

1. 实验题目:网络攻防实验环境搭建与测试

2. 实验内容:

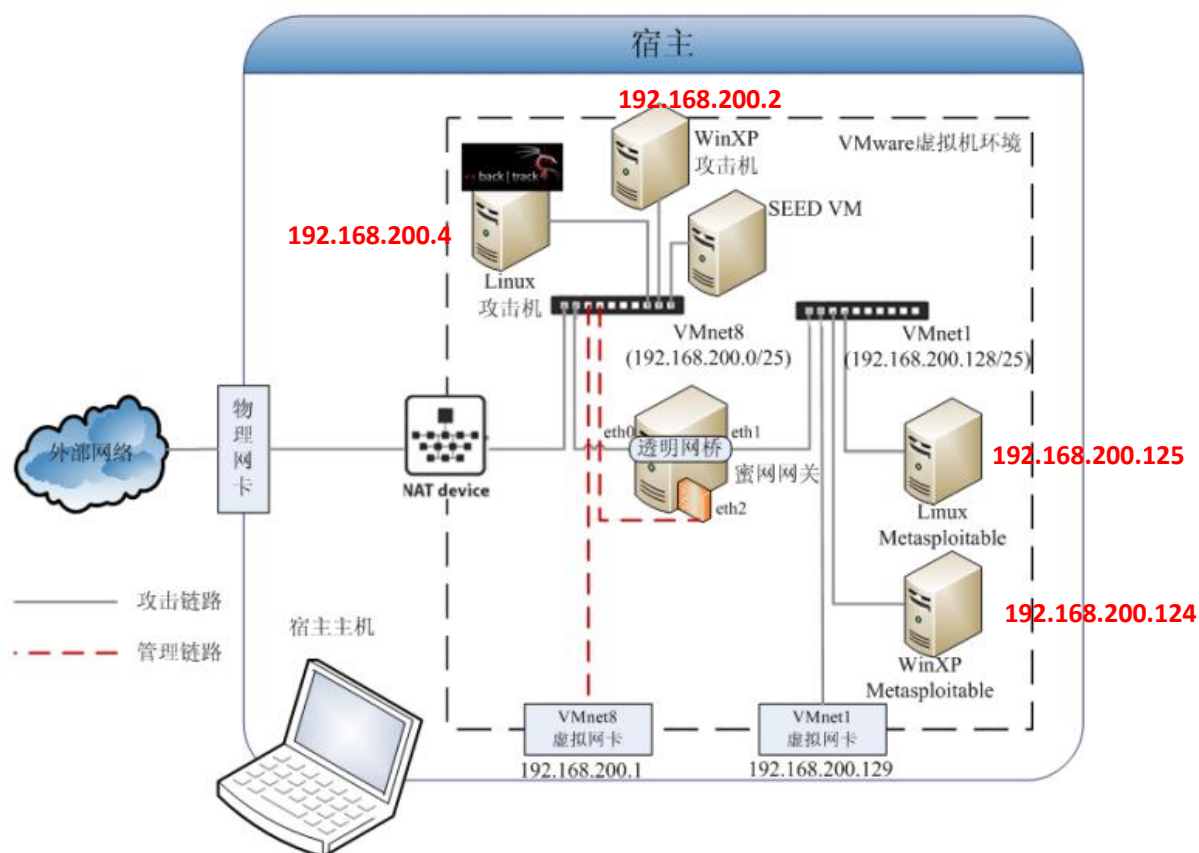
利用虚拟蜜网技术进行网络攻防实验环境构建，并进行网络连通性测试与验证。

3. 实验要求:

详细说明网络攻防实验环境的结构和组成模块；搭建和测试过程及遇到的问题；解决问题的过程、方法和收获等。

4. 实验过程:

4.1 网络攻防环境拓扑图:



4.2 攻击机、靶机及蜜网网关的配置

XP 攻击机: (网卡 NAT 模式)

```
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
```

BT4 攻击机: (网卡 NAT 模式)

```
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ea:a3:d4
          inet addr:192.168.200.4  Bcast:192.168.200.127  Mask:255.255.255.128
          inet6 addr: fe80::20c:29ff:feea:a3d4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3801 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2589750 (2.5 MB)  TX bytes:354914 (354.9 KB)
          Interrupt:18 Base address:0x2000
```

Win2000 靶机 (网卡 host-only 模式)

```
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    Description . . . . .           : VMware Accelerated A

    Physical Address. . . . .       : 00-0C-29-DB-43-95
    DHCP Enabled. . . . .           : No
    IP Address. . . . .              : 192.168.200.124
    Subnet Mask . . . . .            : 255.255.255.128
    Default Gateway . . . . .       : 192.168.200.1
    DNS Servers . . . . .            : 1.0.0.1
```

Ubuntu 靶机(网卡 host-only 模式)

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:12:43:a9
          inet addr:192.168.200.125  Bcast:192.168.200.127  Mask:255.255.255.128
          inet6 addr: fe80::20c:29ff:fe12:43a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21817 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1377 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1692405 (1.6 MB)  TX bytes:103046 (100.6 KB)
          Interrupt:17 Base address:0x2000
```

Honeywall

```
[root@roo-test ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F1:A6:1C
          UP BROADCAST RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:7692 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6360 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3028331 (2.8 MiB)  TX bytes:605068 (590.8 KiB)
          Interrupt:51 Base address:0x2000

[root@roo-test ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0C:29:F1:A6:26
          UP BROADCAST RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:7268 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:728268 (711.1 KiB)  TX bytes:293713 (286.8 KiB)
          Interrupt:75 Base address:0x2080

[root@roo-test ~]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:0C:29:F1:A6:30
          inet addr:192.168.200.8  Bcast:192.168.200.127  Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3549 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1665 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:468936 (457.9 KiB)  TX bytes:1668866 (1.5 MiB)
          Interrupt:67 Base address:0x2400
```

4.3 测试截图

(1) 在 XP 攻击机上，用 NMAP 扫描和用 metasploit 渗透攻击测试。实验截图如下：

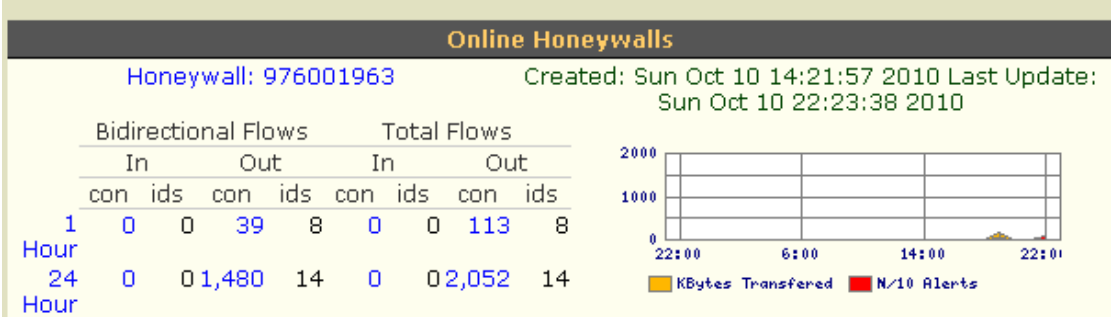


Figure 1 攻击后观察 Walleye 的摘要视图

Include	Exclude	Destination IP	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes
+++	<input type="checkbox"/>	255.255.255.255	20	0	1	1	88	22,528	0	0	8	2,048	0	
+++	<input type="checkbox"/>	224.0.1.24	4	0	1	1	4	108	0	0	1	27	0	
+++	<input type="checkbox"/>	192.168.200.129	7	0	7	2	89	6,638	54	2,148	44	3,080	9	35
+++	<input type="checkbox"/>	192.168.200.127	46	0	2	2	249	31,726	0	0	23	4,179	0	
+++	<input type="checkbox"/>	192.168.200.124	1,905	12	466	987	3,206	154,877	2,808	94,510	20	2,572	24	3,22
+++	<input type="checkbox"/>	192.168.200.2	32	2	31	9	125	8,296	81	1,868	25	5,350	30	67
+++	<input type="checkbox"/>	192.168.200.1	1	0	1	1	45	3,150	0	0	45	3,150	0	
+++	<input type="checkbox"/>	0.0.0.0	37	0	1	1	1,332	107,110	0	0	441	34,839	0	

Apply checkbox filters

Figure 2 观察 Walleye 中，192.168.200.124 靶机上流量很大

(Previous Page)	Start	1	2	3	4	5	6	7	8	9
October 10th 19:55:24	00:04:01	192.168.200.124	0	0.0.0.0						
UDP	1101 (pt2-discover)	34 kB 441 pkts -->	1101 (pt2-discover)							
0	os unkn	<--0 kB 0 pkts	---							
October 10th 19:55:36	00:00:03	192.168.200.2	0	192.168.200.124						
ICMP	8 (8)	0 kB 4 pkts ->	0 (0)							
0	os unkn	<--0 kB 4 pkts	---							
October 10th 19:56:16	00:00:00	192.168.200.2	0	192.168.200.124						
TCP	39807 (39807)	0 kB 1 pkts ->	35500 (35500)							
2	SunOS	<--0 kB 1 pkts	---							
October 10th 19:56:16	00:00:00	192.168.200.2	0	192.168.200.124						
TCP	39807 (39807)	0 kB 1 pkts ->	13782 (bpcd)							
2	SunOS	<--0 kB 1 pkts	---							
October 10th 19:56:16	00:00:00	192.168.200.2	0	192.168.200.124						
TCP	39807 (39807)	0 kB 1 pkts ->	5800 (5800)							
2	UNKNOWN	<--0 kB 1 pkts	---							
October 10th 19:56:16	00:00:00	192.168.200.2	0	192.168.200.124						
TCP	39807 (39807)	0 kB 1 pkts ->	5801 (5801)							
2	UNKNOWN	<--0 kB 1 pkts	---							
October 10th 19:56:16	00:00:00	192.168.200.2	0	192.168.200.124						
TCP	39807 (39807)	0 kB 1 pkts ->	49157 (49157)							

Figure 3 观察 Walleye 的网络连接视图，显示了扫描时每个连接的信息

```
[*] Started reverse handler on 192.168.200.2:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.200.124[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.200.124[135] ...
[*] Sending exploit ...
[*] Command shell session 1 opened (192.168.200.2:4444 -> 192.168.200.124:1106) at 2010-10-11 11:32:40 +0800
[*] The DCERPC service did not reply to our request

(C) 版权所有 1985-1998 Microsoft Corp.
C:\WINNT\system32>
```

Figure 4 Metasploit3 攻击成功时，获得了靶机的 shell

October 10th 21:55:19	00:00:01	192.168.200.2	0	192.168.200.124
TCP	3298 (deskview)	2 kB 7 pkts -	135 (epmap)	
27	Windows	<--0 kB 5 pkts	---	
October 10th 21:55:20	00:06:35	PID: 192.168.200.124	0	192.168.200.2
TCP	1084 (ansoft-lm-2)	5 kB 25 pkts 4444 (krb524)		
26	Windows	<--0 kB 30 pkts	---	
October 10th 22:02:48	00:00:01	192.168.200.2	0	192.168.200.124
TCP	3340 (anet-m)	2 kB 7 pkts -	135 (epmap)	
27	Windows	<--0 kB 5 pkts	---	
October 10th 22:02:48	00:00:01	PID: 192.168.200.124	0	192.168.200.2
TCP	1085 (webobjects)	0 kB 3 pkts -4444 (krb524)		
2	Windows	<--0 kB 3 pkts	---	

Figure 5 攻击机对靶机的 135 端口发送一个连接，然后靶机向攻击机的 4444 发送一个方向的 shell 连接

(2) 在 BT4 攻击机上，用 nmap 做 syn 扫描

```

root@bt:~# nmap -sS 192.168.200.125 syn

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-10-11 22:21 CST
Failed to resolve given hostname/IP: syn. Note that you can't use '/mask' AND
1-4,7,100-' style IP ranges
Nmap scan report for 192.168.200.125
Host is up (0.0029s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:12:43:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds
root@bt:~#

```

Figure 6 扫描获取靶机上开放的端口信息







	October 11th 02:25:30 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 2 pkts 21 (ftp) → 6 SunOS <-0 kB 1 pkts —
	October 11th 02:25:30 00:00:00 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 1 pkts 995 (pop3s) → 2 UNKNOWN <-0 kB 1 pkts —
	October 11th 02:25:30 00:00:01 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 2 pkts 80 (http) → 6 UNKNOWN <-0 kB 1 pkts —
	October 11th 02:25:30 00:00:00 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 1 pkts 5959 (5959) → 2 UNKNOWN <-0 kB 1 pkts —
	October 11th 02:25:30 00:00:00 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 1 pkts 10025 (10025) → 2 UNKNOWN <-0 kB 1 pkts —
	October 11th 02:25:30 00:00:00 192.168.200.4 0 192.168.200.125 TCP 47750 (47750) 0 kB 1 pkts 65389 (65389) →

Figure 7 Walleye 中观察扫描时的连接信息

```
10/11-02:25:30.104550 0:C:29:EA:A3:D4 -> 0:C:29:12:43:A9 type:0x800 len:0x3A
192.168.200.4:47750 -> 192.168.200.125:587 TCP TTL:51 TOS:0x0 ID:1013 IpLen:20 DgmLen:44
*****S* Seq: 0x6E74D2B5 Ack: 0x0 Win: 0x1000 TcpLen: 24
TCP Options (1) => MSS: 1460
```

=====

```
10/11-02:25:30.118245 0:C:29:12:43:A9 -> 0:C:29:EA:A3:D4 type:0x800 len:0x3C
192.168.200.125:587 -> 192.168.200.4:47750 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0x6E74D2B6 Win: 0x0 TcpLen: 20
```

Figure 8 扫描未开启的端口 587，靶机返回一个 ACK+RST 应答，NAMP 转让扫描下一个端口

忘记设置网卡属性了，这两个镜像的网卡默认都是网桥模式，BT4 网卡改为 NAT，ubuntu 改为 host-only 即可解决。最后再做连通性测试。

（5）metasploit3 攻击一次后，退出 shell。第二次及以后始终无法建立新的会话，也不能得到 shell。

解决方法：

可以在命令行中通过 netstat 查看，发现一个连接 4444 端口的目前正在被连接，所以，以后多次尝试再攻击无法成功。

在网络连接中，停用本地连接服务，然后再启用，发现原来建立的连接自动取消了。再次攻击，可以成功。

6. 实验收获

做完该实验的收获有三点：（1）对第三代蜜网有了非常清晰的认识，从原理走向实践，并能够掌握其基本的配置方法。（2）对虚拟机中的三种网卡 NAT/bridge/host-only 模式的工作方式有了了解，特别是 host-only 的工作方式。（3）通过 walleye 查看网络连接信息（图 8 和 9），对 NAMP 的 SYN 扫描的原理很直观的认识。