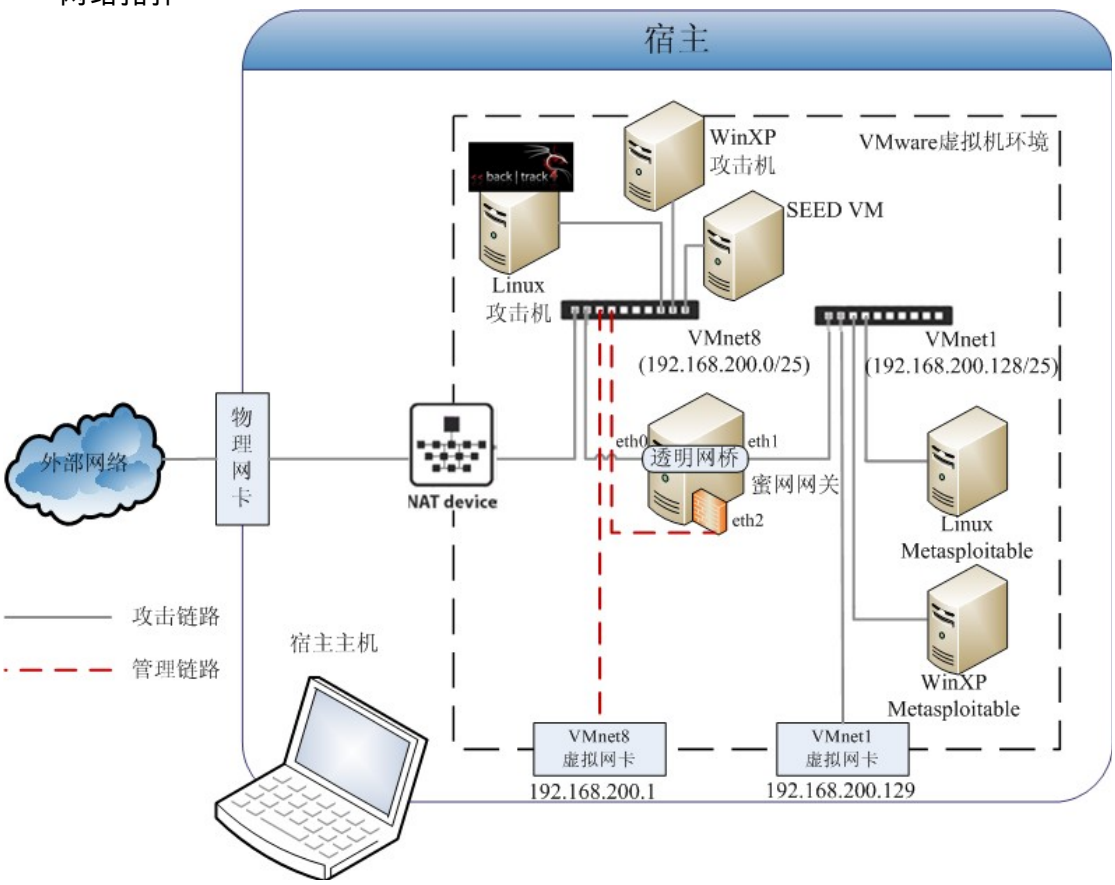
网络攻防实验环境搭建与测试实验报告

黄萍 **1001213630**

一. 网络拓扑



二. 软硬件配置

1. 硬件配置
   - 处理器: Intel Core i3 CPU 2.40GHz
   - 内存: 2.00GB
   - 硬盘: 320G
2. 软件配置
   a) 宿主系统
      - 操作系统: windows 7
      - VMware-workstation-full-7.0.0-203739
   b) 蜜网网关虚拟机
      - Roo Honeywall CDROM v1.4
   c) 攻击机
      - WinXPattacker
      - Back Track 4
   d) 靶机
      - WinXP Metasploitable
      - Linux Metasploitable

三. 虚拟蜜网的构建

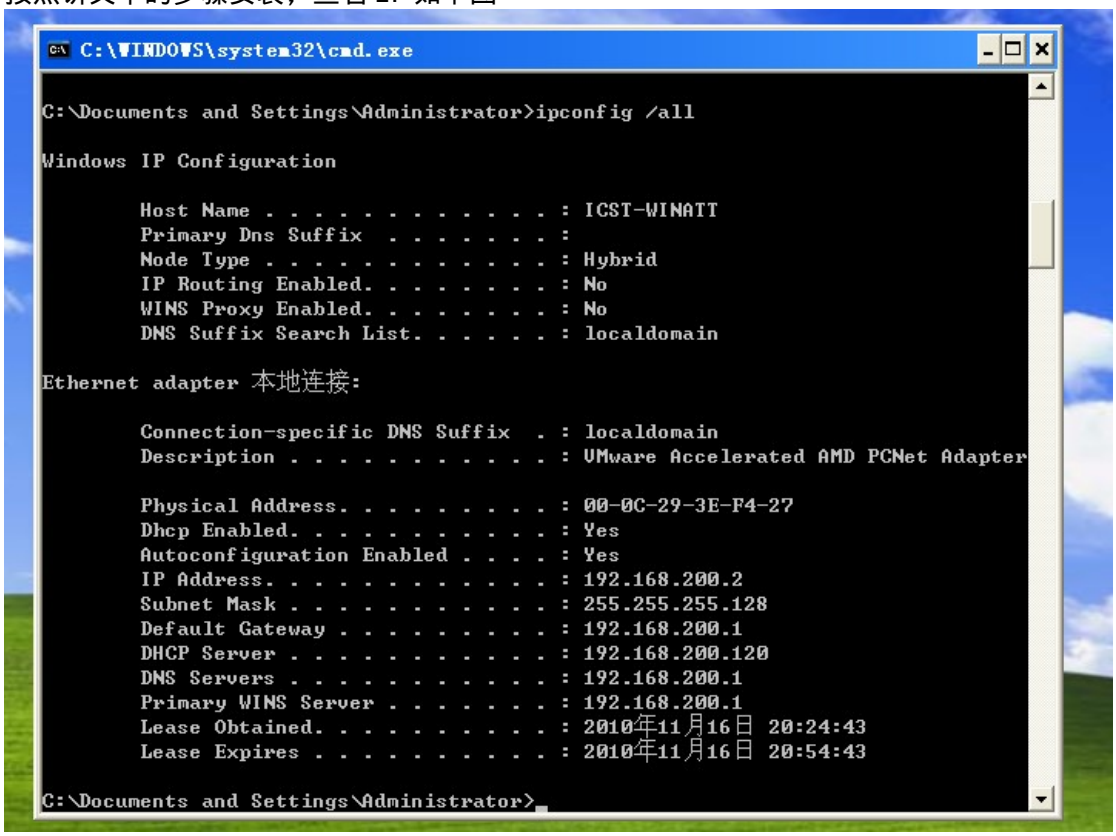
a) VMware 软件安装与配置
   - 按照默认方式安装好 VMware workstation。
   - 按照讲义配置 VMware 网络环境，具体配置如下表所示

虚拟网卡	连接方式	子网 IP
VMnet1	Host-only	192.168.200.128
VMnet8	NAT	192.168.200.0

b) 安装攻击机虚拟机

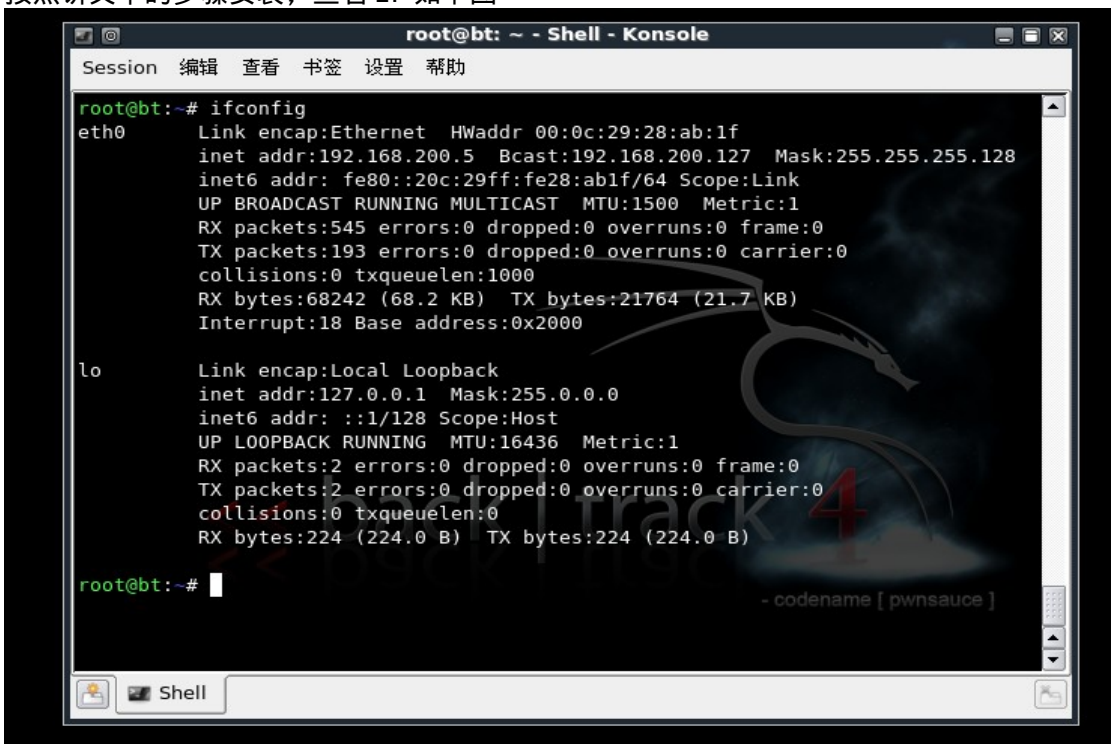
- 安装 WinXPattacker

  按照讲义中的步骤安装，查看 IP 如下图



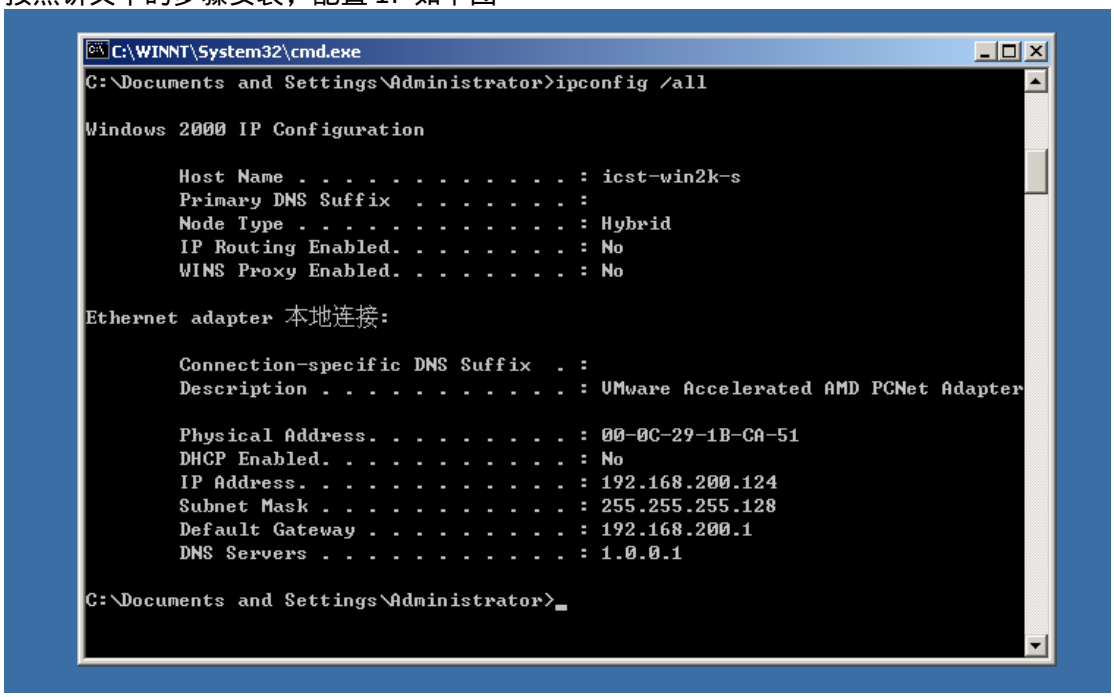
- 安装 Back Track 4

  按照讲义中的步骤安装，查看 IP 如下图

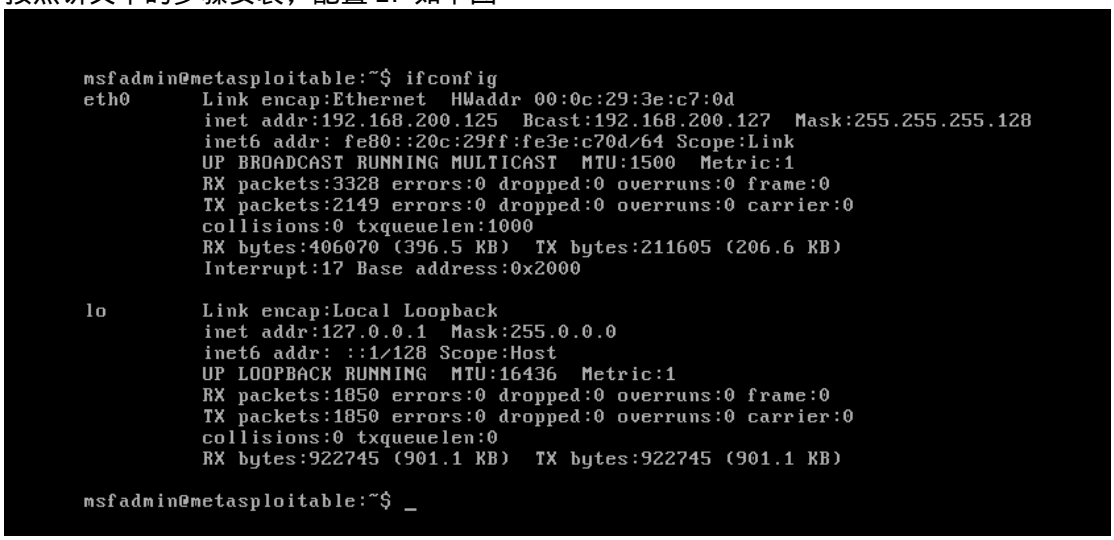


c） 安装靶机虚拟机

- 安装 WinXP Metasploitable
  按照讲义中的步骤安装，配置 IP 如下图



- 安装 Linux Metasploitable
  按照讲义中的步骤安装，配置 IP 如下图



d） 安装与配置蜜网网关

- 按照讲义中的步骤安装，安装成功后如下图所示

```
Honeywall roo-1.4.hw-20090425114538
Kernel 2.6.18-128.1.6.el5 on an i686
roo-test login: roo
Password:
Last login: Thu Nov 11 00:25:55 on tty1
[roo@roo-test ~]$ _
```

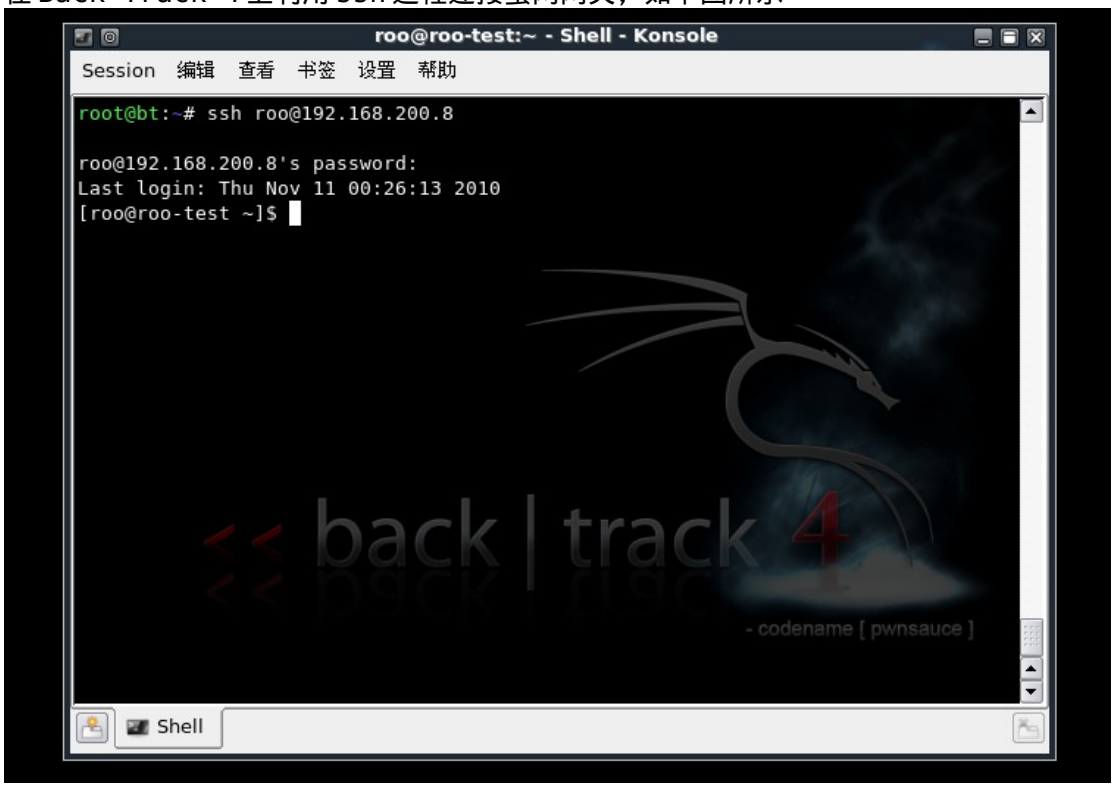
- 配置蜜网网关

  按照讲义中的步骤配置蜜网网关，具体配置如下

  1. 蜜罐信息配置
     - Honeypot IP: 192.168.200.124 192.168.200.125
     - LAN Broadcast Address: 192.168.200.127
     - LAN CIDR Prefix: 192.168.200.0/25
  2. 蜜网网关管理配置
     - 管理接口 IP: 192.168.200.8
     - 管理接口 mask: 255.255.255.128
     - 管理网关 IP: 192.168.200.1
     - 远程控制端 IP 范围: 192.168.200.0/25
  3. Sebek 服务器配置
     - 目标 IP: 192.168.200.8
     - 目标端口: 1101
     - 处理方式: drop
- 测试蜜网网关的远程管理
  - 利用 https 测试 walleye 远程访问

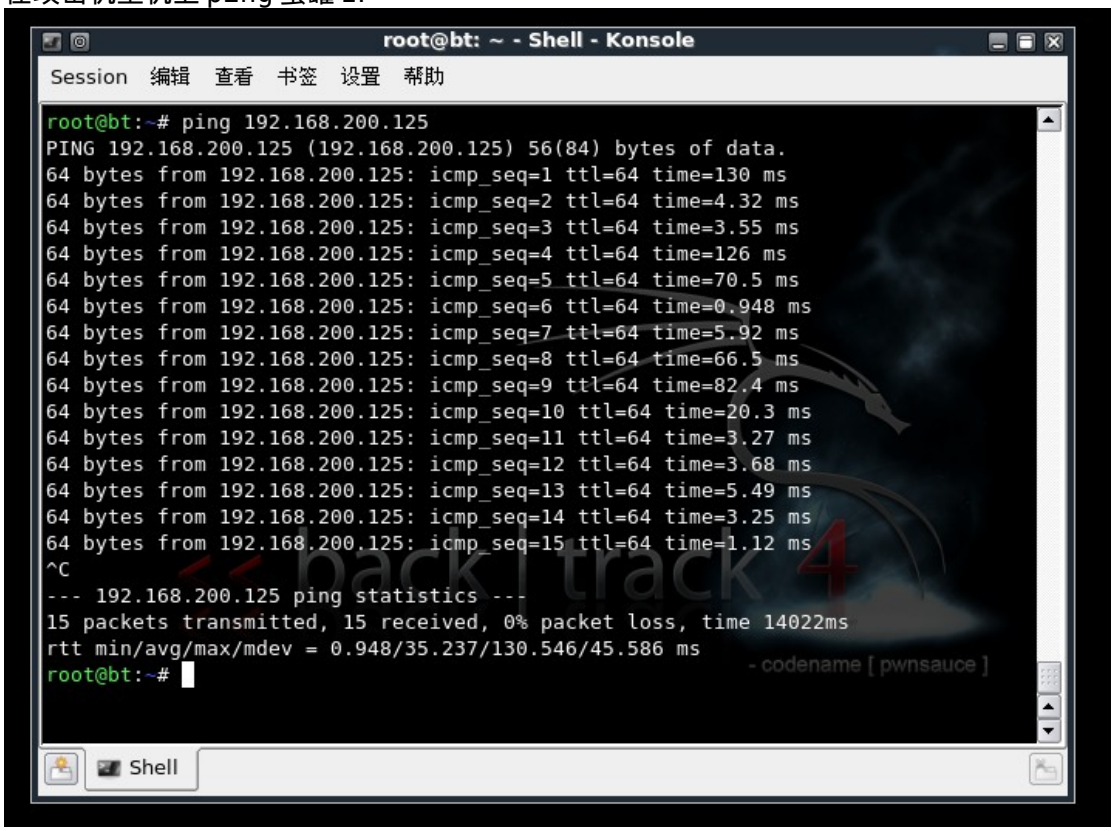
    在 WinXPattacker 上用 https 远程连接 walleye，如下图所示

- 利用 ssh 测试蜜网网关远程访问
  在 Back Track 4 上利用 ssh 远程连接蜜网网关，如下图所示



➢ 测试虚拟机蜜罐和攻击机之间的网络连接

- 在攻击机主机上 ping 蜜罐 IP



在蜜网网关 eth0 上监听 ICMP ping 包，如下图所示

```
[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
00:39:27.244824 IP 192.168.200.5 > 192.168.200.125: ICMP echo request, id 65299,
 seq 1, length 64
00:39:27.248550 IP 192.168.200.125 > 192.168.200.5: ICMP echo reply, id 65299, s
eq 1, length 64
00:39:28.256448 IP 192.168.200.5 > 192.168.200.125: ICMP echo request, id 65299,
 seq 2, length 64
00:39:28.259921 IP 192.168.200.125 > 192.168.200.5: ICMP echo reply, id 65299, s
eq 2, length 64
00:39:29.258529 IP 192.168.200.5 > 192.168.200.125: ICMP echo request, id 65299,
 seq 3, length 64
00:39:29.260985 IP 192.168.200.125 > 192.168.200.5: ICMP echo reply, id 65299, s
eq 3, length 64
00:39:30.260820 IP 192.168.200.5 > 192.168.200.125: ICMP echo request, id 65299,
 seq 4, length 64
00:39:30.263534 IP 192.168.200.125 > 192.168.200.5: ICMP echo reply, id 65299, s
eq 4, length 64

8 packets captured
8 packets received by filter
0 packets dropped by kernel
[root@roo-test ~]#
```

- 在蜜罐上 ping 攻击机 IP

```
msfadmin@metasploitable:~$ ping 192.168.200.5
PING 192.168.200.5 (192.168.200.5) 56(84) bytes of data.
64 bytes from 192.168.200.5: icmp_seq=1 ttl=64 time=1.89 ms
64 bytes from 192.168.200.5: icmp_seq=2 ttl=64 time=3.82 ms
64 bytes from 192.168.200.5: icmp_seq=3 ttl=64 time=4.80 ms
64 bytes from 192.168.200.5: icmp_seq=4 ttl=64 time=4.04 ms

--- 192.168.200.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 1.894/3.641/4.809/1.076 ms
msfadmin@metasploitable:~$ _
```

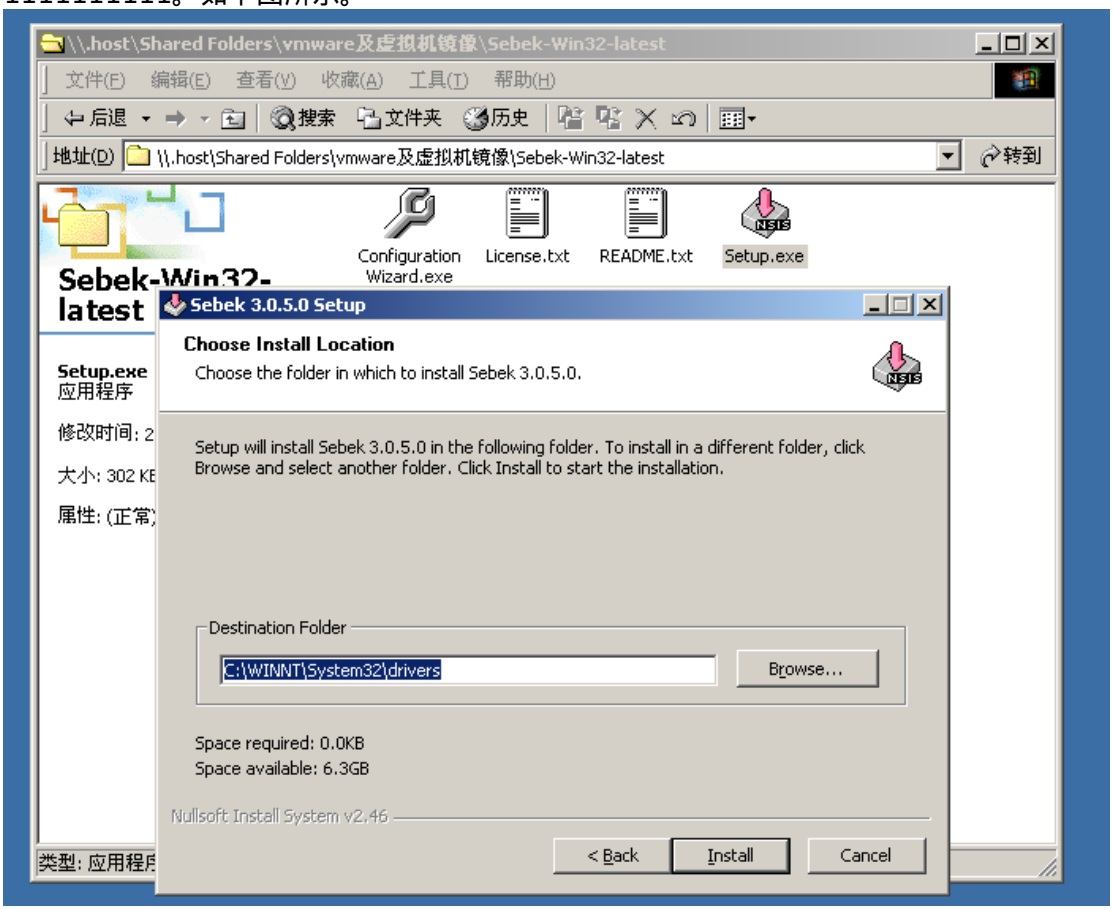
在蜜网网关 eth1 上监听 ICMP ping 包

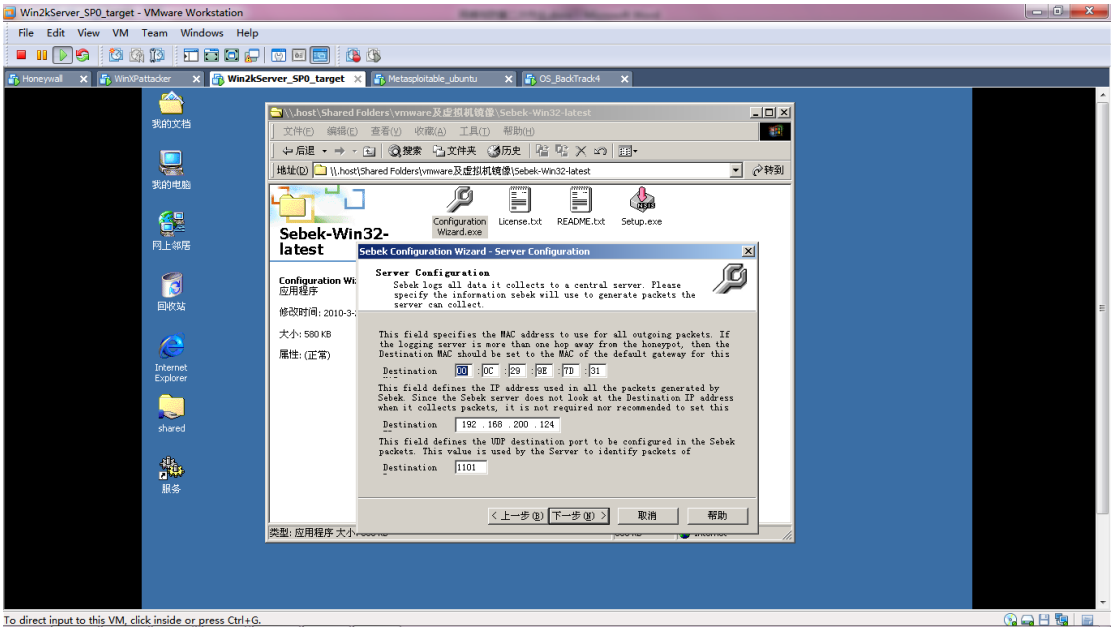
```
[root@roo-test ~]# tcpdump -i eth1 icmp
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
00:44:36.257985 IP 192.168.200.125 > 192.168.200.5: ICMP echo request, id 22295,
 seq 1, length 64
00:44:36.259586 IP 192.168.200.5 > 192.168.200.125: ICMP echo reply, id 22295, s
eq 1, length 64
00:44:37.256986 IP 192.168.200.125 > 192.168.200.5: ICMP echo request, id 22295,
 seq 2, length 64
00:44:37.259903 IP 192.168.200.5 > 192.168.200.125: ICMP echo reply, id 22295, s
eq 2, length 64
00:44:38.259566 IP 192.168.200.125 > 192.168.200.5: ICMP echo request, id 22295,
 seq 3, length 64
00:44:38.262382 IP 192.168.200.5 > 192.168.200.125: ICMP echo reply, id 22295, s
eq 3, length 64
00:44:39.259827 IP 192.168.200.125 > 192.168.200.5: ICMP echo request, id 22295,
 seq 4, length 64
00:44:39.262644 IP 192.168.200.5 > 192.168.200.125: ICMP echo reply, id 22295, s
eq 4, length 64

8 packets captured
8 packets received by filter
0 packets dropped by kernel
[root@roo-test ~]# _
```

四. 攻击测试

a) 蜜罐上安装 Sebek 客户端

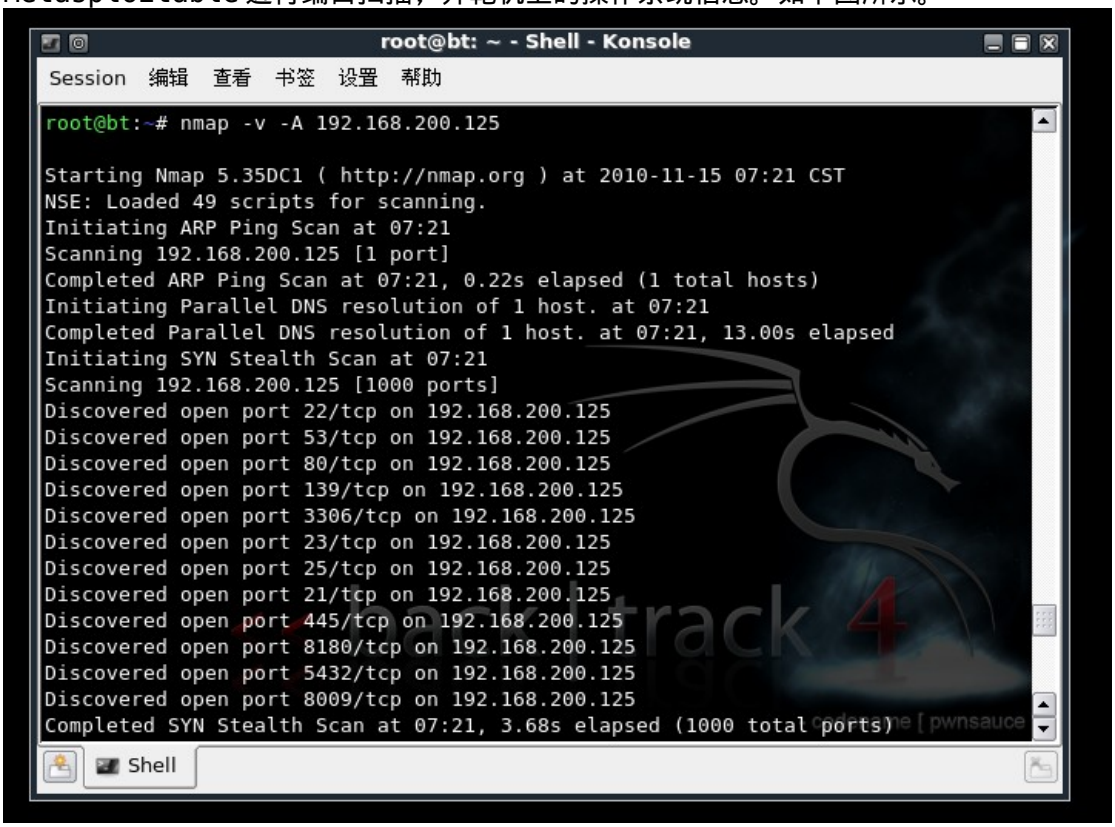
按照讲义中的步骤，安装好 Sebek 客户端后，配置 Sebek 客户端，魔数设为 1111111111。如下图所示。

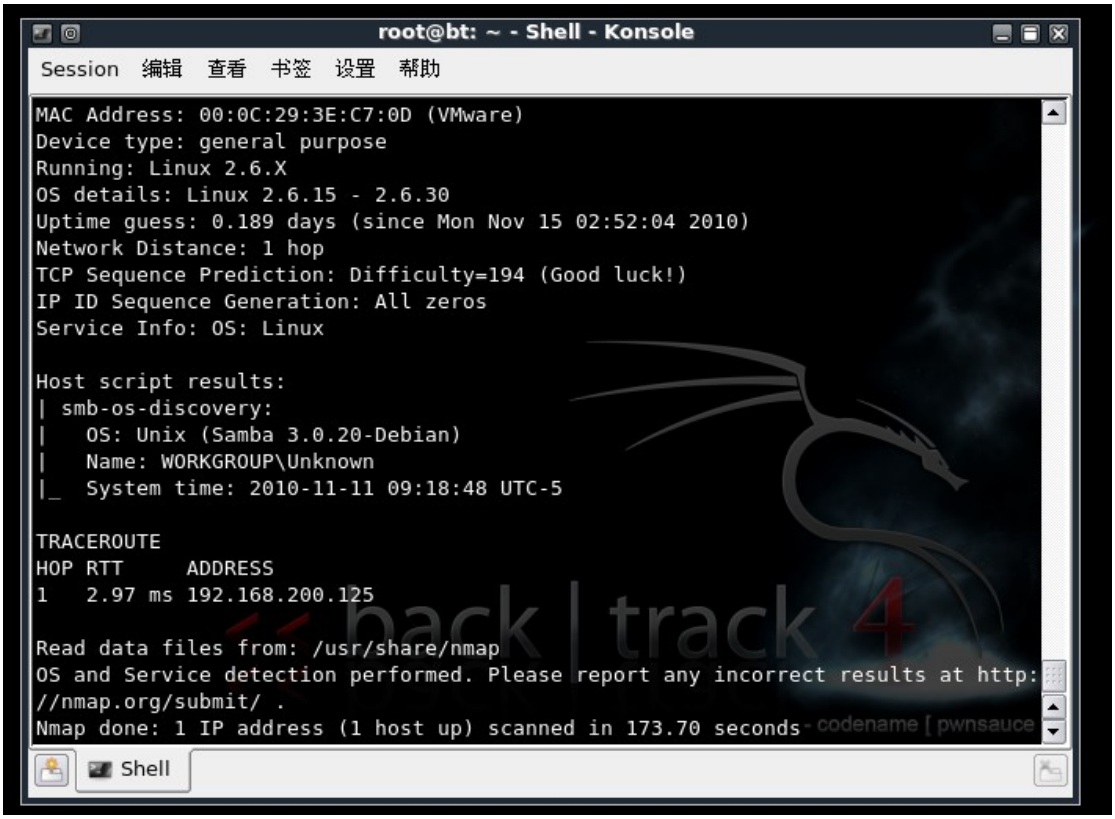




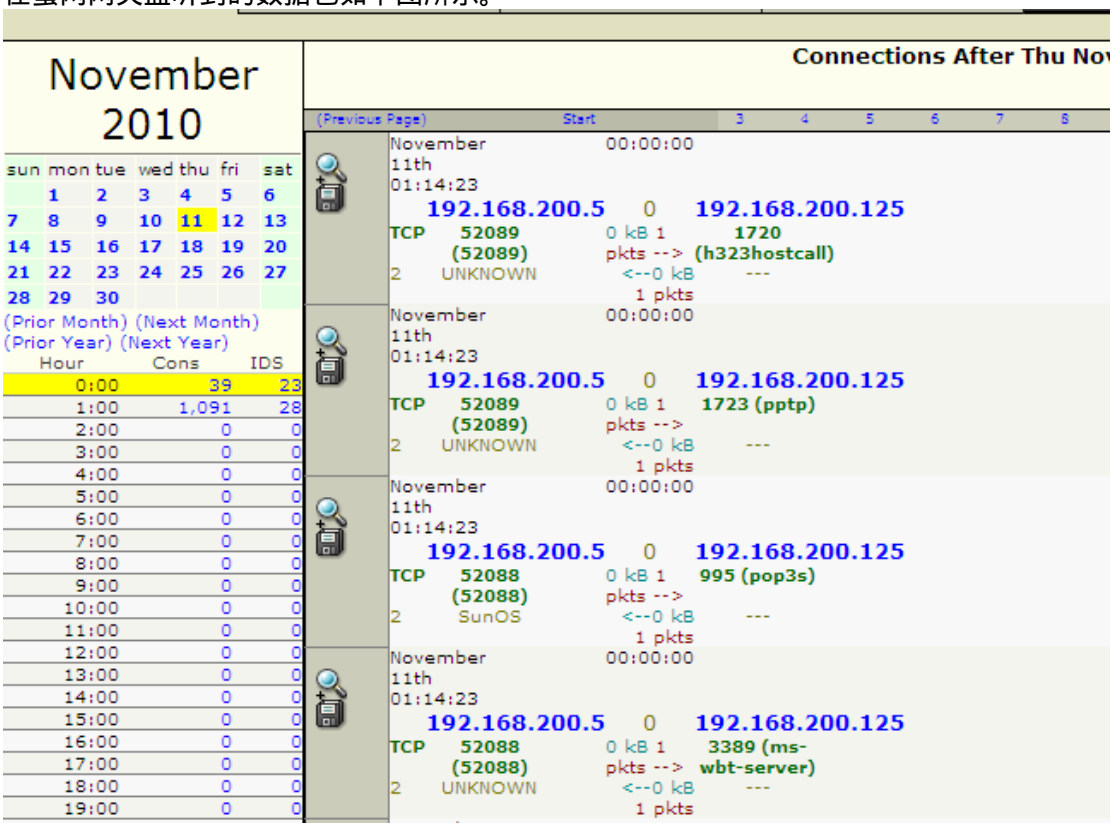
b） 漏洞扫描测试

在攻击机 Back Track 4 上使用 nmap –A –v 192.168.200.125 对 Linux Metasploitable 进行端口扫描，并靶机上的操作系统信息。如下图所示。



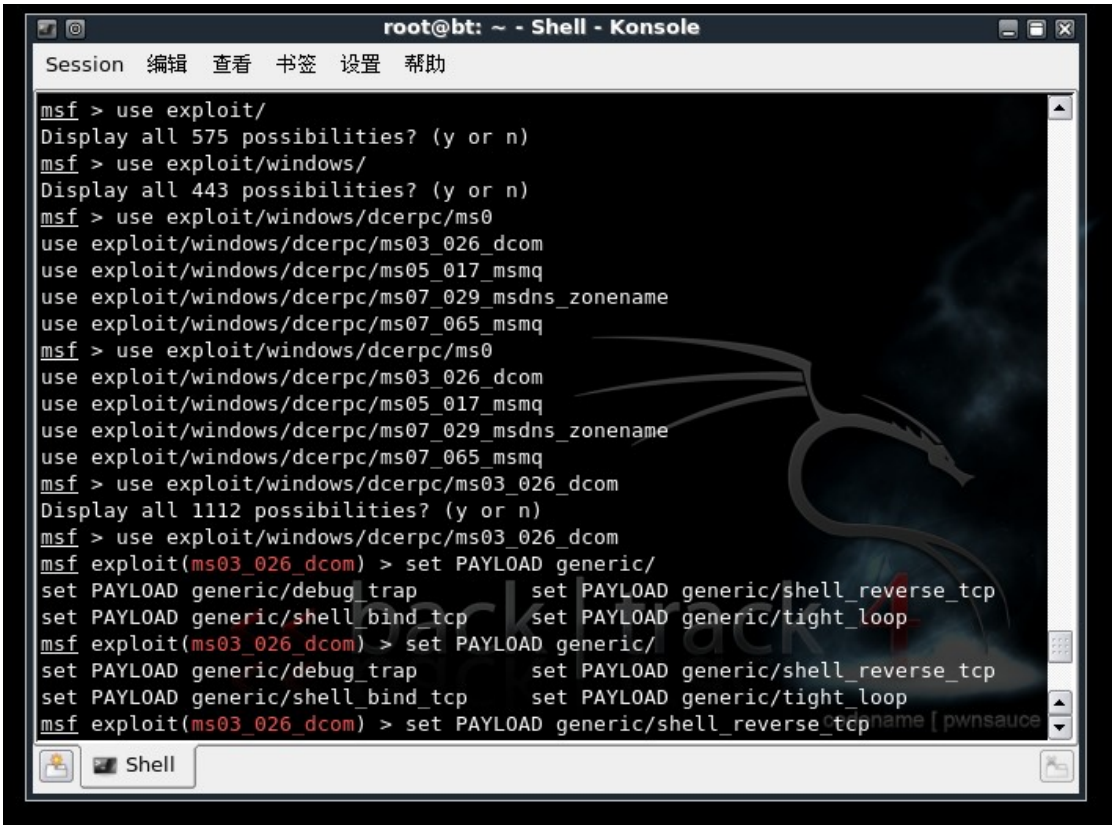


在蜜网网关监听到的数据包如下图所示。



c） 渗透攻击测试

在攻击机 Back Track 4 上运行 msfconsole，对靶机 Linux Metasploitable 进行渗透攻击，如下图所示。



在蜜网网关上监听到的数据包如下图所示。

五． 总结

通过本次实验，掌握了搭建网络攻防实验环境的方法，并且对整个实验环境有了更深刻的理解。由于吸取了其他同学的经验，本次实验完成得比较顺利。但是在使用

nmap 对靶机 Linux Metasploitable 进行扫描时发现一个问题，将使用 nmap 进行端口扫描得出的开放端口的报告与靶机真正开放的端口对比（在 VM_README_Metasploitable_ubuntu.txt 文件中），发现还有两个端口未被扫描到：netbios 137/udp 和 distccd 3632/tcp。不知道是何原因。