反取证虚拟机系统环境

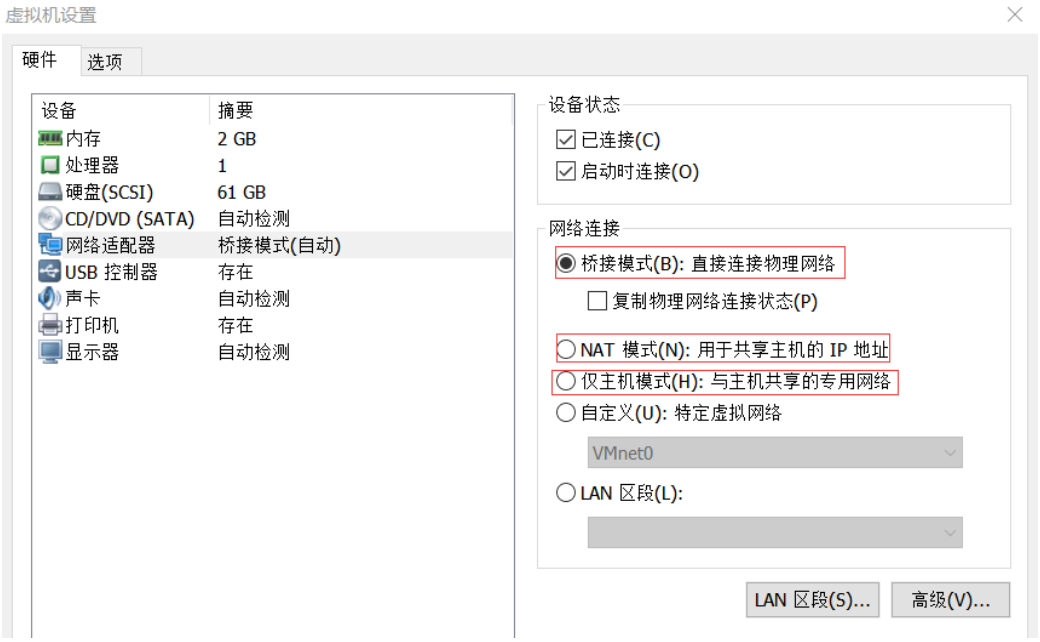
1、虚拟机

对入侵者而言，保护好个人电脑的 MAC 地址和 IP 地址尤为重要。MAC 地址和 IP 地址作为某一时刻、某个地区、某台电脑的全球唯一标识，犹如身份证一般，在取证的时候会作为重要的证据搜索线索。因此隐藏 MAC 地址和 IP 地址在反取证的过程中充当着重要的手段。使用虚拟机可以有效隐藏自己主机真实 MAC 地址和 IP 地址，入侵结束之后可以擦除虚拟机文件，清理案发现场，从而给取证带来了困难。

1.1 VMware Workstation

网络连接模式

VMware 提供了三种主要的网络连接模式，分别是 bridged（桥接模式）、NAT（网络地址转换模式）和 host-only（仅主机模式），如下图。要想在网络管理和维护中合理应用它们，应该先了解一下这三种工作模式。



1、bridged（网桥模式）

在这种模式下，使用 VMnet0 虚拟交换机，虚拟操作系统就像是局域网中的一台独立的主机，与宿主计算机一样，它可以访问网内任何一台机器。在桥接模式下，可以手工配置它的 TCP/IP 配置信息（IP、子网掩码等，而且还要和宿主机器处于同一网段），以实现通过局域网的网关或路由器访问互联网，还可以将 IP 地址和 DNS 设置成“自动获取”。如果你想利用 VMWare 在局域网内新建一个服务器，为局域网用户提供 Web 或网络服务，就应该选择桥接模式。

在桥接模式中，使用 VMnet0 虚拟交换机，此时虚拟机相当与网络上的一台独立计算机与主机一样，拥有一个独立的 IP 地址。

2、NAT（网络地址转换模式）

使用 NAT 模式，就是让虚拟机借助 NAT（网络地址转换）功能，通过宿主机器所在的网络来访问公网。也就是说，使用 NAT 模式可以实现在虚拟系统里访问互联网。NAT 模式下的虚拟机的 TCP/IP 配置信息是由 VMnet8 虚拟网络的 DHCP 服务器提供的，因此 IP 和 DNS 一般设置为“自动获取”，因此虚拟系统也就无法和本局域网中的其他真实主机进行通讯。采用 NAT 模式最大的优势是虚拟系统接入互联网非常简单，你不需要进行任何其他的配置，只需要宿主机器能访问互联网即可。如果你想利用 VMWare 安装一个新的虚拟系统，在虚拟系统中不用进行任何手工配置就能直接访问互联网，建议你采用 NAT 模式。

NAT 模式中使用 Vmnet8 虚拟交换机，此时虚拟机可以通过主机“单向访问”网络上的其他主机，其他主机不能访问虚拟机。

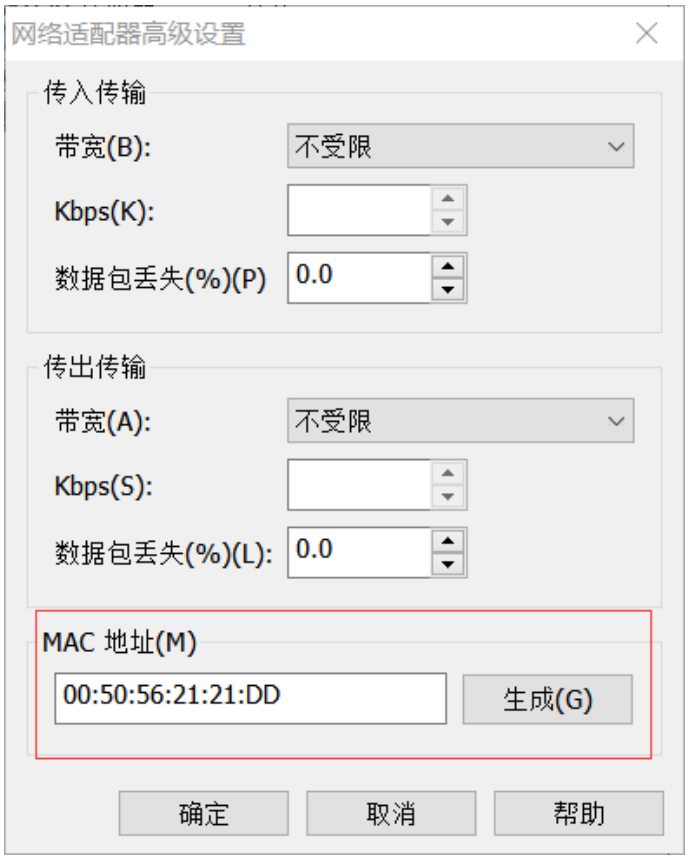
3、host-only（主机模式）

在 host-only 模式中，虚拟机只能与虚拟机、主机互访，但虚拟机和外部的

网络是被隔离开的，也就是不能上 Internet。在 host-only 模式下，虚拟系统的 TCP/IP 配置信息（如 IP 地址、网关地址、DNS 服务器等），都是由 VMnet1 虚拟网络的 DHCP 服务器来动态分配的。Host-Only 的宗旨就是建立一个与外界隔绝的内部网络，来提高内网的安全性。这个功能或许对普通用户来说没有多大意义，但大型服务商会常常利用这个功能。

更改 MAC 地址

在虚拟机设置选项中，依次点击“网络适配器”，“高级”，会弹出如下会话框，即可随时更改 MAC 地址。



1.2 VirtualBox

VirtualBox 是一款开源虚拟机软件，号称是最强的免费虚拟机软件，它不仅具有丰富的特色，而且性能也很优异！它简单易用，支持的虚拟系统包括所有的 Windows、Mac OS X、Linux、OpenBSD、Solaris、IBM OS2 甚至 Android

等操作系统！与同性质的 VMware 比较下，VirtualBox 独到之处包括远端桌面协定（RDP）、iSCSI 及 USB 的支持。可以更改 MAC 地址，网络连接模式和 VMware 类似，这里不在赘述。

除此之外还有其他一些各具特色，功能类似的虚拟机，可以根据自己的爱好和使用体验加以选择。

2、影子系统

2.1 PowerShadow

PowerShadow（影子系统），是隔离保护 Windows 操作系统，同时创建一个和真实操作系统一模一样的虚拟化影像系统。进入影子系统后，所有操作都是虚拟的，所有的病毒和流氓软件都无法感染真正的操作系统。系统出现问题了，或者上网产生垃圾文件，只需轻松的重启电脑，一切又恢复最佳状态。

主要功能作用

1、可以在系统中做任何实验操作，包括对系统有害的；

2、可以用来测试病毒、木马、等危险程序；

3、可以访问危险连接而不受侵害；

4、浏览网页、阅读可疑邮件不留痕迹；

5、不会因为安装和卸载软件而产生垃圾；

6、提供保护系统分区和全盘保护两种模式；

7、重启后系统一切还原。

影子系统实时生成本机内硬盘分区的一个影子，我们称它为“影子模式”。影子模式和正常模式具有完全相同的结构和功能，用户可以在影子系统内做任何在正常系统内能做的一切事情。在正常模式和影子模式之间的实质的差别是：一

切在影子模式内的操作，包括您下载的那些文件，您生成的文件资料或者您更改的设定都会在您退出影子模式时完全消失。所以影子模式可以绝对地保护电脑内的所有数据并清除操作留下的任何痕迹。

2.2 ShadowDefender

ShadowDefender（影子卫士），是一款小巧、功能强大的保护程序，提供一个和 Windows 完全一样的虚拟环境，你的任何操作并不会影响真实的系统，一切改变将在退出影子模式后消失，支持多分区，支持转储，支持排除。

主要功能作用

和影子系统一样也能防机器狗。软件有着漂亮的界面和直观的设置选项，特别是在转储和排除方面胜人一筹。体积小，功能强大，操作简单，性能稳定而较为突出。

1、可以防止所有的病毒和恶意软件；

2、可以在一个安全的环境中测试病毒、木马；

3、上网安全和消除有害的痕迹；

4、消除系统停机时间和维护成本；

5、保持系统不受恶意活动和不必要的更改；

6、重新启动系统恢复到其原始状态。

3、反取证系统

3.1 Tails

Tails（The Amnesic Incognito Live System）是一个实时的操作系统，旨在保护个人隐私，同时也可实现匿名访问网络，能安装在光盘、U 盘或 SD 卡上，可以随身携带，需要时直接从光盘、U 盘或 SD 卡启动之后就能上网，这在提供

了便携性的同时，也能够更好地保护个人隐私。因此被称之为“口袋操作系统”。

它是一个基于 Debian GNU/Linux 操作系统，启动之后会自动运行 Tor，它不向本地系统储存任何数据。系统内部预安装一些软件程序，例如网络浏览器、即时通讯客户端，电子邮件客户端，办公软件，图像和声音编辑器等。这都以安全为理念进行了预配置，并对网络流量进行了匿名性处理。为达到此目标，该系统使用了 Tor 网络，以使得网络流量很难被追踪。

主要功能

1、匿名使用互联网，规避审查；

2、所有连接到互联网的路径都会被迫通过 Tor 网络；

3、不会在你使用的电脑上留下任何痕迹，除非你故意让它显示出来；

4、使用最先进的加密工具为你的文件、电子邮件和即时消息加密；

5、当 Tails 运行时，不会在计算机上留下任何痕迹；

6、整个操作系统加载在内存中，在每次重启或关机后会自动擦除掉，所以不会留下任何运行的痕迹。

3.2 Kodachi

Kodachi Linux 是一款基于 Debian 8.6 的操作系统。它是专为保护用户隐私而设计的，因此具有高度的安全及匿名性，并具备反调查取证的特点。

Kodachi 的使用也非常方便简单，你可以通过 USB 驱动来在你的 PC 上启动它。当你完全启动 Kodachi 操作系统后，你将会建立一个 VPN+Tor+DNScry 服务器的运行环境。你不需要特别了解或学习 Linux 的知识，Kodachi 都为你准备好了你所需要的！整个操作系统都活动在你的临时内存 RAM 下。因此，你一旦你关机，任何的操作痕迹都会被清除，避免你的隐私

泄露及被追踪调查。

Kodachi 是一个实时的操作系统，你可以从几乎任何计算机上来启动它。例如：从 DVD，U 盘或 SD 卡等。它旨在保护你的隐私及匿名性，并帮助你：

匿名使用互联网。所有与 Internet 的连接，都将被强制通过 VPN，然后通过 DNS 加密的 Tor 网络。在你使用的计算机上不会留下任何痕迹，除非你要求保留一些数据痕迹。使用先进的加密和隐私工具加密你的文件，电子邮件和即时消息。

Kodachi 是基于实体 Debian Linux 和 定制 XFCE ，这使得 Kodachi 系统非常的稳定、安全并且独特。

特点

连接 VPN

连接 Tor 和出口节点选择

DNScrypt 服务器运行环境

拥有 Truecrypt 加密– keepass 密码管理系统- 安全云等

免费开源

随机 MAC 地址生成

RAM 关闭/重启时清除

内置 Tor 浏览器

Pidgin 即时通讯

比特币钱包

Litecoin 钱包

免费内置 VPN

DNSCrypt

多个 Tor 出口节点转换器

多个 DNS 选项

Vera 加密

PeerGuardian（P2P 网络安全软件）

自带一系列安全软件

Kodachi 的安装使用：

方式一（推荐）：下载 ISO 文件，并使用免费刻录工具（如 Rufus 或 Linux Live）将其刻录到 U 盘，然后通过插入 PC 来启动。你需按 F12 键（不同电脑类型按键可能不同）进入引导菜单，并更改 BIOS 从 USB 启动。

方式二：下载 ISO 文件，并使用免费刻录工具（如 DAEMON Tools）将其刻录到 DVD 上，然后通过 PC 的光盘启动。

方式三：下载 ISO 文件，使用 Vmware 或 Virtualbox 虚拟机来启动。

注意

不建议在任何电脑上永久安装 Kodachi Linux，因为它会将所有的设置保存在硬盘上，这就违背了该系统反取证的初衷。