什么位置，由此即可大致判断出不稳定的网络结点在什么位置。我们可以通过查询 IP 地址查询下相应结点的位置。可以尝试对一个不稳定的网络进行定位和查找问题。是否还有其他的工具可以进行网络侦查？

尝试使用 Tracert 工具在 window 环境下运行，对比与 Linux 的不同之处，分析其原因。

第三部分　主机操作系统渗透技术

第9章 微软 MS07029 漏洞溢出实验

9.1 实验概述

MS07-029 漏洞全称为：Microsoft Windows DNS 服务器 RPC 接口远程栈溢出漏洞。

这是一个远程执行代码漏洞，DNS 服务器、域控制器和小型企业服务器受到此漏洞威胁最大。攻击者向有该漏洞的系统发送特制的 RPC 报文的话，触发这个溢出，导致 DNS 服务的安全环境可以执行任意指令，完全控制靶机。

9.2 实验目的

1、了解漏洞的形成情况；

2、利用该漏洞获取靶机的 CMDshell。

9.3 实验原理

在靶机已经开启 dns server 的服务和 53、445 端口的情况下，攻击者利用 MS07029 漏洞对靶机进行攻击。首先使用 kali 虚拟机扫描靶机，确保开启了 53 和 445 端口后，使用 windows 虚拟机上的 dns.exe 工具进行溢出，开启 1100 端口作为后门；最后使用 nc 工具连接 1100 端口，控制靶机。

一、漏洞原理

远程过程调用 (RPC) 是一种协议，程序可使用该协议向网络中另一台计算机上的程序请求服务。由于使用 RPC 的程序不必了解支持通信的网络协议的情况，因此 RPC 提高了程序的互操作性。在 RPC 中，发出请求的程序是客户程序，而提供服务的程序是服务器。

DNS 服务器的 RPC 接口在处理畸形请求时存在栈溢出漏洞，影响 DNS 服务器、域控制器和小型企业服务器。如果远程攻击者能够向有漏洞的系统发送特制的 RPC 报文的话，就可以触发这个溢出，导致 DNS 服务的安全环境可以执行任意指令，一台主机甚至整个服务器环境。成功利用此漏洞的攻击者可以远程完全控制受影响的系统，安装程序，查看、更改或删除数据，或者创建拥有完全用户权限的新账户等。

在利用 MS07-029 远程溢出漏洞攻击前，首先找到攻击目标。由于启用了 RPC 服务的 Windows 系统往往会开放 53 和 445 端口，因此攻击者只要使用专业端口扫描工具扫描，即可获取可溢出的主机列表。

曾经的冲击波、震荡波等大规模攻击都是由于 Windows 的 RPC 服务漏洞造成的，MS07-029 远程溢出漏洞也不例外。除了 Windows XP 和 Windows Vista 不会受到这一 DNS 漏洞的影响，Windows 2000 Server SP4、Windows Server 2003 SP1、Windows Server 2003 SP2 都存在这个漏洞。

该远程溢出漏洞危害大，不可不防。这个安全漏洞影响到 Windows 2000 Server 和 Windows Server 2003 服务器软件。每一种语言版本的 Windows 服务器都有相应的补丁，可以根据具体情况下载补丁。

二、Nmap

Nmap 具有实用功能：通过 tcp/ip 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 PING 侦测下属的主机、欺骗扫描、端口过滤探测、直接的 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述。nmap 被开发用于允许系统管理员察看一个大的网络系统有哪些主机以及其上运行何种服务。它支持多种协议的扫描如 UDP，TCP connect()，TCP SYN (half open)，ftp proxy (bounce attack)，Reverse-ident，ICMP (ping sweep)，FIN，ACK sweep，Xmas Tree，SYN sweep 和 Null 扫描。一些常用的参数说明：

表 9.1 nmap 常用参数说明

-sL	仅仅是显示,扫描的 IP 数目,不会进行任何扫描
-sn	ping 扫描,即主机发现
-Pn	不检测主机存活
-sS	TCP SYN 扫描，半开放扫描，扫描速度快，不易被注意到（不完成 TCP 连接）
-sT	TCPConnect()，建立连接，容易被记录；对原始报文控制少，效率低
-sU	激活 UDP 扫描，对 UDP 服务进行扫描，如 DNS/SNMP/DHCP 等，可以和 TCP 扫描结合使用；效率低，开放的和被过滤的端口很少响应

三、Netcat

NetCat（简称 nc），是一款基于 tcp/ip 协议（c/s 模型的）的“瑞士军刀”，可以当作服务器或客户端、端口扫描、端口转发、数据传输等。常用功能：

1、 监听：**nc.exe -vv -l -p 4400**

该命令表示在本地 4400 端口上进行监听。-vv：显示详细的信息；-l：监听入站信息；-p：监听所使用的端口号。

2、连接对方端口：**nc.exe -vv 192.168.5.1 5000**

该命令表示连接 ip 为 192.168.5.1 的 5000 端口。

3、在本地监听端口的同时绑定 shell：**nc.exe -l -p 5555 -t -e cmd.exe**

此时相当于一个 telnet 服务端。在肉鸡上执行该命令，攻击机连接上去可获得 shell。该命令表示在本机 5555 端口上监听并绑定 cmd.exe。-e：程序定向；-t：以 telnet 的形式应答。

4、提交数据包，端口通常为 80：**nc.exe -vv 127.0.0.1 80 <yan.txt**

向 ip 为 127.0.0.1 的 80 端口提交 yan.txt 中的内容。

9.4 实验环境

系统环境：Windows 2003 系统虚拟机两台，其中靶机系统为 windows 2003 SP1
kali linux 虚拟机一台

实验工具：Kali 自带 nmap 工具
dns.exe（在 E:\工具包\dns 文件夹下）
nc 工具（在 E:\工具包\NC（NetCat）文件夹下）

结束

9.5 实验步骤

1、 **靶机开启 DNS Server 服务**

点击“开始->运行”（Win+R），输入“**services.msc**”，打开“服务”，找到“DNS Server”右键点击“重新启动”；如果未启动，双击打开属性设置.