Network Security Survey

Xiaoli Jia[1], Yixian Wen[2]
[1] *Hebei University of Engineering，educational technologies center，Han Dan，China，056038*
[2] *Hebei University of Engineering，educational technologies center，Han Dan，China，056038*
Email: jxl6cjh1ct1@163.com , yixianlmp@qq.com

Abstract: The article has discussed from the method of threatening the security of network and security tactics how to carry on the management of the online security.

Keywords: Network management; Online security; Security countermeasure

网络安全管理概论

贾晓丽[1]，温逸娴[2]
[1] 教育技术中心,河北工程大学,邯郸,中国,056038
[2] 教育技术中心,河北工程大学,邯郸,中国,056038
Email: jxl6cjh1ct1@163.com, yixianlmp@qq.com

摘　要: 文章从威胁网络安全的方法及其安全策略方面探讨了如何进行网络安全的管理。

关键词: 网络管理; 网络安全; 安全性对策

1 网络安全概论

随着人类步入信息社会以及全球“信息高速公路”建设的蓬勃发展，在社会信息化和信息社会化的进程中，数据通信和计算机网络扮演了越来越重要的角色。概略地说，计算机网络是通过各种通信手段相互连接起来的计算机组成的复合系统，它利用通信设备和线路将地理位置不同的信息交换方式及网络操作系统等共享，包括硬件资源和软件资源的共享。

网络本身的共享性、开放性、 广泛性给广大使用者带来了巨大的方便，但我们从网络获取大量信息的同时，随之而来的是互联网上的不良信息、非法入侵、系统漏洞、病毒等一系列问题对应用系统产生的巨大威胁。当前，平均每 20 秒就发生一次入侵计算机网络的事件，超过 1/3 的互联网防火墙被攻破！因此，网络管理就显得尤为重要。

一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。国际标准化组织 ISO 在 ISO IEC7498-4 中定义并描述了开放系统互连，即 OSI 管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为，通常对一个网络管理系统需要定义以下内容：

（1）系统的功能，即一个网络管理系统应具有哪些功能。

（2）网络资源的表示， 网络管理很大一部分是对网络中资源的管理，网络中的资源就是指网络中的硬件、软件以及所提供的服务等，而一个网络管理系统必须在系统中将它们表示出来，才能对其进行管理。

（3）网络管理信息的表示，网络管理系统对网络的管理主要靠系统中网络管理信息的传递来实现，网络管理信息应如何表示、怎样传递、传送的协议是什么，这都是一个网络管理系统必须考虑的问题。

（4）系统的结构，即网络管理系统的结构是怎样的。

2 网络安全被攻击的方法

2.1 “弱”口令

Internet 上的很多入侵是由于采用了“弱”口令，即比较容易猜的而且是不变的口令。在 Internet 上，有两种常用方法可以获得用户的口令：一个是采用网络监视的方法，另一个是分析口令文件。Unix 中的口令以密码形式存放在一个文件中，这个文件是比

较容易得到的，得到这个文件后可以通过很多分析程序或其他方法来分析，如果口令是“弱”的，即长度小于 8 个字符、英语单词或词组、重要日期等，那么分析是十分容易的。

2.2 IP 地址伪装

Indternet 上另一个常用的办法是伪装 IP 地址，一般一个服务器都有相应的可信度客户机地址，这样攻击者可以利用 IP 源路由把自己伪装成可信的客户机地址。

2.3 电子邮件地址伪装

由于 SMTP（Simple Mail Transfer Protocol 即简单邮件传输协议，是一种提供可靠且有效电子邮件传输的协议，主要用于传输系统之间的邮件信息并提供与来信有关的通知）它是十分简单的协议，并不支持安全特性，它可以接受任意主机来的 SMTP 命令，可以把“MAIL FROM:”信息段设定为任意电子邮件地址，这样用户就可以输入和他自己不同的电子邮件地址来欺骗对方。

2.4 有缺陷的 LAN 服务

一些 LAN（Local Area Network）网络服务（如 NIS，即网络信息系统 Network Information System、NFS，即网络文件系统 Network File System）可以极大地简化网络的管理，特别是口令的管理，但是同时也带来了安全方面的缺陷。有些服务本质上是不安全的，比如 NFS，它并不对用户授权，而是对主机授权，一旦授权，它对主机上谁在使用就不能控制，这也能造成安全问题。

2.5 相互信任

某些服务，如 rlogin 即远程登录等，采用相互信任的方法，一旦信任，一台主机上的用户在登录到另一台计算机上去时不再要求给出口令。这种方法的一个好处是用户管理方便，并且在网络上不再传递口令，减少了口令被监听的可能性，但是一旦一个系统被攻破，相互信任的所有系统都可能被入侵。

3 网络的安全性策略

3.1 身份鉴别

其基本模型举例如下：一个用户张三（实际上是一个进程）希望和另一个用户李四建立一条安全的连接，两者之间需要交换信息，另外，有一个入侵者王五，他要截取张三和李四之间交换的信息，并且可能修改、增加有关信息。

然而，一旦身份鉴别协议完成，该协议可以为张三和李四建立一个秘密的对话密钥，张三可以确认对方就是李四，而不是别人，反之依然。

3.2 数字签名

数字签名基于加密技术，是加密技术在认证领域的一个应用，它就是指信息发送者用其私有密钥对从所传报文中提取出的特征数据（或称数字指纹）进行 RSA（Rivest-Shamir-Adleman）算法操作，以保证发信人无法抵赖曾发过该信息（即不可抵赖性），同时也确保信息报文在经签名后未被篡改（即完整性）。当信息接收者收到报文后，就可以用发送者的公钥对数字签名进行验证。

3.3 防火墙技术

防火墙不是简单的能提供网络安全功能的路由器、主机系统或系统的集合，而是一个安全的方法，它对网络提供服务和访问定义并实现更大的安全策略。防火墙的主要目的是对受保护的网络实现访问控制，它要求所有对网络的访问必须通过防火墙的检查，从而实现所定义的安全策略。一般包含如下特性：（1）能支持“除非明确允许，否则能拒绝所有服务”设计策略；（2）应该是灵活的，能适应新的服务；（3）应该能包括高级鉴别机制或能增加高级鉴别机制；（4）能使用过滤技术来允许或拒绝对一个指定主机的访问；（5）过滤手段必须灵活、友好、容易编程，并且能对尽可能多的信息（包括目的 IP 地址、源 IP 地址、目的端口、源端口、协议类型等）进行过滤；（6）在使用注入 Telnet（Internet 上远程登录的一种程序）等的代理服务时要求能使用高级认证机制，以实现安全的口令机制；（7）应该能使用中央电子邮件系统，以建设外界对内部的直接访问。

通过过滤不安全的服务，一个防火墙系统能极大地改善一个网络的安全性和降低网络上主机的危险性，这样只有被允许的协议才能通过防火墙。

3.4 数字证书

数字证书的基础是数据加密技术中的 RSA 加密算法。该算法是一种基于大数不可能质因数分解假设的公匙体系，有可靠的理论保证。它的密钥不是一个字符串，而是一对很大的质数，这两个密钥是互补的，

978-1-935068-18-1 © 2010 SciRes.

其中一个称为公开密钥（public key），另一个称为私用密钥（secret key 或 private key）。

在用作数字证书的同时，RSA 加密算法也可以用于加密传输。如果他人要将一段信息发给某人，可先将这段信息用这人的公用密钥加密后再传输。由于这段密文只能用对应的私用密钥才能解出明文，即使该密文在传输的过程中被人监听截获，也无法得知信息的内容，从而实现了数据传输的隐蔽性和安全性。

更为安全的做法是将电子证书和加密传输结合起来。例如，如果甲要发信给乙，可以先将这段明文用乙的密钥加密，以保证数据的保密性，只有乙能解密阅读；然后再用甲的私用密钥加密，即“签署”甲的个人身份证书。这样，在传输过程中即能保证传输的保密性，又能保证信息发送方的不可抵赖性。

3.5 加强网络安全的人为管理

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理、制定有效的规章制度，对于确保网络的安全、可靠运行，也将起到十分有效的作用。具体包括：确定安全管理等级和安全管理范围；制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。首先是加强立法，及时补充和修订现有的法律法规，用法律手段打击计算机犯罪。其次是加强计算机人员安全防范意识吗，提高人员的安全素质。另外还需要健全的规章制度和有效、易于操作的网络安全管理平台。

3.6 建立安全实时相应和应急恢复的整体防御

没有百分百安全和保密的网络信息，因此要求网络要在被攻击和破坏时能够及时发现、及时反映，尽可能快的恢复网络信息中心的服务，减少损失。

4 结语

总之，网络安全是一个永远说不完的话题。它的潜在危险是来自于多方面的，因此安全防范也应该从多方面去进行。并且由于网络安全问题不断变化，网络安全工作也需要不断地发展。我们只有从多方面下手，制定其安全管理策略，才能不断地解决新问题，使网络更加安全，从而为我们提供更加方便、快捷的服务。

References (参考文献)

[1] Li Jianxia, Computer network security and guard against, science and technology of west china, 2009, 36. P44—45 (Ch).
李建霞，计算机网络安全与防范，中国西部科技，2009，36. P44—45

[2] Hu Kun, Computer network management technique development trend and application, Fu Jian Computer, 2010,1. P30—36(Ch).
胡 坤，计算机网络管理技术发展趋势及应用，福 建 电 脑，2010，1. P30—36