

这是作者的系列网络安全自学教程，主要是关于网安工具和实践操作的在线笔记，特分享出来与博友共勉，希望您们喜欢，一起进步。前文分享了XSS跨站脚本攻击，从原理、示例、危害到三种常见类型（反射型、存储型、DOM型），并结合代码示例进行详细讲解。这篇文章将讲解Powershell基础入门知识，包括常见的用法，涉及基础概念、管道和重定向、执行外部命令、别名用法、变量定义等。Powershell被广泛应用于安全领域，甚至成为每一位Web安全必须掌握的技术。

本文参考了Bilibili的Hack学习老师的课程，同时也结合了作者之前的编程经验进行讲解。作者作为网络安全的小白，分享一些自学基础教程给大家，希望你们喜欢。同时，更希望你能与我一起操作深入进步，后续也将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不容易，大神请飘过，不喜勿喷，谢谢！

下载地址：<https://github.com/eastmountyxz/NetworkSecuritySelf-study>

百度网盘：https://pan.baidu.com/s/1dsunH8EmOB_tlHYXXguOeA 提取码：izeb

文章目录

一.Powershell初识

- 1.基础概念
- 2.为什么强大?
- 3.控制台和快捷键
- 4.数学运算

二.Powershell管道和重定向

- 1.管道
- 2.重定向

三.Powershell执行外部命令及命令集

- 1.外部命令
- 2.命令集

四.Powershell别名使用

- 1.别名基本用法
- 2.自定义别名

五.Powershell变量基础

- 1.基础用法
- 2.变量操作
- 3.自动化变量
- 4.环境变量

六.Powershell调用脚本程序

1.脚本文件执行策略

2.调用脚本程序

七.总结

前文学习:

- [网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
- [网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
- [网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
- [网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
- [网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
- [网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向破解
- [网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨
- [网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具
- [网络安全自学篇] 九.社会工程学之基础概念、IP获取、IP物理定位、文件属性
- [网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码
- [网络安全自学篇] 十一.虚拟机VMware+Kali安装入门及Sqlmap基本用法
- [网络安全自学篇] 十二.Wireshark安装入门及抓取网站用户名密码（一）
- [网络安全自学篇] 十三.Wireshark抓包原理（ARP劫持、MAC泛洪）及数据流追踪和图像抓取（二）
- [网络安全自学篇] 十四.Python攻防之基础常识、正则表达式、Web编程和套接字通信（一）
- [网络安全自学篇] 十五.Python攻防之多线程、C段扫描和数据库编程（二）
- [网络安全自学篇] 十六.Python攻防之弱口令、自定义字典生成及网站暴库防护
- [网络安全自学篇] 十七.Python攻防之构建Web目录扫描器及ip代理池（四）
- [网络安全自学篇] 十八.XSS跨站脚本攻击原理及代码攻防演示（一）

前文欣赏:

- [渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
- [渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
- [渗透&攻防] 三.数据库之差异备份及Caidao利器
- [渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

参考文献:

- <https://www.bilibili.com/video/av66327436> [推荐B站老师视频]
- 《安全之路Web渗透技术及实战案例解析》 陈小兵老师
- [https://baike.baidu.com/item/Windows Power Shell/693789](https://baike.baidu.com/item/Windows%20Power%20Shell/693789)
- <https://www.pstips.net/powershell-piping-and-routing.html>
- <https://www.pstips.net/using-the-powershell-pipeline.html>

声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

一.Powershell初识

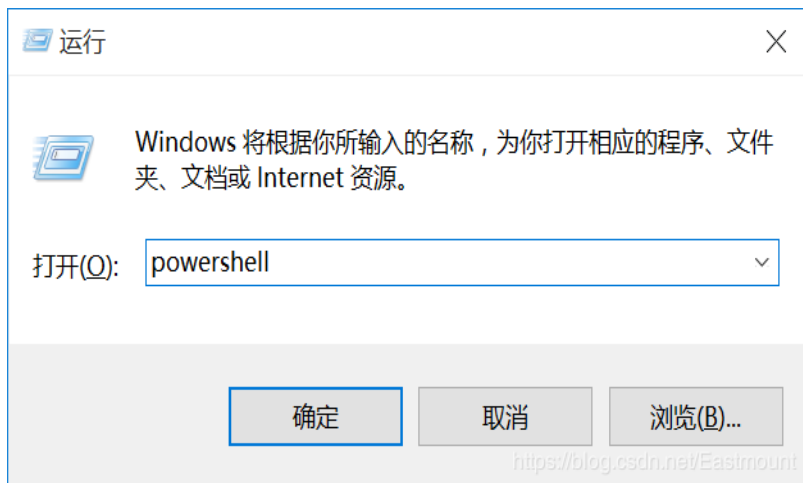
1.基础概念

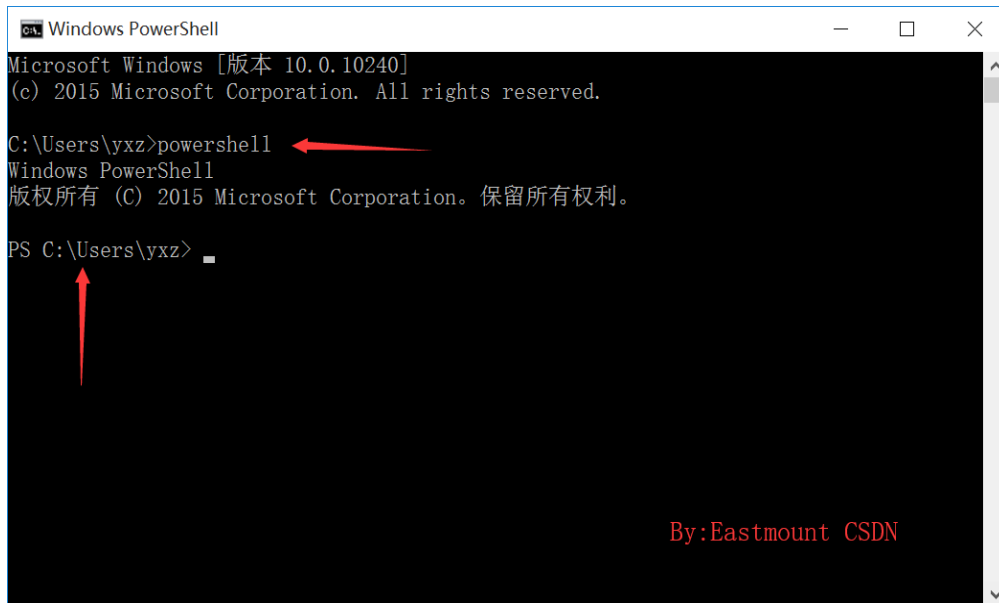
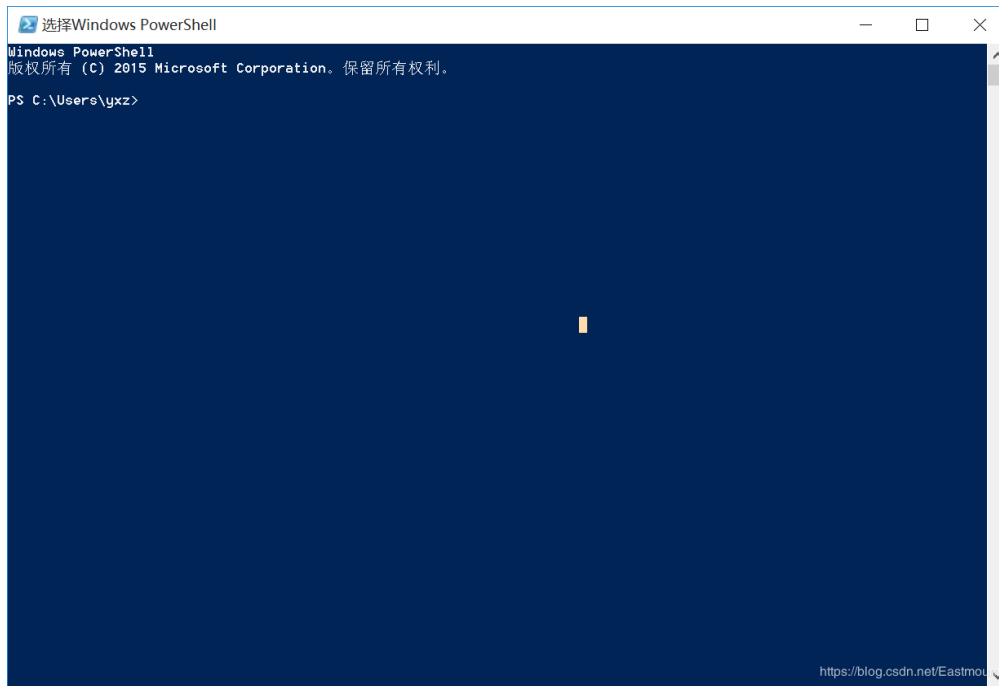
Windows PowerShell 是一种命令行外壳程序和脚本环境，使命令行用户和脚本编写者可以利用 .NET Framework的强大功能。它引入了许多非常用的新概念，从而进一步扩展了您在 Windows 命令提示符和 Windows Script Host 环境中获得的知识 and 创建的脚本。

传统的CMD支持脚本编写，但扩展性不好，而Powershell类似于Linux shell，具有更好的远程处理、工作流、可更新的帮助、预定任务（Scheduled Job）、CIM等优点。

那么，如何进入Powershell呢？

一种方法是在运行中直接输入Powershell打开，另一种方法是CMD中输入Powershell打开。

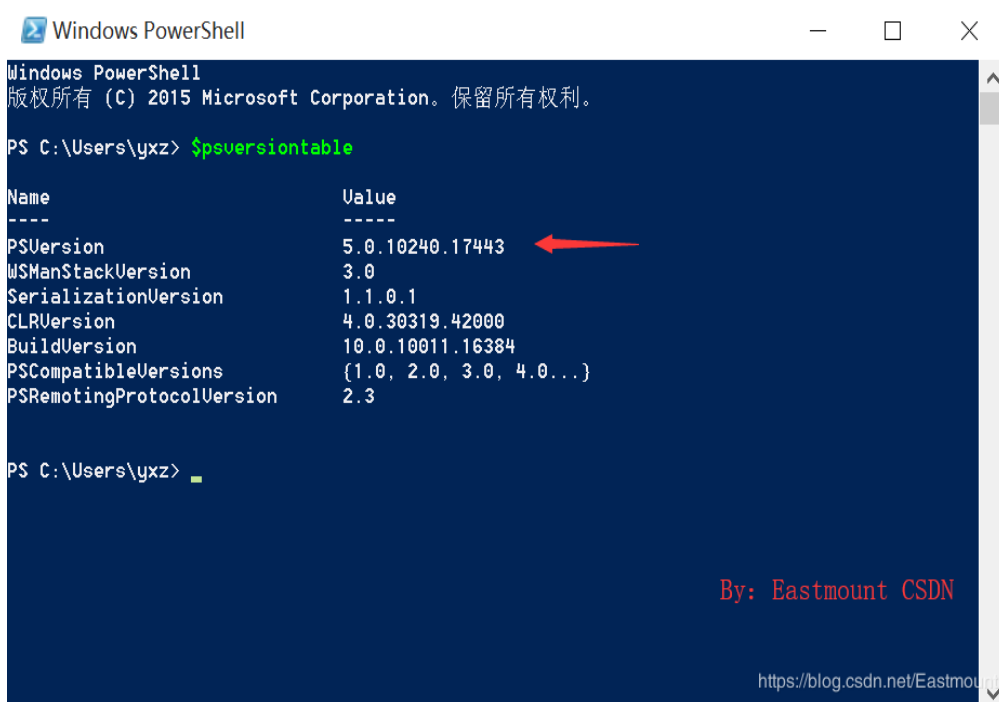




不同操作系统内置的Powershell是不一样的，比如win7或win2008，如何查看版本呢？

`$psversiontable`

输出结果如下图所示：



```
Windows PowerShell
版权所有 (C) 2015 Microsoft Corporation。保留所有权利。

PS C:\Users\yxz> $psversiontable

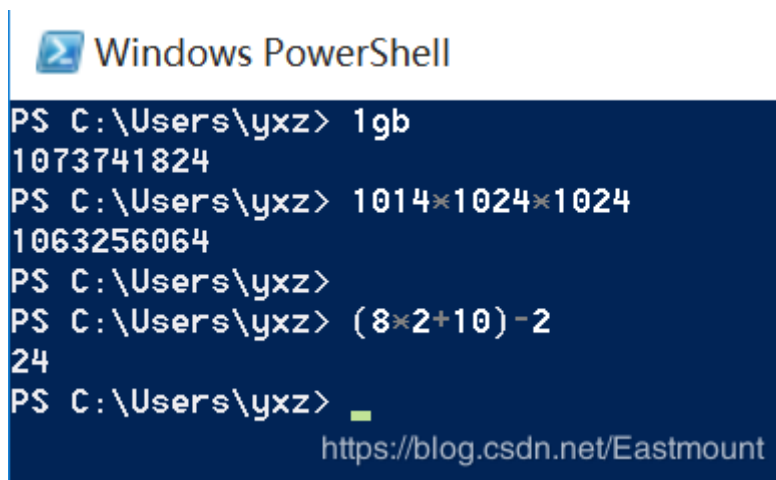
Name                Value
----                -
PSVersion            5.0.10240.17443
WSManStackVersion    3.0
SerializationVersion 1.1.0.1
CLRVersion            4.0.30319.42000
BuildVersion         10.0.10011.16384
PSCCompatibleVersions {1.0, 2.0, 3.0, 4.0...}
PSRemotingProtocolVersion 2.3

PS C:\Users\yxz> _
```

By: Eastmount CSDN
<https://blog.csdn.net/Eastmount>

2.为什么强大?

首先，它可以进行计算任务，包括计算1gb大小（以字节为单位），还有基本的运算。



```
Windows PowerShell

PS C:\Users\yxz> 1gb
1073741824
PS C:\Users\yxz> 1014*1024*1024
1063256064
PS C:\Users\yxz>
PS C:\Users\yxz> (8*2+10)-2
24
PS C:\Users\yxz> _
```

<https://blog.csdn.net/Eastmount>

其次，Powershell可以获取计算机的服务详细信息、状态等。

```
get-service
```

其显示结果如下图所示，采用动词+名词方式命名，比较清楚。

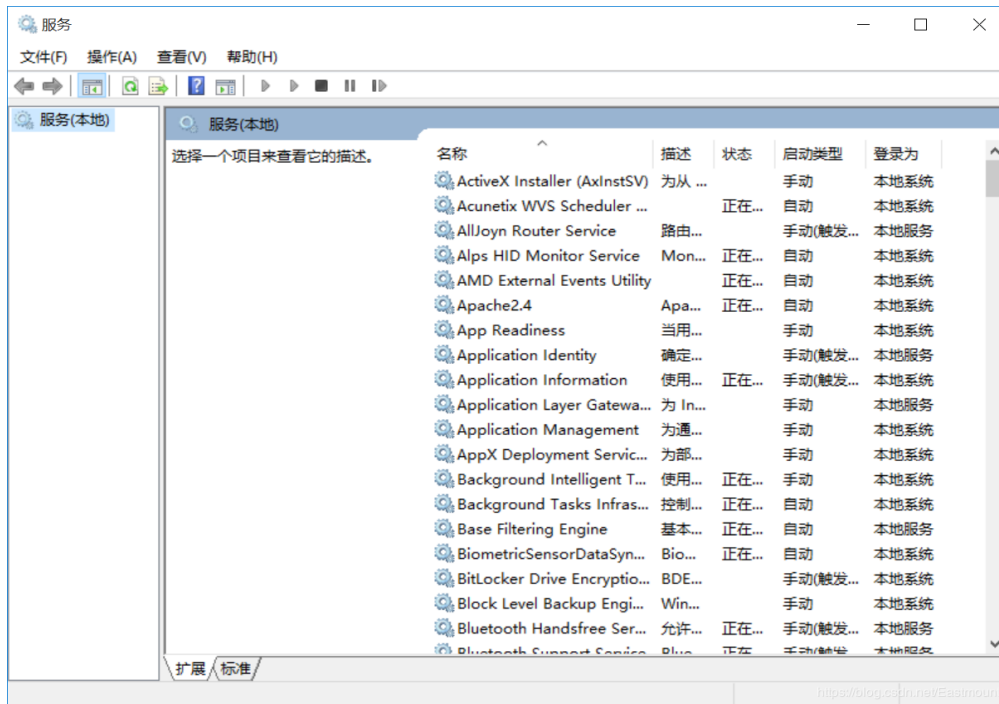
```
Windows PowerShell
PS C:\Users\yxz> get-service

Status Name DisplayName
-----
Running AcuWUSScheduleru10 Acunetix WUS Scheduler v10
Stopped AJRouter AllJoyn Router Service
Stopped ALG Application Layer Gateway Service
Running AMD External Ev... AMD External Events Utility
Running Apache2.4 Apache2.4
Running ApHidMonitorSer... Alps HID Monitor Service
Stopped AppIDSuc Application Identity
Running Appinfo Application Information
Stopped AppMgmt Application Management
Stopped AppReadiness App Readiness
Stopped AppXSvc AppX Deployment Service (AppXSUC)
Running AudioEndpointBu... Windows Audio Endpoint Builder
Running Audiosrv Windows Audio
Stopped AxInstSU ActiveX Installer (AxInstSU)
Stopped BDESUC BitLocker Drive Encryption Service
Running BFE Base Filtering Engine
Running BITS Background Intelligent Transfer Ser...
Running BrokerInfrastru... Background Tasks Infrastructure Ser...
Running Browser Computer Browser
Running BthHFSrv Bluetooth Handsfree Service
Running bthserv Bluetooth Support Service
Stopped CAJ Service Host CAJ Service Host
Stopped CDPSuc CDPSuc
Stopped CertPropSvc Certificate Propagation
Stopped ClipSUC Client License Service (ClipSUC)
Stopped COMSysApp COM+ System Application
Running CoreMessagingRe... CoreMessaging
Running cphs Intel(R) Content Protection HECI Se...
Running cplspcon Intel(R) Content Protection HDCP Se...
Running CryptSvc Cryptographic Services
Stopped CscService Offline Files
```

而CMD中无法获取services的（输入services.msc），它是以图形化方式显示出来的。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\yxz>services.msc
C:\Users\yxz>
```

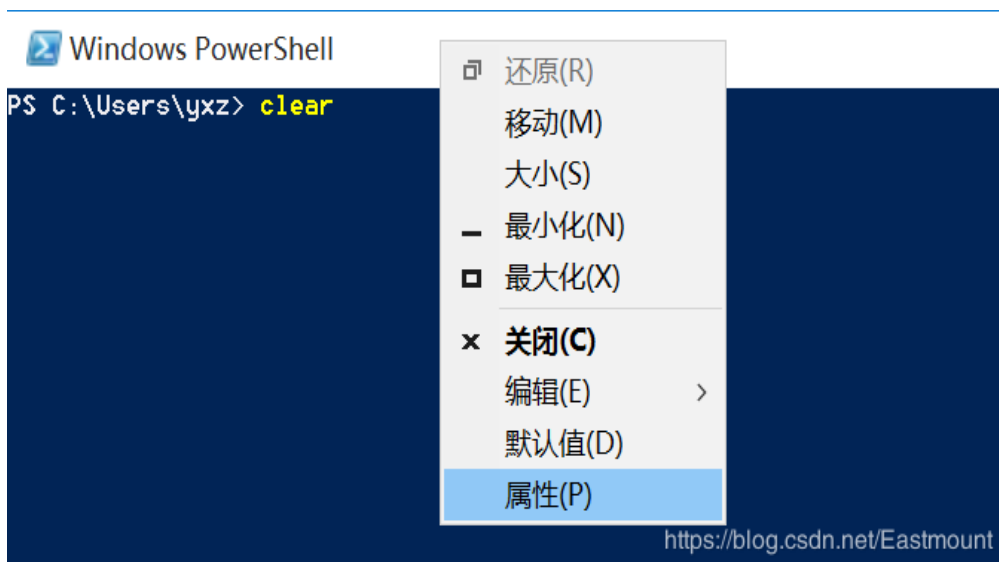


最后，由于Powershell具有以下特点，它被广泛应用于安全领域，甚至成为每一位Web安全必须掌握的技术。

- 方便
- 支持面向对象
- 支持和.net平台交互
- 强大的兼容性，和cmd、vbs相互调用
- 可扩展性好，它可以用来管理活动目录、虚拟机产品等平台

3.控制台和快捷键

鼠标右键属性，可以对Powershell控制台进行编辑，并且它支持两种编辑模式，快速编辑模式默认钩上的。





Powershell快捷键包括:

ALT+F7	清楚命令的历史记录
PgUp PgDn	翻页
Enter	执行当前命令
End	将光标移动至当前命令的末尾
Del	从右开始删除输入的命令字符
Esc	清空当前命令行
F2	自动补充历史命令至指定字符处
F4	删除命令行至光标右边指定字符处
F7	对话框显示命令行历史记录
F8	检索包含指定字符的命令行历史记录
F9	根据命令行的历史记录编号选择命令，历史记录编号可以通过F7查看
左/右	左右移动光标
上/下	切换命令行的历史记录
Home	光标移至命令行字符最左端
Backspace	从右删除命令行字符
Ctrl+C	取消正在执行的命令
Tab	自动补齐命令或文件名

例如，使用快捷键Ctrl+C打断了正在运行的ping指令；使用tab快捷键补齐了service.msc命令。



```
Windows PowerShell
PS C:\Users\yxz> ping www.baidu.com

正在 Ping www.a.shifen.com [163.177.151.109] 具有 32 字节的数据:
来自 163.177.151.109 的回复: 字节=32 时间=135ms TTL=52
来自 163.177.151.109 的回复: 字节=32 时间=106ms TTL=52

163.177.151.109 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 106ms, 最长 = 135ms, 平均 = 120ms
Control-C
PS C:\Users\yxz>
PS C:\Users\yxz> services.msc_
```

4.数学运算

Powershell支持数学运算，比如：

```
PS C:\Users\yxz> 2+4
6
PS C:\Users\yxz> 4-2
2
PS C:\Users\yxz> 4*3
12
PS C:\Users\yxz> 9%2
1
PS C:\Users\yxz> (1+3*5)/2
8
PS C:\Users\yxz> 1gb/1mb
1024
PS C:\Users\yxz> 1gb/1mb*18kb
18874368
PS C:\Users\yxz> 1gb -gt 1mb
True
PS C:\Users\yxz> 0xabcd
43981
```

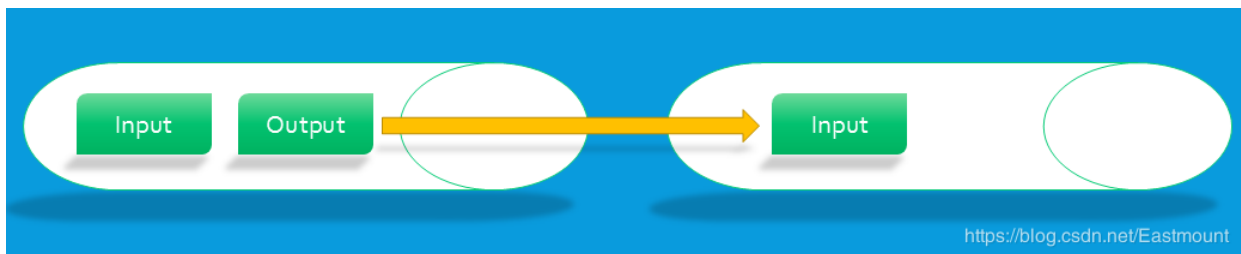
显示结果如下图所示：

```
Windows PowerShell
PS C:\Users\yxz> 2+4
6
PS C:\Users\yxz> 4-2
2
PS C:\Users\yxz> 4*3
12
PS C:\Users\yxz> 9%2
1
PS C:\Users\yxz> (1+3*5)/2
8
PS C:\Users\yxz> 1gb/1mb
1024
PS C:\Users\yxz> 1gb/1mb*18kb
18874368
PS C:\Users\yxz> ps://blog.csdn.net/Eastmount
```

二.Powershell管道和重定向

1.管道

Powershell管道旨在将上一条命令的输出作为下一条命令的输出。



管道并不是什么新事物，以前的Cmd控制台也有重定向的命令，例如Dir | More可以将结果分屏显示。传统的Cmd管道是基于文本的，但是Powershell管道是基于对象。例如：

```
linux: ls
cmd: dir
```

```
Windows PowerShell
PS C:\Users\yxz> ls

目录: C:\Users\yxz

Mode                LastWriteTime         Length Name
----                -
d-----          2018/4/22  22:30             .android
d-----          2019/5/30  20:44             .citespace
d-----          2018/7/27  11:37             .eclipse
d-----          2018/4/24  10:08             .idlerc
d-----          2018/4/22  23:11             .ipython
d-----          2018/7/27  11:37             .jmc
d-----          2018/4/24  14:23             .jupyter
d-----          2019/6/28  11:42             .m2
d-----          2019/10/18  0:10             .matplotlib
d-----          2019/6/27  20:37             .myeclipse
d-----          2019/8/1   14:28             .Neo4jDesktop
d-----          2018/10/20  8:58             .Protege
d-----          2019/10/15 14:58             .spyder2
d-----          2019/2/13  17:04             .sqlmap
d-----          2019/9/10  19:03             .ssh
d-----          2019/9/5   15:10             .zenmap
d-----          2019/3/21  20:26             Anaconda2
d-r---          2018/4/23  0:09             Contacts
d-----          2019/10/26 15:01             Desktop
d-r---          2019/10/8  20:27             Documents
d-r---          2019/10/25 17:00             Downloads
d-r---          2019/5/10  12:41             Favorites
d-r---          2018/4/23  0:09             Links
d-r---          2019/6/6   10:26             Music
```

如果只获取其中的name、mode值，则使用如下指令。

```
ls | format-table name, mode
```

```
Windows PowerShell
PS C:\Users\yxz> ls | format-table name, mode

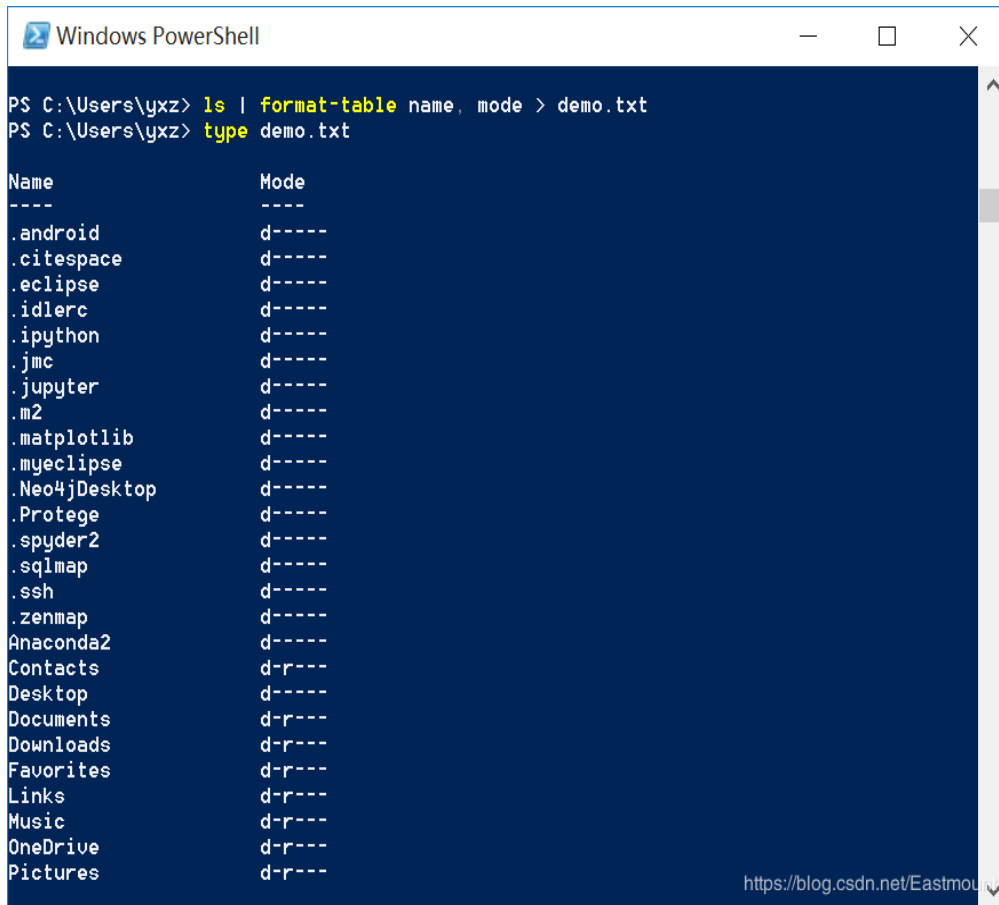
Name                Mode
----                -
.android            d-----
.citespace          d-----
.eclipse            d-----
.idlerc             d-----
.ipython            d-----
.jmc                d-----
.jupyter            d-----
.m2                 d-----
.matplotlib         d-----
.myeclipse          d-----
.Neo4jDesktop       d-----
.Protege            d-----
.spyder2            d-----
.sqlmap             d-----
.ssh                d-----
.zenmap             d-----
Anaconda2           d-----
Contacts            d-r---
Desktop             d-----
Documents           d-r---
Downloads           d-r---
Favorites           d-r---
Links               d-r---
Music               d-r---
OneDrive            d-r---
Pictures            d-r---
pip                 d-----
PubMed              d-----
```

2.重定向

重定向旨在把命令的输出保存到文件中，‘>’为覆盖，’>>’追加。

```
ls | format-table name, mode > demo.txt  
type demo.txt
```

上面代码是将ls显示文件内容的name和mode信息存储至本地demo.txt文件夹中，再调用“type demo.txt”打印文件内容。如果两个 >> 它会在原来的基础上，再进行补充（类似 a+），而单个大于号是删除原来的写入（类似 w）。

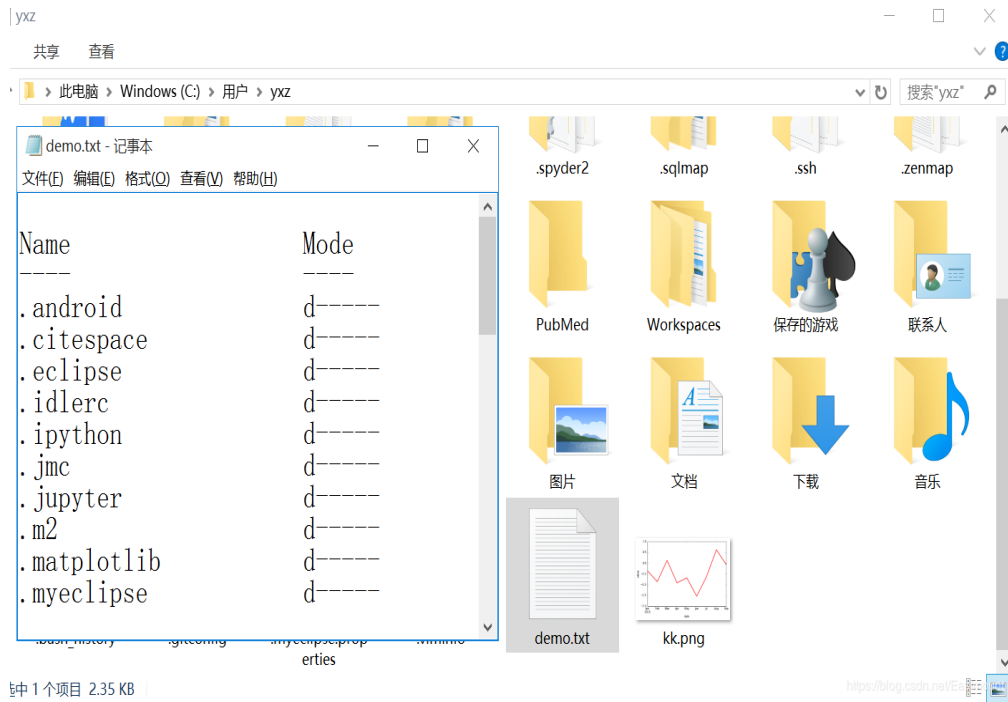


```
Windows PowerShell  
PS C:\Users\yxz> ls | format-table name, mode > demo.txt  
PS C:\Users\yxz> type demo.txt  


| Name          | Mode   |
|---------------|--------|
| ----          | ----   |
| .android      | d----- |
| .citespace    | d----- |
| .eclipse      | d----- |
| .idlerc       | d----- |
| .ipython      | d----- |
| .jmc          | d----- |
| .jupyter      | d----- |
| .m2           | d----- |
| .matplotlib   | d----- |
| .myeclipse    | d----- |
| .Neo4jDesktop | d----- |
| .Protege      | d----- |
| .spyder2      | d----- |
| .sqlmap       | d----- |
| .ssh          | d----- |
| .zenmap       | d----- |
| Anaconda2     | d----- |
| Contacts      | d-r--- |
| Desktop       | d----- |
| Documents     | d-r--- |
| Downloads     | d-r--- |
| Favorites     | d-r--- |
| Links         | d-r--- |
| Music         | d-r--- |
| OneDrive      | d-r--- |
| Pictures      | d-r--- |

  
https://blog.csdn.net/Eastmou
```

输出结果如下图所示。



三.Powershell执行外部命令及命令集

1.外部命令

Powershell是CMD的一个扩展，仍然能够让CMD中的命令在Powershell中使用，Powershell初始化时会加载CMD应用程序，所以CMD命令正常情况下在Powershell中都能使用，例如ipconfig。

查看端口信息

```
netstat -ano
```

包括协议、本地地址、外部地址、状态、PID（进程号）。

```

Windows PowerShell
PS C:\Users\yxz> netstat -ano

活动连接

协议 本地地址          外部地址          状态          PID
TCP  0.0.0.0:80         0.0.0.0:0         LISTENING     2420
TCP  0.0.0.0:135        0.0.0.0:0         LISTENING     848
TCP  0.0.0.0:443        0.0.0.0:0         LISTENING     2420
TCP  0.0.0.0:445        0.0.0.0:0         LISTENING     4
TCP  0.0.0.0:1536       0.0.0.0:0         LISTENING     572
TCP  0.0.0.0:1537       0.0.0.0:0         LISTENING     1300
TCP  0.0.0.0:1538       0.0.0.0:0         LISTENING     1004
TCP  0.0.0.0:1539       0.0.0.0:0         LISTENING     1808
TCP  0.0.0.0:1540       0.0.0.0:0         LISTENING     652
TCP  0.0.0.0:1542       0.0.0.0:0         LISTENING     644
TCP  0.0.0.0:2383       0.0.0.0:0         LISTENING     4036
TCP  0.0.0.0:3306       0.0.0.0:0         LISTENING     2812
TCP  0.0.0.0:5357       0.0.0.0:0         LISTENING     4
TCP  0.0.0.0:6002       0.0.0.0:0         LISTENING     2912
TCP  0.0.0.0:7001       0.0.0.0:0         LISTENING     2880
TCP  0.0.0.0:7002       0.0.0.0:0         LISTENING     2880
TCP  0.0.0.0:16602      0.0.0.0:0         LISTENING     2744
TCP  0.0.0.0:16603      0.0.0.0:0         LISTENING     2744
TCP  0.0.0.0:50451      0.0.0.0:0         LISTENING     14556
TCP  127.0.0.1:1434     0.0.0.0:0         LISTENING     3544
TCP  127.0.0.1:1541     0.0.0.0:0         LISTENING     3544
TCP  127.0.0.1:4300     0.0.0.0:0         LISTENING     14556
TCP  127.0.0.1:4301     0.0.0.0:0         LISTENING     14556
TCP  127.0.0.1:6559     0.0.0.0:0         LISTENING     7760
TCP  127.0.0.1:8183     0.0.0.0:0         LISTENING     2388
TCP  127.0.0.1:10000    0.0.0.0:0         LISTENING     2868
TCP  127.0.0.1:27018    0.0.0.0:0         LISTENING     2396

```

查看网络配置信息

ipconfig

```

Windows PowerShell
PS C:\Users\yxz> ipconfig

Windows IP 配置

以太网适配器 以太网:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 以太网 2:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 Npcap Loopback Adapter:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址 . . . . . : fe80::14d5:b749:d5c1:4ae4%16
    自动配置 IPv4 地址 . . . . . : 169.254.74.228
    子网掩码 . . . . . : 255.255.0.0
    默认网关 . . . . . :

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址 . . . . . : fe80::90b2:8cc0:455f:31cb%22
    IPv4 地址 . . . . . : 192.168.43.110
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.43.30

```

打印路由信息

route print

```

Windows PowerShell
PS C:\Users\yxz> route print
=====
接口列表
15...50 7b 9d f5 e5 9c .....Intel(R) Ethernet Connection I219-U
9...00 25 ec e4 0a 00 .....OrayBoxUPN Virtual Ethernet Adapter
16...02 00 4c 4f 4f 50 .....Npcap Loopback Adapter
22...ac 2b 6e 27 91 a1 .....Intel(R) Dual Band Wireless-AC 3165
14...ac 2b 6e 27 91 a5 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
20...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
18...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
5...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

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           192.168.43.30  192.168.43.110  25
127.0.0.0          255.0.0.0         在链路上      127.0.0.1      306
127.0.0.1          255.255.255.255  在链路上      127.0.0.1      306
127.255.255.255    255.255.255.255  在链路上      127.0.0.1      306
169.254.0.0        255.255.0.0       在链路上      169.254.74.228 266
169.254.74.228     255.255.255.255  在链路上      169.254.74.228 266
169.254.255.255    255.255.255.255  在链路上      169.254.74.228 266
192.168.43.0       255.255.255.0     在链路上      192.168.43.110 281
192.168.43.110     255.255.255.255  在链路上      192.168.43.110 281
192.168.43.255     255.255.255.255  在链路上      192.168.43.110 281
224.0.0.0          240.0.0.0         在链路上      127.0.0.1      306
224.0.0.0          240.0.0.0         在链路上      192.168.43.110 281
224.0.0.0          240.0.0.0         在链路上      169.254.74.228 266
255.255.255.255    255.255.255.255  在链路上      127.0.0.1      306
255.255.255.255    255.255.255.255  在链路上      192.168.43.110 281

```

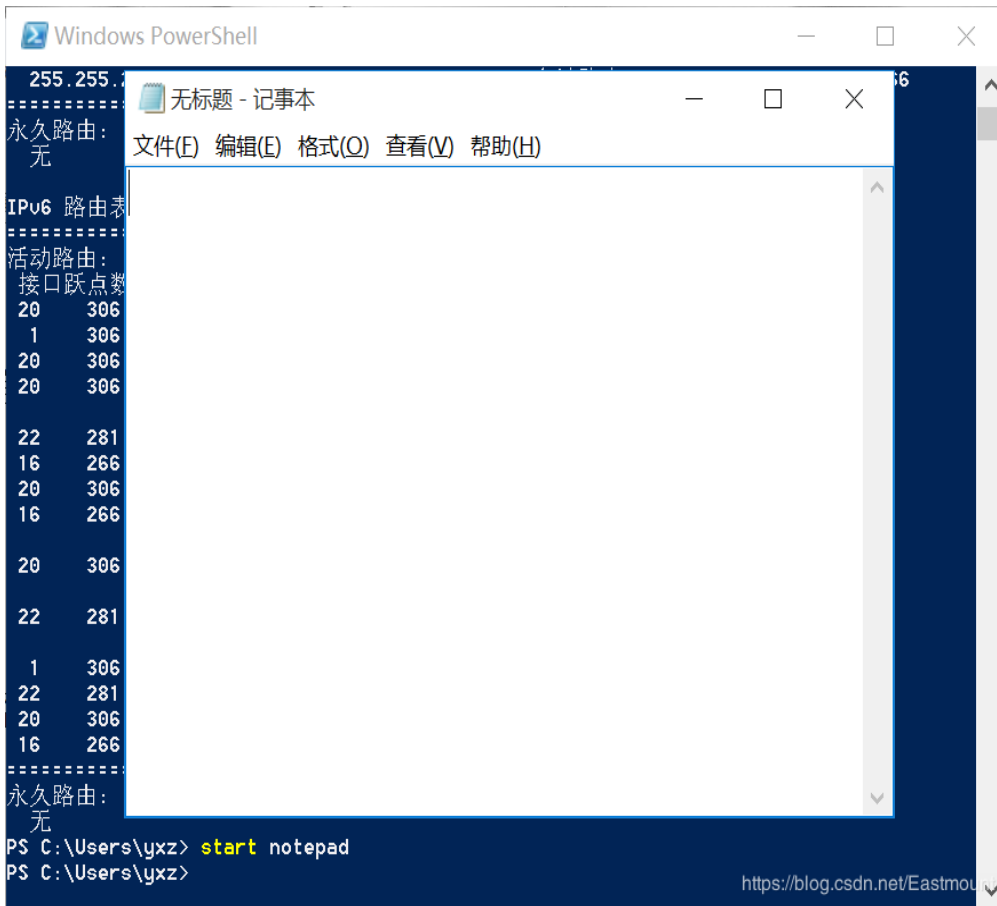
自定义文件路径，打开应用程序

```

start notepad
notepad

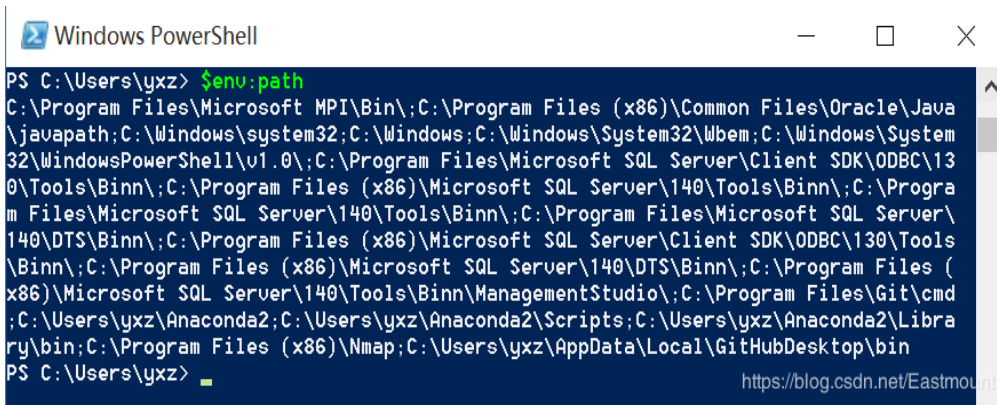
```

notepad放在C盘下面的Windows\System32文件中，能够直接打开。



系统变量

`$env:path`



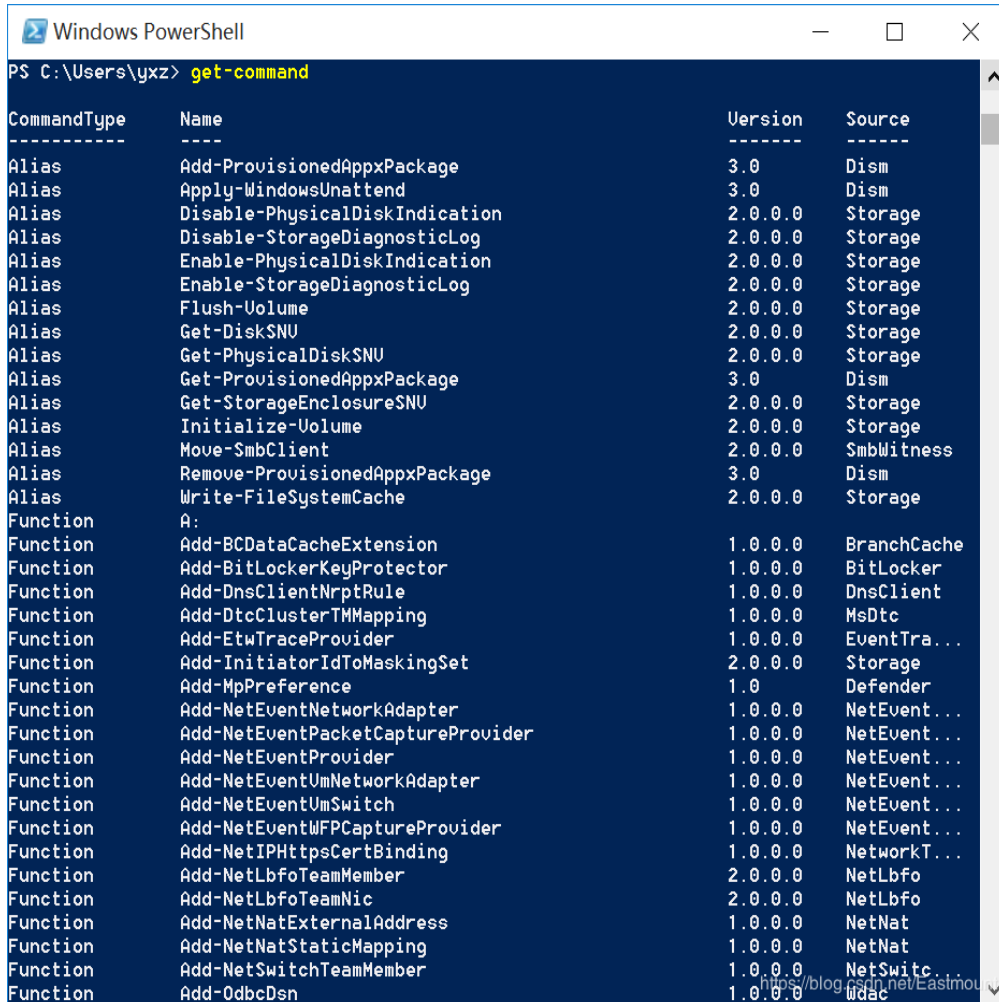
Python可以直接打开，Wordpad不能打开，需要添加环境变量中。



2.命令集

通过get-command获取所有命令，通常是动名词的方式。

get-command



```

Windows PowerShell
PS C:\Users\yxz> get-command

CommandType      Name                                     Version      Source
-----
Alias             Add-ProvisionedAppxPackage             3.0          Dism
Alias             Apply-WindowsUnattend                  3.0          Dism
Alias             Disable-PhysicalDiskIndication         2.0.0.0     Storage
Alias             Disable-StorageDiagnosticLog           2.0.0.0     Storage
Alias             Enable-PhysicalDiskIndication          2.0.0.0     Storage
Alias             Enable-StorageDiagnosticLog            2.0.0.0     Storage
Alias             Flush-Volume                           2.0.0.0     Storage
Alias             Get-DiskSNU                            2.0.0.0     Storage
Alias             Get-PhysicalDiskSNU                    2.0.0.0     Storage
Alias             Get-ProvisionedAppxPackage              3.0          Dism
Alias             Get-StorageEnclosureSNU                 2.0.0.0     Storage
Alias             Initialize-Volume                       2.0.0.0     Storage
Alias             Move-SmbClient                          2.0.0.0     SmbWitness
Alias             Remove-ProvisionedAppxPackage           3.0          Dism
Alias             Write-FileSystemCache                   2.0.0.0     Storage
Function          A:
Function          Add-BCDataCacheExtension                1.0.0.0     BranchCache
Function          Add-BitLockerKeyProtector               1.0.0.0     BitLocker
Function          Add-DnsClientNrptRule                   1.0.0.0     DnsClient
Function          Add-DtcClusterTMMapping                 1.0.0.0     MsDtc
Function          Add-EtwTraceProvider                    1.0.0.0     EventTra...
Function          Add-InitiatorIdToMaskingSet             2.0.0.0     Storage
Function          Add-MpPreference                        1.0         Defender
Function          Add-NetEventNetworkAdapter              1.0.0.0     NetEvent...
Function          Add-NetEventPacketCaptureProvider       1.0.0.0     NetEvent...
Function          Add-NetEventProvider                    1.0.0.0     NetEvent...
Function          Add-NetEventUmNetworkAdapter            1.0.0.0     NetEvent...
Function          Add-NetEventUmSwitch                    1.0.0.0     NetEvent...
Function          Add-NetEventWFPCaptureProvider           1.0.0.0     NetEvent...
Function          Add-NetIPHttpsCertBinding               1.0.0.0     NetworkT...
Function          Add-NetLbfoTeamMember                   2.0.0.0     NetLbfo
Function          Add-NetLbfoTeamNic                      2.0.0.0     NetLbfo
Function          Add-NetNatExternalAddress                1.0.0.0     NetNat
Function          Add-NetNatStaticMapping                  1.0.0.0     NetNat
Function          Add-NetSwitchTeamMember                  1.0.0.0     NetSwitc
Function          Add-OdbcDsn                             1.0.0.0     Wdac
  
```

获取其用法的命令如下，简称gcm。

get-help get-command

```

Windows PowerShell
PS C:\Users\yxz> get-help get-command

名称
    Get-Command

语法
    Get-Command [[-ArgumentList] <Object[]>] [-Verb <string[]>] [-Noun <string[]>] [-Module <string[]>] [-FullyQualifiedModule <ModuleSpecification[]>] [-TotalCount <int>] [-Syntax] [-ShowCommandInfo] [-All] [-ListImported] [-ParameterName <string[]>] [-ParameterType <PSTypeName[]>] [<CommonParameters>]

    Get-Command [[-Name] <string[]>] [[-ArgumentList] <Object[]>] [-Module <string[]>] [-FullyQualifiedModule <ModuleSpecification[]>] [-CommandType <CommandTypes> (Alias | Function | Filter | Cmdlet | ExternalScript | Application | Script | Workflow | Configuration | All)] [-TotalCount <int>] [-Syntax] [-ShowCommandInfo] [-All] [-ListImported] [-ParameterName <string[]>] [-ParameterType <PSTypeName[]>] [<CommonParameters>]

别名
    gcm

备注
    Get-Help 在此计算机上找不到该 cmdlet 的帮助文件。它仅显示部分帮助。
    -- 若要下载并安装包含此 cmdlet 的模块的帮助文件，请使用 Update-Help。
    -- 若要联机查看此 cmdlet 的帮助主题，请键入: "Get-Help Get-Command -Online" 或转到 http://go.microsoft.com/fwlink/?LinkID=113309。

PS C:\Users\yxz>

```

获取进程信息

get-process

```

Windows PowerShell
PS C:\Users\yxz> get-process

Handles      NPM(K)      PM(K)      WS(K)      UM(M)      CPU(s)      Id ProcessName
-----
964          96      117768      94644      542         46.84      11004 360DesktopLite64
2982         228      254996      41356      913        818.91      6820 360tray
69           6         816         4096         48         36.75      11148 ApMsgFwd
106          9         1376         5252         83         56.97      8520 ApntEx
278         21         3592        17088        128        16.56      8396 Apoint
271         12         2196         8612         93         7288      atieclxx
128          7         1040         4384         29         1308      atiesrxx
260         15      11584      16920      1.17        82.95      6108 audiodg
127         11         3000         6552         68         2396      CAJSHost
273         25      31072      36468      50          4.30       976 chrome
3098        146     210240     249520      35 1,411.58    1092 chrome
270         25      37060      41832      33         12.69      3468 chrome
739         70     400272     220964      46 1,563.22    4352 chrome
351         42     114236     75220      76         160.48     6248 chrome
322         10       1700         5788      41          0.13       7296 chrome
277         26     45652     45264      87          74.03     8076 chrome
233         21     19896     24344      24          0.39      8780 chrome
428         64     252032     152020      22        310.52     9044 chrome
282         31     77508     52092      11         30.59     9088 chrome
288         66     169248     113000      31        135.66     9496 chrome
308         29     38412     49424      58          14.88     9744 chrome
262         24     25856     33180      19          2.80     9808 chrome
265         28     47360     43996      75         149.91     9904 chrome
331         37     87932     72508      19         79.20     10116 chrome
108          9       1560         6436      37          0.05     10304 chrome
311         35     87532     65436      03         39.02     10752 chrome
304         29     53764     47884      08         99.84     11240 chrome
262         25     37572     33536      18          2.56     11672 chrome
277         30     67072     38300      49         17.00     12012 chrome
265         24     26860     32996      26          1.22     12320 chrome
269         26     65368     45792      67         61.08     12684 chrome
322         23     54584     32592      08         17.11     13128 chrome
279         31     76544     56848      08         21.95     13580 chrome
435         146    676652     577724      70 3,403.47    14132 chrome
328         38     84744     83188      12         478.84    15764 chrome
314         27     37584     50196      32          8.50     16364 chrome

```

获取当前会话的别名

get-alias

```

Windows PowerShell
PS C:\Users\yxz> get-alias

CommandType      Name                                Version      Source
-----
Alias             % -> ForEach-Object
Alias             ? -> Where-Object
Alias             ac -> Add-Content
Alias             asnp -> Add-PSSnapin
Alias             cat -> Get-Content
Alias             cd -> Set-Location
Alias             CFS -> ConvertFrom-String          3.1.0.0     Microsoft.PowerSh...
Alias             chdir -> Set-Location
Alias             clc -> Clear-Content
Alias             clear -> Clear-Host
Alias             clhy -> Clear-History
Alias             cli -> Clear-Item
Alias             clp -> Clear-ItemProperty
Alias             cls -> Clear-Host
Alias             clv -> Clear-Variable
Alias             cnsn -> Connect-PSSession
Alias             compare -> Compare-Object
Alias             copy -> Copy-Item
Alias             cp -> Copy-Item
Alias             cpi -> Copy-Item
Alias             cpp -> Copy-ItemProperty
Alias             curl -> Invoke-WebRequest
Alias             cupa -> Convert-Path
Alias             dbp -> Disable-PSBreakpoint
Alias             del -> Remove-Item
Alias             diff -> Compare-Object
Alias             dir -> Get-ChildItem
Alias             dsn -> Disconnect-PSSession
Alias             ebp -> Enable-PSBreakpoint
Alias             echo -> Write-Output
Alias             epal -> Export-Alias
Alias             epsv -> Export-Csv
Alias             epsn -> Export-PSSession
Alias             erase -> Remove-Item
Alias             etn -> Enter-PSSession
Alias             exsn -> Exit-PSSession

```

获取输入的历史命令信息

get-history

```

Windows PowerShell
PS C:\Users\yxz> get-history

Id CommandLine
--
1 route print
2 wordpad
3 get-command
4 get-help get-command
5 get-process
6 get-alias

PS C:\Users\yxz> https://blog.csdn.net/Eastmount

```

获取当前时间

get-date

```

PS C:\Users\yxz> get-date

2019年10月28日 0:13:05

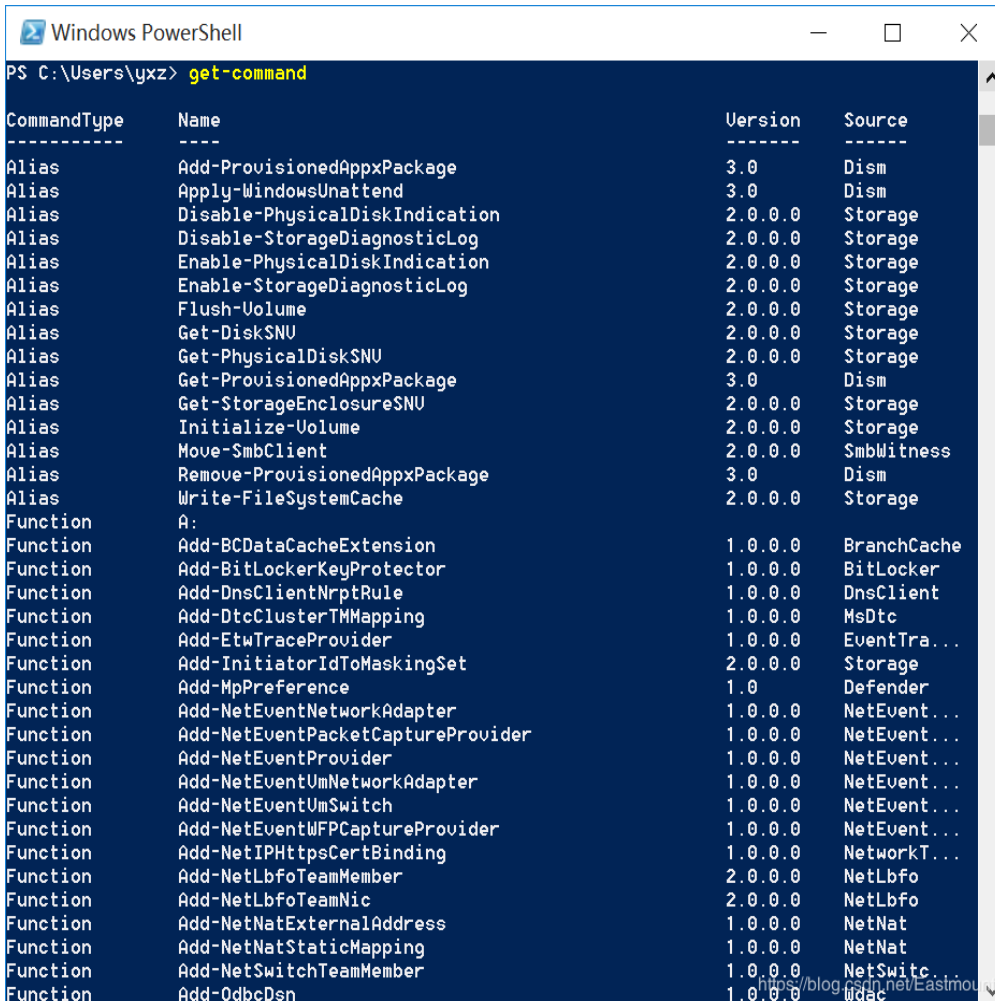
```

四.Powershell别名使用

1.别名基本用法

获取所有命令get-command可以用别名gcm替代。

```
get-command  
gcm
```



```
Windows PowerShell
PS C:\Users\yxz> get-command

CommandType      Name                                     Version      Source
-----
Alias            Add-ProvisionedAppxPackage             3.0          Dism
Alias            Apply-WindowsUnattend                  3.0          Dism
Alias            Disable-PhysicalDiskIndication         2.0.0.0     Storage
Alias            Disable-StorageDiagnosticLog          2.0.0.0     Storage
Alias            Enable-PhysicalDiskIndication          2.0.0.0     Storage
Alias            Enable-StorageDiagnosticLog            2.0.0.0     Storage
Alias            Flush-Uolume                            2.0.0.0     Storage
Alias            Get-DiskSNU                             2.0.0.0     Storage
Alias            Get-PhysicalDiskSNU                    2.0.0.0     Storage
Alias            Get-ProvisionedAppxPackage              3.0          Dism
Alias            Get-StorageEnclosureSNU                 2.0.0.0     Storage
Alias            Initialize-Uolume                       2.0.0.0     Storage
Alias            Move-SmbClient                          2.0.0.0     SmbWitness
Alias            Remove-ProvisionedAppxPackage           3.0          Dism
Alias            Write-FileSystemCache                   2.0.0.0     Storage
Function         A:
Function         Add-BCDataCacheExtension                1.0.0.0     BranchCache
Function         Add-BitLockerKeyProtector               1.0.0.0     BitLocker
Function         Add-DnsClientNrptRule                   1.0.0.0     DnsClient
Function         Add-DtcClusterTMMapping                 1.0.0.0     MsDtc
Function         Add-EtwTraceProvider                    1.0.0.0     EventTra...
Function         Add-InitiatorIdToMaskingSet             2.0.0.0     Storage
Function         Add-MpPreference                        1.0         Defender
Function         Add-NetEventNetworkAdapter              1.0.0.0     NetEvent...
Function         Add-NetEventPacketCaptureProvider       1.0.0.0     NetEvent...
Function         Add-NetEventProvider                    1.0.0.0     NetEvent...
Function         Add-NetEventUmNetworkAdapter            1.0.0.0     NetEvent...
Function         Add-NetEventUmSwitch                    1.0.0.0     NetEvent...
Function         Add-NetEventWFPCaptureProvider           1.0.0.0     NetEvent...
Function         Add-NetIPHttpsCertBinding               1.0.0.0     NetworkT...
Function         Add-NetLbfoTeamMember                   2.0.0.0     NetLbfo
Function         Add-NetLbfoTeamNic                      2.0.0.0     NetLbfo
Function         Add-NetNatExternalAddress               1.0.0.0     NetNat
Function         Add-NetNatStaticMapping                 1.0.0.0     NetNat
Function         Add-NetSwitchTeamMember                 1.0.0.0     NetSwitc...
Function         Add-OdbcDsn                             1.0.0.0     Wdac
```

获取当前目录的所有文件信息get-childitem, 可以用ls、dir两个命令达到同样的效果。

```
get-childitem  
ls  
dir
```

```
Windows PowerShell
PS C:\Users\yxz> get-childitem

目录: C:\Users\yxz

Mode                LastWriteTime         Length Name
----                -
d-----          2018/4/22      22:30         .android
d-----          2019/5/30      20:44         .citespace
d-----          2018/7/27      11:37         .eclipse
d-----          2018/4/24      10:08         .idlerc
d-----          2018/4/22      23:11         .ipython
d-----          2018/7/27      11:37         .jmc
d-----          2018/4/24      14:23         .jupyter
d-----          2019/6/28      11:42         .m2
d-----          2019/10/18         0:10         .matplotlib
d-----          2019/6/27      20:37         .myeclipse
d-----          2019/8/1       14:28         .Neo4jDesktop
d-----          2018/10/20      8:58         .Protege
d-----          2019/10/15     14:58         .spyder2
d-----          2019/2/13      17:04         .sqlmap
d-----          2019/9/10      19:03         .ssh
d-----          2019/9/5       15:10         .zenmap
d-----          2019/3/21      20:26         Anaconda2
d-r--          2018/4/23         0:09         Contacts
d-----          2019/10/26     15:01         Desktop
d-r--          2019/10/8      20:27         Documents
d-r--          2019/10/25     17:00         Downloads
d-r--          2019/5/10      12:41         Favorites
d-r--          2018/4/23         0:09         Links
d-r--          2019/6/6       10:26         Music
d-r--          2019/9/30      10:10         OneDrive
d-r--          2019/10/21      9:36         Pictures
d-----          2018/4/25     12:42         pip
d-----          2019/5/30     13:44         PubMed
d-r--          2018/4/23         0:09         Saved Games
d-r--          2018/4/23         0:09         Searches
d-r--          2019/8/3       17:57         Videos
d-----          2019/6/27      20:37         Workspaces
```

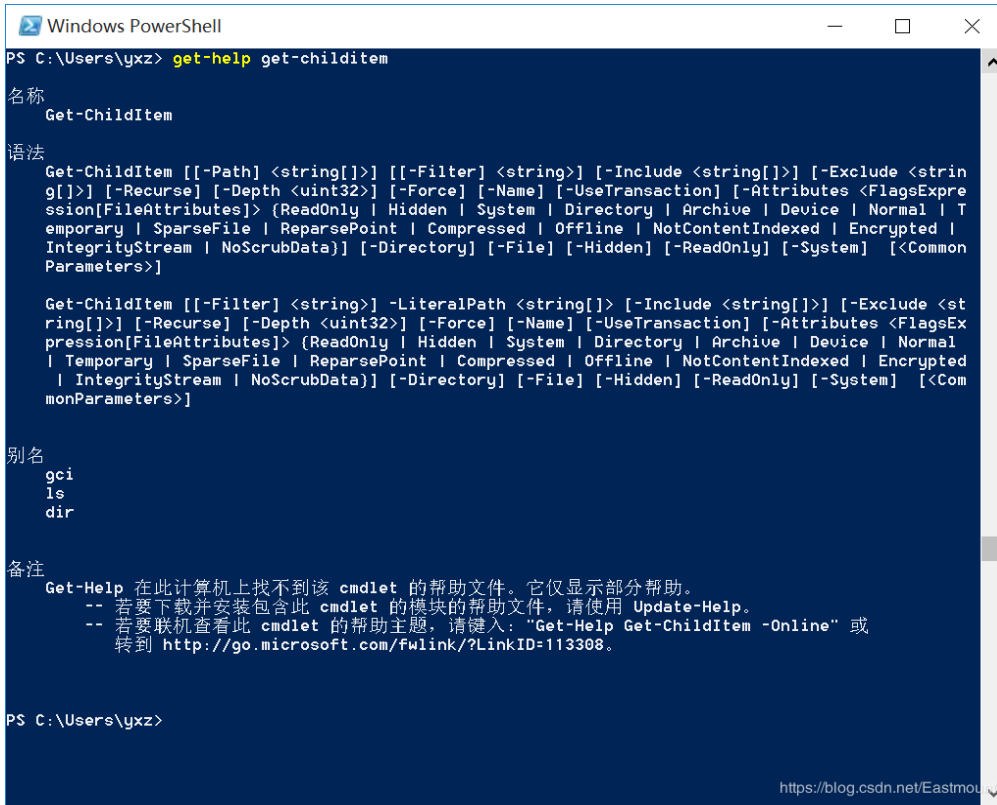
```
Windows PowerShell
PS C:\Users\yxz> dir

目录: C:\Users\yxz

Mode                LastWriteTime         Length Name
----                -
d-----          2018/4/22      22:30         .android
d-----          2019/5/30      20:44         .citespace
d-----          2018/7/27      11:37         .eclipse
d-----          2018/4/24      10:08         .idlerc
d-----          2018/4/22      23:11         .ipython
d-----          2018/7/27      11:37         .jmc
d-----          2018/4/24      14:23         .jupyter
d-----          2019/6/28      11:42         .m2
d-----          2019/10/18         0:10         .matplotlib
d-----          2019/6/27      20:37         .myeclipse
d-----          2019/8/1       14:28         .Neo4jDesktop
d-----          2018/10/20      8:58         .Protege
d-----          2019/10/15     14:58         .spyder2
d-----          2019/2/13      17:04         .sqlmap
d-----          2019/9/10      19:03         .ssh
d-----          2019/9/5       15:10         .zenmap
d-----          2019/3/21      20:26         Anaconda2
d-r--          2018/4/23         0:09         Contacts
d-----          2019/10/26     15:01         Desktop
d-r--          2019/10/8      20:27         Documents
d-r--          2019/10/25     17:00         Downloads
d-r--          2019/5/10      12:41         Favorites
d-r--          2018/4/23         0:09         Links
d-r--          2019/6/6       10:26         Music
d-r--          2019/9/30      10:10         OneDrive
d-r--          2019/10/21      9:36         Pictures
d-----          2018/4/25     12:42         pip
d-----          2019/5/30     13:44         PubMed
d-r--          2018/4/23         0:09         Saved Games
d-r--          2018/4/23         0:09         Searches
d-r--          2019/8/3       17:57         Videos
d-----          2019/6/27      20:37         Workspaces
```

获取相关的帮助信息，其命令如下：

```
get-help get-childitem
```

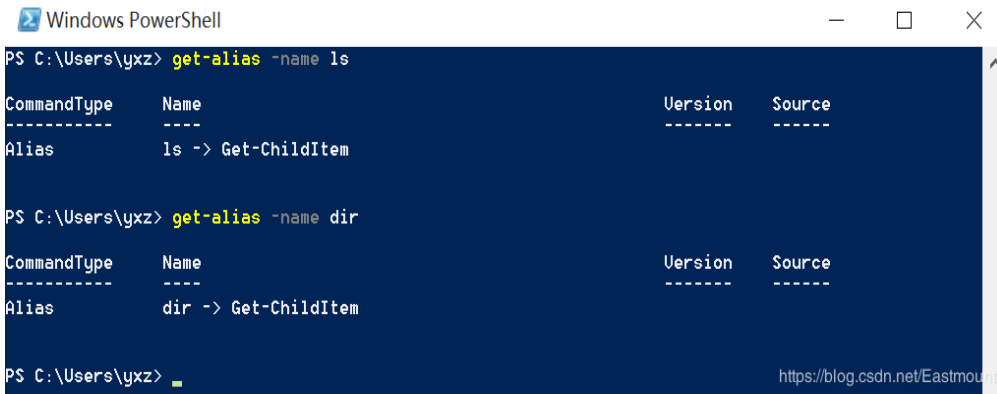


获取别名所对应真实的命令

```

get-alias -name ls
get-alias -name dir

```



查找所有以Remove开头的别名

```

get-alias | where{$_.definition.startswith("Remove")}

```

其中，where来做一个管道的筛选，\$_表示当前的元素，definition 定义一个字符串数组类型。Powershell支持.net强大的类库，里面的definition包括字符串startswith操作，获取字符串开头函数。

```

Windows PowerShell
PS C:\Users\yxz> get-alias | where($_.definition.startswith("Remove"))

CommandType      Name                                     Version      Source
-----
Alias             del -> Remove-Item
Alias             erase -> Remove-Item
Alias             rbp -> Remove-PSBreakpoint
Alias             rd -> Remove-Item
Alias             rdr -> Remove-PSDrive
Alias             ri -> Remove-Item
Alias             rjb -> Remove-Job
Alias             rm -> Remove-Item
Alias             rmdir -> Remove-Item
Alias             rmo -> Remove-Module
Alias             rp -> Remove-ItemProperty
Alias             rsn -> Remove-PSSession
Alias             rsnp -> Remove-PSSnapin
Alias             rv -> Remove-Variable
Alias             rwmi -> Remove-WmiObject

PS C:\Users\yxz>

```

查找所有别名，并调用sort降序排序及计算排列。

```
get-alias | group-object definition | sort -descending Count
```

```

Windows PowerShell
PS C:\Users\yxz> get-alias | group-object definition | sort -descending Count

Count Name                                     Group
-----
6 Remove-Item                             {del, erase, rd, ri...}
3 Get-ChildItem                            {dir, gci, ls}
3 Get-History                              {ghy, h, history}
3 Copy-Item                                {copy, cp, cpi}
3 Invoke-WebRequest                       {curl, iwr, wget}
3 Set-Location                             {cd, chdir, sl}
3 Get-Content                              {cat, gc, type}
3 Move-Item                                 {mi, move, mv}
2 Invoke-History                           {ihy, r}
2 Get-Process                              {gps, ps}
2 Rename-Item                              {ren, rni}
2 New-PSDrive                              {mount, ndr}
2 Set-Variable                             {set, sv}
2 Stop-Process                             {kill, spps}
2 Get-Location                             {gl, pwd}
2 Write-Output                             {echo, write}
2 Start-Process                            {saps, start}
2 Compare-Object                           {compare, diff}
2 Where-Object                              {?, where}
2 ForEach-Object                           {%, foreach}
2 Clear-Host                               {clear, cls}
1 Remove-PSBreakpoint                     {rbp}
1 Push-Location                            {pushd}
1 Out-GridView                             {ogv}
1 Out-Host                                 {oh}
1 Pop-Location                             {popd}
1 Receive-Job                              {rcjb}
1 Tee-Object                               {tee}
1 Set-WMIInstance                          {swmi}
1 Remove-PSDrive                           {rdr}
1 Trace-Command                            {trcm}
1 Receive-PSSession                        {rcsn}
1 Measure-Object                           {measure}
1 Move-ItemProperty                        {mp}
1 New-Alias                                {nal}

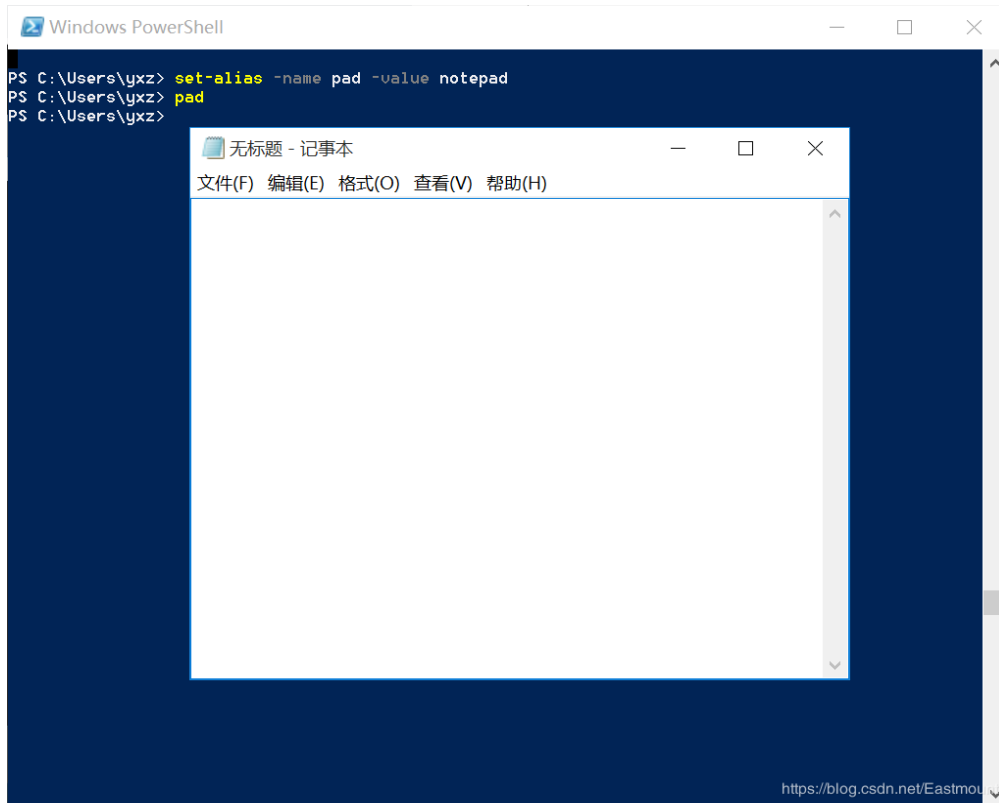
```

注意：自定义别名是临时生效的，当关闭Powershell时就会失效。

2.自定义别名

设置别名，将notepad设置为新的别名pad。pad打开notepad，表明我们的别名创建成功。

```
set-alias -name pad -value notepad
```



别名是临时生成的，关掉Powershell即可失效，也可以撰写命令删除。

```
del alias:pad
```



保存别名

```
export-alias demo.ps
dir
type demo.ps
```



```

Windows PowerShell
PS C:\Users\yxz> export-alias demo.ps
PS C:\Users\yxz> dir

目录: C:\Users\yxz

Mode                LastWriteTime         Length Name
----                -
d-----          2018/4/22            22:30      android
d-----          2019/5/30            20:44      .citespace
d-----          2018/7/27            11:37      .eclipse
d-----          2018/4/24            10:08      .idlerc
d-----          2018/4/22            23:11      .ipython
d-----          2018/7/27            11:37      .jmc
d-----          2018/4/24            14:23      .jupyter
d-----          2019/6/28            11:42      .m2
d-----          2019/10/18           0:10      .matplotlib
d-----          2019/6/27            20:37      .myeclipse
d-----          2019/8/1             14:28      .Neo4jDesktop
d-----          2018/10/20           8:58      .Protege
d-----          2019/10/15           14:58      .spyder2
d-----          2019/2/13            17:04      .sqlmap
d-----          2019/9/10            19:03      .ssh
d-----          2019/9/5             15:10      .zenmap
d-----          2019/3/21            20:26      Anaconda2
d-r-----        2018/4/23             0:09      Contacts
d-r-----        2019/10/26           15:01      Desktop
d-r-----        2019/10/8            20:27      Documents
d-r-----        2019/10/25           17:00      Downloads
d-r-----        2019/5/10            12:41      Favorites
d-r-----        2018/4/23             0:09      Links
d-r-----        2019/6/6             10:26      Music
d-r-----        2019/9/30            10:10      OneDrive
d-r-----        2019/10/21           9:36      Pictures
d-----          2018/4/25            12:42      pip
d-----          2019/5/30            13:44      PubMed
d-r-----        2018/4/23             0:09      Saved Games
d-r-----        2018/4/23             0:09      Searches
d-r-----        2019/8/3             17:57      Videos

```

```

Windows PowerShell
d-r-----        2019/8/3             17:57      Videos
d-----          2019/6/27            20:37      Workspaces
-a-----          2019/10/17           0:58      4011 .bash_history
-a-----          2019/10/16           23:56      212 .gitconfig
-a-----          2019/6/28            11:38      564 .myeclipse.properties
-a-----          2019/9/11            16:14      974 .viminfo
-a-----          2019/10/28           10:11      13558 demo.ps
-a-----          2019/10/26           23:29      2414 demo.txt
-a-----          2018/5/9             13:26      14196 kk.png

PS C:\Users\yxz> type demo.ps
# 别名文件
# 导出者 : yxz
# 日期/时间 : 2019年10月28日 10:11:52
# 计算机: DESKTOP-2PTB11K
"foreach","ForEach-Object","","ReadOnly, AllScope"
"%","ForEach-Object","","ReadOnly, AllScope"
"where","Where-Object","","ReadOnly, AllScope"
"?","Where-Object","","ReadOnly, AllScope"
"ac","Add-Content","","ReadOnly, AllScope"
"clc","Clear-Content","","ReadOnly, AllScope"
"cli","Clear-Item","","ReadOnly, AllScope"
"clp","Clear-ItemProperty","","ReadOnly, AllScope"
"clu","Clear-Variable","","ReadOnly, AllScope"
"compare","Compare-Object","","ReadOnly, AllScope"
"cp","Copy-Item","","ReadOnly, AllScope"
"cpp","Copy-ItemProperty","","ReadOnly, AllScope"
"cupa","Convert-Path","","ReadOnly, AllScope"
"dbp","Disable-PSBreakpoint","","ReadOnly, AllScope"
"diff","Compare-Object","","ReadOnly, AllScope"
"ebp","Enable-PSBreakpoint","","ReadOnly, AllScope"
"epal","Export-Alias","","ReadOnly, AllScope"
"epcsu","Export-Csu","","ReadOnly, AllScope"
"fc","Format-Custom","","ReadOnly, AllScope"
"fl","Format-List","","ReadOnly, AllScope"
"ft","Format-Table","","ReadOnly, AllScope"
"fw","Format-Wide","","ReadOnly, AllScope"
"gal","Get-Alias","","ReadOnly, AllScope"
"gbp","Get-PSBreakpoint","","ReadOnly, AllScope"

```

导入别名命令如下，其中-force表示强制导入。

```
import-alias -force demo.ps
```

五.Powershell变量基础

1.基础用法

Powershell变量跟PHP很类似，如下所示。

```
$name='eastmount'  
$name  
$age=28  
$age
```

```
PS C:\Users\yxz> $name='eastmount'  
PS C:\Users\yxz> $name  
eastmount  
PS C:\Users\yxz> $age=28  
PS C:\Users\yxz> $age  
28  
PS C:\Users\yxz>
```

Powershell对大小写不敏感，\$a 和 \$A 一样。复杂变量用大括号引起来，但不建议同学们这里定义。

```
`${"I am a" var ()}="yxz"  
`${"I am a" var ()}  
$n=(7*6+8)/2  
$n=3.14
```

```
PS C:\Users\yxz> `${"I am a" var ()}="yxz"  
PS C:\Users\yxz> `${"I am a" var ()}  
yxz  
PS C:\Users\yxz> $n=(7*6+8)/2  
PS C:\Users\yxz> $n  
25  
PS C:\Users\yxz> $n=3.14  
PS C:\Users\yxz> $n  
3.14  
PS C:\Users\yxz> https://blog.csdn.net/Eastmount
```

变量也可以设置等于命令。

```
$n=ls
```

```

Windows PowerShell
PS C:\Users\yxz> $n=1s
PS C:\Users\yxz> $n

目录: C:\Users\yxz

Mode                LastWriteTime         Length Name
----                -
d-----          2018/4/22          22:30      android
d-----          2019/5/30          20:44      .citespace
d-----          2018/7/27          11:37      .eclipse
d-----          2018/4/24          10:08      .idlerc
d-----          2018/4/22          23:11      .ipython
d-----          2018/7/27          11:37      .jmc
d-----          2018/4/24          14:23      .jupyter
d-----          2019/6/28          11:42      .m2
d-----          2019/10/18          0:10      .matplotlib
d-----          2019/6/27          20:37      .myeclipse
d-----          2019/8/1           14:28      .Neo4jDesktop
d-----          2018/10/20          8:58      .Protege
d-----          2019/10/15         14:58      .spyder2
d-----          2019/2/13          17:04      .sqlmap
d-----          2019/9/10          19:03      .ssh
d-----          2019/9/5           15:10      .zenmap
d-----          2019/3/21          20:26      Anaconda2
d-r-----        2018/4/23           0:09      Contacts
d-r-----        2019/10/26         15:01      Desktop
d-r-----        2019/10/8          20:27      Documents
d-r-----        2019/10/25         17:00      Downloads
d-r-----        2019/5/10          12:41      Favorites
d-r-----        2018/4/23           0:09      Links
d-r-----        2019/6/6           10:26      Music
d-r-----        2019/9/30          10:10      OneDrive
d-r-----        2019/10/21          9:36      Pictures
d-r-----        2018/4/25          12:42      pip
d-----          2019/5/30          13:44      PubMed
d-r-----        2018/4/23           0:09      Saved Games
d-r-----        2018/4/23           0:09      Searches
d-r-----        2019/8/3           17:57      Videos

```

变量多个同时赋值，但不建议这么写。

```
$n1=$n2=$n3=25
```

```
$n1,$n2,$n3
```

```

PS C:\Users\yxz> $n1=$n2=$n3=25
PS C:\Users\yxz> $n1,$n2,$n3
25
25
25

```

2. 变量操作

变量的基本运算操作

```
$a=2
```

```
$b=10
```

```
$c=a+b
```

```
$a,$b,$c
```

```

PS C:\Users\yxz> $a=2
PS C:\Users\yxz> $b=10
PS C:\Users\yxz> $c=$a+$b
PS C:\Users\yxz> $a,$b,$c
2
10
12
PS C:\Users\yxz>

```

传统变量交换方法

```

$num1=10
$num2=20
$temp=$num1
$num1=$num2
$num2=$temp
$num1,$num2

```

```

PS C:\Users\yxz> $num1=10
PS C:\Users\yxz> $num2=20
PS C:\Users\yxz> $num1,$num2
10
20
PS C:\Users\yxz> $temp=$num1
PS C:\Users\yxz> $num1=$num2
PS C:\Users\yxz> $num2=$temp
PS C:\Users\yxz> $num1,$num2
20
10
PS C:\Users\yxz>

```

现在变量交换的写法

```

$num1=10
$num2=20
$num1,$num2=$num2,$num1
$num1,$num2

```

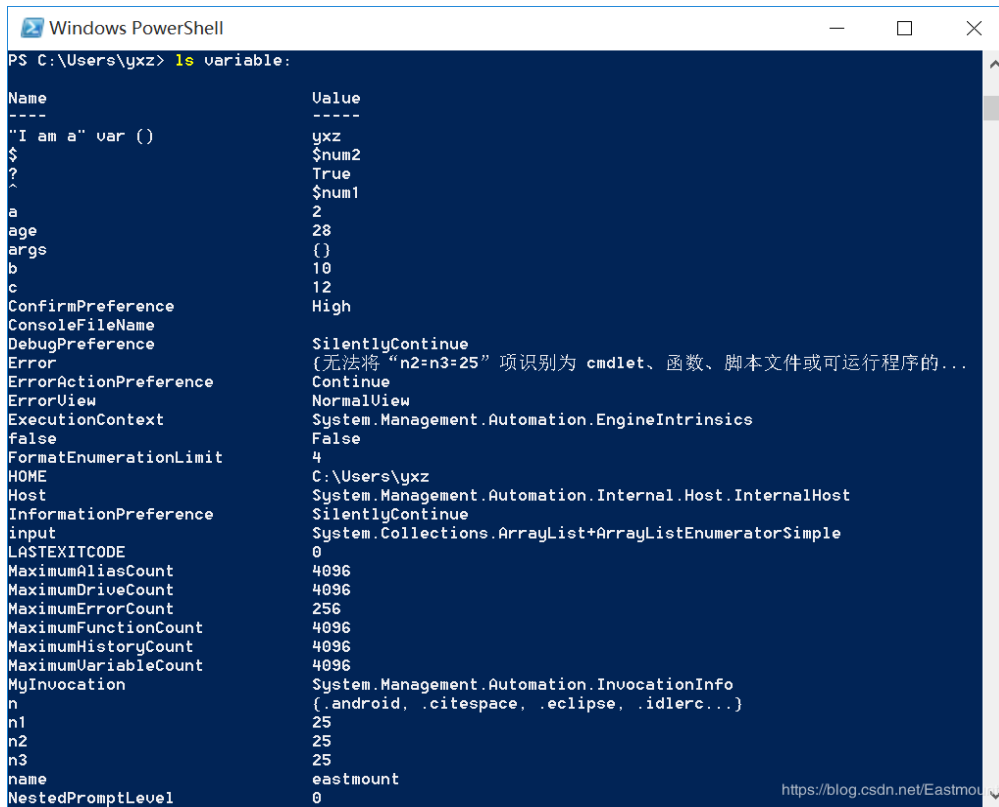
```

PS C:\Users\yxz> $num1=10
PS C:\Users\yxz> $num2=20
PS C:\Users\yxz> $num1,$num2=$num2,$num1
PS C:\Users\yxz> $num1,$num2
20
10
PS C:\Users\yxz>

```

查看当前的变量

```
ls variable:
```



```

Windows PowerShell
PS C:\Users\yxz> ls variable:

Name                Value
----                -
"I am a" var ()    yxz
$                   $num2
?                   True
^                   $num1
a                   2
age                 28
args                ()
b                   10
c                   12
ConfirmPreference  High
ConsoleFileName
DebugPreference    SilentlyContinue
Error               (无法将“n2=n3=25”项识别为 cmdlet、函数、脚本文件或可运行程序的...
ErrorActionPreference Continue
ErrorView           NormalView
ExecutionContext   System.Management.Automation.EngineIntrinsics
false
FormatEnumerationLimit 4
HOME                C:\Users\yxz
Host                System.Management.Automation.Internal.Host.InternalHost
InformationPreference SilentlyContinue
input               System.Collections.ArrayList+ArrayListEnumeratorSimple
LASTEXITCODE        0
MaximumAliasCount   4096
MaximumDriveCount   4096
MaximumErrorCount   256
MaximumFunctionCount 4096
MaximumHistoryCount 4096
MaximumVariableCount 4096
MyInvocation        System.Management.Automation.InvocationInfo
n                   (.android, .citespace, .eclipse, .idlerc...)
n1                  25
n2                  25
n3                  25
name                eastmount
NestedPromptLevel   0

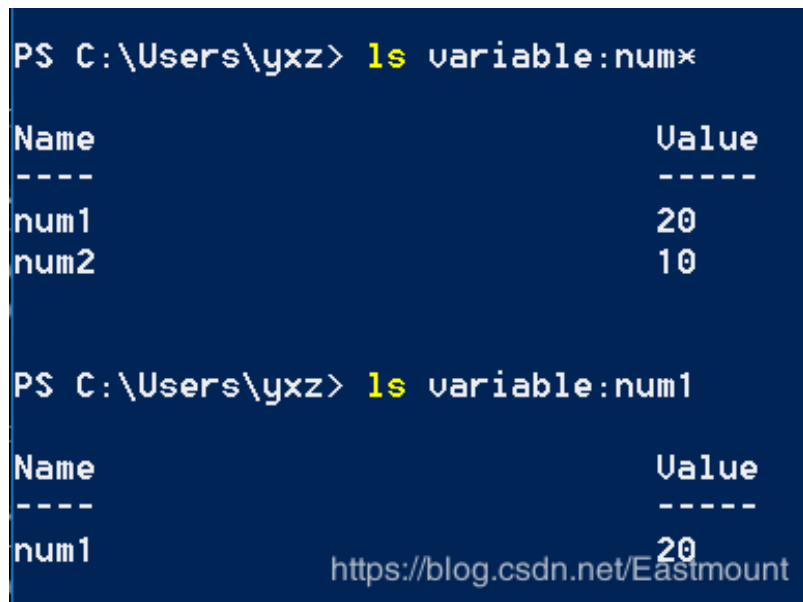
```

查找特定的变量值，星号表示代替所有的值（num开头）。

```

ls variable:num*
ls variable:num1

```



```

PS C:\Users\yxz> ls variable:num*

Name                Value
----                -
num1                 20
num2                 10

PS C:\Users\yxz> ls variable:num1

Name                Value
----                -
num1                 20

```

查找变量是否存在

```

test-path variable:num1
test-path variable:num0

```

```
PS C:\Users\yxz> test-path variable:num1
True
PS C:\Users\yxz> test-path variable:num0
False
```

删除变量

```
del variable:num1
test-path variable:num1
```

```
PS C:\Users\yxz> del variable:num1
PS C:\Users\yxz> test-path variable:num1
False
PS C:\Users\yxz> _
```

专用变量管理的命令

```
clear-variable
remove-variable
new-variable
```

3. 自动化变量

powershell打开会自动加载变量，例如：窗口打开它会自动加载大小，再比如程序的配置信息自动加载。

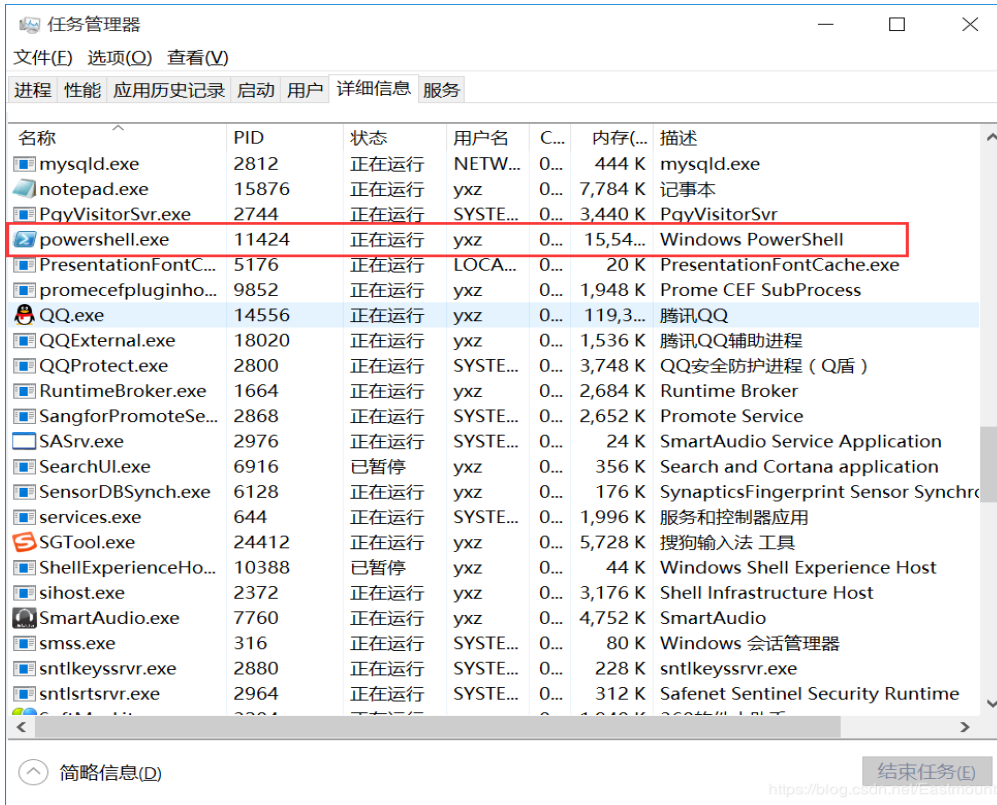
根目录信息

`$home`

```
PS C:\Users\yxz> $home
C:\Users\yxz
PS C:\Users\yxz> $pid
11424
PS C:\Users\yxz> $$
$pid
PS C:\Users\yxz> _
```

当前进程的标志符，该自动化内置变量只能读取，不能写入。

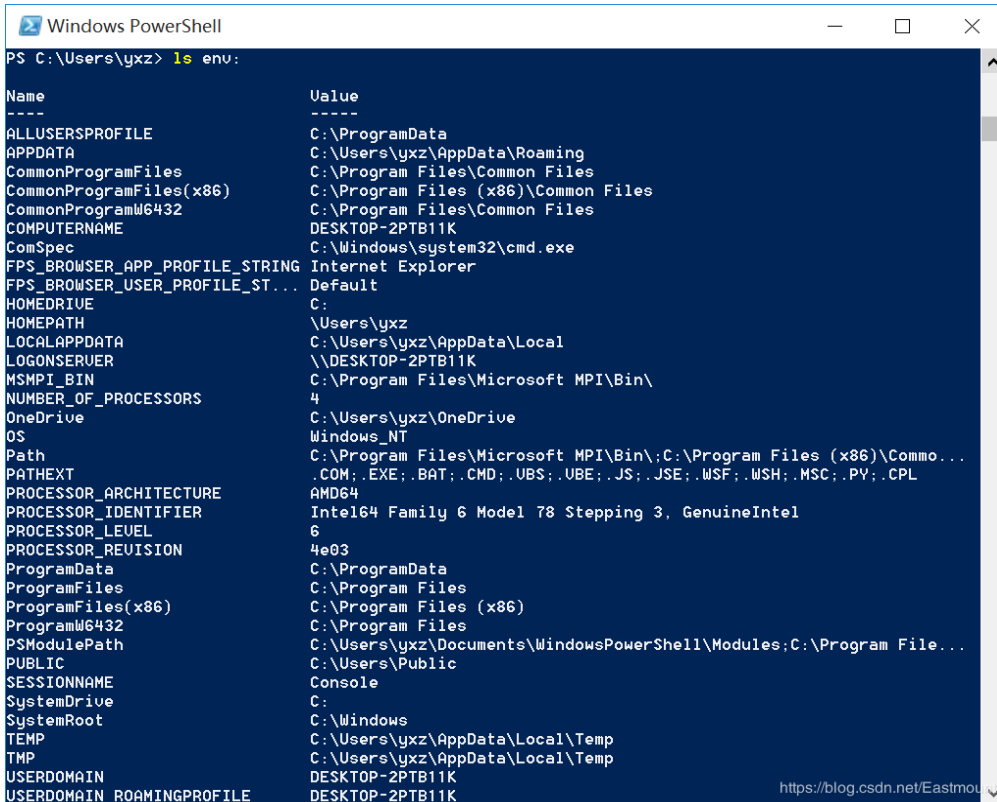
```
$pid
$$
```



4.环境变量

查看当前环境变量

ls env:



打印某个环境变量的值

```
$env:windir
```

```
windir C:\Windows
PS C:\Users\yxz> $env:windir
C:\Windows
PS C:\Users\yxz>
```

创建新的环境变量

```
$env:name='eastmount'
```

```
ls env:na*
```

```
PS C:\Users\yxz> $env:name='eastmount'
PS C:\Users\yxz> ls env:na*

Name                Value
----                -
name                eastmount

PS C:\Users\yxz>
```

删除环境变量

```
del env:name
```

```
ls env:na*
```

```
PS C:\Users\yxz> del env:name
PS C:\Users\yxz> ls env:na*
PS C:\Users\yxz>
```

更新环境变量，注意它只是临时生效，并不会记录到我们的系统中。

```
$env:OS
```

```
$env:OS="Linux"
```

```
$env:OS
```

```
PS C:\Users\yxz> $env:OS
Windows_NT
PS C:\Users\yxz> $env:OS="Linux"
PS C:\Users\yxz> $env:OS
Linux
PS C:\Users\yxz>
```

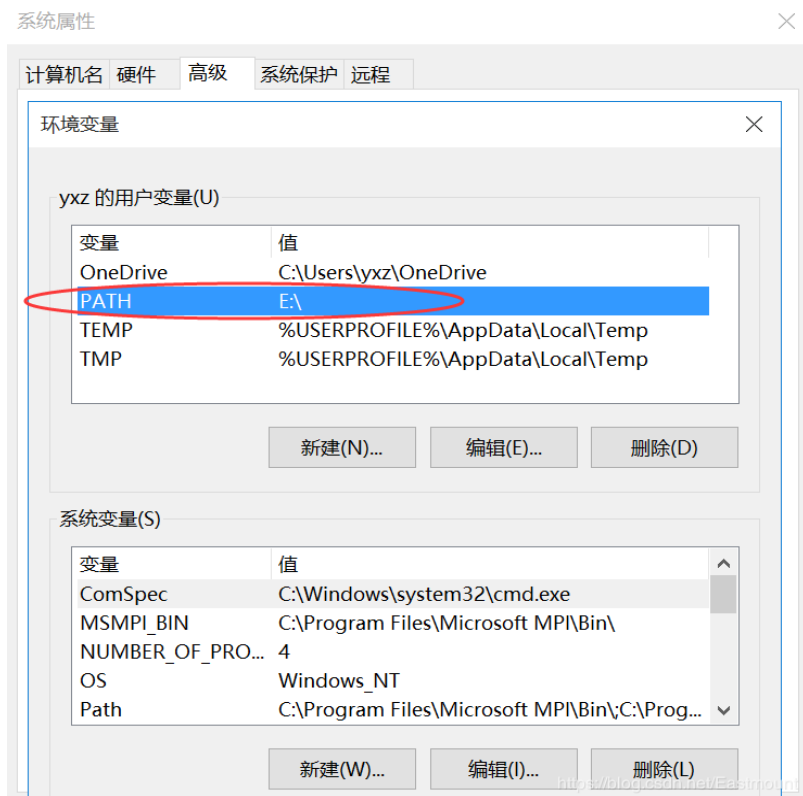

永久生效如何实现呢？增加路径至环境变量PATH中，只对User用户生效。

```
[environment]::setenvironmentvariable("PATH","E:\","User")
[environment]::getenvironmentvariable("PATH","User")
```

系统变量对所有用户都生效，用户变量只对当前用户生效。



生效之后如下图所示，用户变量增加了相关值。

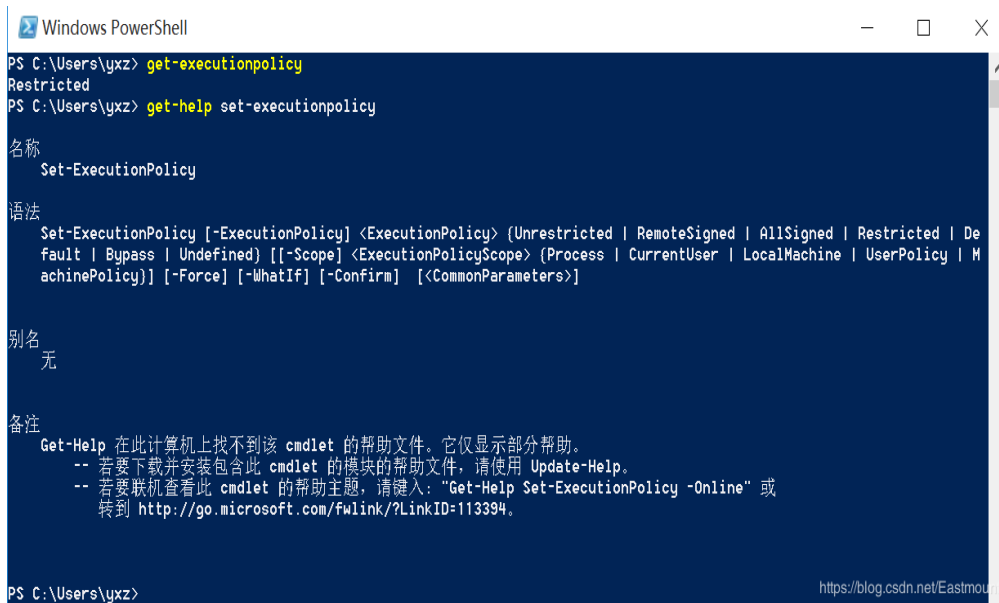


六.Powershell调用脚本程序

1.脚本文件执行策略

首先，发现我们的脚本文件是禁止执行的。

```
get-executionpolicy
```



```
Windows PowerShell
PS C:\Users\yxz> get-executionpolicy
Restricted
PS C:\Users\yxz> get-help set-executionpolicy

名称
    Set-ExecutionPolicy

语法
    Set-ExecutionPolicy [-ExecutionPolicy] <ExecutionPolicy> (Unrestricted | RemoteSigned | AllSigned | Restricted | De
    fault | Bypass | Undefined) [[-Scope] <ExecutionPolicyScope> (Process | CurrentUser | LocalMachine | UserPolicy | M
    achinePolicy)] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]

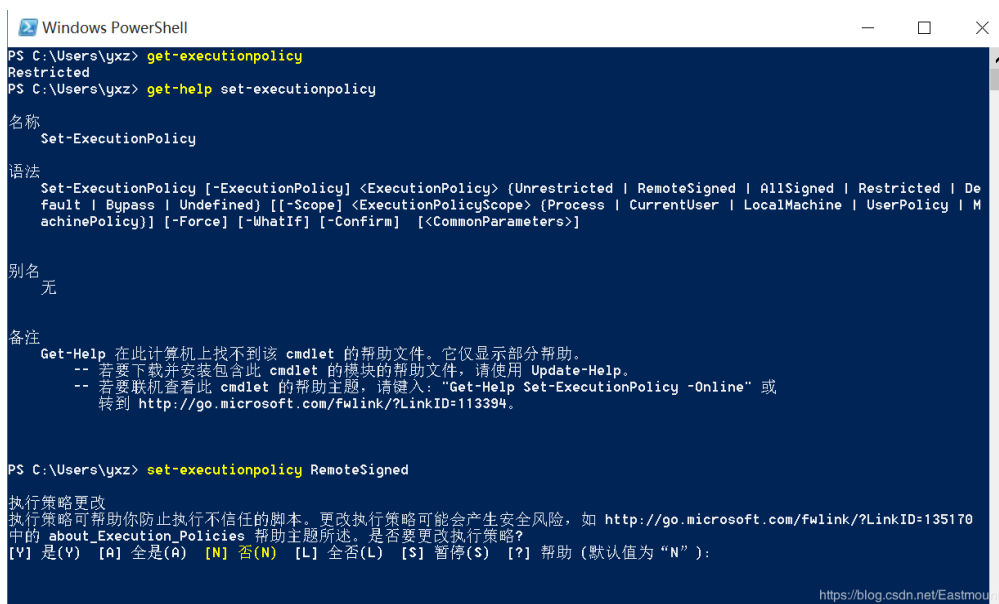
别名
    无

备注
    Get-Help 在此计算机上找不到该 cmdlet 的帮助文件。它仅显示部分帮助。
    -- 若要下载并安装包含此 cmdlet 的模块的帮助文件，请使用 Update-Help。
    -- 若要联机查看此 cmdlet 的帮助主题，请键入：“Get-Help Set-ExecutionPolicy -Online” 或
    转到 http://go.microsoft.com/fwlink/?LinkID=113394。

PS C:\Users\yxz>
```

接着，我们尝试获取策略帮助信息。

```
get-help set-executionpolicy
```



```
Windows PowerShell
PS C:\Users\yxz> get-executionpolicy
Restricted
PS C:\Users\yxz> get-help set-executionpolicy

名称
    Set-ExecutionPolicy

语法
    Set-ExecutionPolicy [-ExecutionPolicy] <ExecutionPolicy> (Unrestricted | RemoteSigned | AllSigned | Restricted | De
    fault | Bypass | Undefined) [[-Scope] <ExecutionPolicyScope> (Process | CurrentUser | LocalMachine | UserPolicy | M
    achinePolicy)] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]

别名
    无

备注
    Get-Help 在此计算机上找不到该 cmdlet 的帮助文件。它仅显示部分帮助。
    -- 若要下载并安装包含此 cmdlet 的模块的帮助文件，请使用 Update-Help。
    -- 若要联机查看此 cmdlet 的帮助主题，请键入：“Get-Help Set-ExecutionPolicy -Online” 或
    转到 http://go.microsoft.com/fwlink/?LinkID=113394。

PS C:\Users\yxz> set-executionpolicy RemoteSigned

执行策略更改
执行策略帮助你防止执行不信任的脚本。更改执行策略可能会产生安全风险，如 http://go.microsoft.com/fwlink/?LinkID=135179
中的 about\_Execution\_Policies 帮助主题所述。是否要更改执行策略？
[V] 是(Y) [A] 全是(A) [N] 否(N) [L] 全否(L) [S] 暂停(S) [?] 帮助(默认为“N”)：

PS C:\Users\yxz>
```

最后修改权限，让其能运行Powershell脚本文件。

```
set-executionpolicy RemoteSigned
```

它会提示你需要启动管理员身份运行。

```
PS C:\Users\yxz\desktop> set-executionpolicy RemoteSigned

执行策略更改
执行策略可帮助你防止执行不信任的脚本。更改执行策略可能会产生安全风险，如 http://go.microsoft.com/fwlink/?LinkID=135170
中的 about_Execution_Policies 帮助主题所述。是否要更改执行策略？
[Y] 是(Y) [A] 全是(A) [N] 否(N) [L] 全否(L) [S] 暂停(S) [?] 帮助 (默认值为“N”)： A
set-executionpolicy : 对注册表项“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell”的
访问被拒绝。 要更改默认(LocalMachine)作用域的执行策略，请使用“以管理员身份运行”选项启动 Windows PowerShell。要更改当
前用户的执行策略，请运行“Set-ExecutionPolicy -Scope CurrentUser”。
所在位置 行:1 字符: 1
+ set-executionpolicy RemoteSigned
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetExecutionPolicyComma
nd
PS C:\Users\yxz\desktop>
```

通过管理员身份打开CMD，再设置其权限即可，设置完成之后可以调用相关的脚本程序。

```
C:\> 管理员: Windows PowerShell

Microsoft Windows [版本 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32> powershell
Windows PowerShell
版权所有 (C) 2015 Microsoft Corporation。保留所有权利。

PS C:\Windows\system32> set-executionpolicy RemoteSigned
PS C:\Windows\system32> █
```

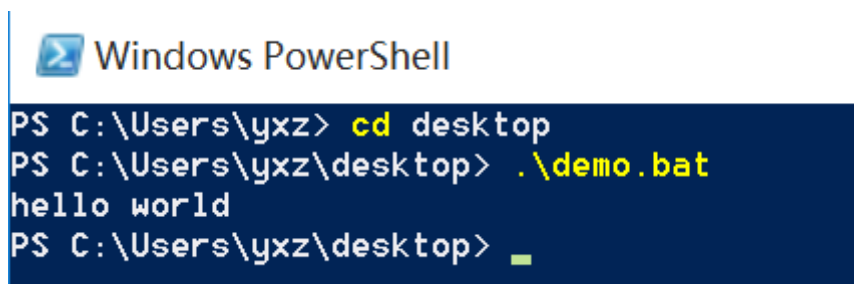
2.调用脚本程序

(1) 定义一个demo.bat文件，其内容如下，关闭回写，打印hello world。

```
@echo off
echo hello world
```

运行命令打开：

```
cd desktop
.\demo.bat
```



```
Windows PowerShell

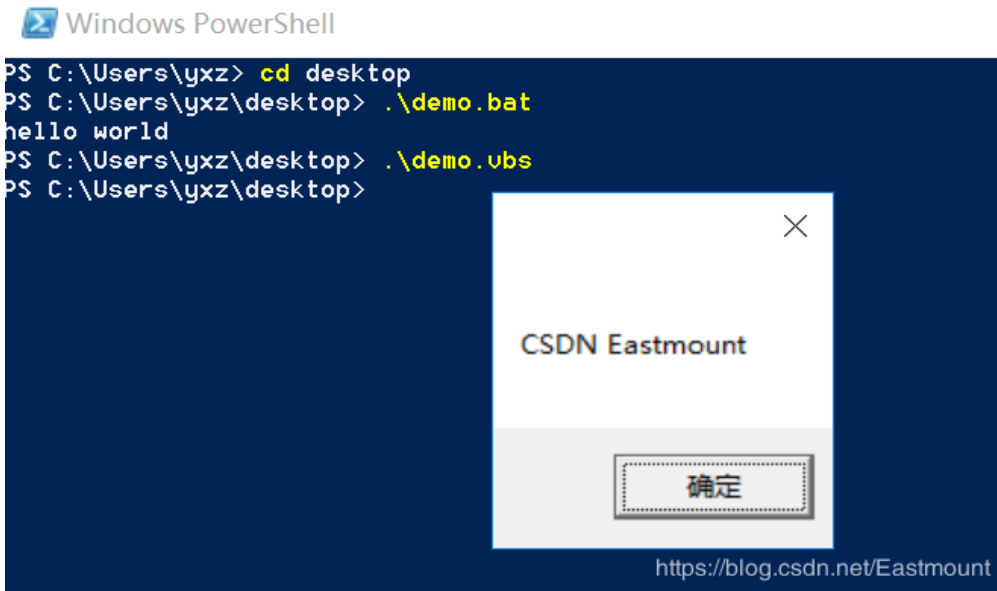
PS C:\Users\yxz> cd desktop
PS C:\Users\yxz\desktop> .\demo.bat
hello world
PS C:\Users\yxz\desktop> █
```

(2) 定义一个demo.vbs文件，内容如下：

msgbox "CSDN Eastmount"

运行命令打开:

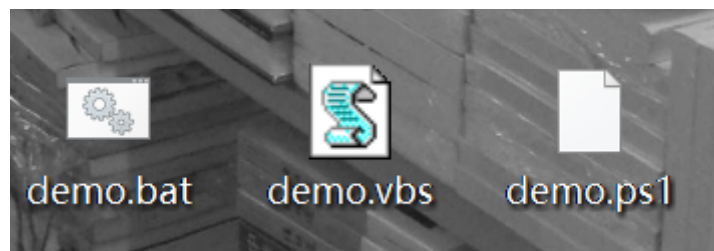
```
cd desktop
.\demo.vbs
```

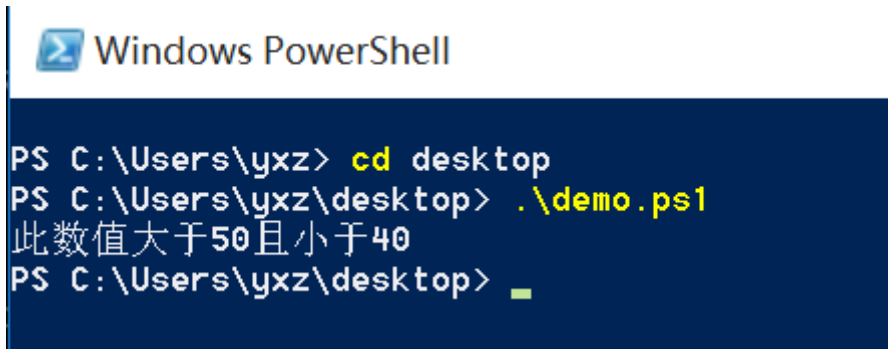


(3) 运行Powershell脚本文件也类似。

```
$number=49
switch($number)
{
    {($_ -lt 50) -and ($_ -gt 40)} {"此数值大于50且小于40"}
    50 {"此数值等于50"}
    {$_ -gt 50} {"此数值大于50"}
}
```

运行结果如下图所示:





```

Windows PowerShell

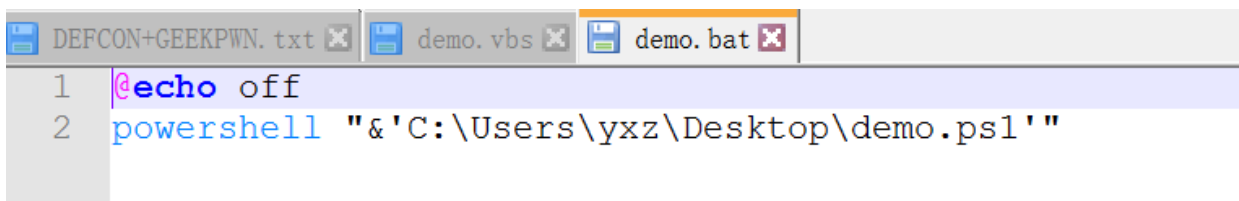
PS C:\Users\yxz> cd desktop
PS C:\Users\yxz\Desktop> .\demo.ps1
此数值大于50且小于40
PS C:\Users\yxz\Desktop>

```

那么，如何在CMD中运行Powershell文件呢？

我们将demo.bat修改为如下内容，其中&表示运行。

```
@echo off
powershell "&'C:\Users\yxz\Desktop\demo.ps1'"
```



```

DEFCON+GEEKPWN. txt demo.vbs demo.bat
1 @echo off
2 powershell "&'C:\Users\yxz\Desktop\demo.ps1'"

```

运行命令：

```
cd desktop
.\demo.bat
```

下面方法也可以直接运行

```
start demo.bat
demo.bat
```



```

C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\yxz>cd desktop

C:\Users\yxz\Desktop>.\demo.bat
此数值大于50且小于40

C:\Users\yxz\Desktop>

```

<https://blog.csdn.net/Eastmount>

七.总结

“没有网络安全就没有国家安全，没有信息化就没有现代化”，这是我第三次听院士授课。每次的感受都很震撼，他们是这个国家的脊梁，总能站在国家和民族的角度去思考问题、解决问题，用通俗易懂的图表去诠释知识，去构建祖国的重大工程和梦想，致敬。侠之为大，为国为民。补充一句，沈院士很早就到了会场修改PPT，特别增加了区块链的知识。



很多大牛和老师的分享都让我受益匪浅，来自清华大学和俄亥俄州立大学的两位张老师的分享是我第三次听了，但还是很懵，下次争取能听懂。来年在雄安新区举办，希望能像学弟和学妹一样，站上讲台，加油！

(By:Eastmount 2019-10-28 下午6点 <http://blog.csdn.net/eastmount/>)