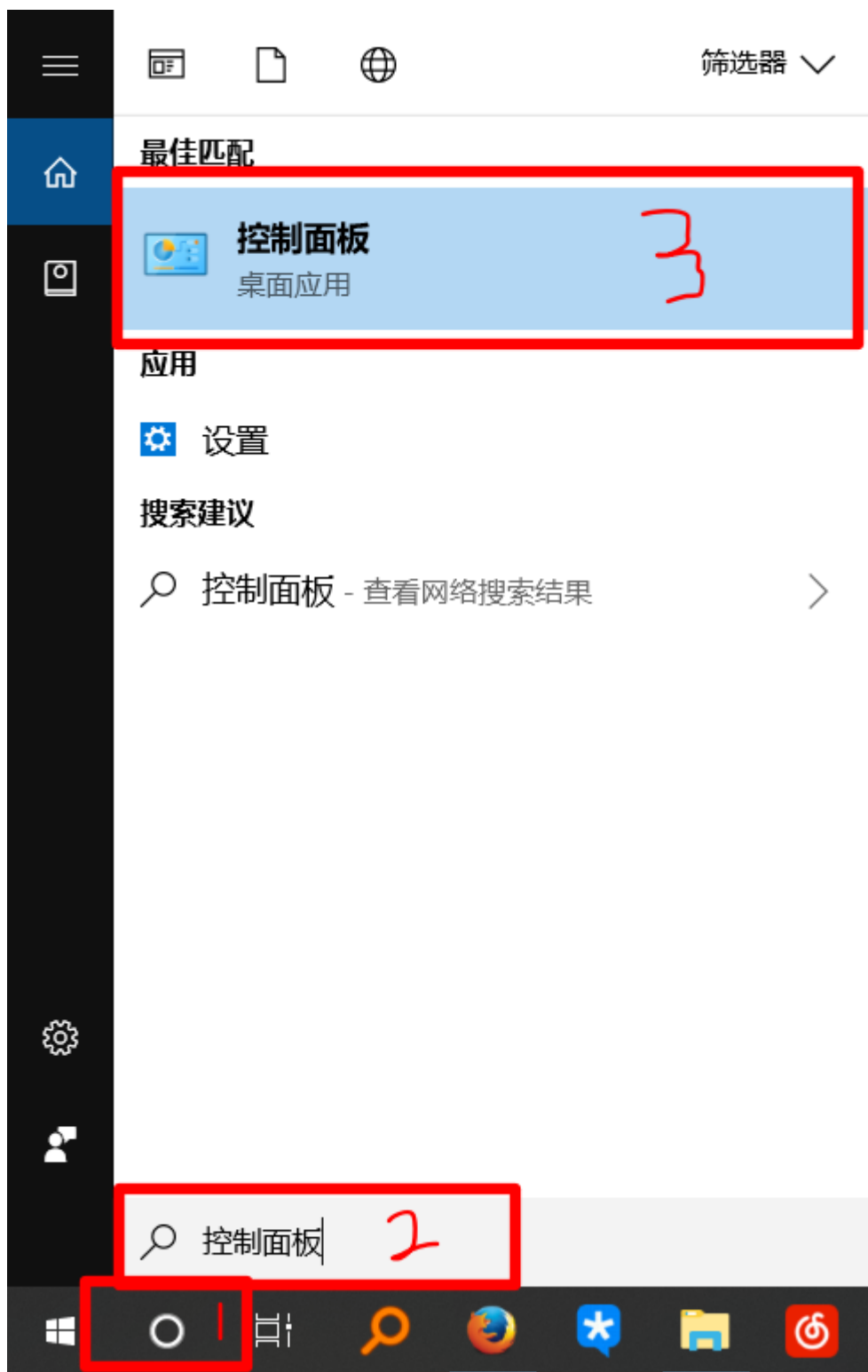
C:\Users\hp>nc

C:\Users\hp>nc
Cmd line:
```

### 法三：安装ubuntu子系统（需要win10）

首先要先 启用 [适用于 Linux 的 windows 子系统]，步骤如下：

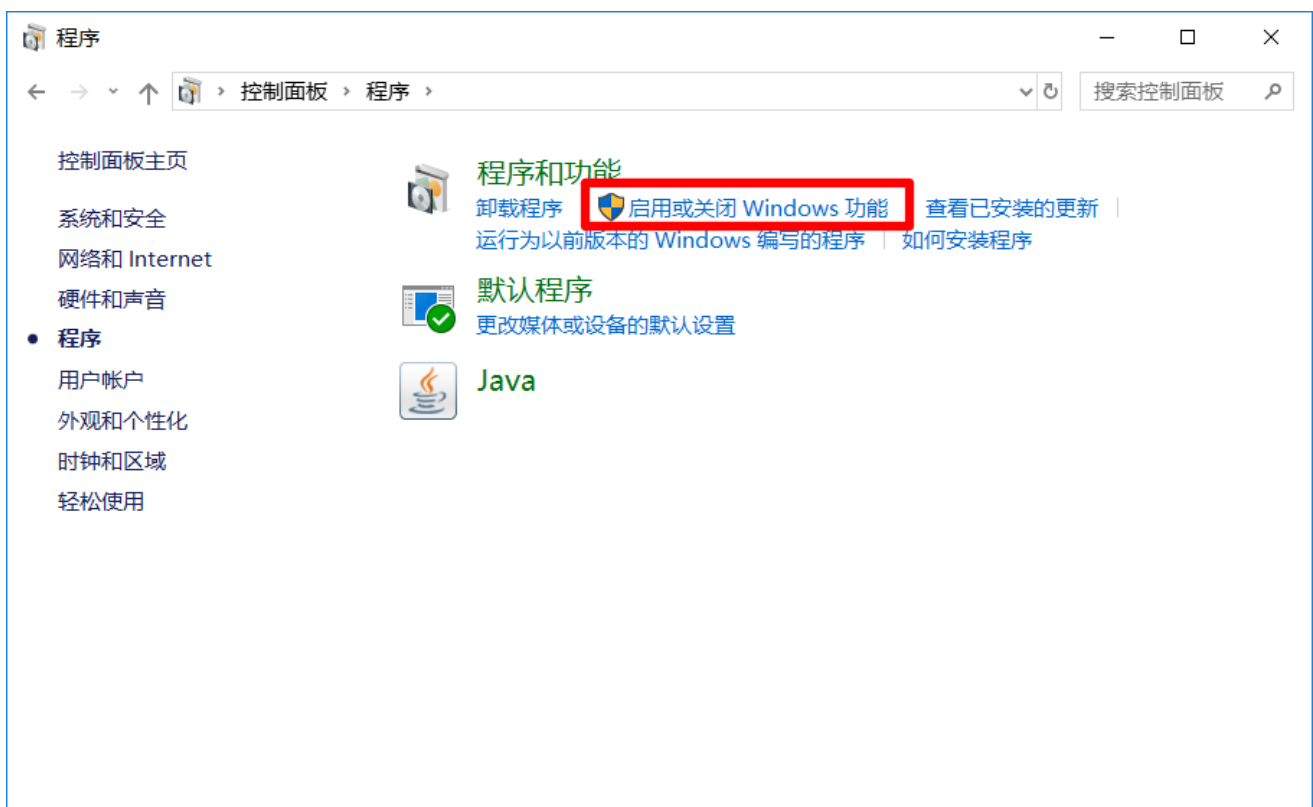
在左下角（任务栏）里找到小娜 ，然后打开，搜索 控制面板，然后打开 Microsoft Store。



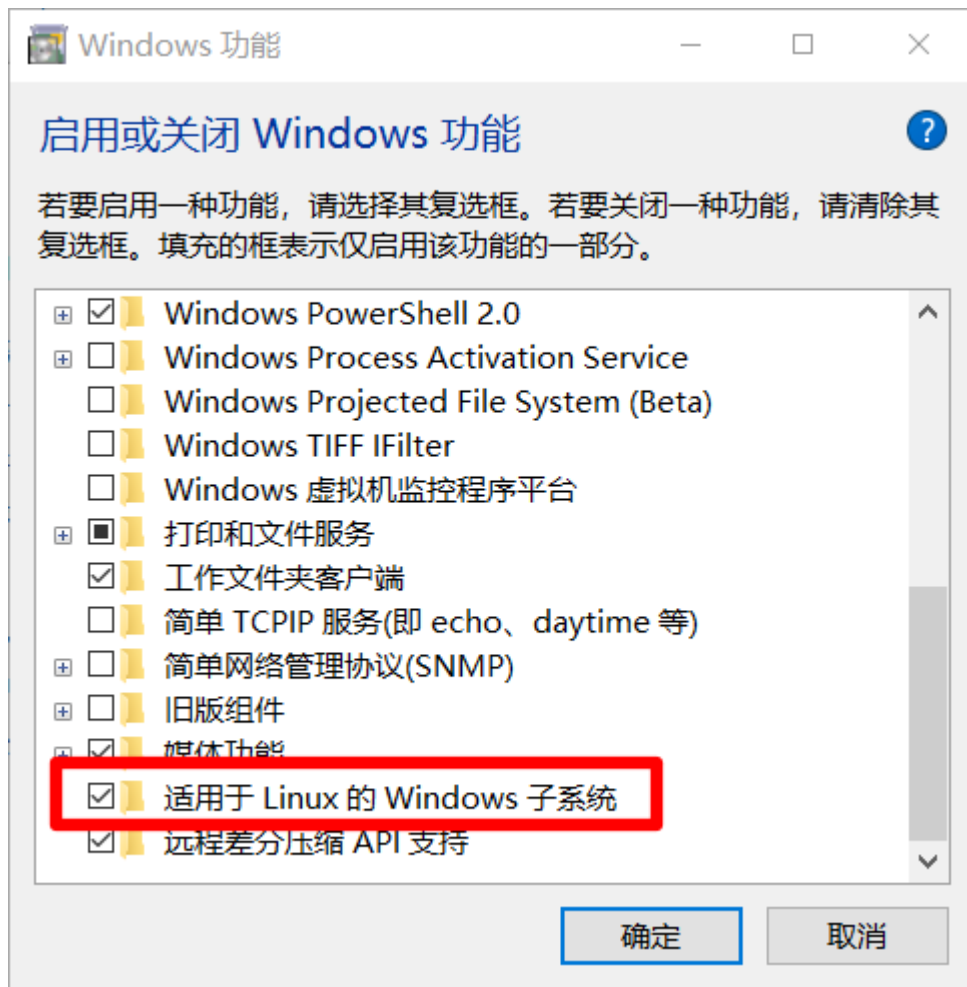
然后点击 程序



再点击 `启用或关闭Windows功能`



在里面找到 `适用于Linux的Windows子系统`，打上勾，然后点击确定，等待功能配置完成并重启系统。



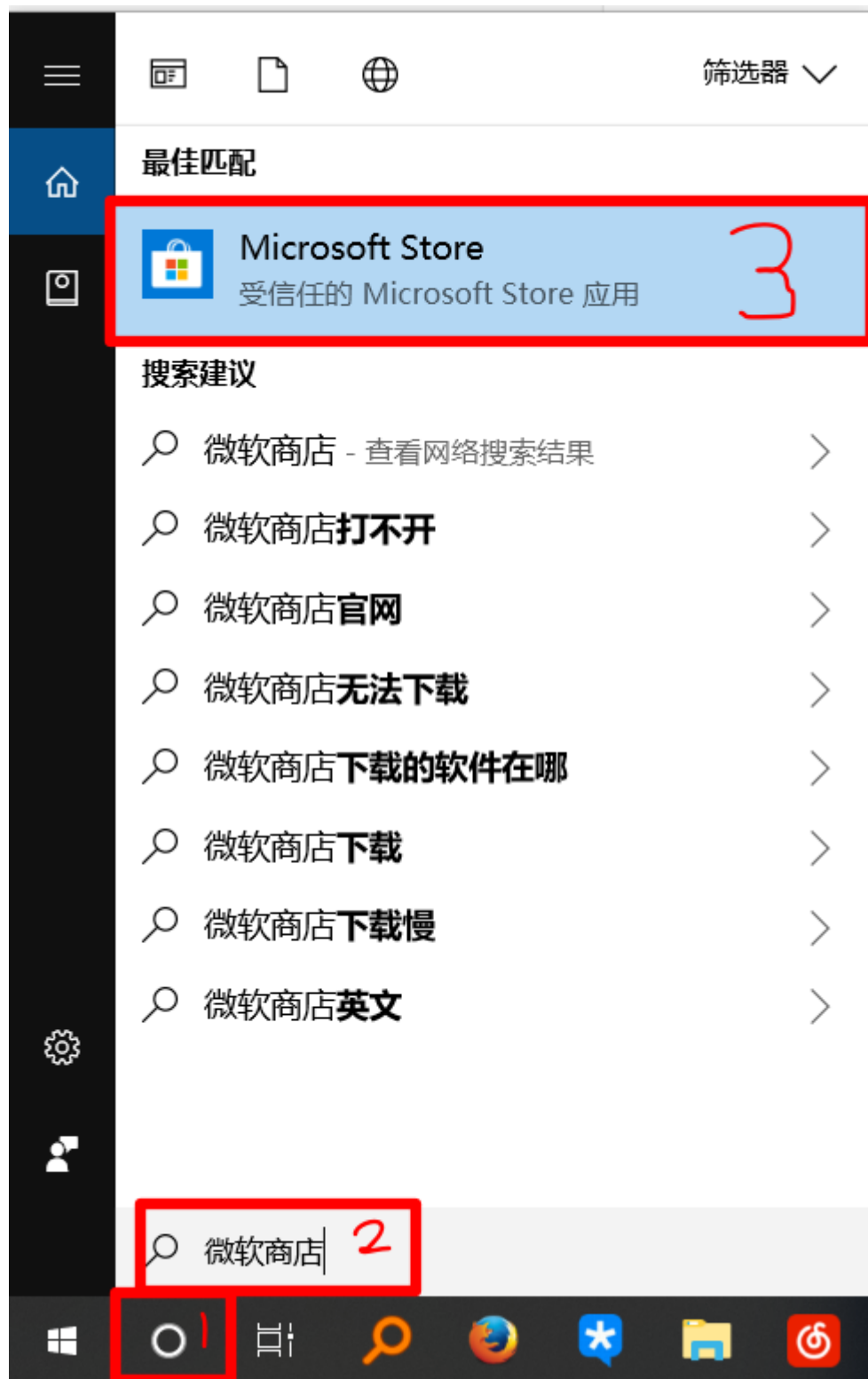
然后就是下载ubuntu子系统：

在左下角（任务栏）里找到小娜

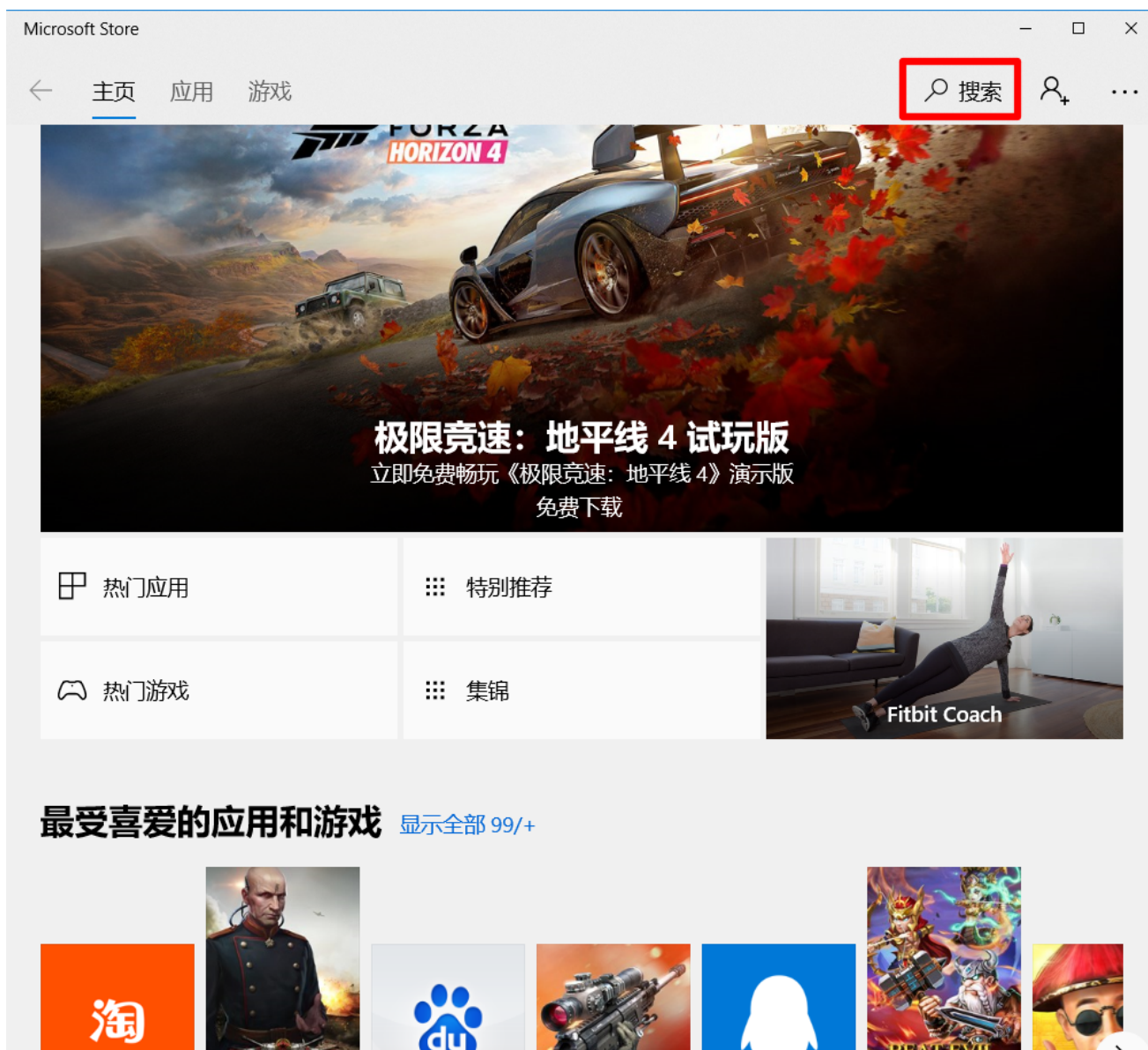


，然后打开，搜索 微软商店 或者 Microsoft Store，然后打开

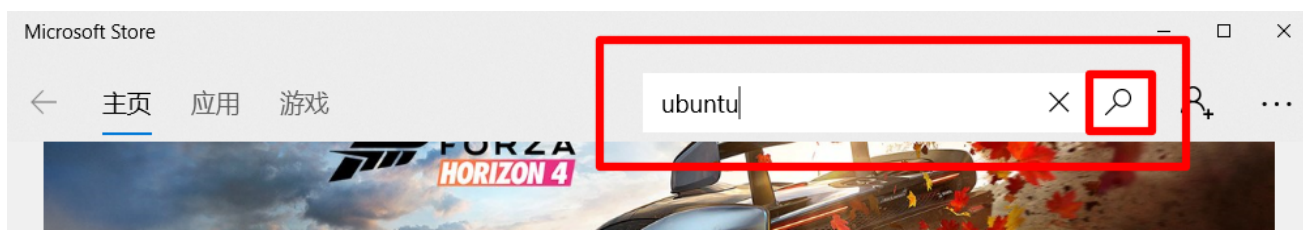
Microsoft Store。



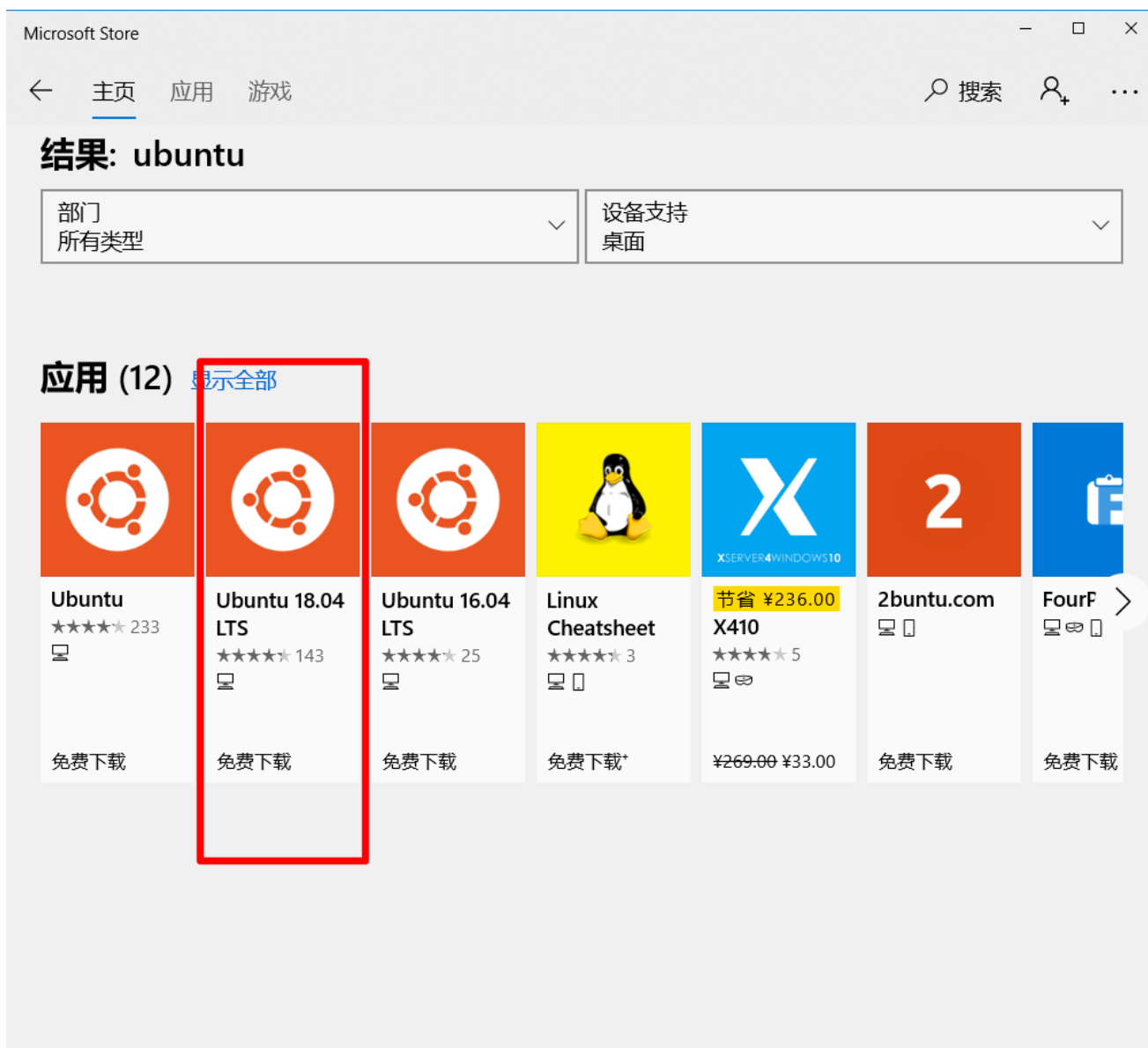
然后点击搜索键



而后输入 `ubuntu`，然后键入回车或是点击搜索按钮。



然后会显示数个软件，选择 `Ubuntu 18.04LTS` 打开。



然后点击获取，（图和我的不一样是正常的，我是用已经安装好的，用另外一个软件的图片）





## Ubuntu

Canonical Group Limited • Developer tools > Utilities

[共享](#)

★★★★★ 233

Ubuntu on Windows allows one to use Ubuntu Terminal and run Ubuntu command line utilities including bash, ssh, git, apt and many more.

[更多](#)



免费

获取

你可以在 Xbox One 主机上购买。(你所在的地区不支持通过 microsoft.com 购买。)

点击获取后，会弹出一个弹窗，点击 [不，谢谢](#) 即可。

## 跨设备使用

通过 Microsoft 登录，并在任何兼容设备上使用。

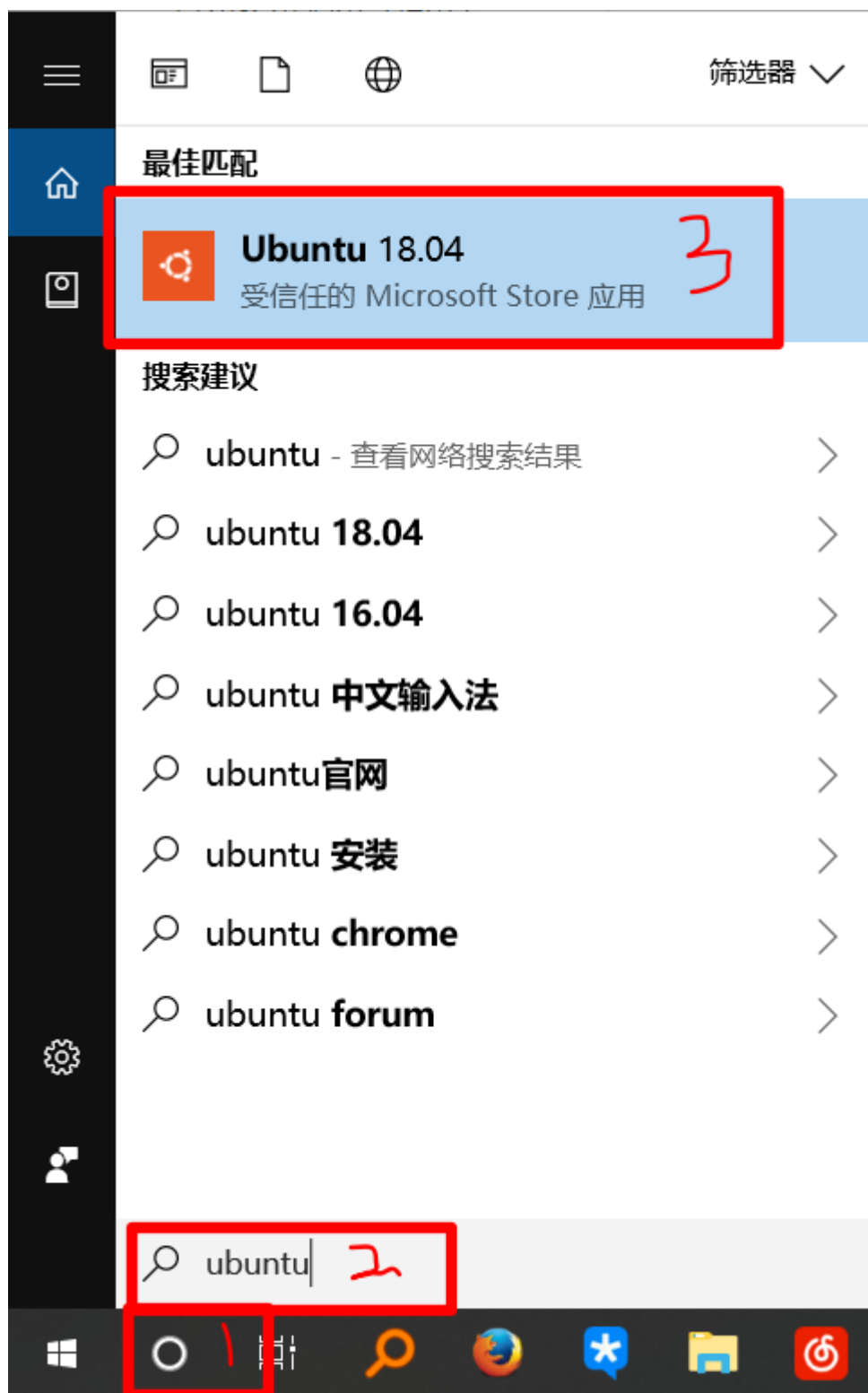
不，谢谢

登录

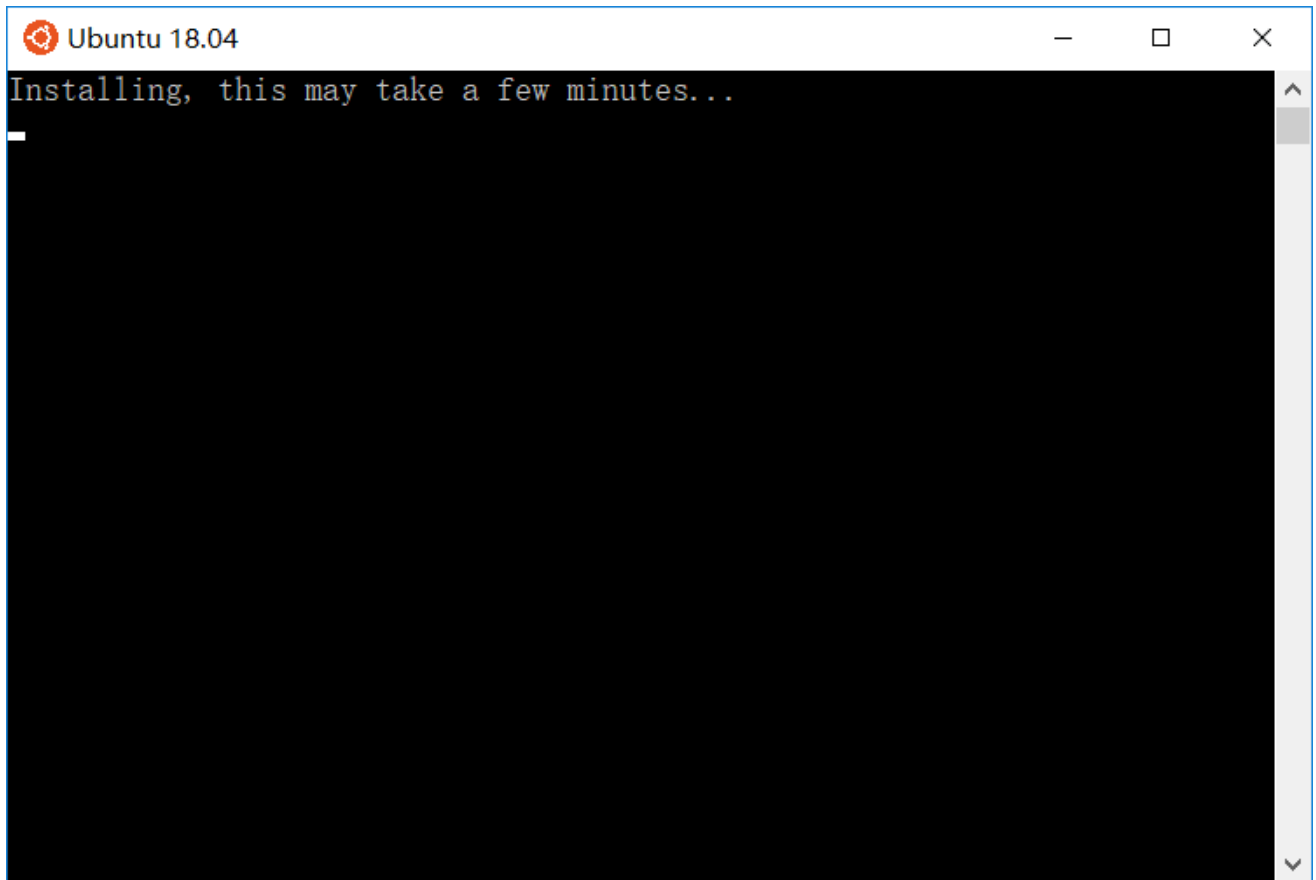
然后等待安装完毕。

配置ubuntu:

在左下角（任务栏）里找到小娜 ，然后打开，搜索 `ubuntu`，然后打开 `Ubuntu 18.04`。



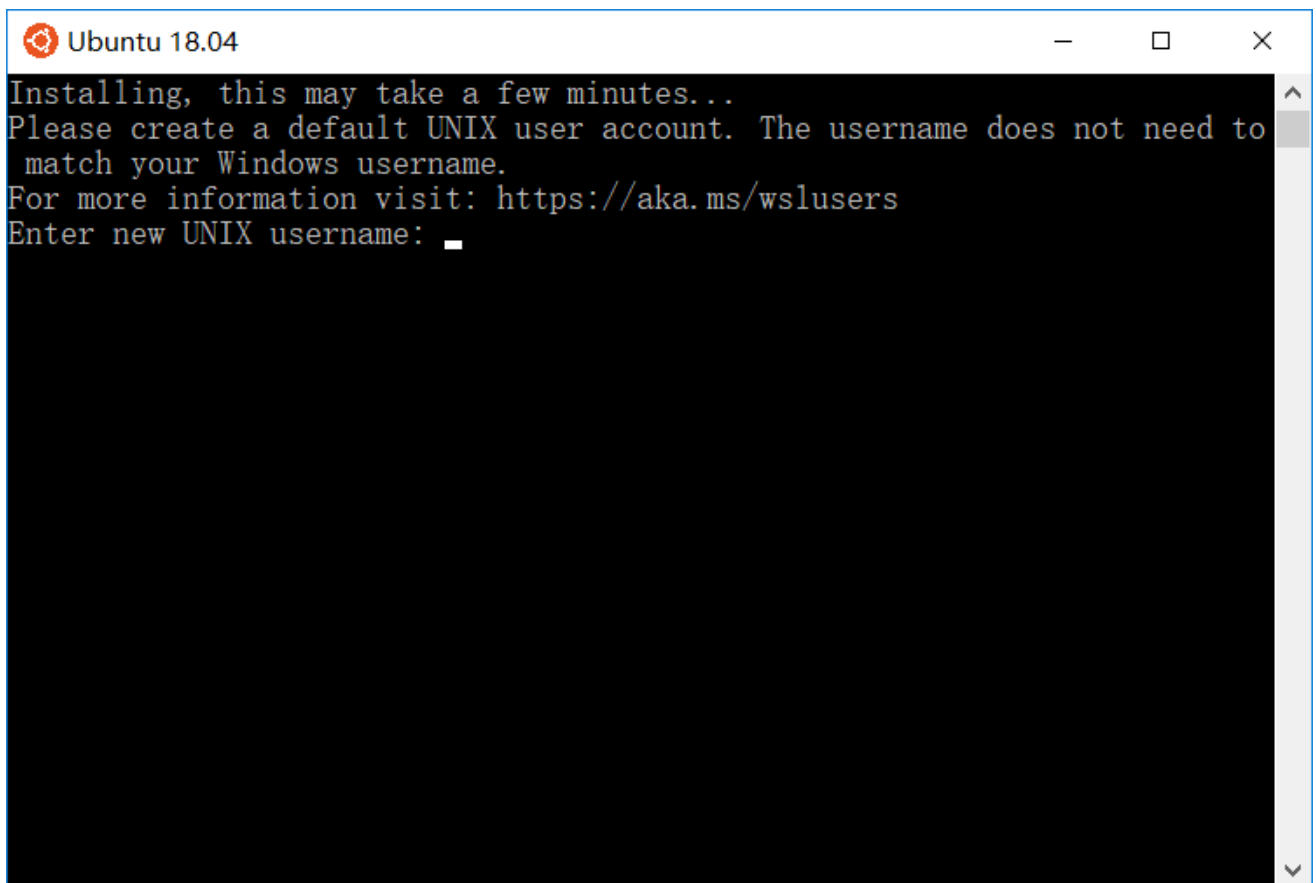
打开后，等待初始化。



A terminal window titled "Ubuntu 18.04" with standard window controls. The text inside the terminal reads: "Installing, this may take a few minutes..." followed by a single underscore character on the next line. The terminal has a black background and a light gray scrollbar on the right.

```
Ubuntu 18.04
Installing, this may take a few minutes...
_
```

许久没有反应，则可以键入回车，然后会弹出以下内容，即为正常。



A terminal window titled "Ubuntu 18.04" with standard window controls. The text inside the terminal reads: "Installing, this may take a few minutes..." followed by instructions to create a default UNIX user account, a URL for more information, and a prompt to enter a new UNIX username. The prompt is followed by a single underscore character. The terminal has a black background and a light gray scrollbar on the right.

```
Ubuntu 18.04
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to
match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: _
```

接下来就是新建用户，若遇到用户名是已经被占用的，请重试。注意：linux环境下输入密码是直接没有任何显示的。

完成以上操作后，键入nc，没有异常，即安装完成，可以进入下一节。

```
ma@LAPTOP-TCFTP77V:~$ nc
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
        [-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
```

## 法四：使用虚拟机VM，安装Linux系统。

略，请自行百度。

Linux系统建议：`kali` 或者 `ubuntu`。

## 使用教程

### 法一：使用Powercat

打开方法请看安装教程，**注意每次重新打开 powershell 都要重新输入以下指令。**

```
IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1')
```

使用方法如下：

```
Usage: powercat [-c or -l] [-p port] [options]
```

例如题目的给的IP地址是 `192.168.232.134`，端口号是 `6666`，我们输入的指令为 `powercat -c 192.1668.232.134 6666`，然后就会接收到回显，按照题目提示操作即可。

```
PS D:\辅助\powercat-master\powercat-master> powercat -c 192.168.232.134 6666
```

强制退出程序方法：

- 1、输入 `Ctrl+C`
- 2、关闭窗口

### 法二：使用netcat

打开命令行使用（打开方式不懂得回安装教程查看），**注意：记得关闭杀毒软件后使用**

使用方法

```
[v1.11 NT www.vulnwatch.org/netcat/]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [options] [hostname] [port]
```

例如题目的给的IP地址是 `192.168.232.134`，端口号是 `6666`，我们输入的指令为 `nc 192.1668.232.134 6666`，然后就会接收到回显，按照题目提示操作即可。

```
C:\Users\hp>nc 47.107.33.15 45361
```

强制退出程序方法：

1、输入 `Ctrl+C`

2、关闭窗口

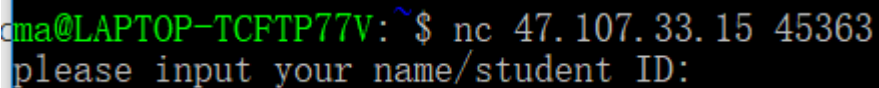
### 法三：使用ubuntu子系统

打开ubuntu使用（打开方式不懂得回安装教程查看）。

使用方法

```
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-w recvlimit] [-w timeout]
        [-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
```

例如题目的给的IP地址是 `192.168.232.134`，端口号是 `6666`，我们输入的指令为 `nc 192.1668.232.134 6666`，然后就会接收到回显，按照题目提示操作即可。



```
ama@LAPTOP-TCFTP77V: ~$ nc 47.107.33.15 45363
please input your name/student ID:
```

强制退出程序方法：

1、输入 `Ctrl+C`

2、关闭窗口

### 法四：使用linux系统。

使用方法请查看 法三：ubuntu子系统。