DOI:10.13844/j.cnki.jxddxb.2011.02.013

TCP/IP 协议的安全性浅析

李龙光,何伊斐
(江西电视广播大学 江西 南昌 330046)

摘 要:人们在享受网络技术带来的便利的同时,安全问题逐渐引起关注,成为计算机领域的研究热点之一。本文在介绍互联网中所使用的 TCP/IP 协议的基础上,对 TCP/IP 协议的安全性进行了较细致的讨论,从理论上分析了协议中几种主要的安全隐患,并提出了相关处理办法。

关键词:TCP/IP;安全;协议
中图分类号: 文献标识码:A 文章编号:1008-3537(2011)02-0075-04

引言

TCP/IP 协议组是目前使用最广泛的网络互连协议。但 TCP/IP 协议组本身存在着一些安全性问题。按照 OSI 体系划分,TCP/IP 协议可分为数据链路层、网络层、传输层和应用层。本文将按照顺序从底层到高层的顺序对 TCP/IP 协议现有的主要安全机制进行一些分析,并对提升协议安全的可能性提出一些构想。

TCP/IP 作为 Internet 使用的标准协议集,加之 TCP/IP 自身的缺陷、网络的开放性,成为黑客实施网络攻击的重点目标。TCP/IP 协议是在可信赖的环境之下建立的,考虑到网络互连缺乏对安全方面的考虑,这种基于地址的协议本身就会泄露口令,而且经常会运行一些无关的程序,这些都是网络本身的缺陷。互连网技术屏蔽了底层网络硬件细节,使得异种网络之间可以互相通信。这就给黑客们攻击网络以可乘之机。由于大量重要的应用程序都以 TCP 作为它们的基本传输层协议,所以 TCP 的安全性问题会给网络带来非常严重的后果。

1 TCP/IP 协议的基本知识

1.1 TCP/IP 的历史概述

TCP/IP(Transmission Control Protocol/Internet Protocol 的简写,中文译名为传输控制协议/互联网络协议)协议是当今 Internet 最基本的协议。

在 1969 年,为美苏冷战期间,美国政府机构试图发展出一套机制,用来连接各个离散的网络系统,以应付战争危机的需求。这个计划,就是由美国国防部委托 Advanced Research Project Agency 发展的 ARPANET 网络系统,研究当部份电脑网络遭到攻击而瘫痪后,是否能够通过其他未瘫痪的线路来传送资料。

ARPANET 的构想和原理,包括了一组电脑通信细节的网络标准,以及一组用来连接网络和选择网络交通路径的协议,就是大名鼎鼎的 TCP/IP 网际网络协议。从 1985 年开始,TCP/IP 网络迅速扩展至美国 欧洲好几百个大学 政府机构 研究实验室。它的发展大大超过了人们的预期,而且每年以超过 15% 的速度成长,到了 1994 年,使用 TCP/IP 协议的电脑已经超过三百万台之多。及后数年,由于 Internet 的爆炸性成长,TCP/IP 协议已经成为无人不知 无人不用的电脑网络协议了[1]。

1.2 TCP/IP 参考模型

TCP/IP 协议的开发研制人员将 Internet 分为四个层次,以便于理解,它也称为互联网分层模型或互联网分层参考模型,如图 1.1:

[收稿日期] 2011-03-08
[作者简介] 李龙光,男,江西广播电视大学开放学院教师,研究方向:网络技术;
何伊斐,男,江西广播电视大学开放学院教师,研究方向:网络技术。

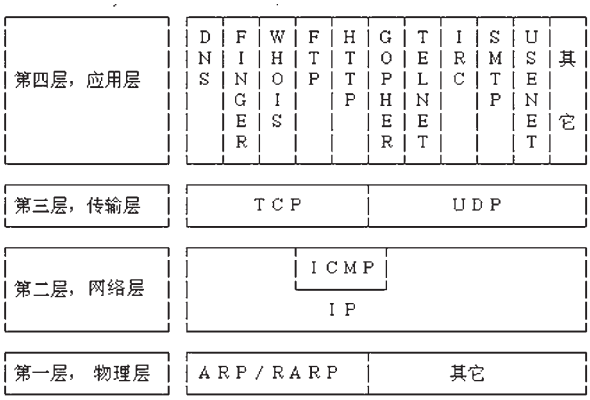

图 1.1 TCP/IP 参考模型

物理层：对应于网络的基本硬件，这也是 Internet 物理构成，即我们可以看得见的硬件设备，如 PC 机、互连网服务器、网络设备等，必须对这些硬件设备的电气特性作一个规范，使这些设备都能够互相连接并兼容使用。

网络层：即 Internet 层，定义了互联网中传输的“信息包”格式，以及从一个用户通过一个或多个路由器到最终目标的“信息包”转发机制。

传输层：为两个用户进程之间建立、管理和拆除可靠而又有效的端到端连接。

应用层：它定义了应用程序使用互联网的规程。

1.3　TCP/IP 的几个常用命令

(1) ping

当网络运行中出现故障时，采用这个实用程序来预测故障和确定故障源是非常有效的。如果 ping 不成功，则可以推断故障出现在以下几个方面：网线是否连通，网络适配器配置是否正确，IP 地址是否可用等；如果执行 ping 成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面，ping 成功只能保证当前主机与目的主机间存在一条连通的物理路径。它还提供了许多参数，如–t 使当前主机不断地向目的主机发送数据，–n 可以自己确定向目的主机发送的数据帧数等等，使用 Ctrl+C 可以中断 ping 命令[2]。

```
C:\>ping www.sina.com.cn
Pinging www.chinacache.sina.com.cn [61.163.239.134] with 32 bytes of data:
//从 61.163.239.134 返回信息情况
Reply from 61.163.239.134: bytes=32 time=821ms TTL=242
Reply from 61.163.239.134: bytes=32 time=1081ms TTL=242
Request timed out. //超时
Request timed out. //超时
Ping statistics for 61.163.239.134:      //发送、接收和丢失包的情况
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),  //整个过程所花费的时间
Approximate round trip times in milli-seconds:
Minimum = 821ms, Maximum =  1081ms, Average =  475ms
```

图 1.3 ping 示意图

(2) tracert

这个程序的功能是判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。还可以使用参数–d 决定是否解析主机名。

```
C:\>tracert www.sina.com.cn
//跟踪路由 202.108.37.40，最多 30 跳
Tracing route to tucana.sina.com.cn [60.28.175.136]  //DNS 解析到的 sina 服务器 IP
over a maximum of 30 hops:
  1    *       *       *     Request timed out.
  2    30 ms    30 ms    31 ms  117.8.5.157
  3    31 ms    31 ms    31 ms  117.8.1.133
  4    31 ms    31 ms    30 ms  117.8.1.154
  5    31 ms    31 ms    31 ms  60.28.31.86
  6    31 ms    31 ms    31 ms  60.28.253.162
  7    31 ms    31 ms    31 ms  60.28.175.136
Trace complete. //跟踪结束
```

图 1.4 tracert 示意图

(3) netstat

这个命令可以看到当前网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，如协议类型、当前主机与远程主机的 IP 地址以及它们之间的连接状态等。常用的参数为：–e 用以显示以太网的统计信息；–s 显示所有协议的使用状态，这些协议包括 TCP、UDP 和 IP，一般这两个参数都是结合在一起使用的–se。另外–p 可以选择特定的协议并查看其具体使用信息，–n 以数字形式显示地址和端口号，–a 可以显示所有主机的端口号，–r 则显示当前主机的详细路由信息。

```
C:\netstat -n
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1521         127.0.0.1:1522         ESTABLISHED
  TCP    192.168.1.100:1654     209.85.133.100:443     CLOSE_WAIT
  TCP    192.168.1.100:2649     194.129.79.23:80       LAST_ACK
  TCP    192.168.1.100:2681     210.52.223.34:80       TIME_WAIT
  TCP    192.168.1.100:2714     194.129.79.23:80       FIN_WAIT_1
```

图 1.5 netstat 示意图

(4) ipconfig

对于一个陌生的计算机网络环境，要了解自己计算机的网络配置参数，可以使用这个命令轻松实现，ipconfig /all。

```
C:\>ipconfig /all
Windows IP Configuration    //IP 配置
      Host Name . . . . . . . . . . . . : xxxx  //主机名
      Primary DNS Suffix  . . . . . . . :  //主 DNS
      Node Type . . . . . . . . . . . . : Unknown  //节点类型
      IP Routing Enabled. . . . . . . . : No  //IP 路由使能
      WINS Proxy Enabled. . . . . . . . : No //WINS 代理使能
Ethernet adapter 本地连接:
      Connection-specific DNS Suffix  . : //连接指定的 DNS
      Description . . . . . . . . . . . : NVIDIA nForce Networking Controllerr//
网卡类型
      Physical Address. . . . . . . . . : 00-11-D8-6B-C2-F1//物理地址
      DHCP Enabled. . . . . . . . . . . : No  //DHCP 使能
      IP Address. . . . . . . . . . . . : 192.168.0.7  //IP 地址
      Subnet Mask . . . . . . . . . . . : 255.255.255.0  //子网掩码
      Default Gateway . . . . . . . . . : 192.168.0.1  //默认网关
```

图 1.6 ipconfig 示意图

2 TCP/IP 协议安全性能分析

2.1 TCP/IP 协议的缺陷分析

TCP/IP 协议的设计与实现使不同计算机之间、不同操作平台之间的通信成为可能。但是,TCP/IP 协议是在网络规模不大、应用范围不广、计算机技术尚不够发达的情况下设计与实现的,当时的一种普遍认识是:安全性同题是上层的问题与底层协议无关,因此 TCP/IP 在安全性方面做得不够完善。随着网络规模、计算机技术的日益发展,TCP/IP 存在的不可克服的脆弱性,越来越阻碍着 TCP/IP 的进一步广泛使用,也难以满足未来网络发展的需求。由于 TCP/IP 协议族本身存在一些安全缺陷, 所以即使正确地实现了它,TCP/IP 网络仍会受到攻击。像序列号欺骗、路由攻击、源地址欺骗和授权欺骗等。对于 TCP/IP 协议族的安全缺陷可得出三个结论:

(1)依赖于 IP 源地址的认证是极其不安全的;

(2)大量的入侵都源于序列号攻击;

(3)大多数网络控制机制都是危险的,而且基于以太网的数据包易被监听, 入侵者甚至可以更改 IP 或 MAC 地址,致使攻击方式更加复杂。[3]

2.1.1 数据链路层的脆弱性

在以太网中,数据以“帧”为单位进行传输。任何主机发送的帧都会到达与其处于同一网段的所有主机的网络接口,而每一个网络接口都有一个唯一的硬件地址,即网卡的 MAC 地址。信息以数据包的形式传送,其报头包含了目的主机的 MAC 地址, 如果其携带的 MAC 地址是自己的或者是广播地址, 那么就会将数据帧交给 IP 层,否则丢掉。网络上也存在一些能接收所有数据包的接口,攻击通过某些手段使网卡工作在监听模式下, 从而达到非法窃取他人信息的目的。[4]

处理方法:

(1)对网络中传输的数据进行加密,使攻击方无法正确还原窃取的数据,并且传输的数据是经过压缩的,可以加快传输的速度。

(2)安装检测软件,做到防范于未然。

(3)改用交换式的网络拓扑结构。因为在交换式以太网中,数据只会被发往目的地址的网卡,其他网卡接收不到数据包,但是交换机的成本比较高。

2.1.2 网络层的脆弱性

(一) IP 协议的安全性能分析

IP 协议是 TCP/IP 的心脏,也是网络层中最重要的协议。IP 层接收由更低层发来的数据包,并把该数据包发送到更高层 TCP 或 UDP 层;IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层但是 IP 数据包是不可靠的,它不能确认数据包是按顺序发送的或者没有被破坏。IP 数据包中含有发送它的主机的地址(源地址)和接收它的主机的地址(目的地址),高层的 TCP 和 UDP 服务在接收数据包时,通常假设包中的源地址是有效的。IP 地址形成了许多服务的认证基础, 这些服务相信数据包是从一个有效的主机发送来的。IP 确认包含一个 IP 地址的源路径选项。可以用来指定一条源地址和目的地址之间的直接路径。对于一些 TCP 和 UDP 的服务来说,使用了该选项的 IP 包好象是从路径上的最后一个系统传递过来的,而不是来自于它的真实地点。IP 源路径是为了测试而存在的, 说明了它可以被用来欺骗系统进行平常被禁止的连接,许多依靠 IP 源地址做确认的服务将产生问题并且会被非法人侵。IP 源路径允许 IP 数据包自己选择一条通往系统目的主机的路径。设想攻击者试图与防火墙后面的一个不可到达的主机 A 连接。他只需要在送出的请求报文中设置 IP 源路径选项,使报文有一个目的地址指向防火墙,而最终地址是主机 A。当报文到达防火墙时被允许通过,因为它指向防火墙而不是主机 A 防火墙的 IP 层处理该报文的源路径被改变,并发送到内部网上,报文就这样到达了不可到达的主机 A。[5]

处理方法:

(1)尽量减少计算机间的信任关系,对可以获得计算机之间信任关系的命令必须采取限制措施。

(2)在网络配置上加以防御,对子网外发起的攻击,可以设置路由器和防火墙来阻断非子网内的 IP 的连入,同时过滤掉有源路由的数据报文, 对子网内部则要采用加密 TCP 来加密数据,以防数据被修改。

(二) ICMP 漏洞用来传送一些关于网络和主机的控制信息,如目标主机是不可到达的、路由的重定向等。常用的 Ping 命令就是使用 ICMP 协议。Ping 程序是通过发送一个 ICMP 回应请求消息和接收一个响应的 ICMP 回应来测试主机的连通性。通常也可以得到一些附加信息,如收发数据包的往返时间。

处理方法:

(1)给操作系统定期打上安全补丁。

(2)利用防火墙来阻止 Ping,然而这样也会阻挡一些合法应用,所以只需阻止被分段的 Ping。这样在大多数系

统上只允许一般合法的 64Byte 的 Ping 通过，就能挡住那些长度大于 MTU 的 ICMP 数据包，从而防止此类攻击。

(三)ARP 欺骗，即 ARP 重定向，就是向目标主机发送报文，其中含有攻击者伪造的 IP 地址和 MAC 地址，目标主机收到该报文后，会用报文中伪造的信息刷新 ARP 缓存。如果攻击者定时向目标主机发送该报文，而且时间间隔比 ARP 缓存的超时间隔小的话，目标主机就会一直维持着一张含有错误信息的 ARP 缓存表。[6]

处理方法：

(1)使用静态的 IP 地址至硬件地址的对应表，最简单的办法是将 IP 地址和硬件地址进行静态绑定。

(2)定期检查 ARP 请求，使用 ARP 监视工具监视并探测网络中的 ARP 欺骗。

2.1.3 传输层的脆弱性

主要是 TCP 会话劫持，TCP 会话劫持与 IP 欺骗不一样，IP 欺骗是针对 TCP 三次握手过程进行的攻击，而 TCP 会话劫持是跳过连接过程，对一个已经建立的连接进行攻击。TCP 通过三次握手建立连接以后，主要采用滑动窗口机制来验证对方发送的数据。如果对方发送的数据不在自己的接收窗口内，则丢弃此数据这种发送序号不在对方接收窗口的状态称为非同步状态。当通信双方进入非同步状态后，攻击者可以伪造发送序号在有效接收窗口内的报文，也可以截获报文，篡改内容后，再修改发送序号而接收方会认为数据是有效数据。[7]受这种攻击的主要原因来自于 TCP/IP 协议本身的脆弱点，TCP 协议并不对数据包进行加密和认证，确认数据包的主要根据就是判断序列号是否正确。

处理方法：

(1)最主要的方法是在传输层对数据进行加密。

(2)使用安全协议，对通信和会话加密，如使用 SSH 代替 Telnet。

(3)加强认证，不仅在建立会话时进行认证，还要对同一个 IP 发出的多个 SYN 请求报文进行限量，使主机对应的 TCP 端口资源不能耗尽，保证合法用户对主机的该端口能够正常使用。

(4)在主要的网段中安装入侵检测系统。

2.1.4 应用层的脆弱性

DNS 欺骗是一种复杂的攻击，但比 IP 欺骗要简单。攻击者伪造机器名称和网络的信息，当主机需要将一个域名转化为 IP 地址时，向某 DNS 服务器发送一个查询请求。同样，将 IP 地址转化为域名时，可发送一个反查询请求。如果服务器在进行 DNS 查询时人为地给出攻击者自己的应答信息，DNS 欺骗就会产生。因为网络上的主机都信任 DNS 服务器，一个被破坏的 DNS 服务器就可以将客户引导到非法的服务器。

处理方法：

(1)直接用 IP 访问重要的服务，可以避开 DNS 欺骗攻击。

(2) 最根本的解决办法就是加密所有对外的数据流。对服务器来说，尽量使用 SSH 等有加密支持的协议。

结束与展望

本论文在讨论了 TCP/IP 协议的基础上，分析了网络主机截获 IP 数据包的可行性，然后根据 TCP/IP 协议中定义的字段含义进行篡改，实现黑客的功能。TCP/IP 协议作为未来互联网发展的基本目标之一，其安全显得越来越重要，随着其技术在不断完善和发展，新的标准和规范在不断的制定，展望未来网络的发展，可以预见，Internet 未来安全的功防对决还将继续，TCP/IP 协议的安全机制也会越来越完善。一个全新的网络世界也会随之到来。

参考文献：

[1]w.Richard Stevens 著，TCP/IP 协议详解[M].机械工业出版社，2000.4

[2]胡道元，计算机局域网[M].清华大学出版社，2003

[3]辛志东，李祥和等.局域网中的 ARP 重定向攻击及防御措施[M].计算机信息，2005

[4]楚狂.网络安全与防火墙技术[M]人民邮电出版社，2000

[5]卢津榕，冯宝坤.解读黑客[M].希望电子出版社，2001

[6]谢谦.计算机网络实验教程[M].电子工业出版社，2000

[7]徐国爱.网络安全[M].北京邮电大学出版社，2004

责任编辑：刘石玉
校　　对：里　仁