网络风险评估中网络节点关联性的研究

张永铮[1)] 方滨兴[1)] 迟 悦[2)] 云晓春[2)]
[1)](中国科学院计算技术研究所信息智能与信息安全研究中心 北京 100080)
[2)](哈尔滨工业大学计算机网络与信息安全技术研究中心 哈尔滨 150001)

摘 要 在网络风险评估领域中,为了提高评估的准确性,很多研究工作中都引入了网络节点间的连通性,然而,这种性质还不足以表达出各节点间基于物理连通关系之上的某种特殊的逻辑关系,如一方对另一方独有资源的控制关系.为此,文中引入了网络节点关联性(NNC)的概念,通过对实践过程中若干种访问情景的分析,提出了 NNC 的分类方法,然后讨论了 NNC 的发现方法,并举例阐明了 NNC 在网络风险评估中的应用及作用.通过深入地分析和对比可以看出,利用 NNC 可以将若干孤立的弱点联系起来,有助于分析网络的安全风险;此外,NNC 在包含各协议层连通性的基础上丰富了网络节点间独有的特权关系,利用 NNC 也有助于提高检测网络弱点和网络攻击的准确性.

关键词 网络安全;网络风险评估;弱点分析;网络节点关联性;网络攻击
中图法分类号 TP393

Research on Network Node Correlation in Network Risk Assessment

ZHANG Yong-Zheng[1)] FANG Bin-Xing[1)] CHI Yue[2)] YUN Xiao-Chun[2)]
[1)](*Research Center of Information Intelligent and Information Security, Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080)
[2)](*Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin* 150001)

Abstract In the field of network risk assessment, to enhance the accuracy of assessment, the connectivity between network nodes has been introduced to many studies. However, this characteristic is not sufficient for expressing certain special logical relations over physical connective relations between nodes, such as one party's control on particular resources of the other party. Therefore, this paper introduces a conception of network node correlation (NNC). Through analyzing several access scenarios in practice, this paper proposes a NNC taxonomy, then discusses NNC detection methods, and an example is given to illustrate the application and effect of NNC in network risk assessment. Deep analysis and comparison show that using NNC can help to correlate some isolated vulnerabilities to analyze the security risk of networks. Moreover, NNC adds privilege relations between network nodes on the basis of the connectivity of protocol layers so that using NNC also helps to improve the accuracy of detecting network vulnerabilities and attacks.

Keywords network security; network risk assessment; vulnerability analysis; network node correlation; network attack

1 引 言

计算机的高度互联给人们的生活带来了翻天覆地的变化,但同时也给网络黑客提供了更多的攻击途径和攻击目标.实践表明,若干孤立的弱点(即安全漏洞)尽管影响很小,但如果被黑客通过网络有机地组织起来加以利用,则可能给网络系统安全带来

收稿日期:2005-03-22;修改稿收到日期:2006-09-25.本课题得到国家自然科学基金(60403033)和国家"十五"预研项目基金(4131571)资助.张永铮,男,1978 年生,博士,助理研究员,主要研究方向为网络与信息安全、安全评估等.E-mail:zhangyongzheng@software.ict.ac.cn.方滨兴,男,1960 年生,博士,教授,博士生导师,主要研究领域为网络与信息安全.迟 悦,女,1979 年生,博士研究生,主要研究方向为网络与信息安全.云晓春,男,1971 年生,博士,教授,博士生导师,主要研究领域为网络与信息安全.

巨大的风险影响. 在风险评估领域中，计算机的互联使得对网络系统的评估与对单机系统的评估有很大不同，网络信息系统的风险分析随着网络互联程度的日趋复杂变得愈来愈困难，而这种风险分析的成败关键在于能否准确而有效地检测出网络中的所有弱点. 因此，近年来，国内外的研究人员纷纷对网络弱点的检测展开研究. Ritchey 和 Ammann 在文献[1]中首次提出了一种网络弱点的模型检测方法，他们认为一次成功的攻击所必需的条件之一是保证各节点主机的基本连通，并将连通性(connectivity)定义为一个主机与其他主机通信的能力，在他们的模型中，他们利用 Mayer 等人提出的一个防火墙分析引擎[2]，发现网络中各节点主机的连通性，并基于此连通性的知识检测出网络弱点. 文献[3]提出的网络连通性模型描述了网络节点在 TCP/IP 结构模型中各协议层的通信状况，Jajodia 等在此工作的基础上设计了一个拓扑弱点分析工具(Topological Vulnerability Analysis，TVA)[4]，并取得了较好的效果. 由此可见，充分理解和深入研究网络中各节点主机之间的互联性是实现网络弱点检测的重要环节，也是正确评估网络信息系统安全风险的基础. 然而，前面的工作仅仅考虑了节点间各协议层上的连通性，我们认为这种性质不足以表达出各节点间基于物理连通关系之上的某种特殊的逻辑关系，如一方对另一方独有资源的控制关系. 为此，我们提出了网络节点关联性(NNC)的概念及其相关定义，通过对实践过程中若干种访问情景的深入分析，设计了 NNC 的分类方法，然后我们讨论了 NNC 4 种发现方法的特点，给出了 NNC 发现系统的框架，并举例阐明了 NNC 在我们的网络风险评估方法中的应用及作用.

本文的目的在于：(1)力图发现网络中不同孤立弱点之间的联系，为风险评估提供更准确的决策信息；(2)将网络节点连通性进一步拓展为关联性，有助于网络弱点与网络攻击的检测.

2　网络节点关联性

在实际的工作与生活中，我们不可避免地要使用网络，如处理邮件、浏览网页、发布信息，或者远程登录某些设备从事相关的作业等等. 在这些利用网络的实践中，我们发现在网络节点与节点的用户之间总是存在着一种特殊的访问关系，这种特殊性不仅体现在关系一方对另一方资源的专有控制权上，而且还表现在这种关系的独有性上，即不是所有的节点之间都存在这种关系. 例如，主机 A 上的用户可以利用 rsh 服务不需要通过身份认证就可以获得主机 B 上某用户的控制权限；又例，主机 C 在防火墙的保护下，防火墙外的主机 B 不可以直接访问 C，而防火墙内的主机 A 则可以直接访问 C. 同时，设备使用人员的固定性也使节点主机间的这种访问关系呈现出一种稳定性，于是，当攻击者成功入侵节点 A 后，他不仅控制了 A 的部分、甚至全部资源，而且同时他也通过这种特殊关系拥有了对节点 C 一定程度的访问特权，可见这种特殊的访问关系使攻击者获得了意想不到的攻击效果. 因此，我们有必要对这种能够给网络系统中关联资源带来风险的访问关系进行深入的研究.

2.1　NNC 的定义

为便于讨论 NNC，我们首先给出部件的概念.

定义 1(部件).　将网络信息系统中的一台计算机设备称为一个网络节点，并将网络节点上的用户、操作系统、应用程序或服务称为网络节点上的主体，而将网络节点 n 及其上的主体 s 构成的数对 (n, s) 称之为节点 n 上的一个部件，记为 C_{ns}.

在网络信息系统中，功能各异的计算机被电缆互联起来. 传输于电缆上的各种服务信息和数据操作往往使计算机的部件之间形成了众多特殊的访问逻辑关系. 在文献[5]中，Yau 提出了一个所谓“安全依赖关系”的概念，并以此来描述两个部件之间潜在的逻辑关系. 引入这一思想，本文针对安全风险方面的问题，也引入一个“网络节点之间的关联关系”，称之为 NNC. 下面对 NNC 进行定义.

定义 2(网络节点关联性(Network Node Correlation，NNC)).　如果一个攻击者在成功入侵网络节点 A 之后，利用 A 上的某部件 C_{Ai} 对节点 B 上某部件 C_{Bj} 的访问关系，从而继续攻击节点 B，那么这种可被利用的访问关系被称为部件 C_{Ai} 到 C_{Bj} 的 NNC，书写为 $NNC_{Ai,Bj}$. 在不混淆的情况下，亦可简写为节点 A 到 B 的一个 NNC_{AB}. $NNC_{Ai,Bj}$ 的风险信息可用一个有序六元组 $\langle A, i, B, j, P, W\rangle$ 来描述，其中，i, j 分别为节点 A, B 上的主体；P 表示利用该 NNC 进行攻击的成功的概率，$P\in[0, 1]$；W 表示一个部件对另一个部件的影响程度，$W\in[0, +\infty)$. 需要强调的是：(1)本文所指的访问关系均是已授权的，即符合各节点主机的安全策略，而不考虑攻击、入侵等非授权访问关系；(2)属性 P 和 W 的量化标准应取决于具体的实践经验、历史数据及主观期望等方面.

由上述定义可知，各网络节点上的部件和 NNC 能够在物理网络的基础上构建出一个逻辑关系网络，我们称之为访问关系网络，如图 1 所示，其中，

$A \sim D$ 为网络节点主机，一条有向边表示一个 NNC，有向边连接网络节点上的两个部件.

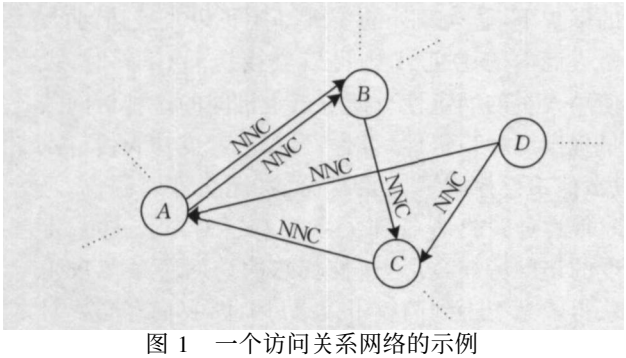


图 1 一个访问关系网络的示例

2.2 访问情景分析

为了能够深入理解各种类型的 NNC 关系，我们首先分析一下几个典型的访问情景. 本文中，我们将访问者执行访问操作的计算机称为访问机，将提供服务的被访问的计算机称为服务机，而系统用户通常是指由操作系统提供的、对系统资源具有独立控制权限的以及能够运行程序的用户，根据其控制权限的不同，可大致分为远程访问用户、普通用户和管理员用户(超级用户)等.

情景 **1**. 涉及防火墙的访问带来防火墙内外的差异.

防火墙作为一种常见的安全设施，在网络安全实践中已被广泛采用. 网络的管理者可以通过一定的安全策略设置防火墙，使其允许或阻断远程访问者对某些服务的访问，这种设置通过改变各节点完备的连通性，使不同位置的访问者的访问权产生了差异，即使得能够访问防火墙内服务的访问者客观上比被防火墙阻断的访问者的访问特权要多.

情景 **2**. 基于不同协议的服务访问带来控制权限的差异.

一般来说，通过 http 协议进行访问只能获取和发布信息，而在授权的情况下通过 ssh 访问则可以获得主机的全部系统资源.

上述两个情景表现出访问者一系列递增的权限，从穿过防火墙的特权到收发信息权，从服务机的部分控制权到全部控制权. 因此，在服务者提供各种服务的同时也将或多或少的某种权限赋予了访问者，而这种权限是访问者独有的. 如果攻击者通过攻击弱点等非法入侵手段成为了这种访问者，那么他不仅继承了这种访问者的系统权限，而且还具有了该访问者所独有的某种访问关系为其带来的额外权限.

2.3 NNC 的分类及量化

由于我们提出的 NNC 在连通性的这种物理关系的基础上更强调各节点部件间的一种带有权限特性的逻辑关系，因此对节点、主体和概率等各维属性上的分类的意义不大，所以我们仅着重考虑 NNC 在影响程度 W 上的分类. 为了使分类具有完整性且避免二义性，我们采用决策树的方法给出分类准则，NNC 影响程度分类的决策树如图 2 所示，其中，每个终态 $W_i(i=1 \sim 7)$ 表示一个类别，而终态 W_0 应为空，因为符合该条件的访问关系无现实意义，即该类 NNC 在各协议层都是不连通的，如遭到防火墙阻断

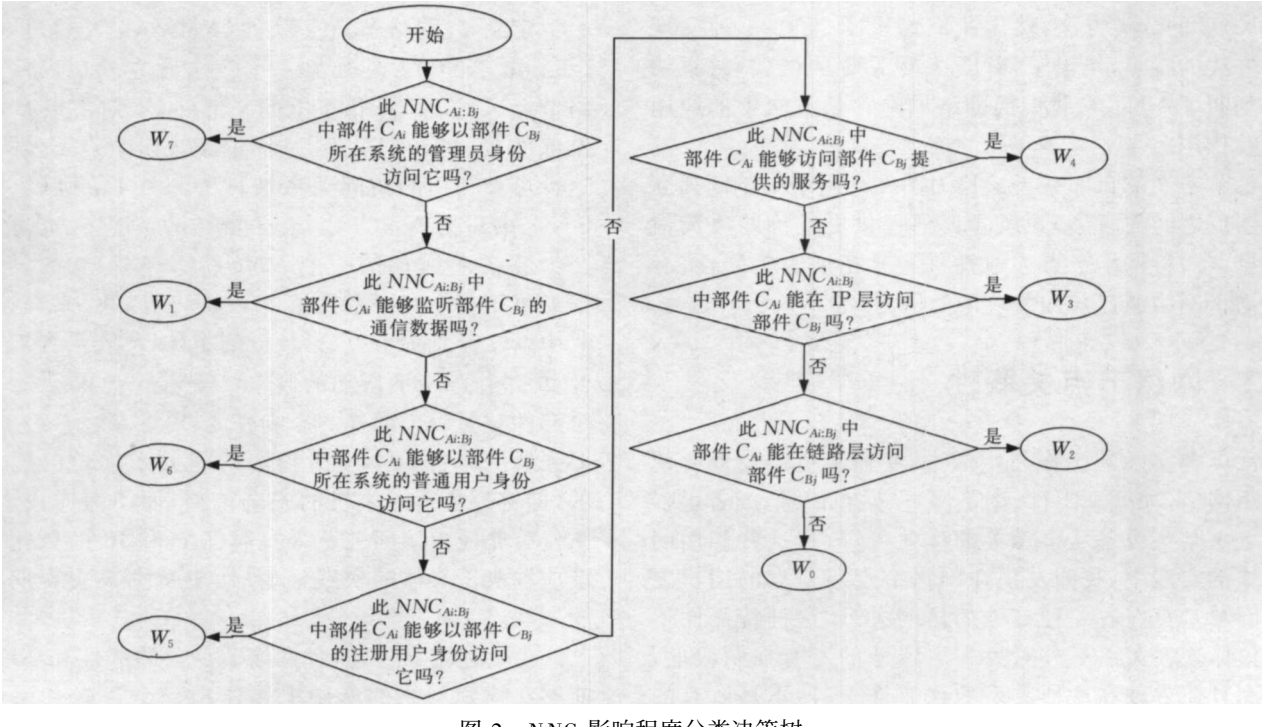


图 2 NNC 影响程度分类决策树

或无该物理链路等，并且它不存在监听与被监听的特殊关系.

依照上述准则，我们可以将所有的 NNC 分成七类，表 1 给出了各类 NNC 的分类描述及量化. 我们需要强调的是影响属性是否需要量化应根据用户的实际需求而定，不应盲目地追求量化，但如果用户期望用数字的形式刻画 NNC 的影响程度，那么本文中所有量化属性的量化标准应来源于具体的实践经验、历史数据、主观期望及设计思想等方面. 从访问情景分析中我们可以看出，各个类别的量化权值随其所涉及的权限的多少或重要程度的不同呈偏序关系，即 $W_7 > W_6 > W_5 > W_4 > W_3 > W_2$. 例如，一个访问者能够分别以某普通用户和管理员身份登陆一台服务机，若以管理员身份登陆，那么他能够完全控制所有系统资源(包括其他用户资源)，我们将之归为 W_7 类，而以普通用户登陆，则只能控制公共系统资源及其自身资源，应属 W_6 类. 显然，该访问者以管理员身份访问该服务机所拥有的权限要高于或多于以普通用户身份登陆所获得的权限，因此有 $W_7 > W_6$，其它情况可依此类推. 本文中我们依照上述偏序关系在 0～1 的范围内对每类 NNC 实施量化，量值范围以及具体取值可以在以后的研究和实践过程中根据需求进行适当的调整.

表 1　NNC 的分类描述及量化

类型	权值	描　　述
W_7	1.0	访问者能够以服务机系统管理员的身份执行命令，完全控制所有系统资源.
W_6	0.7	访问者能够以服务机系统普通用户身份执行命令，控制部分系统资源及该用户资源.
W_5	0.5	访问者能够以服务部件注册用户身份获取或发布公共和个人信息，但不能执行系统命令.
W_4	0.3	访问者能够以服务部件匿名用户身份获取或发布公共信息，这种关系仅仅表明传输层的连通性，如穿过防火墙访问内部服务部件等.
W_3	0.2	访问者仅能在 IP 层访问服务机，这种关系体现 IP 层的连通性.
W_2	0.1	访问者仅能在链路层访问服务机，这种关系体现链路层的连通性，是为解决 ARP 攻击等问题而设计的.
W_1	0.8	是一种特殊的 NNC 关系，体现了访问节点与服务节点之间监听与被监听的关系，这种关系是攻击者获得攻击信息的重要手段.

严格地说，W_1 类 NNC 不是一种直接的访问关系，它所表达的含义是，访问者自身无法访问服务机，但可以利用监听并分析该服务机的网络通信数据的方法获得机密信息，如用户名、密码等，从而可以对服务机进行访问. 由于这种情形的存在，使得访问者和服务机之间可能存在一种关联，所以我们将这类 NNC 关系归为 W_1 类. 也正由于这类 NNC 如被攻击者利用，会对服务机造成很大的安全威胁，如窃取管理员等用户的密码，所以我们认为该类 NNC 的影响属性权值介于 W_7 和 W_6 之间比较合适.

研究 NNC 的分类方法不仅使我们深入理解各种类型 NNC 的特点及其含义，而且我们可以将 NNC 归纳成几种简单而清晰的模式，这样便于研究人员进一步发现 NNC.

2.4　NNC 的发现

从实践工作中可知，NNC 的发现方法可分为自动方法和手动方法，其中自动方法主要包括主动探测、被动监听和分析网络及安全设备的配置文件，而手动方法是指由节点主机的使用者做出分析报告，这几种方法的简单描述和特点如表 2 所示.

表 2　几种 NNC 发现方法及其特点

方法		特点简介
自动	主动探测	使用 Nmap①、Nessus②、Traceroute③等已有的探测工具在管理域内、外的不同地点对网络进行探测. 该方法可以获得网络的部分连通状况及相关服务，即发现部分 $W_1 \sim W_4$ 类 NNC，而发现 NNC 的数量需取决于扫描工具的布点数，但无法发现更高级别的 NNC 关系.
	被动监听	通过对网络通信数据的采集与分析进一步发现 NNC. 该方法同样可以获得网络的部分连通状况以及部分更高级别的 NNC 关系，而发现 NNC 的准确程度与数量需取决于采集到的网络数据的质与量. 这种方法在某种程度上是主动探测方法的补充与提高，但仅通过分析网络数据发现高级别 NNC 关系的准确性不能保证.
	分析配置文件	通过分析交换机、路由器、防火墙等网络及安全设备上的配置文件得到网络节点间的连通性[2]. 该方法可以获得部分 $W_2 \sim W_4$ 类 NNC，并且在管理员变更配置文件后可以立刻更新 NNC，避免了探测和监听方法的时间延迟的缺点，但该方法需要网络及安全设备的控制权，而且同样无法获得更高级别的 NNC 关系.
手动	使用者报告	由每个节点主机等设备的使用者根据本文提出的 NNC 的定义与类别特点分析并报告自己的 NNC. 由于使用者对自己的业务往来和访问行为非常熟悉，所以该方法能够准确地获得各节点及部件之间的高级别 NNC 关系，但无法获得 W_1 类 NNC，并且需要人的参与.

通过对上述方法的分析，我们可以看出每种方法都有自己独特的作用，所以我们采用融合技术将这 4 种方法结合起来，以期待更充分更准确地发

① Nmap. Security Scanner. http://www.insecure.org, 2006
② Nessus. Remote Security Scanner. http://www.nessus.org, 2005
③ Traceroute. ftp://ftp.ee.lbl.gov/traceroute.tar.gz, 2006

现网络中的 NNC 关系，而融合的策略及具体的实施方法并不是本文讨论的重点. 图 3 给出了 NNC 发现系统的框架，其中，NNCB 表示存放 NNC 的数据库. 使用者分析模块完成以下工作：由使用者分析自己的业务情况和访问行为，并根据本文提出的 NNC 的定义及分类方法对它们进行描述，并形成报告. 主动探测、被动监听、分析配置文件和使用者分析等 4 个发现模块应采用统一格式的报告，提交至融合中心，然后由融合中心根据一定的策略整合所有报告的内容，并存入 NNCB，为风险评估、入侵检测、病毒扩散等安全领域的应用提供有效的信息支持.

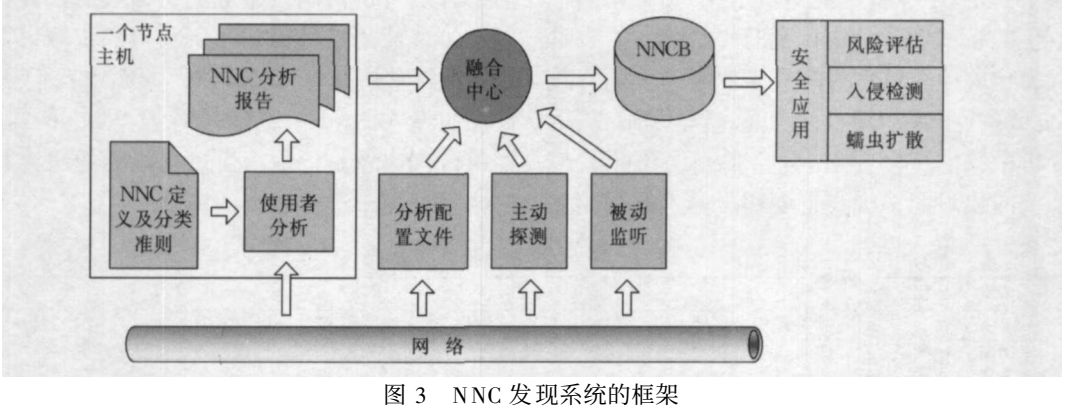


图 3 NNC 发现系统的框架

3 风险评估应用

在本节中，我们举例阐明 NNC 关系在网络风险评估领域中的应用与作用. 图 4 给出了一个网络实例的组织结构，节点 A 是外网中的一台 PC 机，节点 B，C，D 分别是网络信息服务器、数据库、管理机，它们和防火墙组成了一个内网. 我们对这个网络实例有以下规定：

(1) 防火墙的安全策略是：仅允许外网计算机访问节点 B 的 WWW 服务和节点 D 的所有端口，对其它节点和端口的访问均进行阻断，从内网向外网的访问不进行限制.

(2) 内网所有节点主机没有设置防火墙，可以任意访问.

(3) 节点 B 的 Rsh(remote shell)服务将节点 D 设置为信任主机，即节点 D 上的用户不用通过身份验证即可在节点 B 上执行 shell 命令.

(4) 节点 B 的 WWW 服务可向节点 C 的数据库中读写信息，但不能管理数据库；节点 D 通过 Rsh 服务和 Snmp 服务管理节点 B.

(5) 节点 B 的 Snmp 服务具有弱点 Vul. 1：泄漏系统及网络设备信息；节点 D 具有弱点 Vul. 2：缓冲区溢出漏洞，可使攻击者获得系统管理员权限；其它节点主机均无弱点.

(6) 攻击者在节点 A 发动攻击，他的目的是修改节点 C 的 Oracle 数据库中的信息.

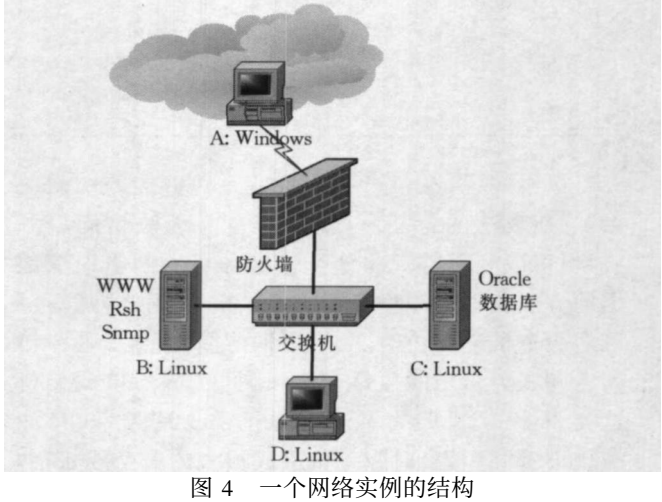


图 4 一个网络实例的结构

3.1 NNC 的产生

为了简单且说明问题，我们采用主动探测结合使用者报告的方法发现与内网有关的 NNC. 首先，我们分别在外网节点 A 和内网节点 B，C，D 上用扫描工具探测内网的连通性，由于内网节点由交换机连接而成，所以各节点之间不存在相互监听的情况，于是，我们可以得到以下 NNC 关系：

$\langle A, *, B, \text{www}, 1, W_4\rangle\langle A, *, D, *, 1, W_4\rangle$

$\langle B, *, C, *, 1, W_4\rangle\langle B, *, D, *, 1, W_4\rangle$

$\langle C, *, B, *, 1, W_4\rangle\langle C, *, D, *, 1, W_4\rangle$

$\langle D, *, B, *, 1, W_4\rangle\langle D, *, C, *, 1, W_4\rangle$

然后，分别由节点 B、C 和 D 的使用者或管理者提交 NNC 分析报告. 考虑节点 B，由于 WWW 服务向节点 C 的数据库读写数据，故有$\langle B, \text{www}, C, \text{oracle}, -, W_5\rangle$；对节点 D，如前文所述，它通过 Rsh

和 Snmp 管理节点 B，所以有〈D，root，B，rsh，1，W_7〉，〈D，root，B，snmp，－，W_5〉. 在上述 NNC 中，“ *”表示任意，概率 P 为“－”表示不能确定.

最后，我们将所有的 NNC 数据融合到一起. 为便于表达，我们给一些 NNC 做上标号，于是有

〈A，*，B，www，1，W_4〉　　(N_0)
〈A，*，D，*，1，W_4〉　　(N_1)
〈B，www，C，oracle，－，W_5〉　　(N_2)
〈B，*，D，*，1，W_4〉
〈B，*，C，*/oracle，1，W_4〉
〈C，*，B，*，1，W_4〉
〈C，*，D，*，1，W_4〉
〈D，root，B，rsh，1，W_7〉　　(N_3)
〈D，root，B，snmp，－，W_5〉　　(N_4)
〈D，*，B，*/rsh：snmp，1，W_4〉
〈D，*，C，*，1，W_4〉

其中形如“ */root：snmp”的表达式表示除 root 和 snmp 以外的所有主体.

3.2　风险评估

目前，对网络的风险评估方法有很多，为了能够对三种评估方法作横向的比较，并且更好地阐明引入 NNC 关系的作用，我们采用分析攻击路径的方法来评估网络的安全风险. 根据前文对实例的分析，我们已经得到了 NNC 关系和节点状况，从而可以构造出此实例的访问关系网络，如图 5 所示，为了重点突出、表达清晰，图中省略了部分 NNC 关系.

(1) 传统的评估方法

使用 Nessus、ISS[①] 等知名的弱点扫描工具探测网络中的每个节点主机，以便发现它们的弱点，然后以这些孤立的弱点作为评估依据. 我们对上述实例应用该方法可以得到如下评估结论：发现两个弱点 Vul. 1 和 Vul. 2，由于攻击者无法访问 B 的 Snmp 服务，所以弱点 Vul. 1 无风险，仅弱点 Vul. 2 有风险，攻击路径为 A N_1，如图 5(a) 所示，攻击者无法实现预期目的.

(2) 拓扑弱点分析方法

文献[4] 中提出的方法，该方法借助 Nessus 工具生成网络描述，并结合带有条件属性的弱点攻击方法，产生网络攻击路径. 应用该方法可得到如下评估结论：攻击者可以利用弱点 Vul. 2 获得 D 的管理员权限，进而利用弱点 Vul. 1 获得 B 的系统信息，但由于节点 C 无弱点，所以无法继续攻击 C，攻击路径为 A N_1 D N_4 B，如图 5(b) 所示，攻击者无法实现预期目的.

(3) 基于 NNC 的评估方法

我们提出的基于 NNC 的评估方法的主要思想是：首先生成 NNC 库，然后利用已有的扫描工具发现孤立的弱点，根据弱点与 NNC 的联系分析网络攻击路径，从而评估网络风险. 在上述实例中，利用弱点 Vul. 2 的前提是可以访问节点 D，成功利用的结果是获得 D 的 root 权限，于是攻击者可凭此获得 D 的 root 权限，又由于 N_3 的存在，攻击者可以获得 B 的 root 权限，通过对本地的监听可以获取 WWW 服务访问 Oracle 的用户和口令，从而，依靠 N_2 修改 Oracle 中的数据. 同理利用 N_4 使攻击者可以管理节点 B，与利用弱点 Vul. 1 相比，能够获得更多的权限. 需要说明的是，在分析的过程中，N_0 和 N_2 是不能关联起来的，因为访问 Oracle 需要身份认证，仅依靠访问 WWW 服务的能力是不够的. 由此给出评估报告：攻击路径为 A N_1 D N_3 B N_2 C 和 A N_1 D N_4 B，如图 5(c) 所示，攻击者能够实现预期目的.

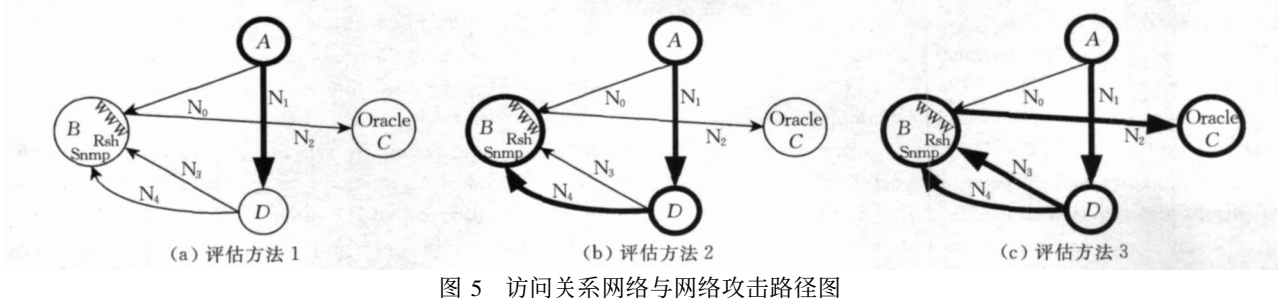


图 5　访问关系网络与网络攻击路径图

基于 NNC 的方法之所以能够发现从 A 到 C 的网络攻击路径，原因就在于它不仅考虑了网络节点的连通性，而且引入了节点间的一种合法的关联性，由此可以看出，NNC 的引入丰富了网络节点间的联系，提高了检测网络弱点及网络攻击的准确性. 通过对网络攻击路径的分析，我们可以获知网络存在的弱点以及不同的攻击者对网络不同资源的威胁情况，从而评估一个网络的安全状况，同时，通过消除

① Internet Security Systems. System Scanner. http://www.iss.net, 2006.

个别弱点,控制关键的 NNC,就可以有效地降低网络的安全风险. 因此,能否准确地发现网络攻击路径就成为评估网络安全性成败的关键之处.

4 结 论

本文在讨论 NNC 研究的目的及意义的基础上,给出了相关定义,并通过若干访问情景的分析,设计了一个 NNC 分类方法,深入分析了 NNC 的发现方法,通过一个网络风险分析的实例,阐明了 NNC 在风险评估领域中的应用和作用. 与前面的研究工作相比,NNC 具有以下优势:(1) 利用 NNC 可以将若干孤立的弱点联系起来,有助于分析网络的安全风险;(2) NNC 在包含各协议层连通性的基础上丰富了网络节点间独有的特权联系,提高了检测网络弱点和网络攻击的准确性;(3) 揭示了网络中发生的不同事件间的连带性,为病毒传播、入侵检测等其它安全领域的研究提供帮助.

参 考 文 献

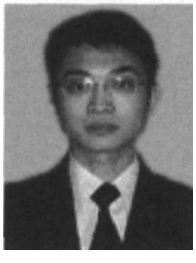
[1] Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California, 2000: 156-165

[2] Mayer A, Wool A, Ziskind E. Fang: A firewall analysis engine//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California, 2000: 177-187

[3] Ritchey R, O'Berry B, Noel S. Representing TCP/IP connectivity for topological analysis of network security//Proceedings of the 18th Annual Computer Security Applications Conference. Las Vegas, Nevada, 2002: 25-31

[4] Jajodia S, Noel S, O'Berry B. Topological analysis of network attack vulnerability//Kumar V, Srivastava J, Lazarevic A et al. Managing Cyber Threats: Issues, Approaches and Challenges. New York: Springer, 2005: 248-266

[5] Yau S S, Zhang X Y. Computer network intrusion detection, assessment and prevention based on security dependency relation//Proceedings of the 23rd Annual International Computer Software & Applications Conference. Phoenix, USA, 1999: 86-91



ZHANG Yong Zheng, born in 1978, Ph.D.. His research interests include network and information security, security assessment, etc.

FANG Bin Xing, born in 1960, professor, Ph.D. supervisor. His research interests include network and information security.

CHI Yue, born in 1979, Ph.D. candidate. Her research interests include network and information security.

YUN Xiao Chun, born in 1971, professor, Ph.D. supervisor. His research interests include network and information security.

Background

The research of this paper is one part of two projects, "Security Analysis Technology" and "Research of Internet Worm Active Control Technology Based on Worm Countermeasure", which are respectively supported by the "Tenth Five Year Plan" of National Pre-research Program under grant No. 4131571 and the National Natural Science Foundation of China under grant No. 60403033. The former is to develop a security analysis or assessment technology of computer and network systems. The latter is to propose a novel active control technology of Internet worms. Network node correlations are required and emphasized in these two projects. Deeply understanding network node correlations is an important step of detecting and evaluating network vulnerabilities, and is also a basis of active control technology of Internet worms which rely on the vulnerabilities to propagate.

In the field of risk assessment, the practice shows that although each risk of several isolated vulnerabilities is very low, but if they are organically exploited by hackers using a network, they can greatly threaten the security of network systems. The interconnection of computers leads to the great differences of evaluating network systems and evaluating host systems. The risk analysis of network systems becomes more and more difficult with increasingly complicated interlinks. But the key of the analysis relies on how to accurately and effectively identify all network vulnerabilities. Therefore, more and more researchers begin to study network vulnerability detection in recent years. The concept of network node connectivity is all introduced into their work. However, the existing work is not enough to reflect some special logical relations over physical connections, such as one party's control on particular resources of the other party.

Therefore, this paper proposes a conception of network node correlation (NNC) and discusses NNC classification, detection and its application in network risk assessment. The research of this paper mainly helps to find the correlations between different isolated vulnerabilities and network nodes to provide more accurate decision making information for risk assessment, and also helps to further study the propagation and countermeasure of worms.