电子科技大学信息与软件工程学院

标准实验报告

（实验）课程名称网络安全技术

电子科技大学教务处制表

电子科技大学

实　验　报　告

学生姓名：　　学 号：　　指导教师：

实验地点：　　实验时间：

一、实验室名称：

二、实验项目名称：CMD 命令与端口扫描实验

三、实验学时：　4　学时

（一）实验目的

熟悉 PING、NSLOOKUP 等网络命令的使用。通过使用网络扫描软件了解主机端口和服务的开放情况，从而进一步获取系统信息，找出系统安全漏洞。本实验中将使用 X-SCAN 来进行主机和网络扫描。通过本次试验，读者可以了解到端口（port）与服务（service）开放的风险，增强在计算机系统和网络安全防护方面的意识。

（二）实验内容

（1）了解 ping 命令的原理和功能，以及相关参数。

（2）了解 nslookup 命令的原理和功能，以及相关参数。

（3）了解 tracert 命令的原理和功能，以及相关参数。

（4）使用 X-SCAN 对特定主机进行扫描。

四、实验原理

配置好 DNS 服务器，添加了相应的记录之后，只要 IP 地址保持不变，一般情况下我们就不再需要去维护 DNS 的数据文件了。不过在确认域名解释正常之前我们最好是测试一下所有的配置是否正常。使用 ping 命令可以检查网络联通情况，不过 Ping 指令只是一个简单检查命令，虽然在输入的参数是域名的情况下会通过 DNS 进行查询，但是它只能查询 A 类型和 CNAME 类型的记录，而且只会告诉你域名是否存在，其他的信息一概欠奉。所以如果你需要对 DNS 的故障进行排错就必须熟练另一个更强大的工具 nslookup。这个命令可以指定查询的类型，可以查到 DNS 记录的生存时间还可以指定使用那个 DNS 服务器进行解释

TTL：(Time To Live)生存时间,是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地。例如，不正确的路由表可能导致包的无限循环。一个解决方法就是在一段时间后丢弃这个包，然后给发送者一个报文，由发送者决定是否要重发。TTL 的初值通常是系统缺省值，是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围，超过此时间就把包丢弃。由于每个路由器都至少要把 TTL 域减一，TTL 通常表示包在被丢弃前最多能经过的路由器个数。当记数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。

五、实验器材（设备、元器件）

（一）学生每人一台 PC，安装 WindowsXP/2000 操作系统。两人一组。
（二）局域网络环境。
（三）个人 PC 安装网络扫描软件 X-SCAN。

六、实验步骤

（一）Ping 命令

（1）使用 cmd 命令进入 DOS 命令窗口。

（2）使用 ping /?或直接输入 ping 后回车进入 ping 帮助界面，了解 ping 命令参数和功能含义。

（3）使用“ping　IP 地址”和“ping －t　IP 地址”，测试目标主机可达性，记录返回信息，比较两者的不同。

（4）解析主机名(netbios)，使用“ping －a　IP 地址”，记录返回信息。

（5）自定义 ping 数据包的大小和数量，“ping　-l xx　-n xx　IP 地址”，记录返回信息。

（6）使用“ping IP 地址”命令，分析到达目的主机经过的路由数。

（7）常见操作系统的默认 TTL 值。

TTL=32 Windows 9x/Me
TTL=64 LINUX
TTL=128 Windows 200x/XP
TTL=255 Unix

修改本机的 TTL 值。

打开注册表编辑器，展开“HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Tcpip/Parameters”，找到“DefaultTTL”，将该值修改为十进制的小于 255 的数字，如果没有“DefaultTTL”项，那么新建一个 DWORD 类型的“DefaultTTL”项并指定希望设置的值，然后重启机器。修改前后使用“ping 127.0.0.1”命令，分析结果是否不同。

（二）Nslookup 命令

（1）查询 IP 地址， nslookup 最简单的用法就是查询域名对应的 IP 地址，包括 A 记录和 CNAME 记录，如果查到的是 CNAME 记录还会返回别名记录的设置情况。使用“nslookup www.uestc.edu.cn 或 www.sina.com.cn”命令。

（2）指定查询记录类型的指令格式如下：

nslookup –qt=类型 目标域名

注意 qt 必须小写。

类型可以是一下字符，不区分大小写：

A 地址记录(Ipv4)

AAAA 地址记录（Ipv6）

CNAME 别名记录

MX 邮件服务器记录

NS 名字服务器记录

PTR 反向记录（从 IP 地址解释域名）

使用“nslookup –qt=mx 或 ns uestc.edu.cn 或 sina.com.cn”命令。

（3）在默认情况下 nslookup 使用的是我们在本机 TCP/IP 配置中的 DNS 服务器进行查询，但有时候我们需要指定一个特定的服务器进行查询试验。通过指定服务器直接查询授权服务器的结果避免其他服务器缓存的结果。命令格式如下：

nslookup [-qt=类型] 目标域名 指定的 DNS 服务器 IP 或域名

如“nslookup -qt=ns edu.cn 202.112.0.35”或“nslookup -qt=ns uestc.edu.cn 202.112.14.161”命令。

（4）检查域名的缓存时间需要我们使用一个新的参数：-d。

使用“nslookup –d [其他的参数] 目标域名 [指定的服务器地址]”，分析结果，ttl 数值就是域名记录的生存时间。

（三）tracert 命令

（1）在命令提示符窗口中输入：Tracert。了解该命令的详细参数说明。

（2）输入 tracert www.uestc.edu.cn，查看到达目的地所经过的路由。

（3）输入：tracert –d www.uestc.edu.cn。参数-d的意思是指定不将 IP 地址解析到主机名称

（4）输入：tracert –h 10 www.uestc.edu.cn，指定最大10跳。

（四）X-SCAN 端口扫描软件

（1）设置检测范围：实验室子网段或一段 IP 地址；

（2）设置扫描模块；

（3）设置并发扫描及端口相关设置：并发线程值越大速度越快建议为 500，并发主机值越大扫描主机越多建议为 10，建议跳过 PING 不通的主机；

（4）设置待检测端口，确定检测方式；

（5）记录扫描结果，分析结果内容。

（五）简单端口扫描软件设计

编制一个可通过 TCP Connect 进行端口扫描的简单程序，支持对单 IP 的连续端口进行扫描。

参考命令行：程序名 IP startport stopport

七、实验数据及结果分析

(按实验步骤顺序填写代码、数据或截图，并进行简要文字说明，评分标准：实验内容完整 70%，文字说明清晰 20%，报告格式规范 10%)

八、实验结论、心得体会

九、对本实验过程及方法、手段的改进建议

报告评分：

指导教师签字：