

# 课程2讲义：基于第三代蜜网的VNet网络攻防实验环境构建

The Artemis Project/狩猎女神项目组

诸葛建伟

## 一、先决条件

在阅读本文前，请先阅读Know Your Enemy: Honeynets, Know Your Enemy: GenII Honeynets和Know Your Enemy: Honeywall CDROM Roo，对Honeynets的概念和第三代Honeynet (Roo)技术有个清晰的认识，并完全了解Roo的部署软/硬件要求。

## 二、VMware软件介绍

VMware 软件是 VMware 公司 (<http://www.vmware.com/>) 出品的优秀虚拟机产品，可以在宿主主机上通过模拟硬件构建多台虚拟主机。VMware 软件版本主要有 VMware Player (免费)、VMware Workstation、VMware GSX Server (目前 license 免费)、VMware ESX Server 等版本，本文档基于最普遍使用的 VMware Workstation，具体版本为 VMware-workstation-full-7.0.0-203739。

运行在 VMware 虚拟机软件上操作系统的网络连接方式有三种：

- 桥接方式 (Bridge)：在桥接方式下，VMware 模拟一个虚拟的网卡给客户系统，主系统对于客户系统来说相当于是一个桥接器。客户系统好像是有自己的网卡一样，自己直接连上网络，也就是说客户系统对于外部直接可见。

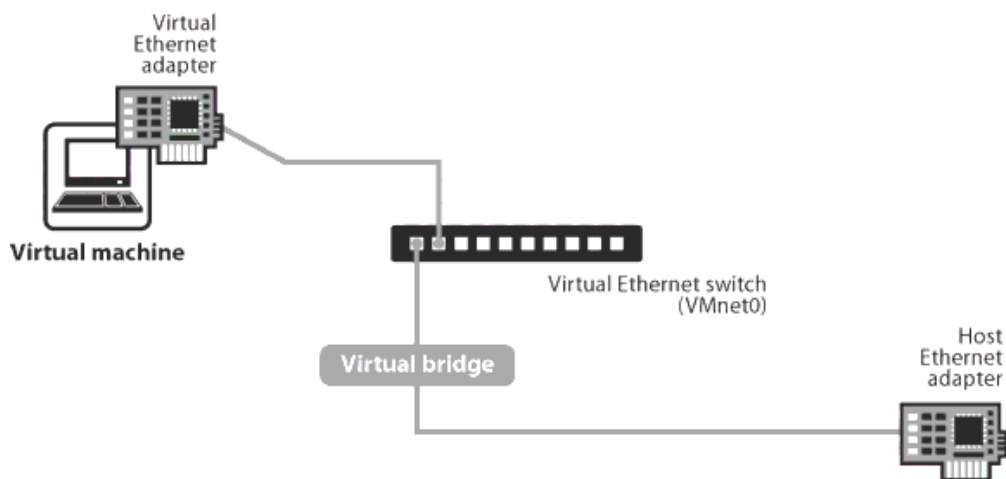


图 1 VMware 支持的桥接连接方式示意图

- 网络地址转换方式 (NAT): 在这种方式下, 客户系统不能自己连接网络, 而必须通过主系统对所有进出网络的客户系统收发的数据包做地址转换。在这种方式下, 客户系统对于外部不可见。

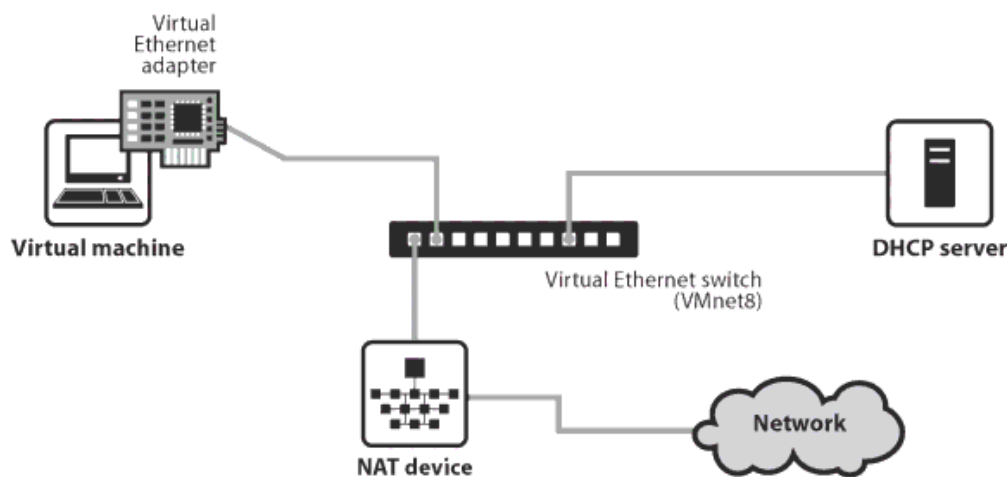


图 2 VMware 支持的 NAT 连接方式示意图

- 主机方式 (Host-Only): 在这种方式下, 主系统模拟一个虚拟的交换机, 所有的客户系统通过这个交换机进出网络。在这种方式下, 如果主系统是用公网 IP 连接 Internet, 那客户系统只能用私有 IP。但是如果我们另外安装一个系统通过桥接方式连接 Internet (这时这个系统成为一个桥接器), 则我们可以设置这些客户系统的 IP 为公网 IP, 直接从这个虚拟的桥接器连接 Internet, 下面将会看到, 我们正是通过这种方式来搭建我们的虚拟蜜网。

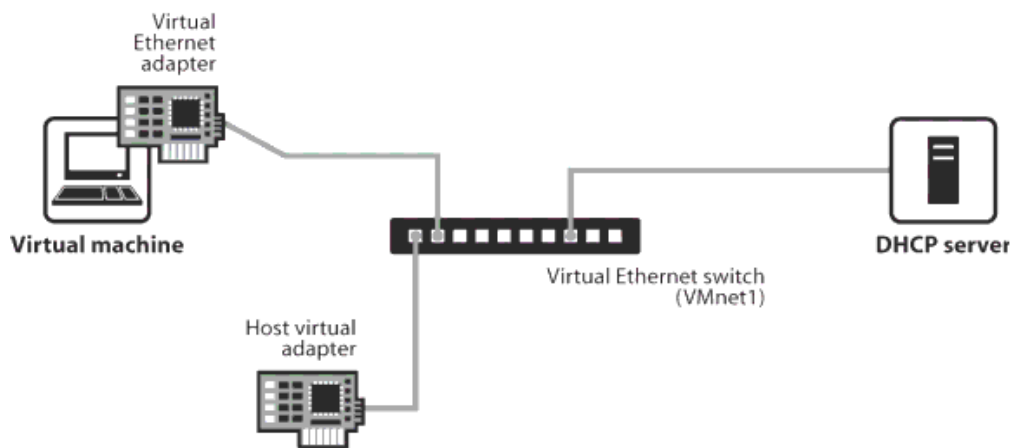


图 3 VMware 支持的 host-only 连接方式示意图

### 三、网络拓扑及软硬件需求

#### 3.1 网络拓扑

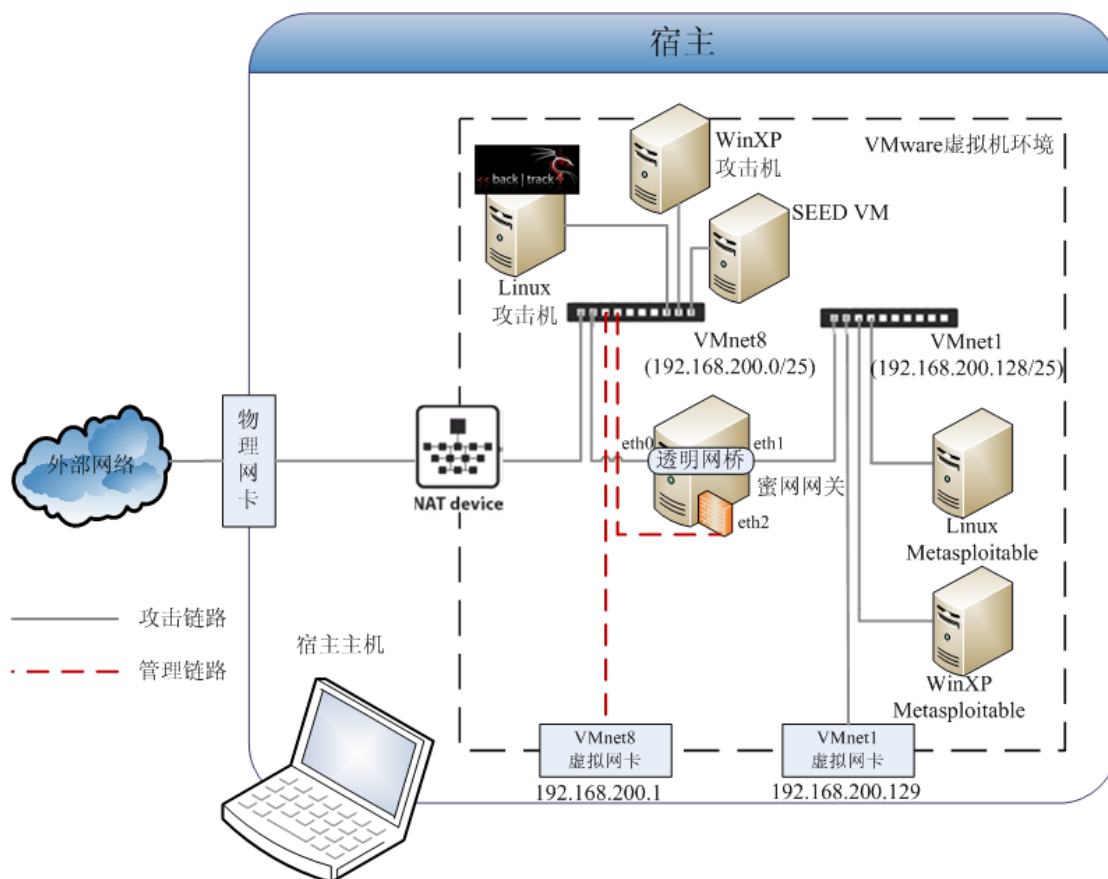


图 4 虚拟蜜网网络拓扑结构

## 3.2 软硬件需求

基于Win32平台构建虚拟蜜网的硬件配置建议如下：

- 至少 P4 CPU，建议 2.0G Hz 以上
- 至少 1G 内存，建议 2G 以上
- 至少 20G 硬盘，建议 40G 以上

软件配置包括：

宿主主机：

- 操作系统：Win2K/WinXP，本文档基于 Windows XP SP2
- VMware Workstation for Win32 ， 本 文 档 使 用  
VMware-workstation-full-7.0.0-203739

蜜网网关虚拟机：

- Roo Honeywall CDROM v1.4

攻击机和靶机的镜像见课程 2 slides，本文档采用如下：

- WinXPattacker 作为攻击机
- Win2kServer\_SP0\_target 作为靶机

注：为安全起见，请将宿主主机上的网线拔掉，开始进行下述四、五中的实验。

## 四、虚拟蜜网的构建

### 4.1 VMware 软件安装与配置

默认方式安装 VMware Workstation 软件全过程。

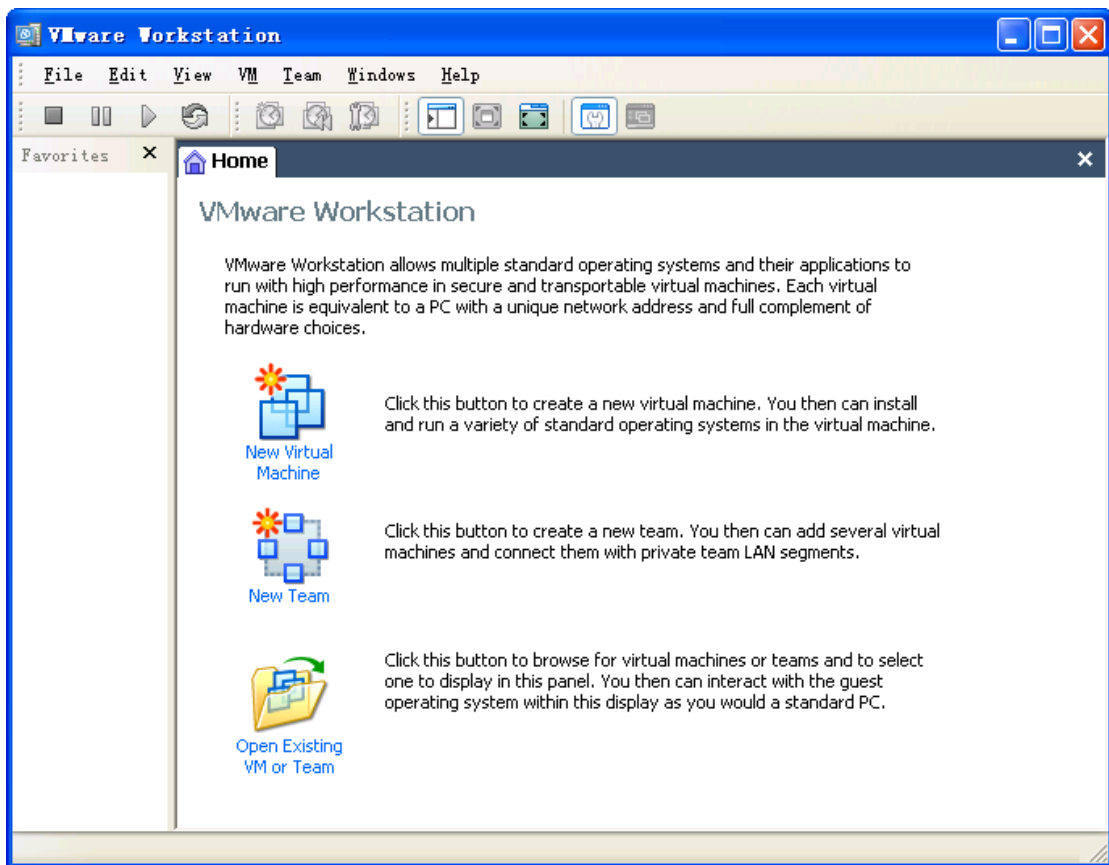


图 5 安装完 VMware Workstation

## 4.2 VMware 网络环境配置

在 VMware 中 Edit --> Virtual Network Editor,

选择 VMnet1, 设置如下

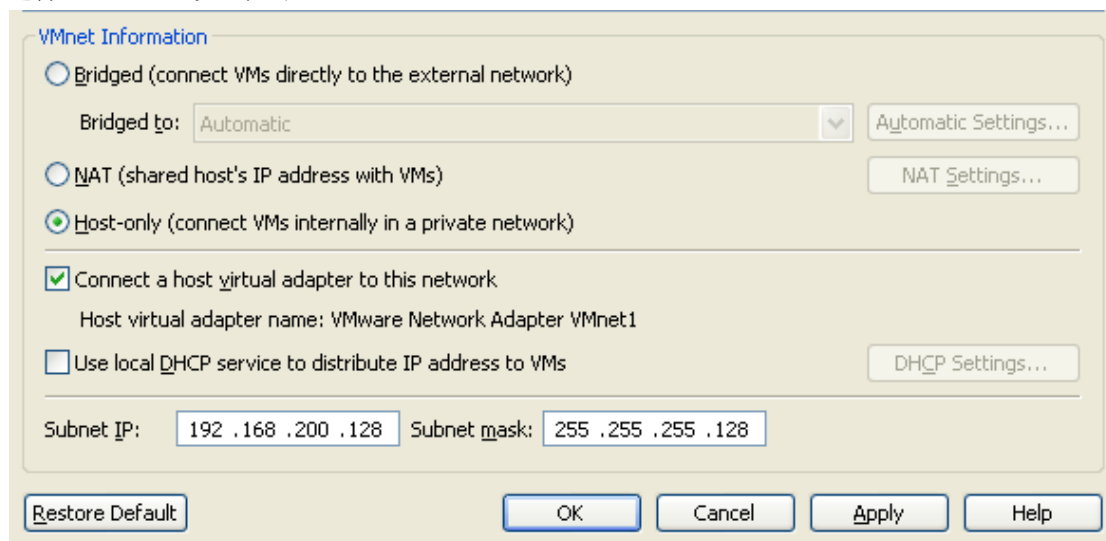


图 6 VMnet1 的设置

选择 VMnet8，设置如下

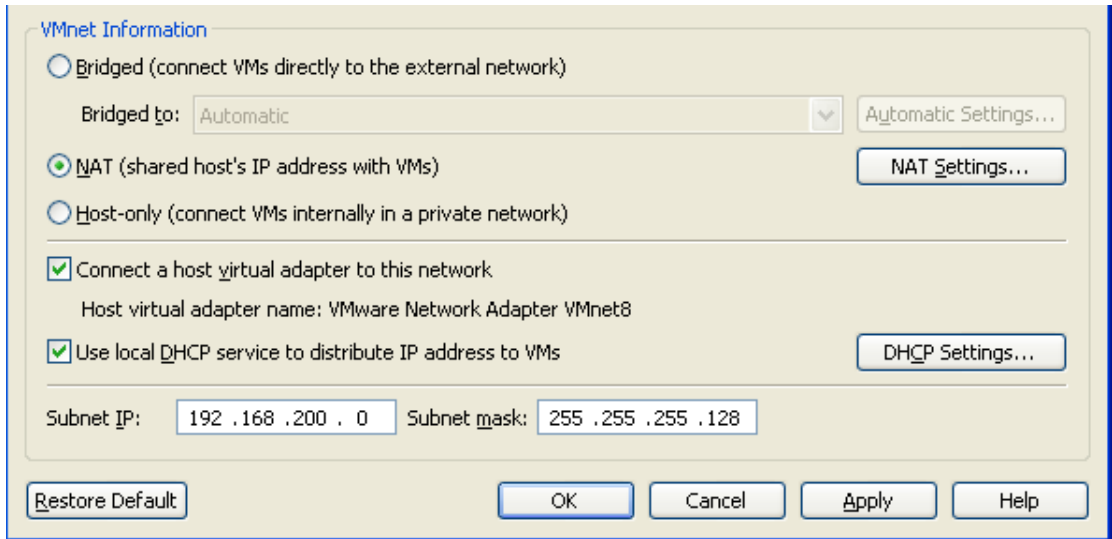


图 7 VMnet8 的设置

点击图 7 中的 NAT Settings，设置如下：

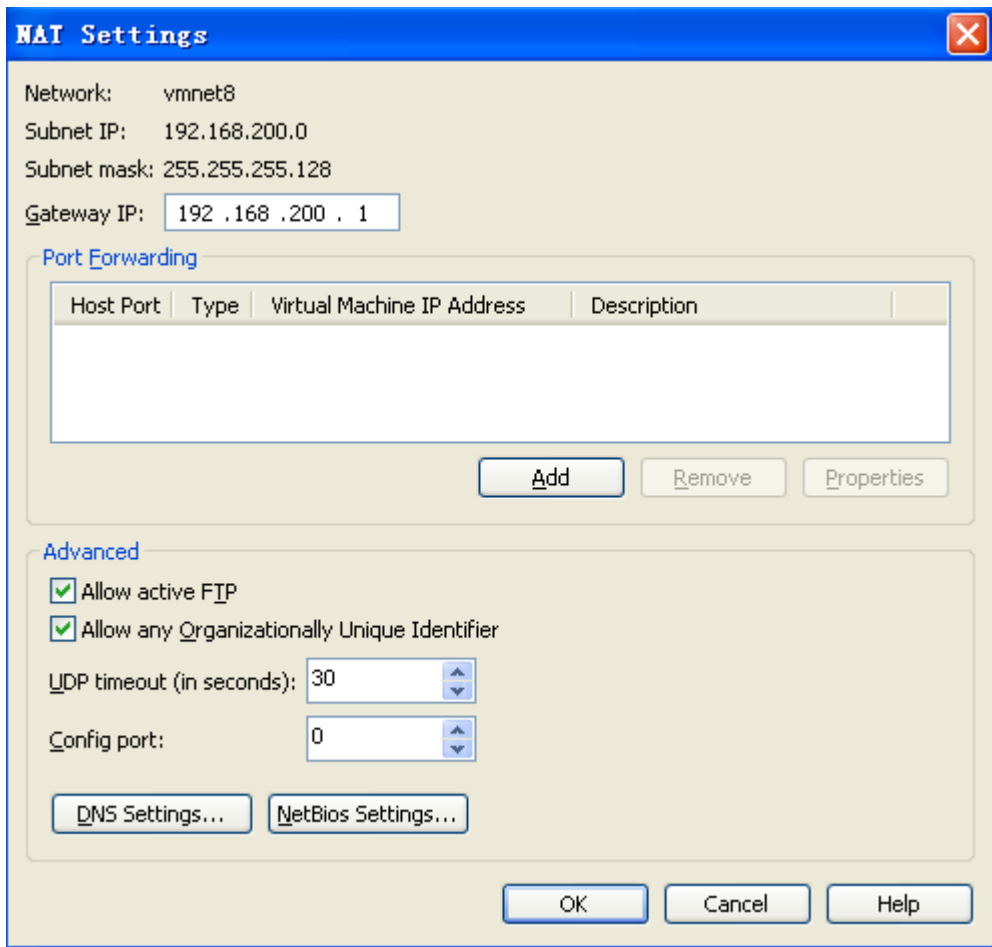


图 8 VMnet8 中 NAT 的设置

点击图 7 中的 DHCP Settings，设置如下：

（注意：为了留一些 IP 给靶机，在这里 End IP address 没有设为 192.168.200.126）

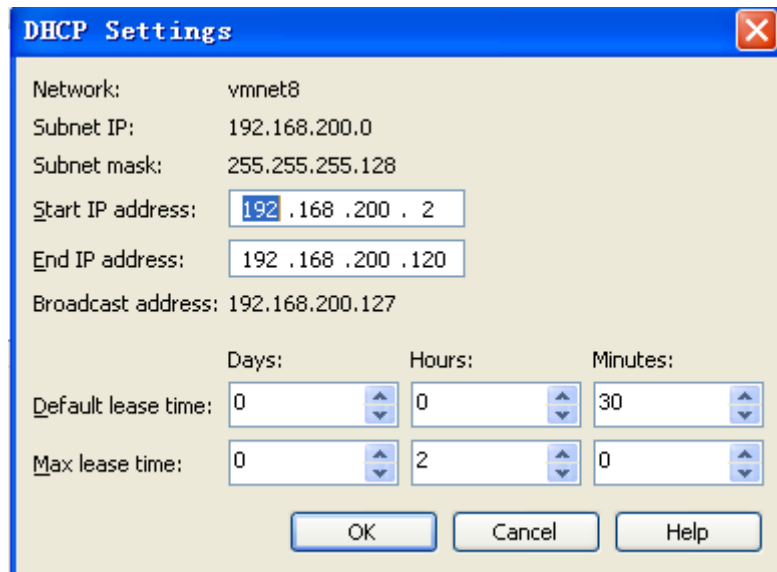


图 9 VMnet8 中 DHCP 的设置

### 4.3 安装攻击机虚拟机

1. 从课程 ftp 上下载并解压 WinXPattacker 的 rar 镜像到某一目录
2. File --> Open，选择你的解压目录，选择相应 vmx 文件
3. 配置攻击机虚拟机的硬件

鼠标选择 WinXPattacker 的选项卡，菜单中选择 VM --> Settings，Hardware 选项卡中选择点击 Memory，在右侧设置合适大小（注意这项在虚拟机开启时不可设置，可先将该虚拟机 power off，设置好之后，再 power on）

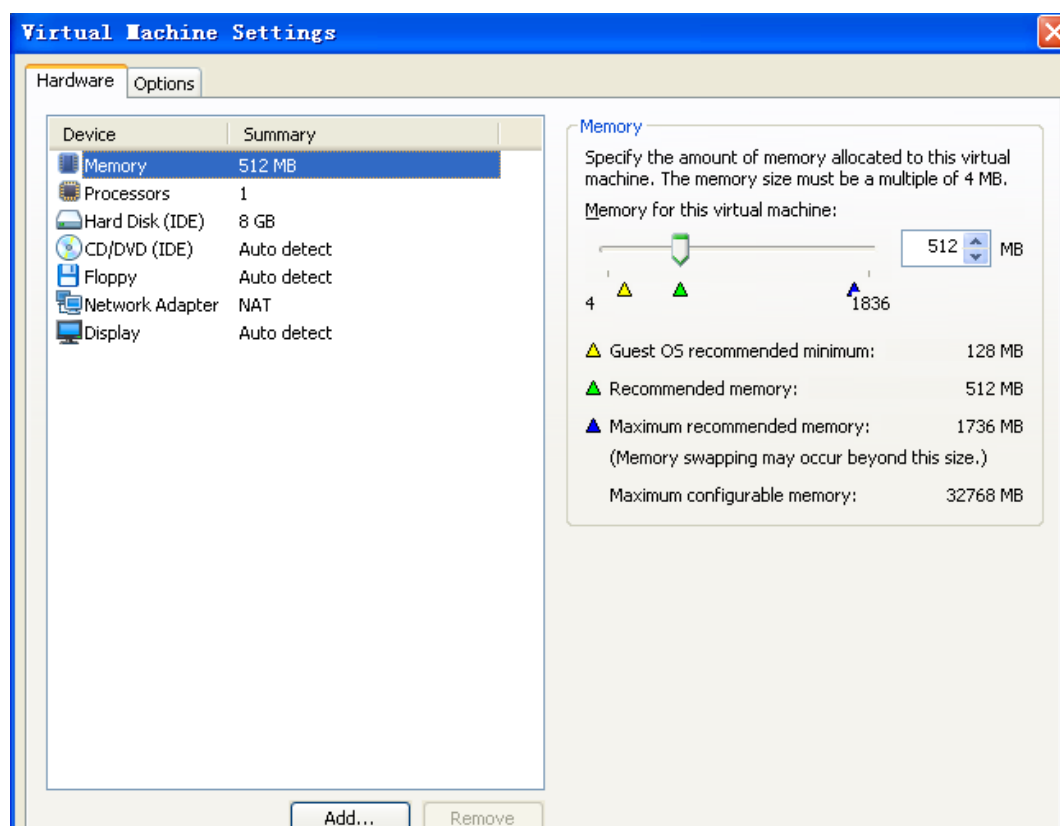


图 10 攻击机虚拟机的虚拟内存设置

Hardware 选项卡中选择点击 Network Adaptor，在右侧设置为 NAT

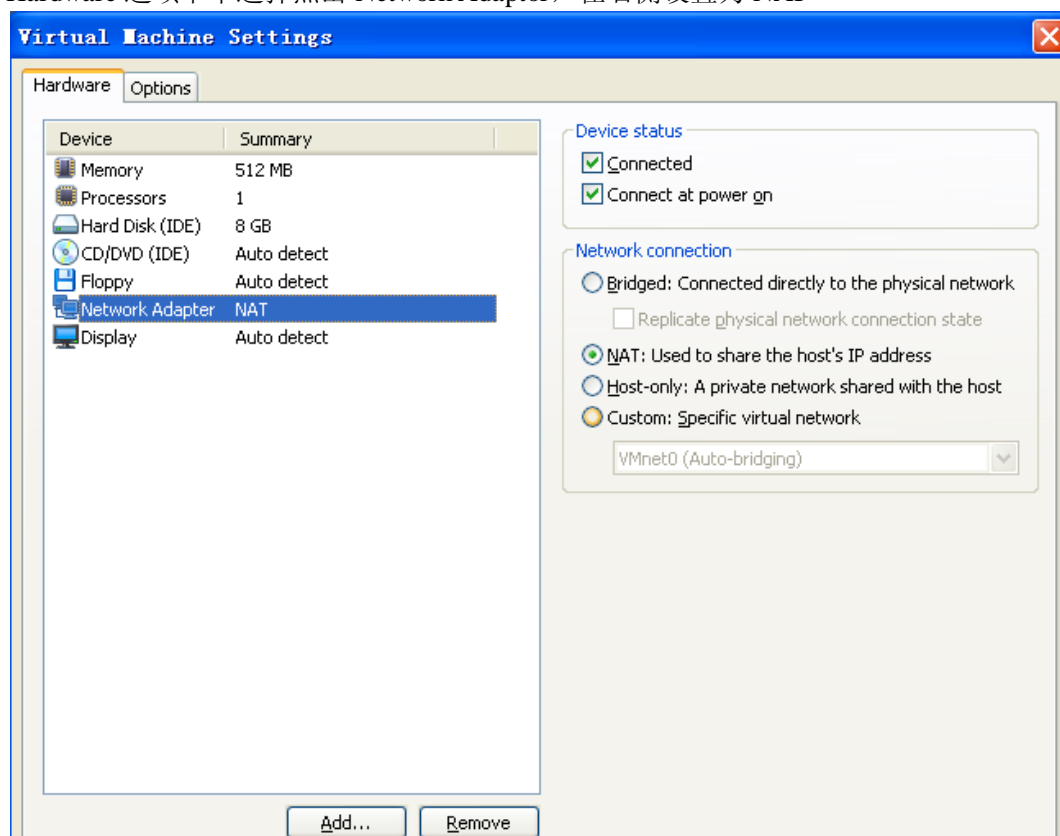


图 11 攻击机虚拟机联网方式设置为 NAT



#### 4. 查看攻击机虚拟机的 ip

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . .               : 192.168.200.2
    Subnet Mask . . . . .             : 255.255.255.128
    Default Gateway . . . . .         : 192.168.200.1
```

图 12 DHCP 动态分配给攻击机虚拟机的 IP 地址为 192.168.200.2

## 4.4 安装靶机虚拟机

1. 从课程 ftp 上下载并解压 Win2kServer\_SP0\_target 的 rar 镜像到某一目录
2. File --> Open, 选择你的解压目录, 选择相应 vmx 文件
3. 配置靶机虚拟机的硬件

鼠标选择 Win2kServer\_SP0\_target 的选项卡, 菜单中选择 VM --> Settings, Hardware 选项卡中选择点击 Memory, 在右侧设置合适大小 (注意这项在虚拟机开启时不可设置, 可先将该虚拟机 power off, 设置好之后, 再 power on)

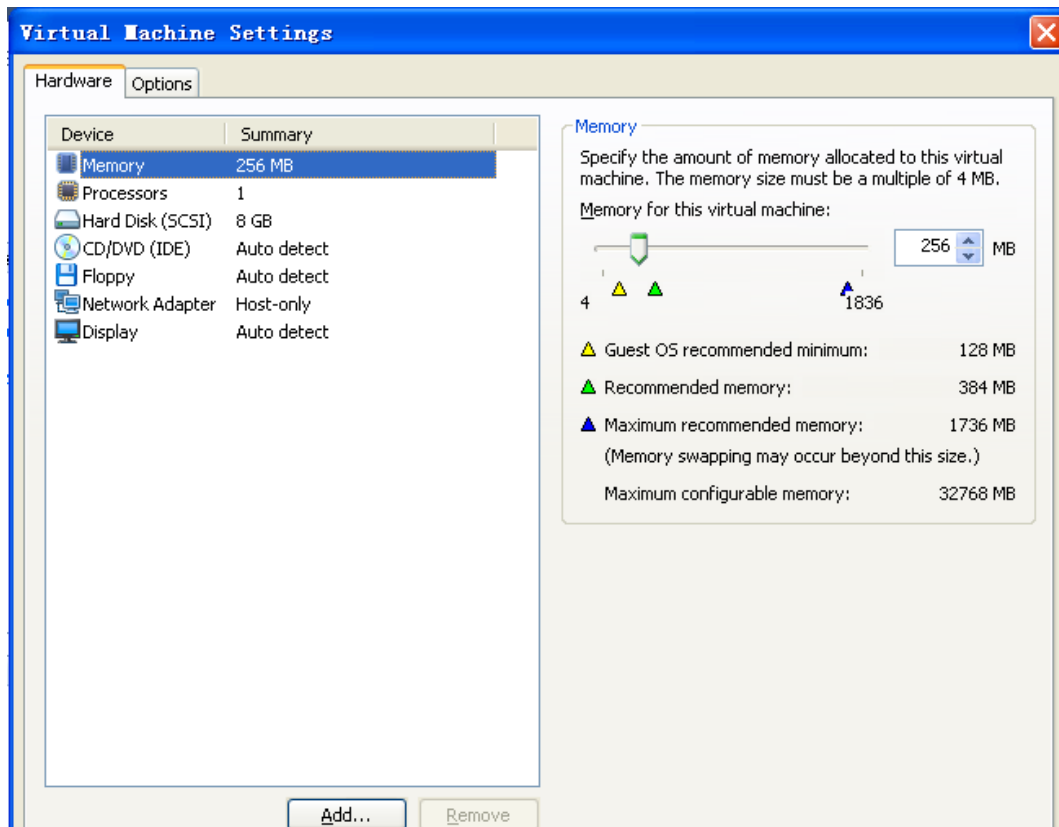


图 13 靶机虚拟机的虚拟内存设置

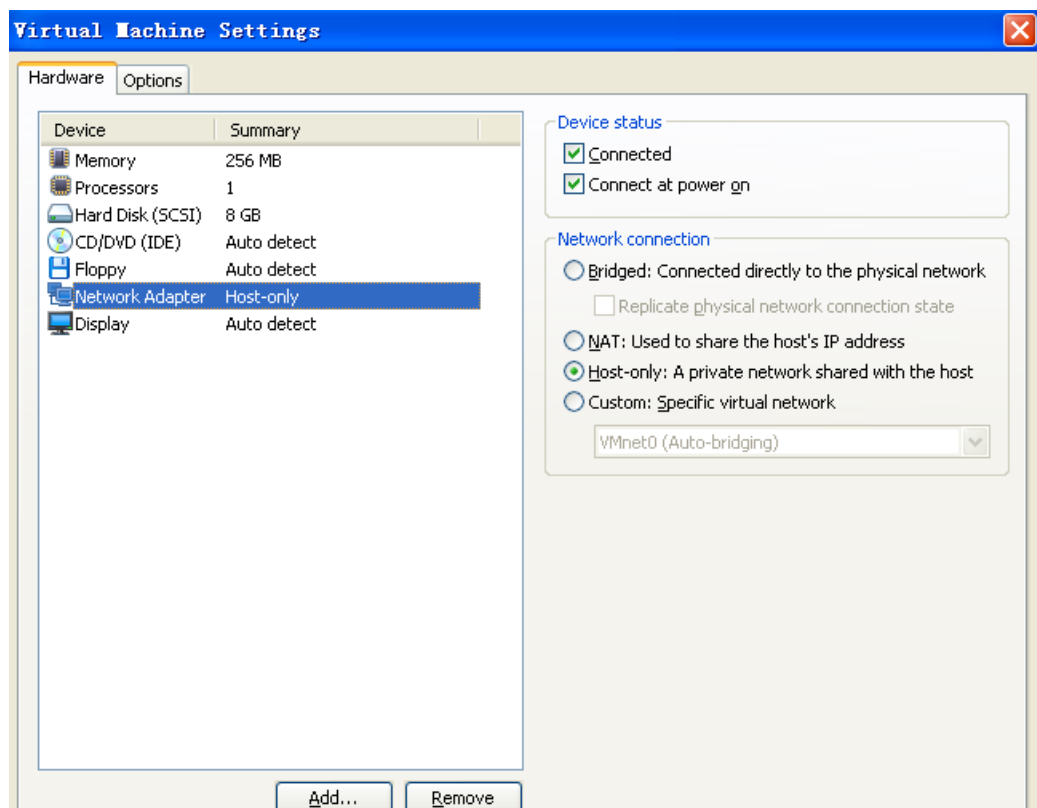


图 14 靶机虚拟机联网方式设置为 Host-Only

#### 4. 配置靶机虚拟机的 ip 和网关

找一个在 192.168.200.0/25 网段的，且不在图 9 的 DHCP 分配范围的 ip，我们这里选择 192.168.200.124，配置如下

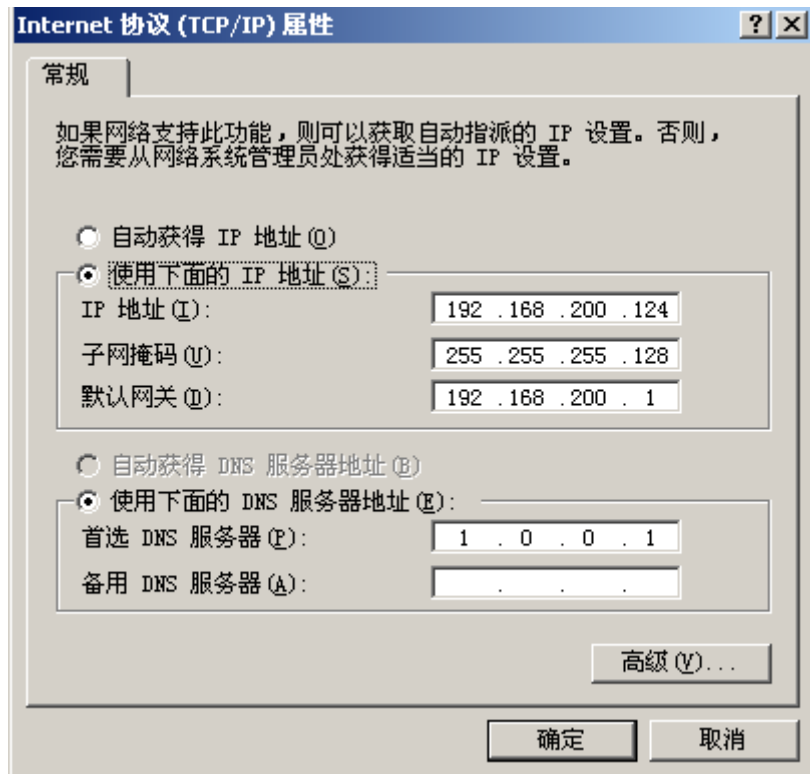


图 15 配置靶机虚拟机的 ip 和网关

## 4.5 安装蜜网网关虚拟机

1. File --> New --> Virtual machine, 新建虚拟机，选择 Custom 安装

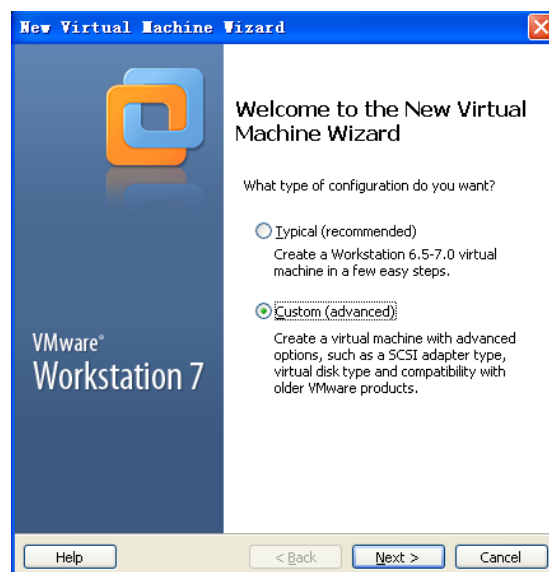


图 16 选择 Custom 安装

## 2. 设置 VMware Workstation 版本

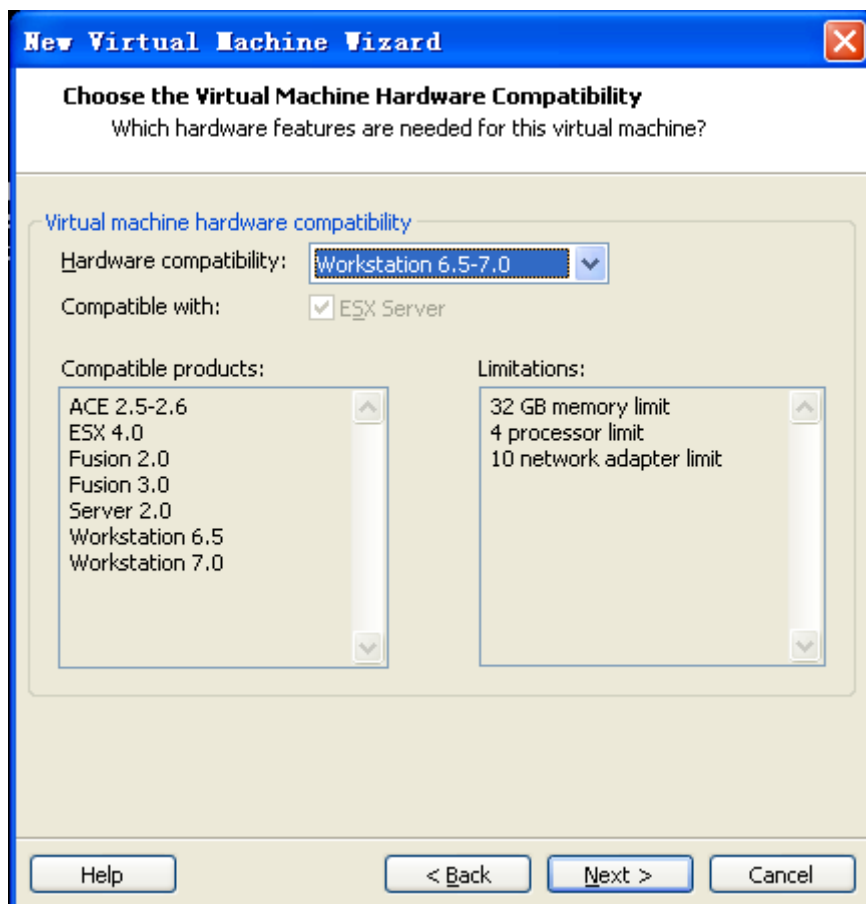


图 17 设置 VMware Workstation 版本为 6.5-7.0

## 3. 设置 CDROM 为蜜网网关 Roo v1.4 软件 ISO

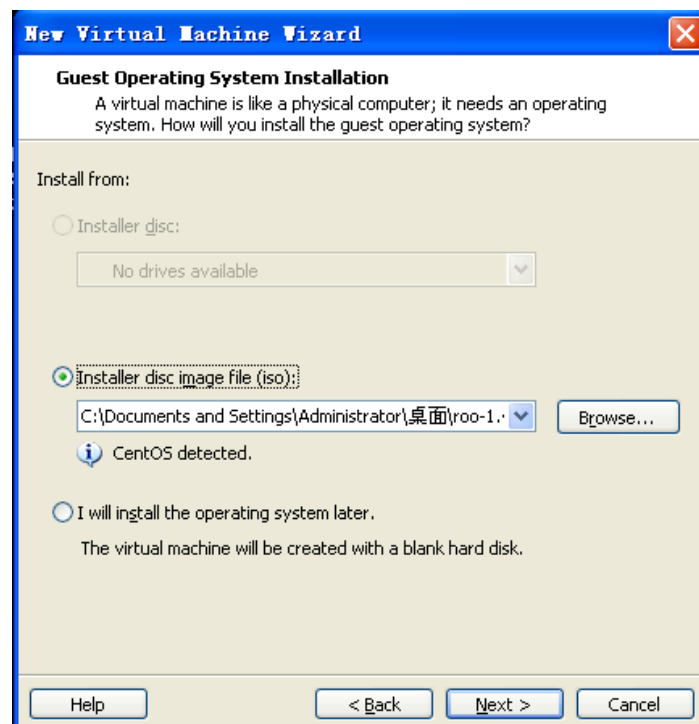


图 18 设置 CDROM 为蜜网网关 Roo v1.4 软件 ISO

#### 4. 设置蜜网网关虚拟机命名与路径

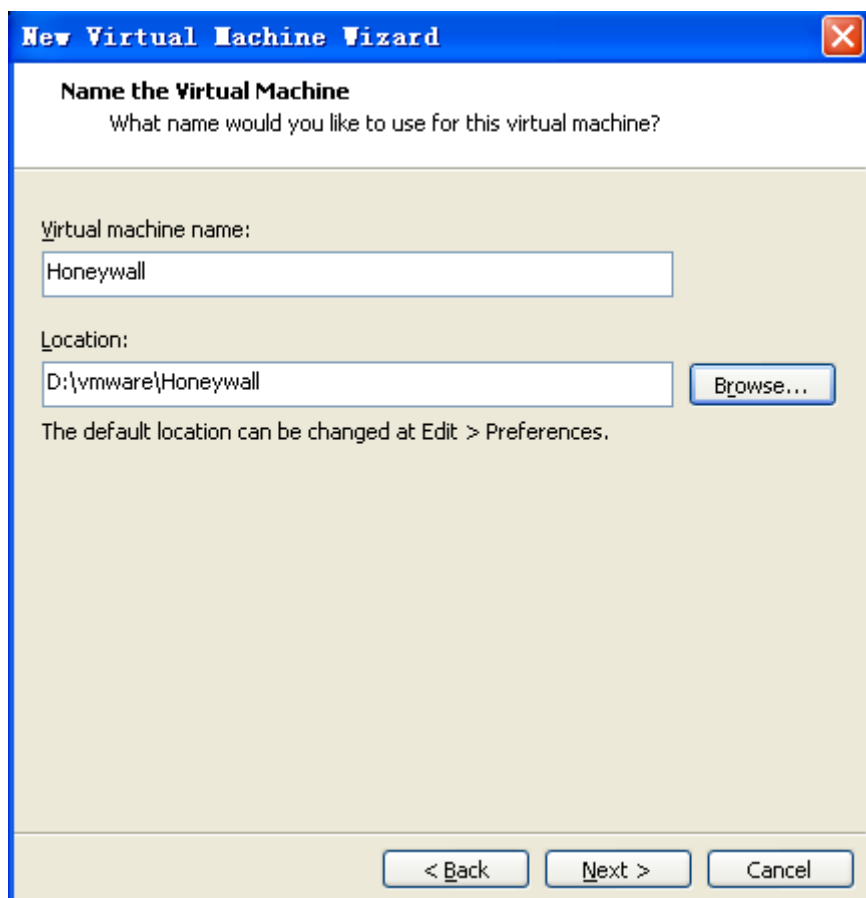


图 19 设置蜜网网关虚拟机命名与路径

#### 5. 设置蜜网网关虚拟硬件

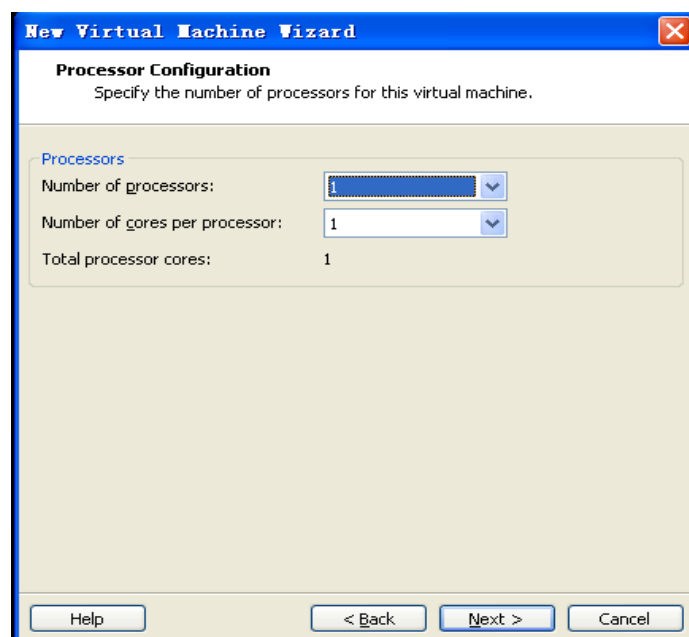


图 20 设置虚拟 CPU，选择单处理器

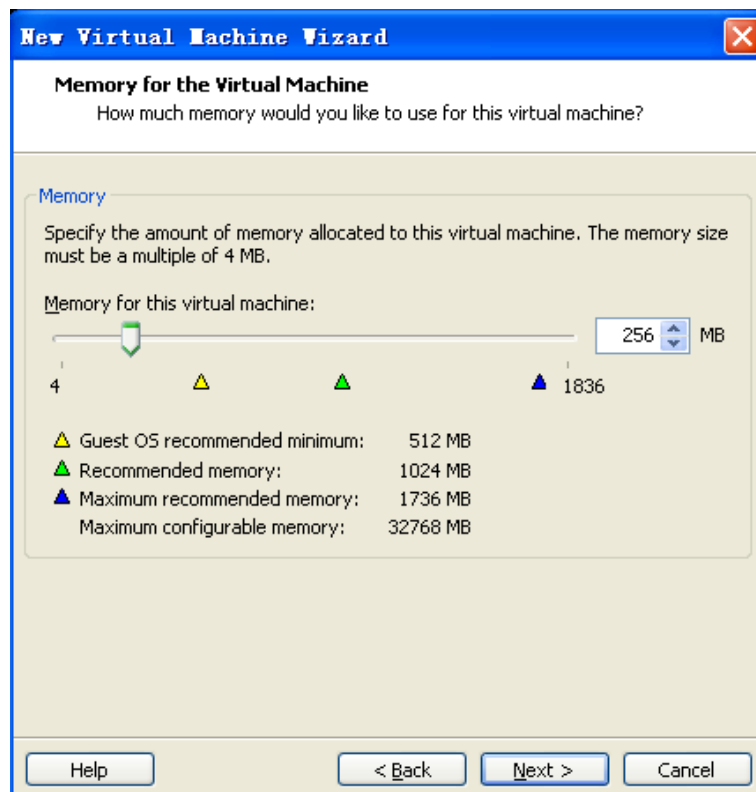


图 21 设置蜜网网关虚拟机内存大小，建议 256M

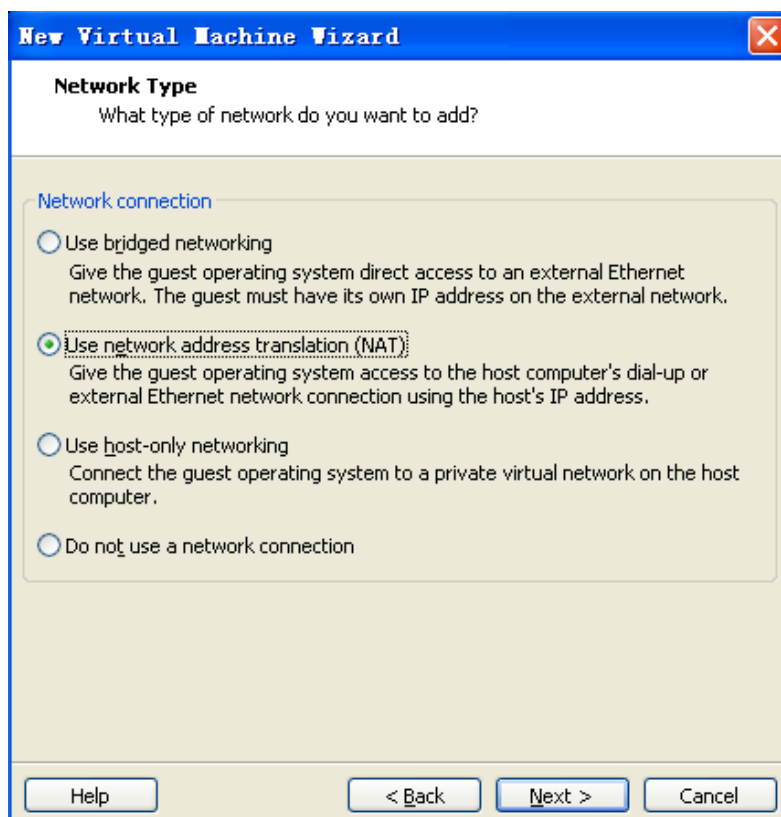


图 22 设置网络连接方式，选择 NAT 模式，后面需另加两个网卡

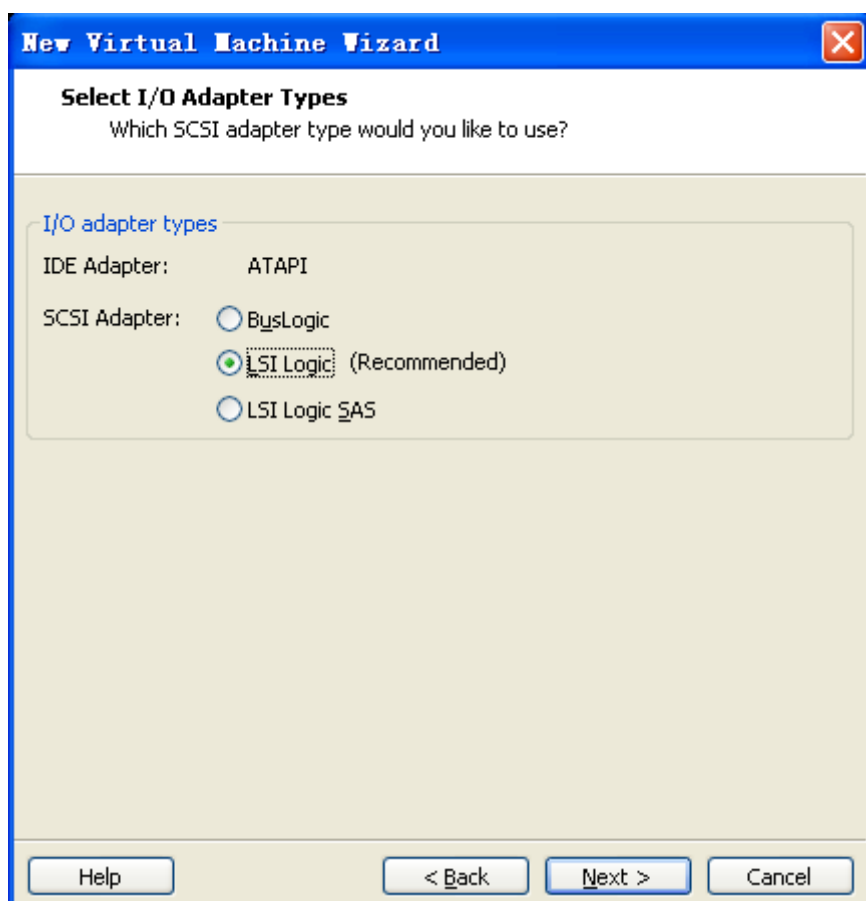


图 23 设置虚拟硬盘接口类型，SCSI 接口选择为 LSI Logic

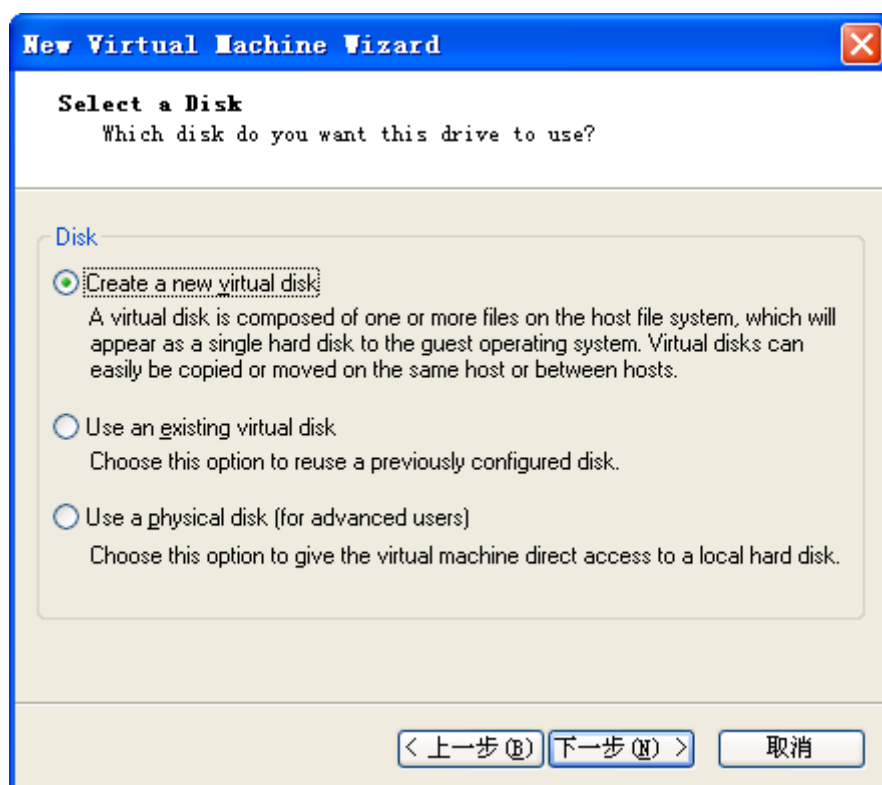


图 24 创建虚拟硬盘

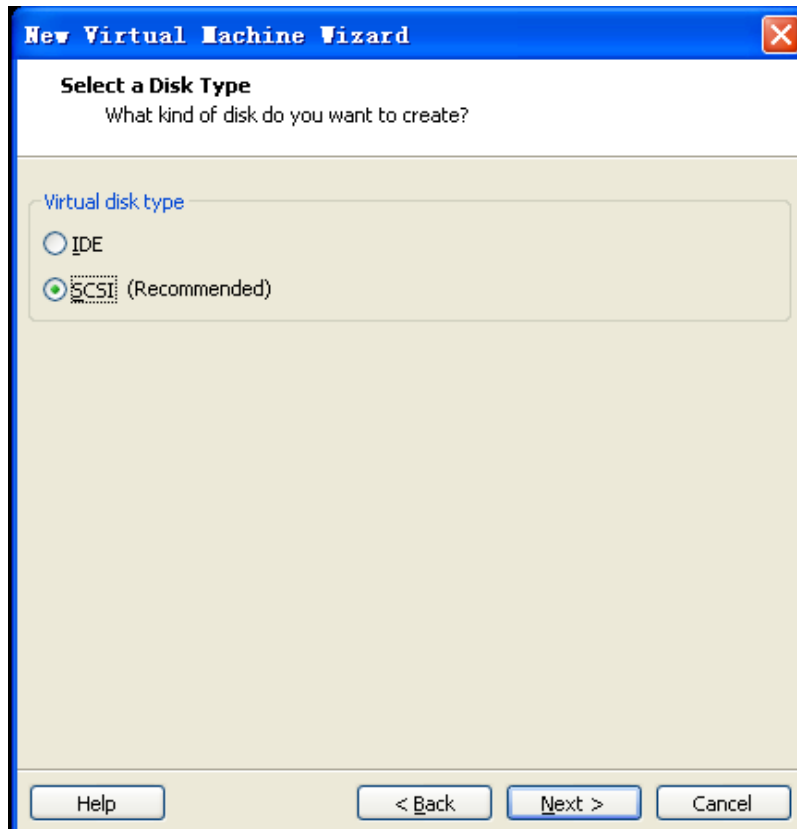


图 25 设置虚拟硬盘为 SCSI 硬盘

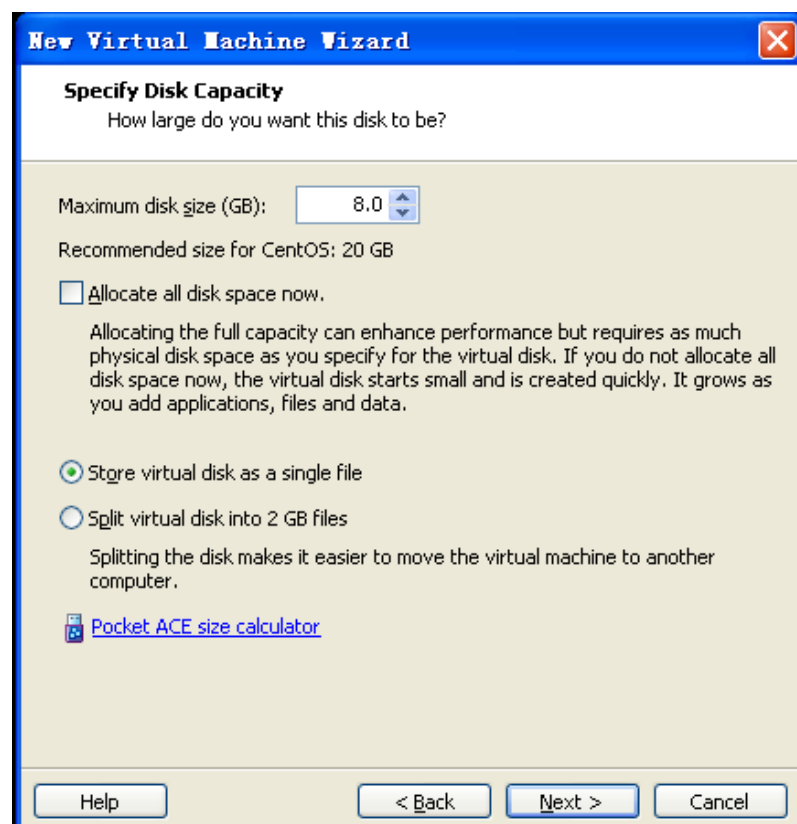


图 26 设置虚拟硬盘大小为 8G，无需立即分配全部空间



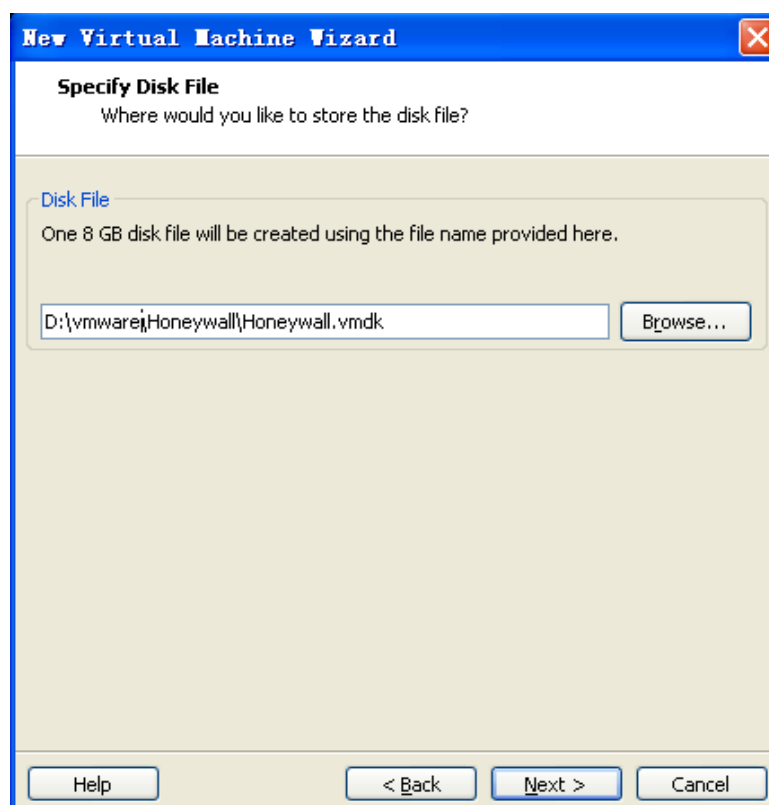


图 27 指定虚拟硬盘文件的绝对路径，注意必须给出全绝对路径，不要出现中文字符

## 6. 添加两块网卡

点击下图中 Customize Hardware

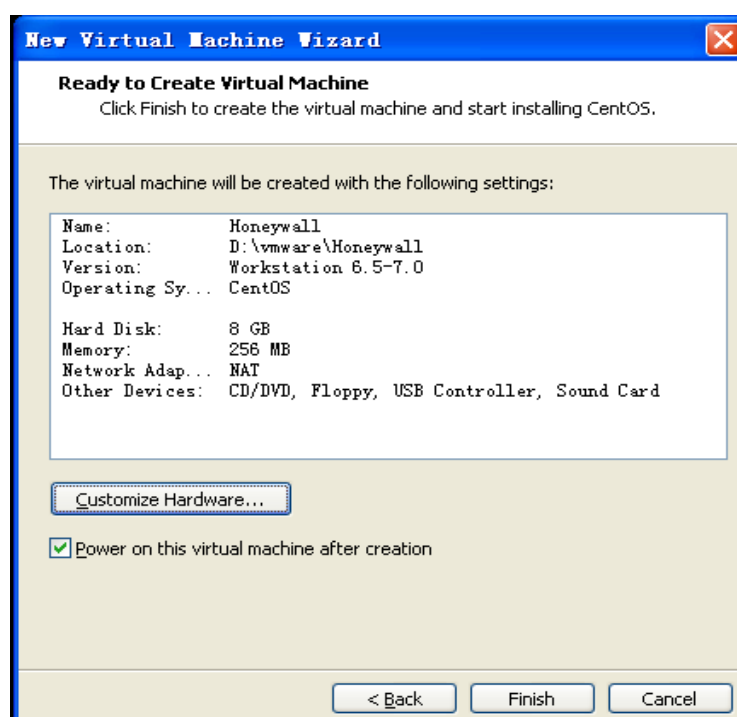


图 28 显示配置

点击下图中 add 按钮，按照提示步骤添加两块网卡，其中 Ethernet 2 设为 Host-only, Ethernet3 设为 NAT，添加后如图 30 所示

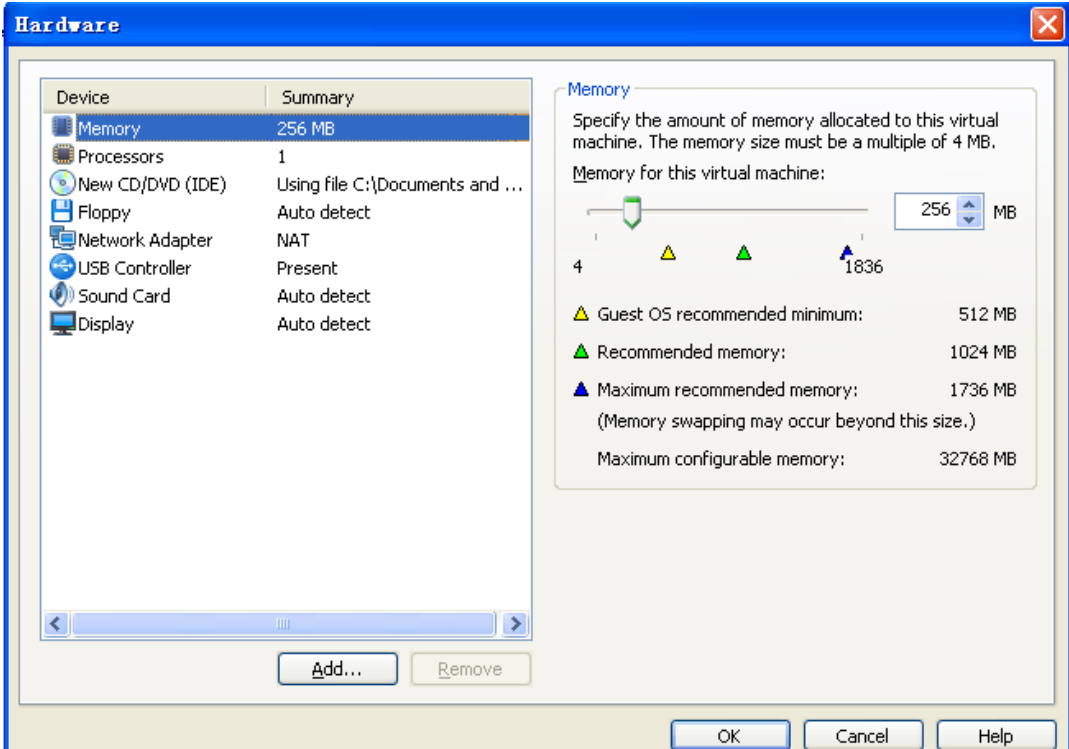


图 29 Hardware 配置

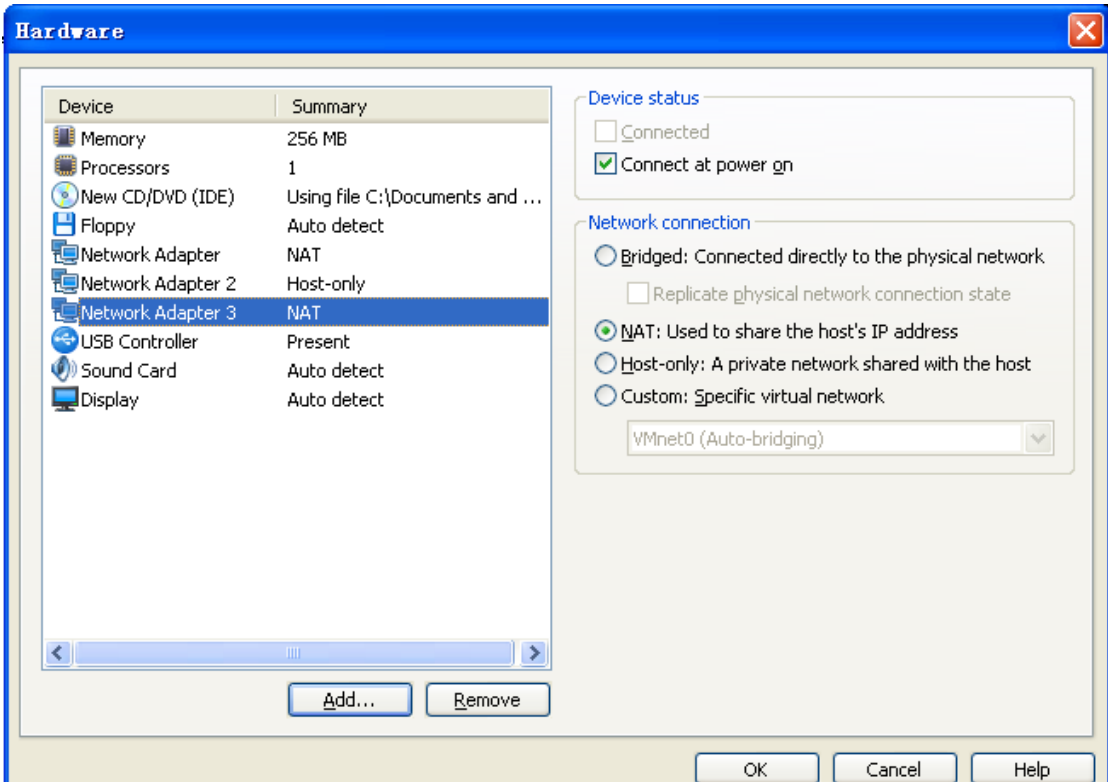


图 30 添加两块网卡之后的配置

7. 安装蜜网网关软件

启动蜜网网关虚拟机，进入如下安装界面。

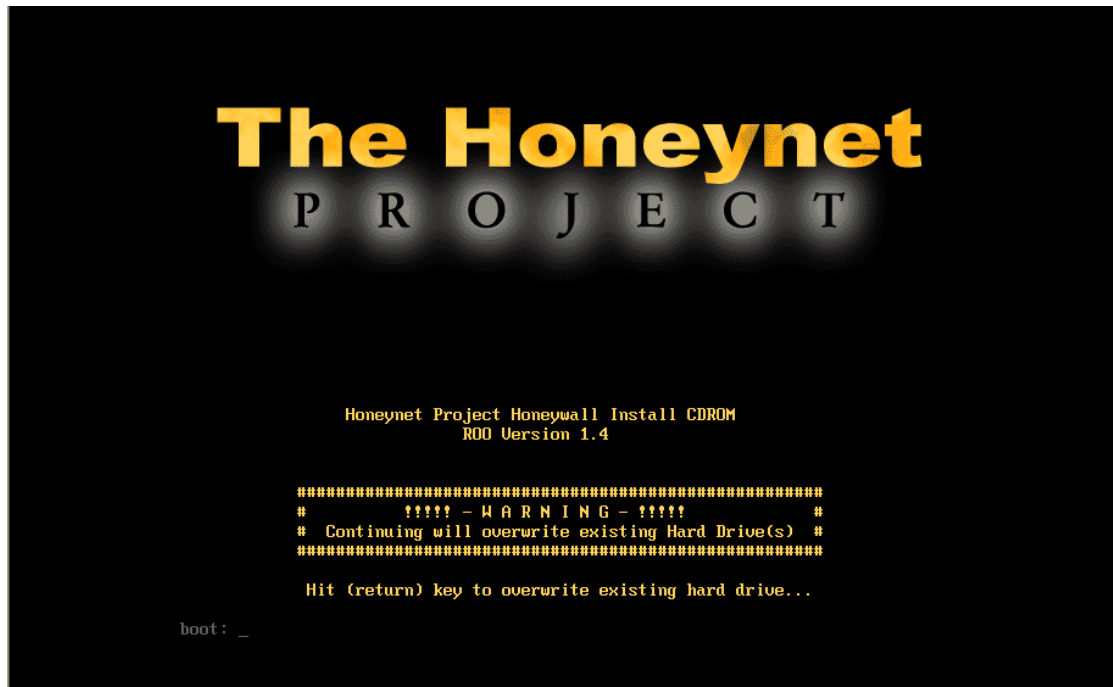


图 31 安装蜜网网关软件，键入回车键确认开始安装

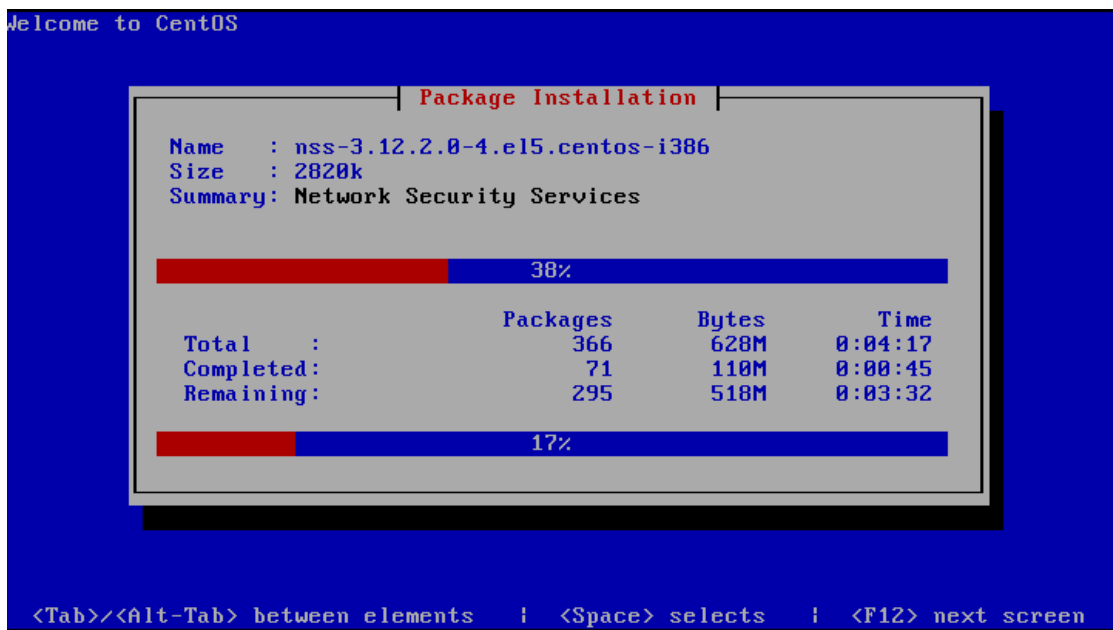
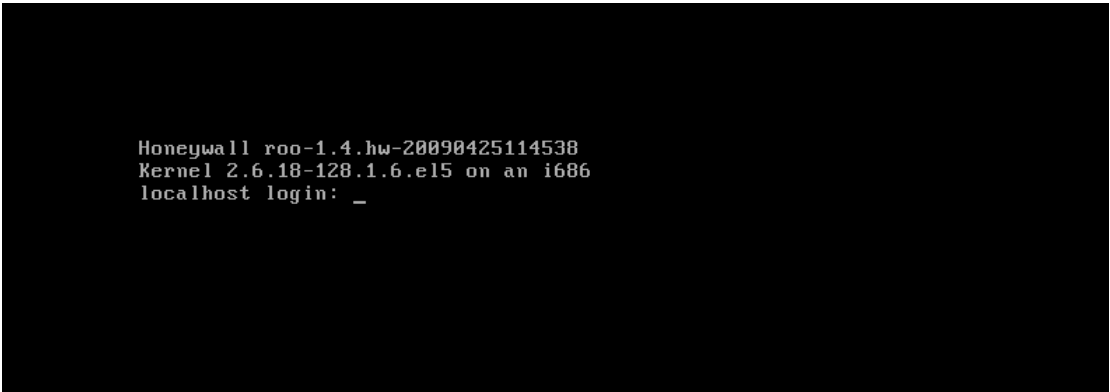


图 32 蜜网网关软件安装过程



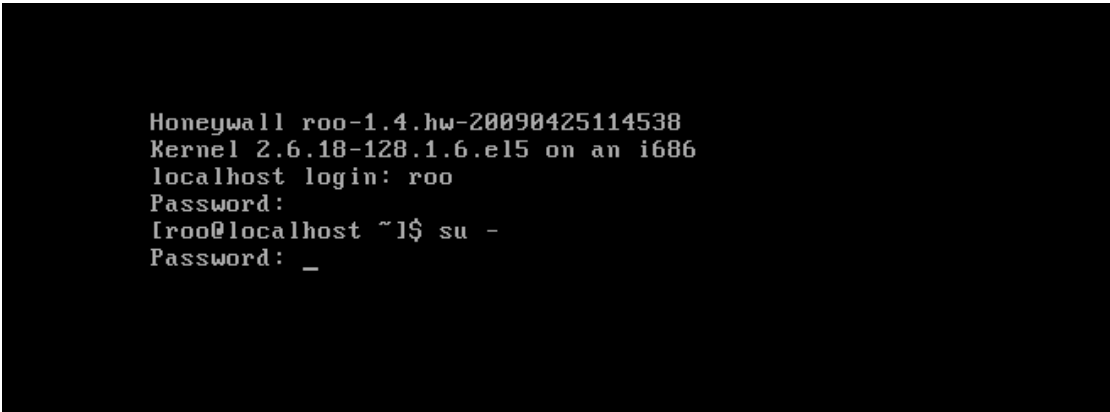
```
Honeywall roo-1.4.hw-20090425114538
Kernel 2.6.18-128.1.6.el5 on an i686
localhost login: _
```

图 33 蜜网网关软件安装完毕，进入登录界面

## 4.6 配置蜜网网关虚拟机

### 1. 登录蜜网网关

以 roo/honey 缺省用户/口令登录，使用 su - 提升到 root 帐号，缺省口令也为 honey



```
Honeywall roo-1.4.hw-20090425114538
Kernel 2.6.18-128.1.6.el5 on an i686
localhost login: roo
Password:
[roo@localhost ~]# su -
Password: _
```

图 34 登录蜜网网关

### 2. 蜜网网关初始配置

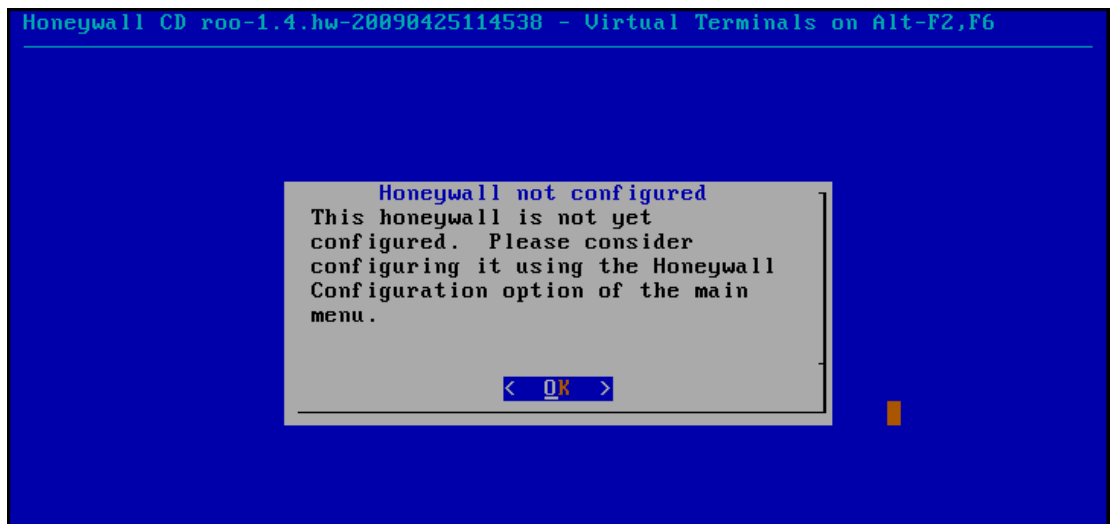


图 35 蜜网网关初始配置界面

如未进入此初始配置界面，则在 shell 中执行

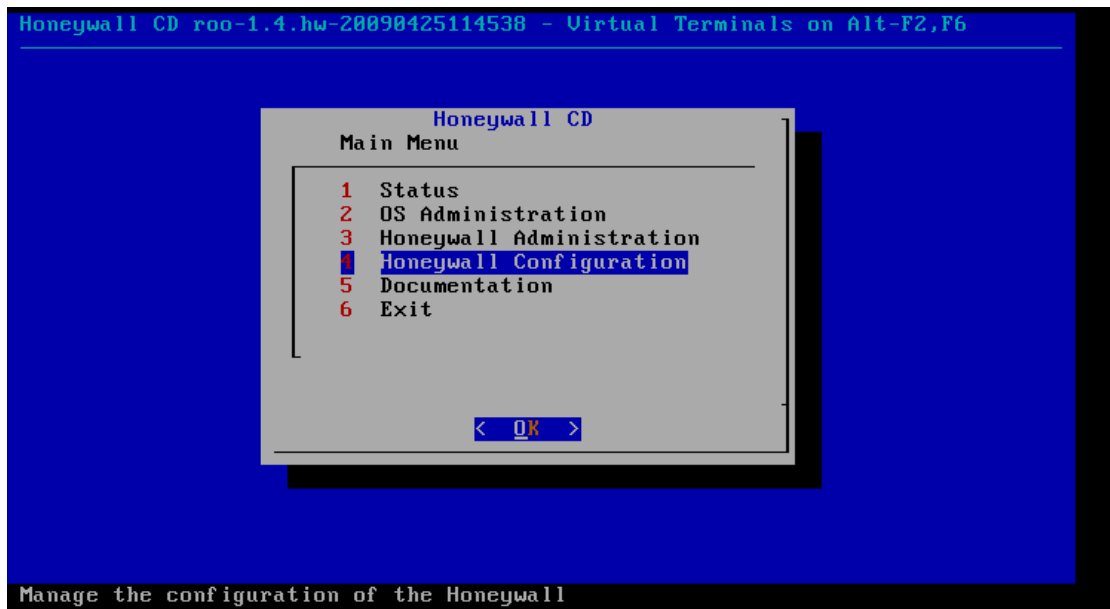


图 36 蜜网网关配置菜单选项界面，选择 4 Honeywall Configuration 进行配置

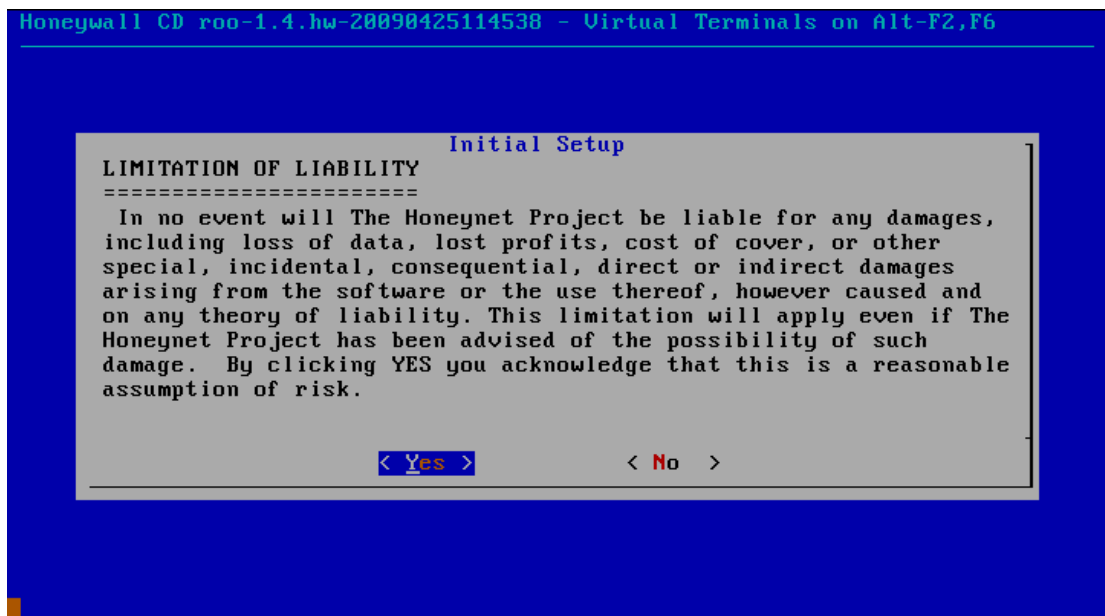


图 37 对 The Honeynet Project 的不承担风险声明选择 Yes

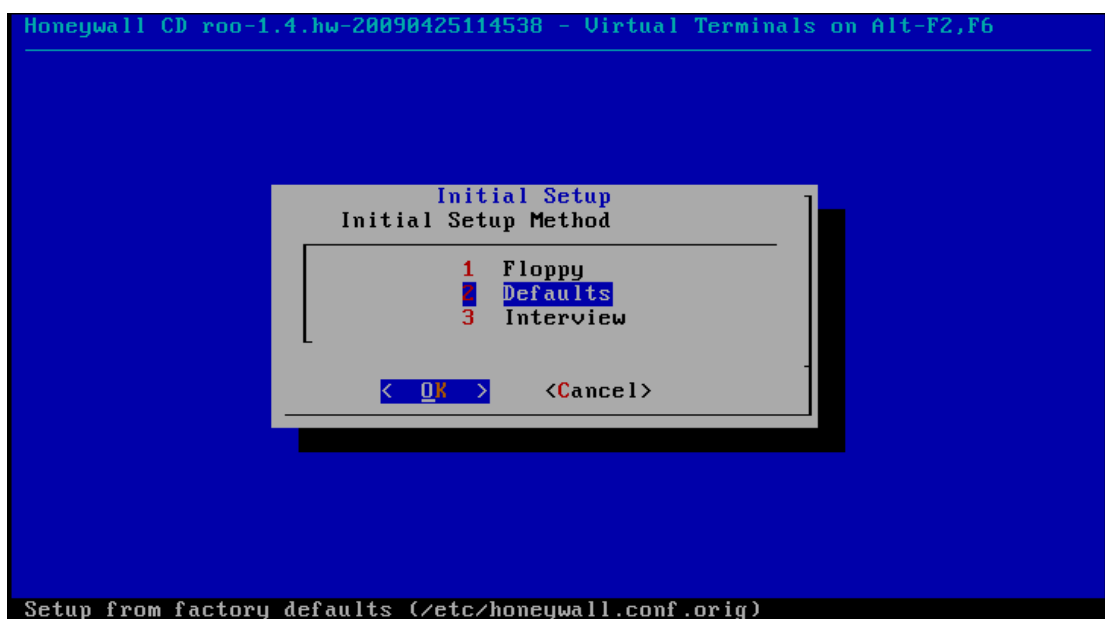


图 38 选择 Defaults 配置方式

接下来会 rebuild，稍等片刻

### 3. 蜜罐信息配置

命令行 menu 进入蜜网网关配置界面，选择 4 HoneyWall Configuration

选择 1 Mode and IP Information

选择 2 Honeypot IP Address

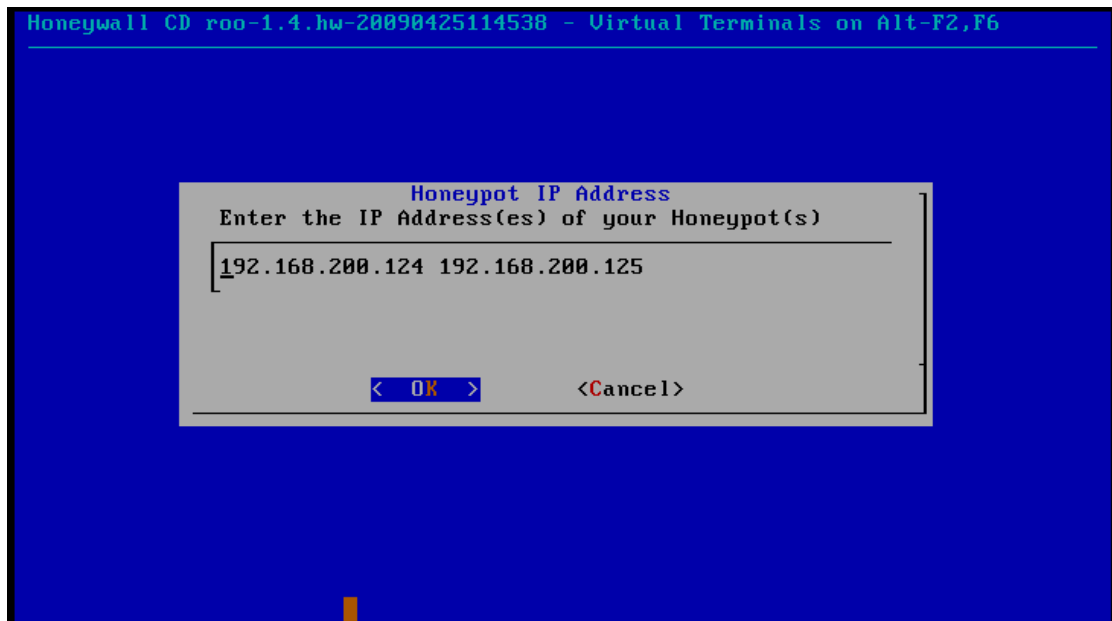


图 39 蜜罐 IP 信息配置，空格分隔多个 IP 地址，注：目前 Roo 尚不支持蜜网网络中具有不同网段的蜜罐 IP 地址

选择 5 LAN Broadcast Address

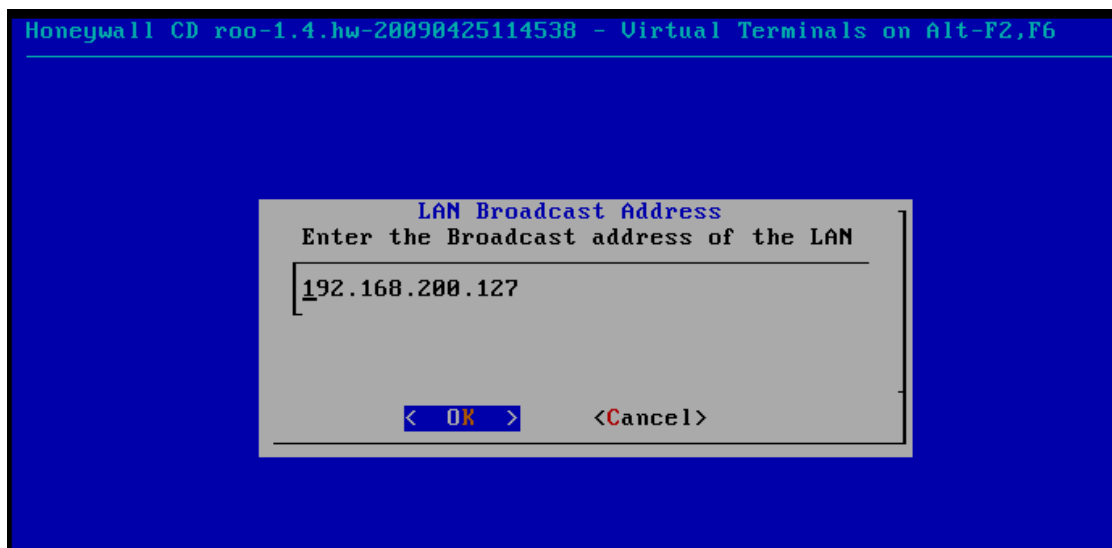


图 40 蜜网网段的广播 IP 地址

选择 6 LAN CIDR Prefix

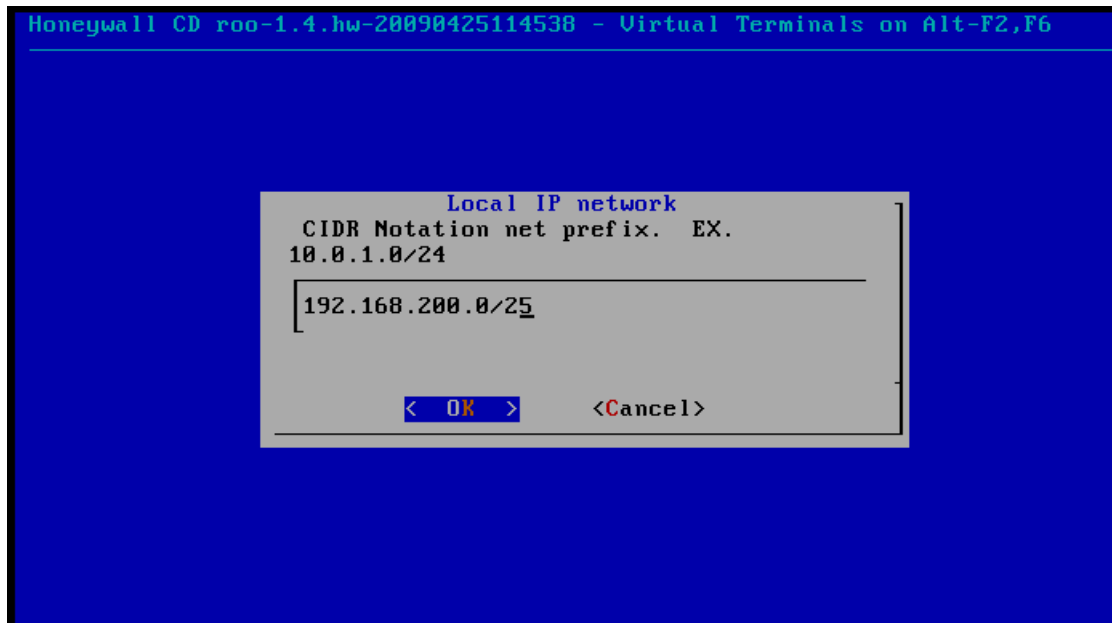


图 41 蜜网网段配置，CIDR 格式

#### 4. 蜜网网关管理配置

蜜网网关配置主界面，选择 4 HoneyWall Configuration

选择 2 Remote Management

选择 1 Management IP Address

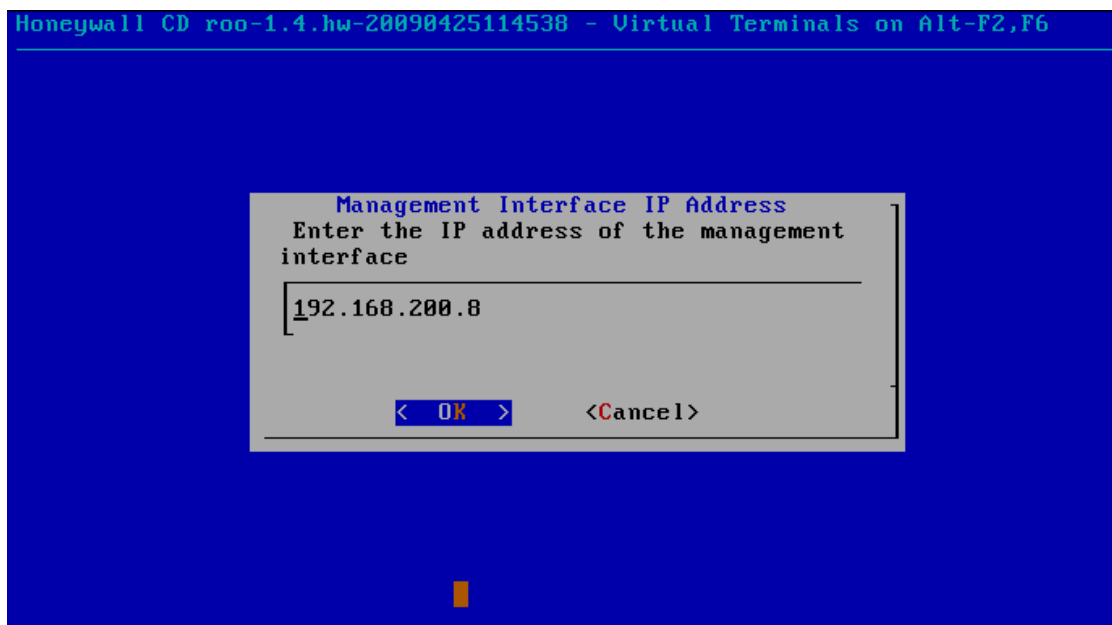


图 42 设置管理口的 IP 地址

选择 2 Management Netmask



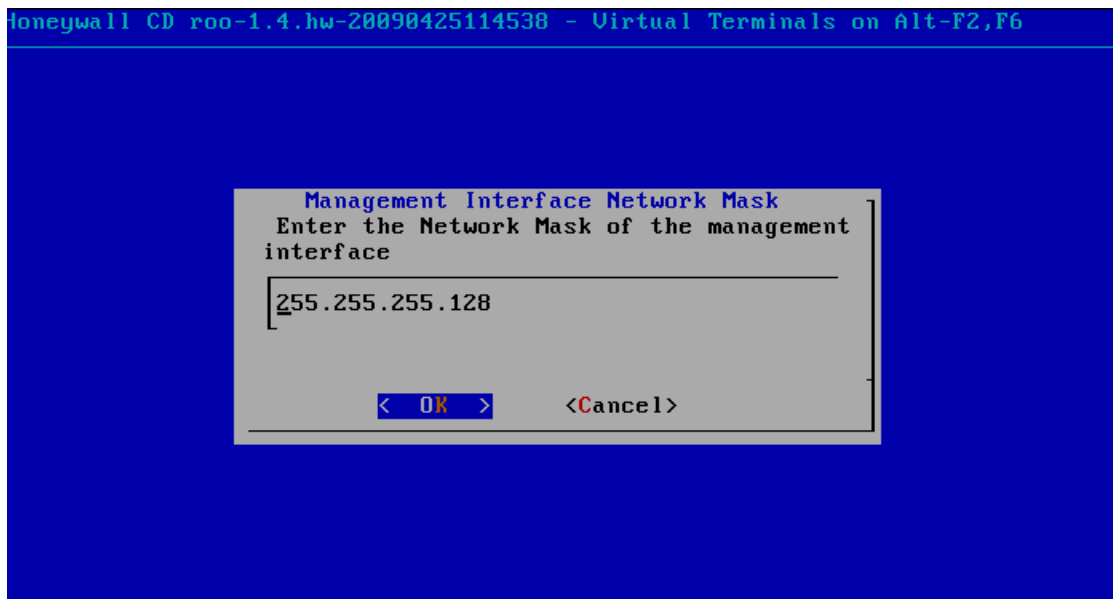


图 43 管理口 IP 地址的掩码

选择 3 Management Gateway

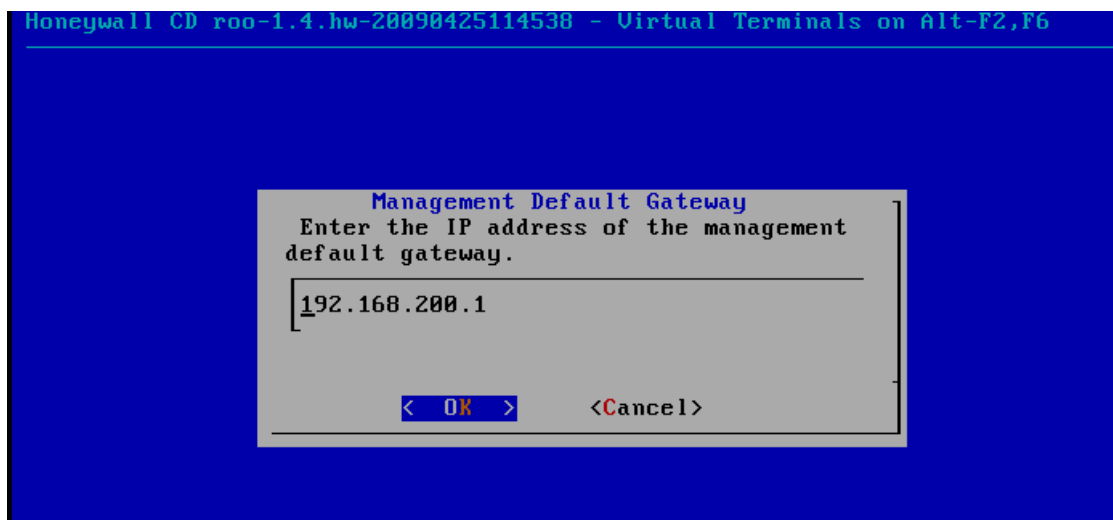


图 44 管理口的网关

选择 7 Manager，设置可以管理蜜网网关的远程控制端 IP 范围，以 CIDR 格式填写，可有多  
个 IP 网段，中间用空格分隔

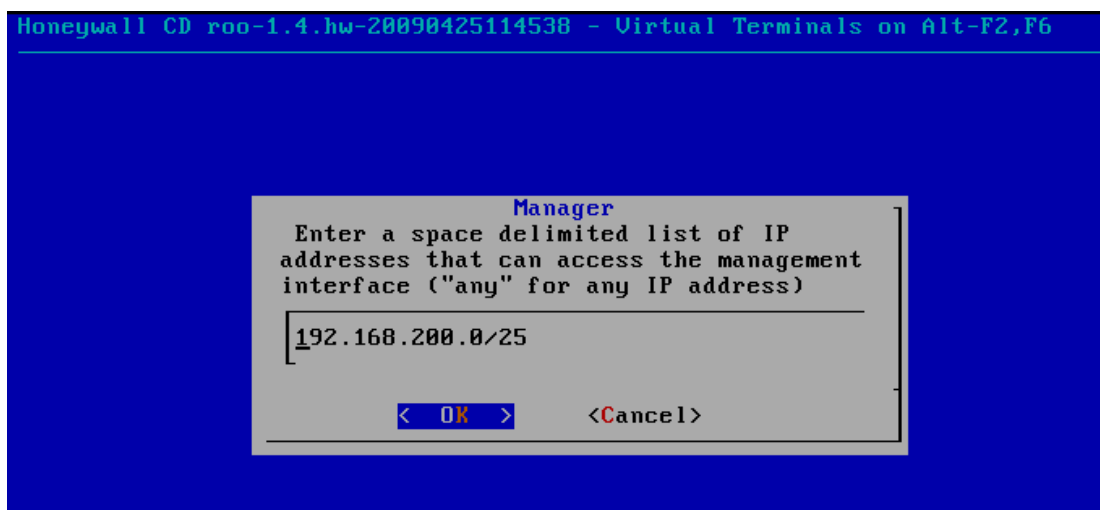


图 45 蜜网网关管理网段

## 5. Sebek 服务器端配置

蜜网网关配置主界面，选择 4 HoneyWall Configuration

选择 11 Sebek

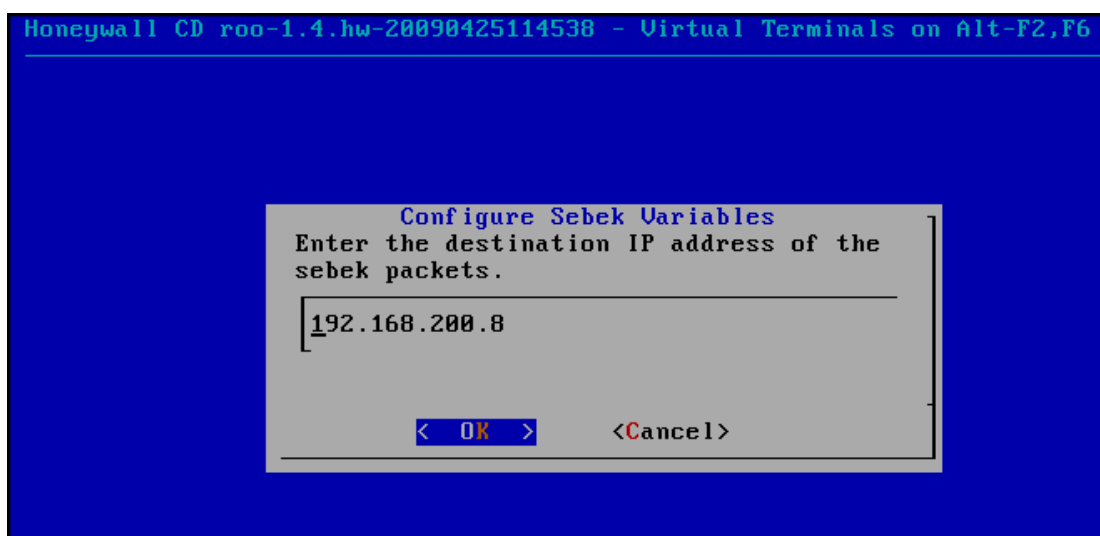


图 46 Sebek 服务器端 IP 地址，设置为管理口 IP

目标端口选择为 1101，Sebek 数据包处理选项选择为 Drop

## 4.7 测试蜜网网关的远程管理

Honeywall 上的防火墙设置不允许 icmp 协议访问管理口

同时会设置允许访问 ssh 和 https 的管理网段。下面测试 https 的远程管理

### 1 测试 walleye 远程访问

在 192.168.200.2 这台虚拟机上访问 <https://192.168.200.8> , 结果如下

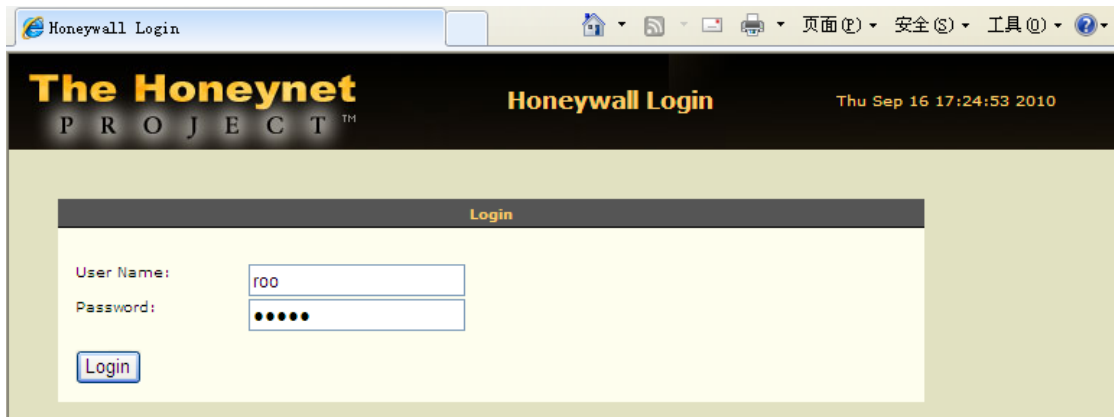


图 47 远程连接 Walleye

出现一个修改密码的界面，按要求修改密码之后，进入如下界面

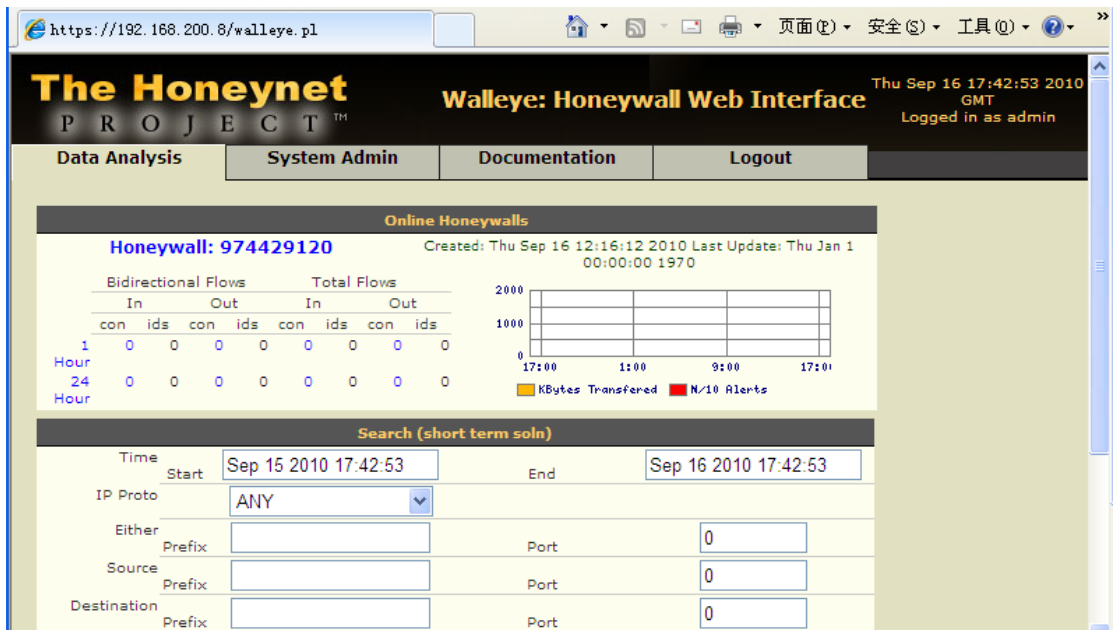


图 48 Walleye 远程管理界面

#### 4.8 测试虚拟机蜜罐和攻击机主机之间的网络连接

在攻击机主机上 ping 虚拟机蜜罐 IP

```

C:\Documents and Settings\Administrator>ping 192.168.200.124

Pinging 192.168.200.124 with 32 bytes of data:

Reply from 192.168.200.124: bytes=32 time=1ms TTL=128
Reply from 192.168.200.124: bytes=32 time<1ms TTL=128
Reply from 192.168.200.124: bytes=32 time<1ms TTL=128
Reply from 192.168.200.124: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.200.124:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

图 49 测试攻击机虚拟机到蜜罐虚拟机的连通性

在虚拟机蜜罐上 ping 攻击机虚拟机 IP

```

C:\Documents and Settings\Administrator>ping 192.168.200.2

Pinging 192.168.200.2 with 32 bytes of data:

Reply from 192.168.200.2: bytes=32 time<10ms TTL=128
Reply from 192.168.200.2: bytes=32 time<10ms TTL=128
Reply from 192.168.200.2: bytes=32 time=15ms TTL=128
Reply from 192.168.200.2: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.200.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms

```

图 50 测试蜜罐虚拟机到攻击机虚拟机的连通性

在蜜网网关上监听 ICMP ping 包是否通过外网口和内网口，**注意，以下命令必须得在 root 权限下操作**

```

[root@roo-test ~]# tcpdump -i eth0 icmp
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
17:13:31.627501 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 25856, length 40
17:13:31.628502 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 25856, length 40
17:13:32.630001 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 26112, length 40
17:13:32.630732 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 26112, length 40
17:13:33.630349 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 26368, length 40
17:13:33.632319 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 26368, length 40
17:13:34.630794 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 26624, length 40
17:13:34.631648 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 26624, length 40

```

图 51 攻击机 ping 靶机的时候，tcpdump -i eth0 icmp

```

[root@roo-test ~]# tcpdump -i eth1 icmp
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
17:16:48.849443 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 26880, length 40
17:16:48.849644 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 26880, length 40
17:16:49.827072 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 27136, length 40
17:16:49.827298 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 27136, length 40
17:16:50.827430 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 27392, length 40
17:16:50.827639 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 27392, length 40
17:16:51.828916 IP 192.168.200.2 > 192.168.200.124: ICMP echo request, id 512, seq 27648, length 40
17:16:51.829134 IP 192.168.200.124 > 192.168.200.2: ICMP echo reply, id 512, seq 27648, length 40

```

图 52 攻击机 ping 靶机的时候，tcpdump -i eth1 icmp

```

[root@roo-test ~]# tcpdump -i eth0 icmp
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
17:18:35.104257 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 6400, length 40
17:18:35.104847 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 6400, length 40
17:18:36.092720 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 6656, length 40
17:18:36.093006 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 6656, length 40
17:18:37.095029 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 6912, length 40
17:18:37.095237 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 6912, length 40
17:18:38.097519 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 7168, length 40
17:18:38.097775 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 7168, length 40

```

图 53 靶机 ping 攻击机的时候，tcpdump -i eth0 icmp

```

[root@roo-test ~]# tcpdump -i eth1 icmp
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
17:20:33.014001 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 7424, length 40
17:20:33.015379 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 7424, length 40
17:20:34.016542 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 7680, length 40
17:20:34.017525 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 7680, length 40
17:20:35.003986 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 7936, length 40
17:20:35.005502 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 7936, length 40
17:20:36.008288 IP 192.168.200.124 > 192.168.200.2: ICMP echo request, id 512, seq 8192, length 40
17:20:36.009269 IP 192.168.200.2 > 192.168.200.124: ICMP echo reply, id 512, seq 8192, length 40

```

图 54 靶机 ping 攻击机的时候，tcpdump -i eth1 icmp

通过测试后，说明虚拟机蜜罐和外部网络之间的网络连接（通过蜜网网关 eth0 和 eth1

所构成的网桥）没有问题。

## 五、攻击测试

### 5.1 虚拟机蜜罐上安装 Sebek 客户端

#### 1. 在 Win32 虚拟机蜜罐上安装 Sebek 客户端

将 Sebek-Win32-3.0.4.zip 或 Sebek-Win32-latest.zip (<http://www.savidtech.com/sebek/>)

通过网络共享拷贝到虚拟机蜜罐中，解压后执行 Setup.exe 进行安装。

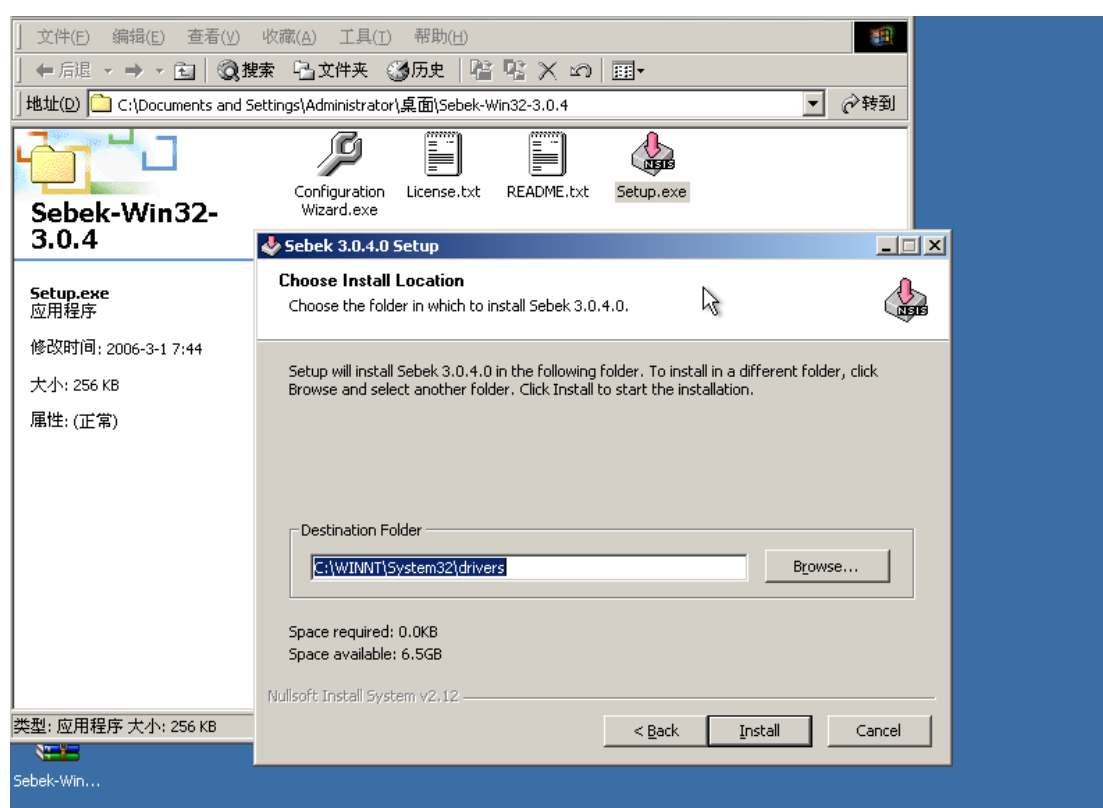


图 55 安装 Sebek Win32 系统监控软件

在蜜网网关虚拟机上执行 `ifconfig eth2`，得到管理口 eth2 的 MAC 地址，填入下图所示的 Sebek 服务器端配置对话框。

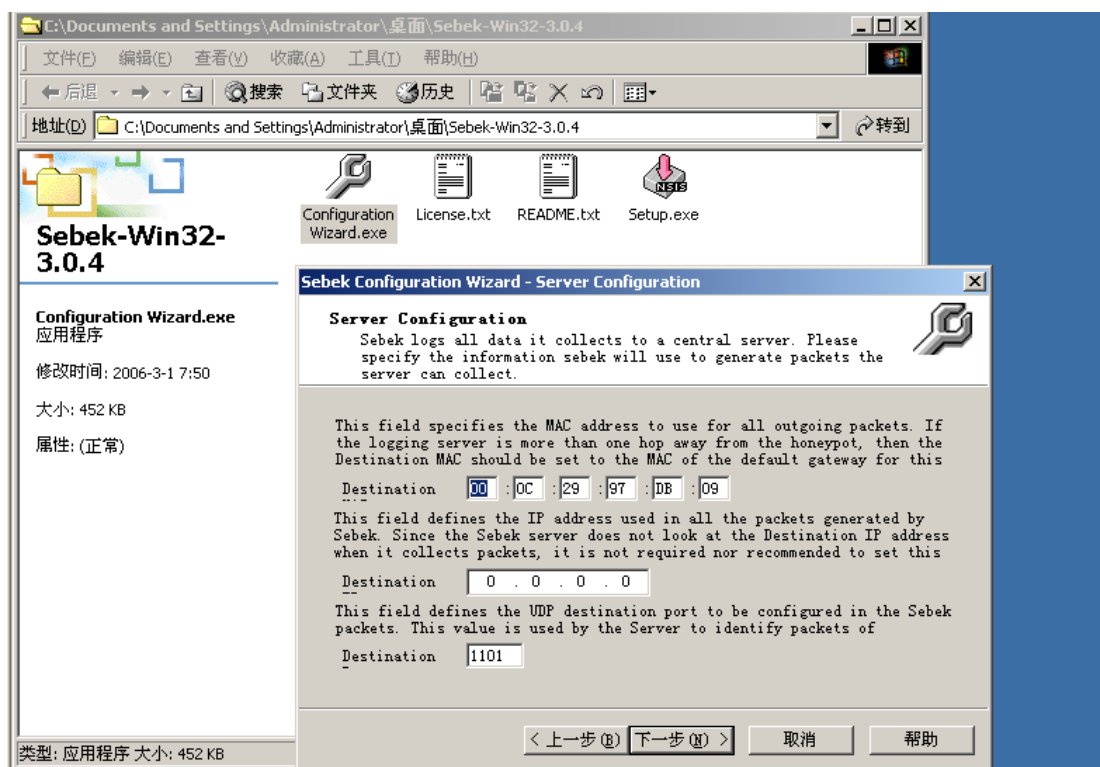


图 56 配置 Sebek Win32 系统监控软件

随机生成或填写 Magic Number，需保证同一蜜网中每台蜜罐主机上均安装 Sebek，且 Sebek 使用的 Magic Number 保持一致，使得 Sebek 的上传通讯在蜜网中对攻击者隐蔽（即使攻击者获取了蜜罐主机的控制权，并启用网络监听器进行监听）。重新启动主机，建立 snapshot。

## 5.2 漏洞扫描测试

在攻击机虚拟机上用 nmap 扫描蜜罐虚拟机 192.168.200.124

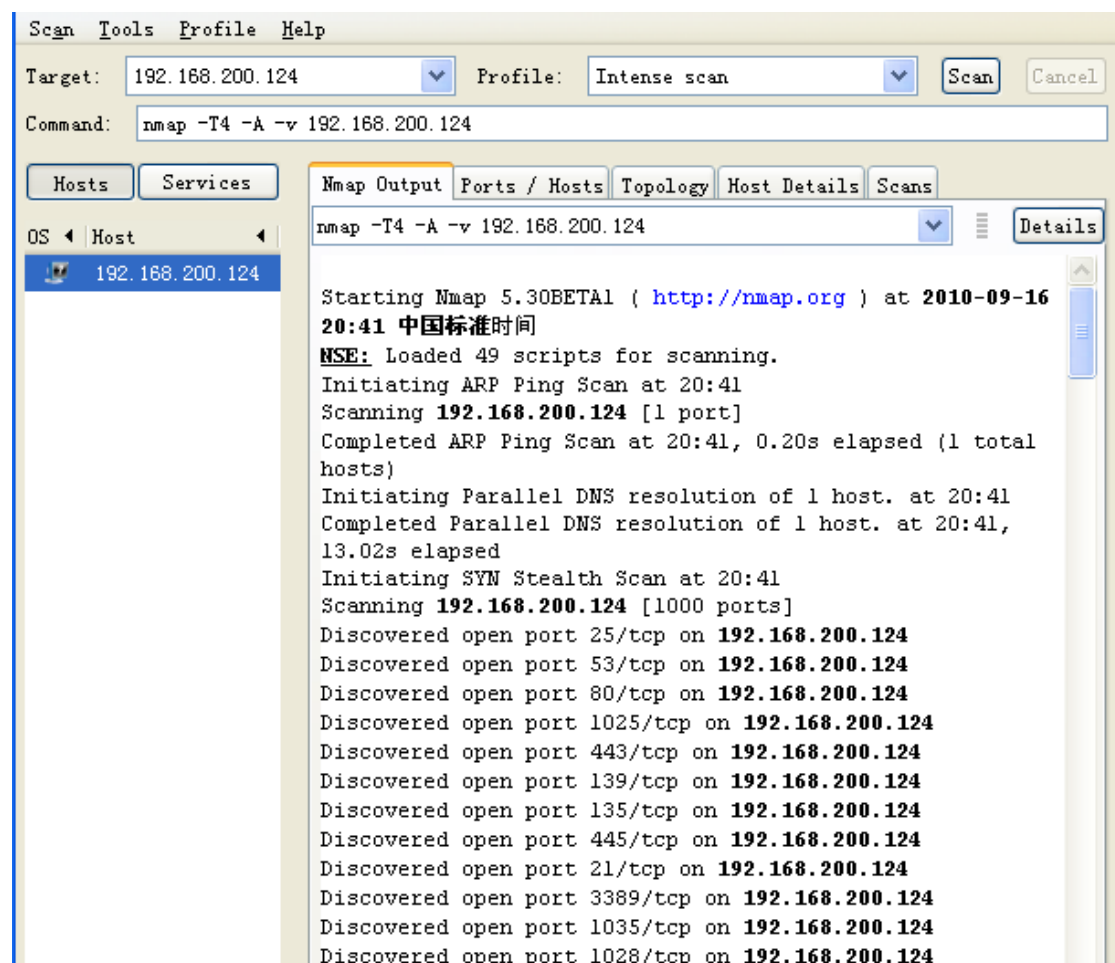


图 57 (1) nmap 对虚拟机蜜罐进行扫描测试



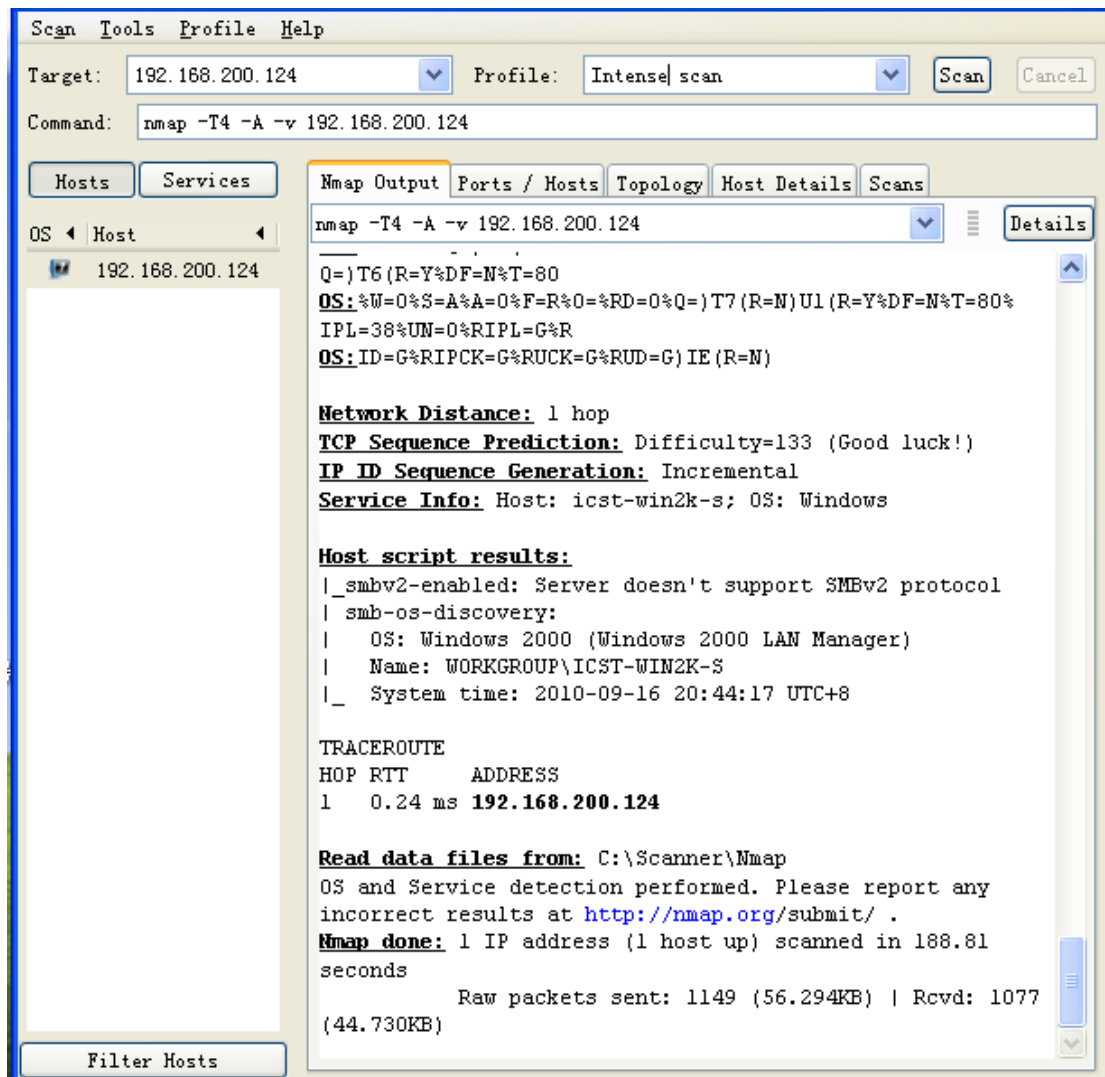


图 57 (2) nmap 对虚拟机蜜罐进行扫描测试

注：由于目前 Sebek Client for Win32 版本的稳定性较差，大规模的扫描和渗透测试很可能会造成 Sebek 的崩溃从而引发 BSOD（Blue Screen of Death）。

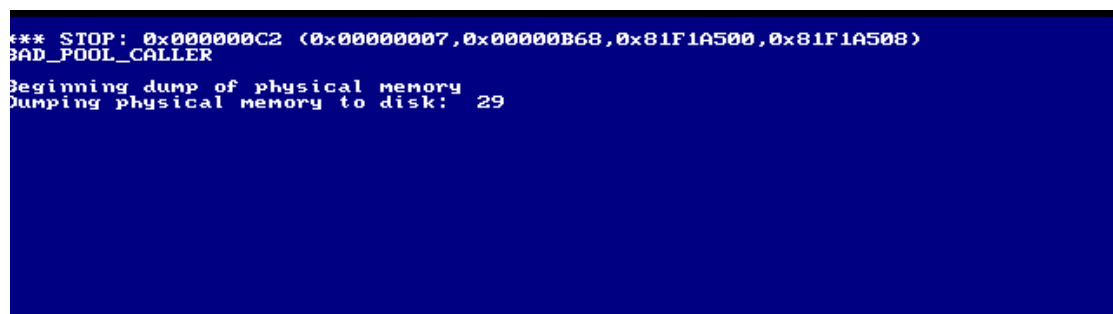


图 58 虚拟机蜜罐蓝屏

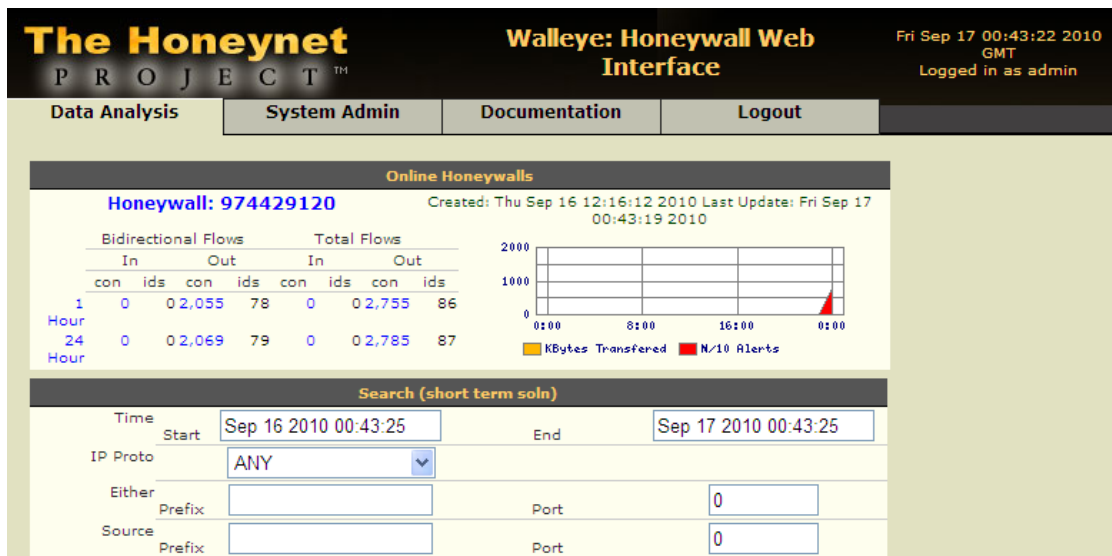


图 59 蜜网网关捕获的漏洞扫描过程的摘要视图

在蜜网网关上对 nmap 漏洞扫描过程中的每个网络连接都进行了完备的记录，从图 59 蜜网网关数据摘要视图可发现正在扫描的 192.168.200.2 攻击机 IP，图 60 则显示了其扫描的每个网络连接详细信息。



for Windows 并安装。

2. Metasploit 渗透攻击测试

运行 MSFConsole，按图输入针对 MS03-026 即插即用服务漏洞的渗透攻击命令，获得反向的 shell。（注：需打开攻击机虚拟机的个人防火墙，如微软防火墙，使得能够接收 4444 端口的连入）。

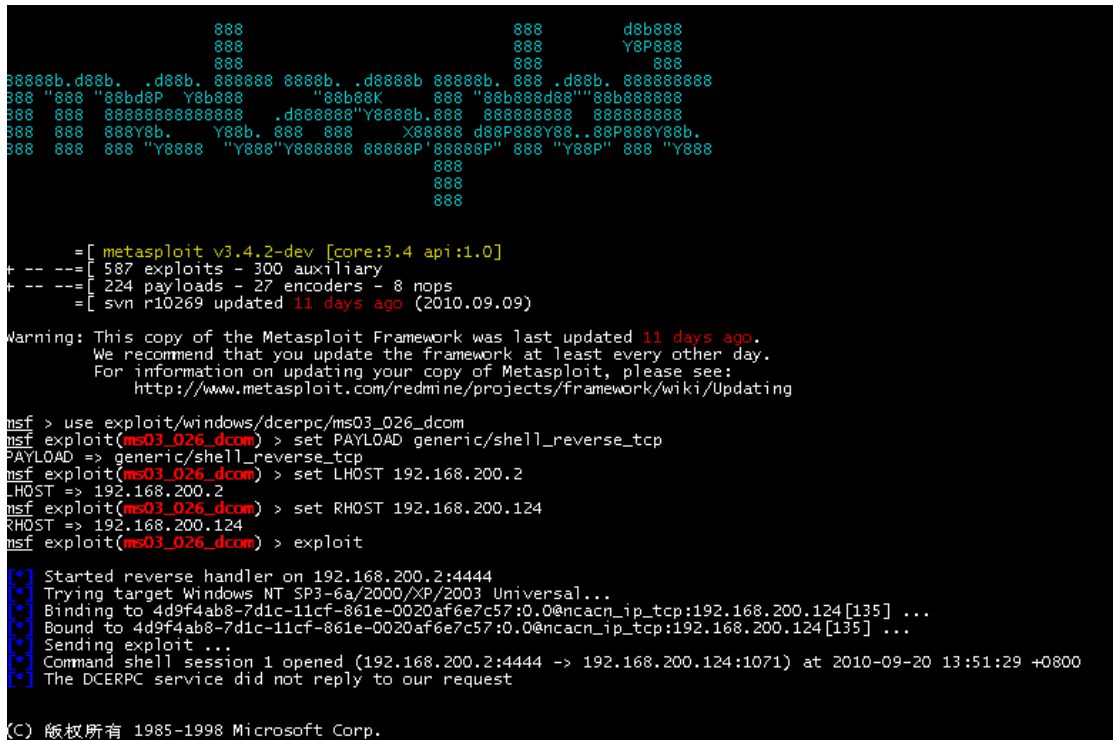


图 61 MS03\_026\_dcom 漏洞渗透攻击过程

3. 对蜜网网关记录的攻击数据进行分析，验证蜜网的攻击数据捕获和分析功能

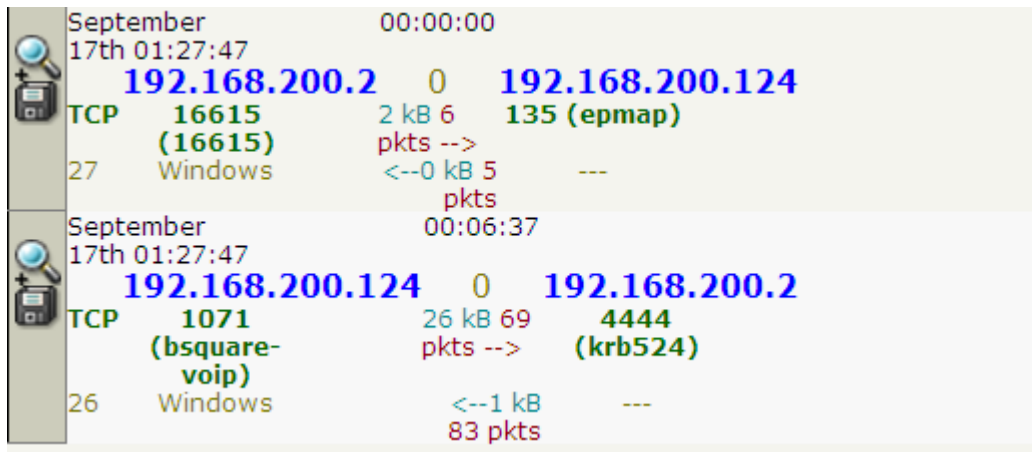


图 62 攻击机向靶机发起的向内连接视图以及靶机向外发起的反向 shell 连接

## 六、总结

本文档给出了在Win32平台基于VMWare软件部署并测试第三代虚拟蜜网的详细步骤和过程, 最终的攻击测试过程和蜜网网关对这些攻击测试的数据捕获和分析能力说明了第三代蜜网技术已经达到了较为成熟的阶段, 在对互联网安全威胁的捕获分析方面可以发挥较大的作用。