第 3 章

网络攻击与安全评估

本章要点：

☑ 网络攻击的概念及分类
☑ 计算机及网络的漏洞分析
☑ 网络脆弱性的评估技术
☑ 网络风险的识别与评估方法
☑ 网络风险管理

3.1 网络攻击的概念及分类

随着网络规模飞速扩大、网络结构和协议日趋复杂、网络应用领域和用户群体不断扩大，出于各种目的的网络安全事件呈迅速增长的趋势，而且网络攻击的技术和手段也逐步多样化，造成的损失也越来越大。本节给出网络攻击的基本概念，以及网络攻击的分类方法。

3.1.1 网络攻击的基本概念

网络攻击是指网络用户未经授权的访问尝试或者使用尝试，其攻击目标主要是破坏网络信息的保密性、网络信息的完整性、网络服务的可用性、网络信息的非否认性（抗抵赖）和网络运行的可控性。目前的网络攻击事件动机多是为了个人利益或表现自己，或者是针对某个事件进行报复性攻击；其攻击工具是个人编程实现或者是网上现成工具的利用，这些工具功能单一，只能是单独使用，缺乏与其他攻击工具的配合、协同能力；攻击的目标也是不确定的：一般是一些知名网站，高级黑客以安全级别较高的军队或政府的信息系统为目标；对网络攻击的研究多是从个人兴趣出发研究一些攻击的技术和技巧，国家级的对网络攻击的研究也有，但多是从攻击技术、攻击手段或战术、战法方面进行的，真正从网络攻击的整体体系进行理论和相关技术研究的还未见公开。网络攻击如果上升为国家行为，网络攻击的目标则是敌对方的包括军事在内的信息系统，或其他民用信息系统，攻击的目的包括获取军事情报，瘫痪敌方指挥控制系统，干扰敌方的经济、金融秩序，对敌方展开心理攻势，进行舆论宣传等。

网络攻击的一般流程为隐藏攻击位置，收集目标系统信息，根据收集到的目标系统的信息，通过脆弱性分析，挖掘出其存在的脆弱性，利用这种脆弱性获取目标系统的一定的权限，

即文件的读权限，写权限，执行命令、代码的权限等；如有必要和可能将提升并获取目标系统的根权限。获取目标系统的权限后，根据攻击的目的进行相应的操作（如读、写、删除），安装攻击软件，攻击扩展，最后留下后门、清除攻击痕迹；在获得目标系统的一定权限后，如无法进一步提升权限，攻击者可能在控制一定数量主机和网络资源后实施拒绝服务攻击。

在实际的网络攻击中，攻击者还可能在收集到目标主机的信息后，搭建与目标相近的攻击环境和场景，进行模拟攻击，以发现在攻击中可能遇到的情况，从而在攻击实施时提高攻击的效率和成功率。

3.1.2 网络攻击的分类

网络安全研究的一个关键问题是对网络攻击的认识，对网络攻击进行分类是网络安全研究的一个重要方面。通过对网络攻击和漏洞分析，我们可以清楚地了解每一类攻击的特性，找出攻击与漏洞之间的内在关系，从而更好地进行防御并维护网络的安全。网络攻击分类的主要依据有计算机系统中的安全漏洞、攻击的效果、攻击的技术手段、攻击的检测、攻击所造成的后果等。

1. 矩阵分类法

Perry 和 Mallich 对经验术语分类法进行了一定的改进，提出了一种基于脆弱性和可能的攻击者的二维结构的分类方法，这就可以将攻击用一个简单的二维矩阵描述，矩阵项有可能的攻击者包括操作员、程序员、数据录入员、内部用户、外部用户、和入侵者；可能造成的影响有物理破坏、信息破坏、数据干扰、窃取服务、浏览信息和窃取信息，如表 3-1 所示。

表 3-1 基于脆弱性和可能的攻击者的网络攻击分类

可能的攻击者 / 造成的影响	操作员	程序员	数据录入员	内部用户	外部用户	入侵者
物理破坏	电源短路					
信息破坏	删除磁盘	恶意软件			恶意软件	拨号
数据干扰		恶意软件	伪造数据入口			
窃取服务		窃取用户账号		未授权操作	拨号	
浏览信息	窃取介质			未授权访问	拨号	
窃取信息				未授权操作访问	拨号	

2. 基于攻击手段的分类

网络攻击手段可以从理论和技术两个层面来区分，一是理论攻击，二是技术攻击。所谓理论攻击，就是密码学意义上的攻击，只专注于攻击概念或攻击过程与算法，而不考虑具体的技术实现；技术攻击与特定的网络协议、操作系统及应用程序相关，存在明显可操作的攻击步骤，攻击者可借用一定的分析手段和攻击工具来达到特定的攻击目的。一般而言，理论攻击是技术攻击的理论基础，几乎每种技术攻击都可以最终归结为某类理论攻击。例如对路由器路由表、DNS（Domain Name Server）服务器域名表的窜改就属于密码

学上的完整性侵犯，TCP序列号猜测攻击可归入密码学上的假冒攻击；但理论攻击却未必能成为现实可行的技术攻击。例如差分密码分析已是一种较为成熟的对迭代分组密码的理论攻击方法，然而要将其变为技术攻击手段，切实破译某一特定密文，仍存在需要获取大量明文选择及大量专家干预的困难，即存在数据复杂性和处理复杂性。同样，密码学意义上的理论攻击所涵盖的对某些加密算法的攻击、对签名算法的攻击、对密钥交换和认证协议的攻击也未必能举出确实有效的实现方法。因此，到目前为止，对网络攻击的分类主要着眼于技术层次，因为在这一层面上，攻击与特定的网络系统相关，存在明确可操作的步骤和可预期的结果。

3. 基于攻击过程的分类

这种分类法不是试图列举所有的计算机安全漏洞和所有可能的攻击方法，而是想提供一个宽泛的、兼容的框架。分类是面向过程的而不是某单一属性的分类类别。Stallings表述了一个简单的安全威胁分类过程模型，确切地说这个模型不是基于攻击过程意义上的过程而是指对通信过程实施攻击的方式。Stallings定义了以下四种网络攻击类型：中断(Interruption)、窃听(Interception)、篡改 (Modification)、伪造(Fabrication)，其示意图如图3-1所示。

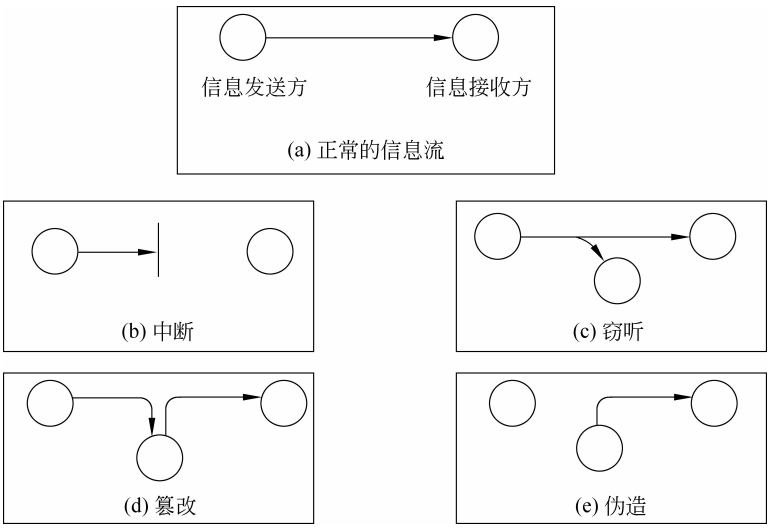

图3-1　基于过程的攻击分类

4. 基于攻击目的的分类

对网络攻击也可以按攻击的目的分为拒绝服务、信息利用、信息收集和假消息攻击等几种。本书分别对其进行概要介绍并提供了相应的防御方法。

(1) 拒绝服务攻击：拒绝服务攻击企图通过使目标服务计算机崩溃或把它压垮来阻止目标提供服务，服务拒绝攻击是最容易实施的攻击行为，常见工具包括LOIC、XOIC、HULK和DDOSIM-Layer等。主要方式包括：

① 死亡之ping。

概览：由于在早期的阶段，路由器对包的最大尺寸都有限制，许多操作系统对TCP/

IP栈的实现在ICMP包上都是规定64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，当产生畸形的，声称自己的尺寸超过ICMP上限的包（也就是加载的尺寸超过64 KB上限）时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接受方当机。

防御：现在所有的标准TCP/IP实现都已实现对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，包括从Windows 98之后的Windows NT（Service Pack 3之后），Linux、Solaris和Mac OS都具有抵抗一般死亡之ping攻击的能力。此外，对防火墙进行配置，阻断ICMP以及任何未知协议，都讲防止此类攻击。

② 泪滴。

概览：泪滴攻击（tear drop）利用那些在TCP/IP栈实现中信任IP碎片的包的标题头所包含的信息来实现攻击。IP分段含有指示该分段所包含的是原包的哪一段的信息，某些TCP/IP（包括Service Pack 4以前的NT）在收到含有重叠偏移的伪造分段时将崩溃。

防御：服务器应用最新的服务包，或者在设置防火墙时对分段进行重组，而不是转发它们。

③ UDP洪水。

概览：各种各样的假冒攻击利用简单的TCP/IP服务，如Chargen和Echo来传送毫无用处的占满带宽的数据。通过伪造与某一主机的Chargen服务之间的一次UDP连接，回复地址指向开着Echo服务的一台主机，这样就生成在两台主机之间的足够多的无用数据流，如果足够多的数据流就会导致带宽的服务攻击。

防御：关掉不必要的TCP/IP服务，或者对防火墙进行配置阻断来自Internet的对这些服务的UDP请求。

④ SYN洪水。

概览：一些TCP/IP栈的实现只能等待从有限数量的计算机发来的ACK消息，因为它们只有有限的内存缓冲区用于创建连接，如果这一缓冲区充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直到缓冲区里的连接企图超时。在一些创建连接不受限制的实现中，SYN洪水（SYN flood）具有类似的影响。

防御：在防火墙上过滤来自同一主机的后续连接。未来的SYN洪水令人担忧，由于SYN洪水并不寻求响应，所以无法从一个简单高容量的传输中鉴别出来。

⑤ Land攻击。

概览：在Land攻击中，一个特别打造的SYN包它的原地址和目标地址都被设置成某一个服务器地址，此举将导致接收服务器向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，每一个这样的连接都将保留直到超时。对Land攻击反应不同，许多UNIX实现将崩溃，而NT变得极其缓慢（大约持续5分钟）。

防御：打最新的补丁，或者在防火墙进行配置，将那些在外部接口上入站的含有内部源地址滤掉（包括10域、127域、192.168域、172.16到172.31域）。

⑥ Smurf攻击。

概览：一个简单的Smurf攻击通过使用将回复地址设置成受害网络的广播地址的

ICMP 应答请求(ping)数据包来淹没受害主机的方式进行,最终导致该网络的所有主机都对此 ICMP 应答请求做出答复,导致网络阻塞,比死亡之 ping 洪水的流量高出一或两个数量级。更加复杂的 Smurf 将源地址改为第三方的受害者,最终导致第三方雪崩。

防御:为了防止黑客利用你的网络攻击他人,关闭外部路由器或防火墙的广播地址特性。为防止被攻击,在防火墙上设置规则,丢弃掉 ICMP 包。

⑦ Fraggle 攻击。

概览:Fraggle 攻击对 Smurf 攻击做了简单的修改,使用的是 UDP 应答消息而非 ICMP。

防御:在防火墙上过滤掉 UDP 应答消息。

⑧ 电子邮件炸弹。

概览:电子邮件炸弹是最古老的匿名攻击之一,通过设置一台机器不断大量地向同一地址发送电子邮件,攻击者能够耗尽接收者网络的带宽。

防御:对邮件地址进行配置,自动删除来自同一主机的过量或重复的消息。

⑨ 畸形消息攻击。

概览:各类操作系统上的许多服务都存在此类问题,由于这些服务在处理信息之前没有进行适当正确的错误校验,在收到畸形的信息可能会崩溃。

防御:打最新的服务补丁。

(2) 分布式拒绝服务攻击。

概览:分布式拒绝服务(Distributed Denial of Service,DDoS)攻击指借助于客户/服务器技术,将多个计算机联合起来作为攻击平台,分布式运行 TFN(Tribe Flood Network)等工具,对一个或多个目标发动 DDoS 攻击,从而成倍地提高拒绝服务攻击的威力。攻击者利用客户/服务器技术和代理通信技术,主控程序能在几秒钟内激活成百上千次代理程序的运行。

防御:采取合适的安全域划分,配置防火墙、入侵检测和防范系统,减缓攻击。采用分布式组网、负载均衡、提升网络系统容量等可靠性措施,增强网络信息系统总体服务能力。DDoS deflate 是一款免费的用来防御和减轻 DDoS 攻击的脚本,它通过 netstat 监测跟踪创建大量网络连接的 IP 地址,在检测到某个结点超过预设限制时,该程序会通过应用层防火墙或网络防火墙 IPtables 禁止或阻挡这些攻击者的 IP。

(3) 控制利用型攻击。

利用型攻击是一类试图直接对你的机器进行控制利用的攻击,最常见的有如下三种。

① 口令猜测及利用。

概览:一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 服务的可利用的用户账号,成功的口令猜测能实施对机器的控制利用。

防御:要选用难以猜测的口令,例如词和标点符号的组合;定期更改口令。确保像 NFS、NetBIOS 和 Telnet 这样的服务不暴露在公共范围。

② 特洛伊木马远程控制。

概览:特洛伊木马是一种或是直接由一个黑客,或是通过一个不令人起疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限,安装此程序的人就可以直

接远程控制目标系统。最有效的一种称为后门程序，恶意程序包括 NetBus、BackOrifice 和 BO2k，用于控制系统的良性程序如 netcat、VNC、pcAnywhere。理想的后门程序透明运行。

防御：避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机上的监听 TCP 服务。

③ 缓冲区溢出提升权限。

概览：由于在很多的计算机和网络服务程序中，疏忽大意的程序员使用 strcpy()、strcat()类似的不进行有效位检查的函数，最终可能导致恶意用户编写一小段利用程序来进一步打开安全豁口，然后将该代码缀在缓冲区有效载荷末尾，这样当发生缓冲区溢出时，返回指针指向恶意代码，这样系统的控制权就会被夺取。

防御：利用 SafeLib、Tripwire 这样的程序保护系统，或者浏览最新的安全公告不断更新操作系统。

(4) 信息收集型攻击。

信息收集型攻击并不对目标本身造成危害，如其名所示，这类攻击被用来为进一步入侵提供有用的信息。这种攻击主要包括扫描技术、体系结构探测、利用信息服务。

扫描技术包括如下几种。

① 地址扫描和端口扫描。

概览：运用 ping 这样的程序探测目标地址，对此做出响应的表示地址存在。运用 Nmap 或者 X-scan 这样的程序探测开放的目标端口。

防御：在防火墙上过滤掉 ICMP 应答消息。许多防火墙能检测到是否被扫描，并自动阻断扫描数据包。

② 反响映射。

概览：黑客向主机发送虚假消息，然后根据返回“host unreachable”这一消息特征判断出哪些主机是存在的。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的常见消息类型，这些类型包括 RESET 消息、SYN-ACK 消息、DNS 响应包。

防御：NAT 和非路由代理服务器能够自动抵御此类攻击，也可以在防火墙上过滤“host unreachable”ICMP 应答。

③ 慢速扫描。

概览：由于一般扫描侦测器的实现是通过监视某个时间帧里一台特定主机发起的连接的数目(例如每秒 10 次)来决定是否在被扫描，这样黑客可以通过使用扫描速度慢一些的扫描软件进行扫描。

防御：通过引诱服务来对慢速扫描进行侦测。

④ 体系结构探测。

概览：黑客使用具有已知响应类型的数据库的自动工具，对来自目标主机的、对坏数据包传送所做出的响应进行检查。由于每种操作系统都有其独特的响应方法(例如 NT 和 Solaris 的 TCP/IP 堆栈具体实现有所不同)，通过将此独特的响应与数据库中的已知响应进行对比，黑客经常能够确定出目标主机所运行的操作系统。

防御：去掉或修改各种标志，包括操作系统和各种应用服务的，阻断用于识别的端口扰乱对方的攻击计划。

⑤ 利用 DNS 域名转换信息服务。

概览：DNS 协议不对转换或信息性的更新进行身份认证，这使得该协议被人以一些不同的方式加以利用。如果你维护着一台公共的 DNS 服务器，黑客只需实施一次域名转换操作就能得到所要主机的名称以及内部 IP 地址。

防御：在防火墙处过滤掉域转换请求。

⑥ 利用 Finger 服务信息。

概览：黑客使用 Finger 命令来探测一台 Finger 服务器以获取关于该系统的用户的信息。

防御：关闭 Finger 服务并记录尝试连接该服务的对方 IP 地址，或在防火墙上进行过滤。

⑦ 利用 LDAP 服务信息。

概览：黑客使用 LDAP 协议窥探网络内部的系统及其用户的信息。

防御：对于探测内部网的 LDAP 进行阻断并记录，如果在公共机器上提供 LDAP 服务，那么应把 LDAP 服务器放入 DMZ。

(5) 伪造虚假消息攻击。

用于攻击目标配置不正确的消息，主要包括 DNS 高速缓存污染、伪造电子邮件。

① DNS 高速缓存污染。

概览：由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息加进来并把用户引向黑客自己的主机。

防御：在防火墙上过滤入站的 DNS 更新，外部 DNS 服务器不应能更改你的内部服务器对内部机器的认识。

② 伪造电子邮件。

概览：由于 SMTP 并不对邮件发送者的身份进行鉴定，因此黑客可以对你的内部客户伪造电子邮件，声称是来自某个客户认识并相信的人，并附带上可安装的特洛伊木马程序，或者是一个引向恶意网站的连接。

防御：使用 PGP 等安全工具并安装电子邮件证书。

5. 基于多维属性的分类法

Edward 将基于过程的分类法的内涵扩展为更广的攻击过程或攻击操作序列，如图 3-2 所示。

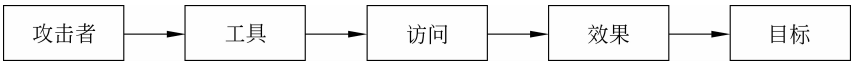

图 3-2　网络攻击操作序列

该分类法是基于多重攻击属性的，按照攻击者类型、使用的工具、攻击所利用的漏洞、被访问的信息、入侵后造成的后果、攻击的目标等属性对网络攻击进行分类构成，如图 3-3 所示，他的分类方法成为多维分类法的经典。他的这篇论文成为美国计算机应急响应小

组(Computer Emergency Response Team,CERT)的重要安全文档。此外基于多维属性的分类法还有 Christ 和林肯实验室的分类法。

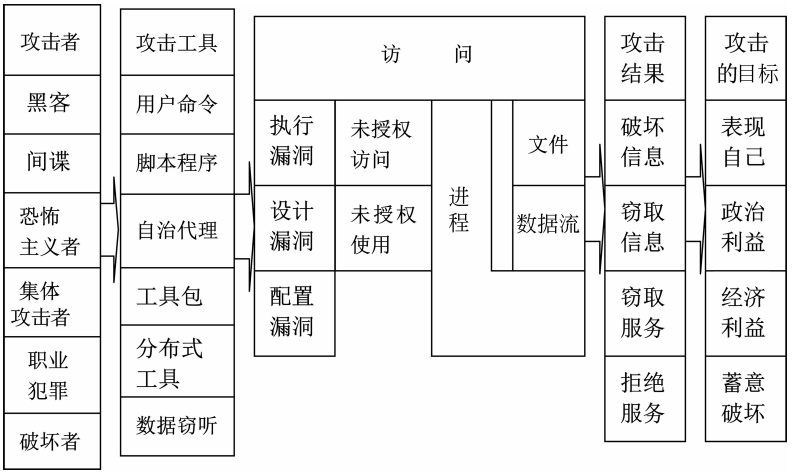

图 3-3　Edward 的多维角度分类法

6. 基于动态攻击演变图的多阶段分类法

Swiler 和 Phillips 等人在 1998 年提出的基于图的攻击建模方法，他们用网络的状态变量集合来表示攻击图的结点，用黑客的动作来表示攻击图的边，并给出了以攻击目标为中心回溯攻击图生成算法及最小攻击代价分析结果，该方法的运行时间对网络的规模具有指数特征。Ammann 提出的基于图搜索的方法，假设网络攻击具有单调性，即黑客在攻击过程中不会放弃已经获得的权限。这种假设在大多数的网络攻击场景中都适用，同时大大降低了算法的复杂度。

基于攻击图思想，可将攻击图技术和动态网络演化结合，提出一种动态攻击演变图模型。该模型借鉴演变图思想将攻击图拓展为随时间域和空间域同时变化的演变攻击图，然后借助子图相似度构建攻击演化阶段模式，分析阶段模式内暂态变化的同时结合时序数据分析阶段模式间的连接变化。入侵路径获取前提是通过手动或自动生成方法生成形式化的攻击图，在多阶段长时间攻击过程中攻击图不可能是一成不变的静态图，在脆弱性变化或权限传递的过程中一定同时受到空间和时间因素的影响，如图 3-4 所示。

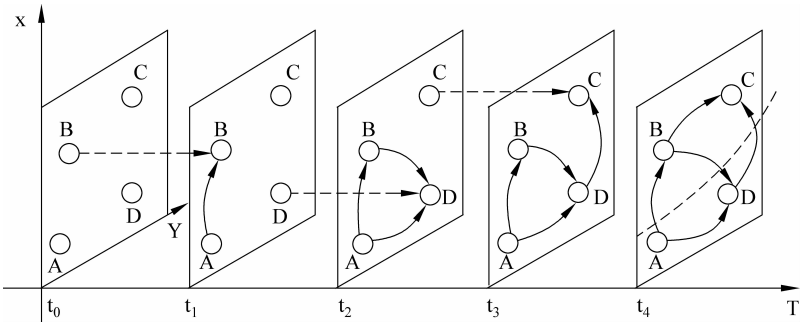

图 3-4　从攻击节点 A 到目标节点 C 的不同时刻多阶段演变过程

由图3-4可知，攻击者A在t_0时刻不具备任何连接，在t_1时刻获取了B的user权限，在t_2时刻其通过B的弱密码安全漏洞或者D的缓冲区溢出漏洞获得了D的root访问权限，进而在t_3时刻获得了C的访问权限，整个过程的叠加图如t_4时刻所示。在复杂系统的不同快照时刻分析每个时刻网络的进化情况是动态网络的优势和研究重点，研究证明，将社交网络、生物网络、网络蠕虫传播结构等复杂系统建模成动态网络，是一种合理有效的攻击表示和分类方式。

7. VERDICT分类法

Lough提出了一种基于攻击特征的攻击分类方法——VERDICT（Validation Exposure Randomness Deallocation Improper Conditions Taxonomy）。其分类方法将攻击分为4类：

（1）不恰当的验证：在未授权访问信息或系统中的不充分或不正确的验证，包括物理安全方面。

（2）不恰当的暴露：系统或信息被不正确的泄露，可能被攻击者直接或间接地开发为弱点。

（3）不恰当的随机性：不充分的随机性或不正确利用随机性导致的攻击。如密码学中随机性的不正确使用。

（4）不恰当的删除：信息使用后被不正确的删除，易遭受的攻击。

它是用来发现网络系统存在的不安全因素，从而对网络系统的安全状况进行安全评估以及进行协议设计的，但对于描述攻击则不适用。VERDICT攻击分类方法缺乏对蠕虫、木马、病毒等恶意代码的分类。

8. 基于复杂网络的攻击分类法

复杂网络抗毁性指的是网络受到攻击时，网络拓扑结构的可靠性，不涉及网络节点和边的可靠性，衡量的是破坏一个系统的难度。复杂网络的攻击方式可分为两种：随机性攻击（random attack）和选择性攻击（selective attack）。随机性攻击就是以某种概率随机破坏网络的节点（边），而选择性攻击是按一定的策略破坏网络的节点（边），一般按照节点的重要性依次进行攻击。选择性攻击的研究最早始于Albert等人，主要关注拓扑结构对复杂网络抗毁性的影响。Holme等人对复杂网络攻击方式做了比较全面的研究，他们将攻击方式分为节点攻击和边攻击，每种攻击方式又包括如下4种不同的策略：

（1）ID（initial degree）攻击方式。根据初始网络节点（边）的度大小顺序来移除节点（边）。

（2）IB（initial betweenness）攻击方式。根据初始网络节点（边）的介数大小顺序来移除节点（边）。

（3）RD（recalculated degree）攻击方式。根据当前网络节点（边）的度大小顺序来移除节点（边）。

（4）RB（recalculated betweenness）攻击方式。根据当前网络节点（边）的介数大小顺序来移除节点（边）。

通过实验发现，WS小世界网络在以上4种攻击方式下的抗毁性差异不大。

9. MIT 林肯实验室的攻击分类方法

MIT 林肯实验室的研究者们提出了一种基于特权提升的多维度攻击分类方法，该分类方法把攻击分为 4 类：User-to-root（U2R）、Remote-to-local（R2L）、Denial-of-Service（DoS）和 Surveilance/probe。这是面向攻击的分类方法，得到了大多数研究者认可。从用户到根权限的特权提升就是攻击效果的一个例子。在攻击过程中，攻击者通常扮演着一定的用户角色并拥有相应的用户权限集。从一般的访问者到普通用户，再到系统管理员，攻击者角色的变化，反映出攻击对目标系统的攻击影响，可以从拥有的资源量的变化，即权限的变化来进行攻击分类。

10. 面向防御的多维度攻击分类方法

大多数攻击具有多阶段的时空特性，一个攻击一般由不同的阶段构成，每个阶段又具有不同的特点。攻击可以用多个属性描述，单一属性无法描述攻击整个过程中各个阶段的特点。现有很多攻击分类研究工作都是从攻击的不同属性和维度进行攻击分类，忽略了描述攻击分类的目的就是为了主动防御和响应攻击这一事实，对攻击危害和防御措施缺乏一致的衡量准则。

根据主动防御的需求，将防御也纳入到攻击属性描述中，全面考虑了攻击成本和损失，对攻击属性进行了提取和分析。在相关攻击分类研究工作的基础上，我们用攻击源头、攻击方式、攻击对象、漏洞利用、攻击自动化程度、攻击目的、攻击成本、攻击损失、防御措施等 9 个攻击属性维度来描述攻击。按照不同的防御措施方法，防御可以分为基于主机的防御和基于网络的防御，也可以分为主动防御和被动防御。表 3-2 以 Code Red 和 Wu-ftpd 攻击为例说明该分类方法的两个攻击实例。

表 3-2　面向防御的多维攻击分类实例

攻击维度	攻击源头	攻击方式	攻击对象	漏洞利用	攻击自动化程度	攻击目的	攻击成本	攻击损失	防御措施
Code Red	本地网络或外部网	构造输入脚本 Stack 缓冲区溢出	Windows IIS web server，版本 4，5，6.0b	配置漏洞 CVE-2001-0500	半自动化	拒绝服务	中	高	安装补丁或关闭 IIS 服务
Wu-ftpd	本地网络或外部网	Stack 缓冲区溢出或 Mapping_chdir 缓冲区溢出	Unix 系统 WU-FTPD 程序	配置漏洞 CVE-1999-0878	半自动化	获取 root 权限	低	高	安装补丁或关闭 ftp 服务

11. 基于检测的攻击分类

Kumar 提出了以检测为目的的攻击分类法，将攻击在系统审计记录中表现出来的特征作为分类的依据。分析这些特征进行，并寻找特征之间的结构化相互关系，从而构造攻击的分类结构。根据网络协议特征分析，可以将攻击行为分为三大类：网络层数据检测到的攻击、传输层数据检测到的攻击和应用层数据检测到的攻击。

3.2　计算机及网络的漏洞分析

网络系统中弱点和漏洞的存在是网络攻击成功的必要条件之一。由于网络系统规模越来越大，系统复杂性逐渐上升，系统内部存在弱点、漏洞几乎不可避免，而且越来越多，据我国国家计算机网络应急技术处理协调中心（National Computer network Emergency Response technical Team/Coordination Center of China，CNCERT/CC）统计报告表明，从2000年到现在，弱点发现呈迅猛增长的趋势。这些可利用的弱点包括应用服务软件中存在的漏洞、网络用户漏洞、通信协议中存在的漏洞、网络业务系统漏洞、程序安全缺陷、操作系统中的漏洞、网络安全产品的弱点、客户软件的弱点及其他非技术性的弱点等。

3.2.1　漏洞的基本概念及分类

本节给出了漏洞的基本概念及分类标准。

1. 漏洞的基本概念

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，它使得攻击者在未被授权的情况下访问或者攻击某个系统成为可能。

计算机漏洞一般包括硬件和软件的漏洞，其中：

（1）硬件漏洞：线路安排过密或晶体管放错了位置等情况都有可能造成硬件漏洞。

（2）软件漏洞：大部分的漏洞都属于软件漏洞，这不仅仅因为软件的种类繁多与数量庞大，更主要的是因为漏洞“需要被发现”这一属性——人们日常使用中直接接触的就是软件产品，软件的使用者更多，导致其中的漏洞被发现的概率更大。

漏洞的属性包括：

（1）普遍存在性：任何复杂系统都或多或少、或明显或暗藏地存在漏洞。

（2）不可根除性：不能根除某个复杂系统中所有的漏洞而使之成为一个完美的系统。

（3）需要发现性：漏洞需要在人们使用某系统的时候才能被发现出来。

（4）可以修复性：人们可以通过各种形式的补丁来修复某一特定的漏洞。

2. 漏洞的分类

随着计算机软硬件系统的日益扩大，系统的复杂性也越来越高，这导致没有人能完全细致地了解整个系统。漏洞的具体成因可能有许多种：工程师设计时考虑不周、程序员编码时不够严谨、企业为了追求效益而故意从简等。但究其根本，我们也许能得到一个更高层面的回答：这个世界上没有完美的事物。漏洞的分类如表3-3所示。

表3-3　漏洞的分类

分类方法	分类内容	
产生原因	有意	恶意
		非恶意
	无意	

续表

分类方法	分类内容	
存在位置	硬件	
	软件	应用软件漏洞
		系统漏洞
		服务端漏洞
攻击原理	拒绝服务	
	缓冲区溢出	
	后门	
	内核错误	
	欺骗	
	提升权限	
	其他攻击方式	

3.2.2 网络漏洞

计算机网络的飞速发展与普及应用，在带给了人们方便的同时，也带来了许多不可避免的网络漏洞。关于网络漏洞，目前还没有一个准确统一的定义。不过还是存在一个较为通俗的网络漏洞的描述性定义：存在于计算机网络系统中的、可能对系统中的组成和数据造成损害的一切因素。

3.2.3 漏洞分级

不同的机构都有各自不同的评级体系和评级标准。国际上承认的一些标准有：微软标准、Oracle标准、法国安全组织的FrSIRT标准、美国计算机紧急响应小组标准（United States Computer Emergency Readiness Team，US-CERT）、国家计算机漏洞库（National Vulnerability Database，NVD）、中国“国家漏洞库”（China's National Vulnerability Database）等。接下来简要介绍其中4种。

1. 微软标准（Microsoft Vulnerability Severity Rating Standards）

（1）危急，无须用户激活的网络蠕虫传播的漏洞。

（2）高，漏洞的利用会危及用户数据的机密性、完整性和有效性。

（3）中，开发利用该漏洞比较困难，漏洞的利用受限于默认配置、验证等因素。

（4）低，漏洞的利用非常困难，或者漏洞的影响非常小。

2. Oracle标准（Vulnerability Security Ratings of Oracle）

（1）高，利用该漏洞基本不需要攻击者掌握专业知识。须立刻对受影响的产品应用补丁。

（2）中，利用该漏洞需要攻击者掌握一些专业知识。对受影响产品应用补丁的顺序

在高级别之后。

(3) 低,利用该漏洞需要攻击者具备相当的专业知识。对受影响产品应用补丁的顺序在中级别之后。

3. FrSIRT 标准(FrSIRT Vulnerability Severity Ratings Standard)

(1) 严重,可远程利用的漏洞,可导致系统崩溃(不需要用户交互)。

(2) 高,可远程利用的漏洞,可导致系统崩溃(需要用户交互)。

(3) 中,可被远程和本地利用,可导致拒绝服务和权限提升的漏洞。

(4) 低,只可本地利用,不能危机系统安全。

4. 美国计算机安全紧急响应小组标准(US-CERT)

US-CERT 用测量值来评价一条漏洞的严重程度,测量值是一个 0～180 的数值。

3.2.4　漏洞的发现

一种方法是当攻击者利用了这些漏洞攻击你的服务器后你就自然知道了;第二种方法就是主动去发现漏洞:使用漏洞扫描工具来对服务器进行扫描,从而发现漏洞。不论你在系统安全性上投入多少财力,攻击者仍然可以发现一些可利用的特征和配置缺陷。发现一个已知的漏洞,远比发现一个未知漏洞要容易得多,这就意味着,多数攻击者所利用的都是常见的漏洞,这些漏洞,均有书面资料记载。

3.2.5　物联网软件服务漏洞分类

嵌入式物联网设备在安全机制和服务的实现方面还面临许多问题,鉴于此,OWASP 物联网项目针对智能设备最常见 IoT 漏洞进行了详细的分类,即如下的 OWASP TOP10 物联网漏洞。

1. 不安全的 Web 接口

一般情况下,攻击者首先会在智能设备的 Web 接口中寻找 XSS、CSRF 和 SQLi 漏洞。此外,这些接口中还经常出现“默认用户名和密码”和“缺乏账户锁定机制”之类的漏洞。

2. 认证/授权漏洞

通常情况下,如果存在这种类型的漏洞,则意味着攻击者可以通过用户的弱密码、密码恢复机制的缺陷以及双因子身份验证机制的缺失来控制智能设备。

3. 不安全的网络服务

这里主要的问题是“开放了不必要的端口”“通过 UPnP 向互联网暴露端口”以及“易受 DoS 攻击的网络服务”。另外,未禁用的 Telnet 也可能被用作攻击向量。

4. 缺乏传输加密/完整性验证

这里的问题主要集中在敏感信息以明文形式传递,SSL/TLS 不可用或配置不当,或使用专有加密协议方面。含有这类漏洞的设备容易受到 MiTM 中间人攻击。

5. 隐私问题

OWASP 将该漏洞定义为“收集的个人信息过多”“收集的信息没有得到适当的保护”,以及“最终用户无权决定允许收集哪类数据”。攻击者可以读取设备的敏感信息,或

使其成为僵尸网络的一部分。

6. 不安全的云接口

这种类型的漏洞意味着，只要攻击者能够访问 Internet，就可以获取私人数据。一方面，用于保护存储在云中的私人数据的加密算法的加密强度通常很弱；另一方面，即使加密算法具有足够的加密强度，仍然可能存在缺乏双因子身份验证，或者允许用户使用弱密码等安全漏洞。部分攻击者可以获得对设备的完全控制权。

7. 不安全移动设备接口

主要问题是“弱密码”“缺乏双因子认证”和“无账户锁定机制”。这种类型的漏洞常见于通过智能手机管理的物联网设备。该漏洞使得攻击者可以像用户那样使用该应用程序。

8. 安全可配置性不足

这个漏洞的本质在于，由于用户无法管理或应用安全机制，导致安全机制无法对设备充分发挥作用。有时，用户根本不知道这些机制的存在。

9. 不安全的软件/固件

攻击者能够安装或更新物联网设备任意固件（无论是官方还是自定义的固件），因为系统没有进行相应的完整性或真实性检查。此外，攻击者还可以通过无线通信完全接管设备。

例如，攻击者可以更新固件并完全接管设备，使设备变成僵尸网络的一部分。

10. 脆弱的物理安全

攻击者可以拆开智能设备，找到该设备的微控制器 MCU、外部存储器等。此外，通过 JTAG 调试器或其他连接器（UART、I2C、SPI），攻击者还可以对固件或外部存储器进行相应的读写操作。攻击者可以在设备中植入后门，获得 root 权限并将设备变为僵尸网络的一部分。

美国国家标准与技术研究院发布了一份关于国际物联网国际网络安全标准化（IoT）状态的白皮书 NISTIR 8200，其中列出了用以提高软件安全的软件保障标准以及相关指南。

3.3 网络脆弱性的评估技术

3.3.1 网络脆弱性的概念

脆弱性是指一个系统的可被非预期利用的方面，例如系统中存在的各种漏洞，可能的威胁就可以利用漏洞给系统造成损失。系统遭受损失，最根本的原因在于本身存在脆弱性。脆弱性是信息系统存在风险的内在原因。网络脆弱性（Network Vulnerability），指网络协议、网络软件、网络服务、主机操作系统及各种主机应用软件在设计及实现上存在种种安全隐患和安全缺陷。如果将所有的脆弱性表示为集合 V，包含的元素可表示为：V＝{硬件缺陷，系统软件漏洞，应用软件漏洞，协议漏洞，管理漏洞，……}。

3.3.2　网络脆弱性的评估

由于信息系统的重要性、计算机网络的开放性、信息系统组成部分的脆弱性和用户的有意、无意不当操作或恶意的破坏企图，使信息系统面临许多风险，这是信息安全问题产生的根本原因。本节介绍网络脆弱性的基本概念及评估方法。

1. 网络脆弱性评估的基本概念

基于成本和效益的考虑，以及对信息技术不断发展的现实认识，解决信息安全问题的思路不是倾尽人力、物力、财力，将风险彻底降为零，达到绝对的安全，而是以把风险降低到信息系统可以接受的水平，从而使信息系统的安全性得到提高为目标的。为了达到该目标，必须知道信息系统面临哪些风险，其分布情况和强度有多大，这是信息系统风险评估工作的重要意义。

目前，在计算机网络脆弱性评估领域所要研究的问题很多，包括脆弱性因素提取、量化指标建立、评估方法确定、评估标准过程、数学模型建立、关键结点分析、关键路径分析、漏洞依赖关系、主机信任关系、评估辅助决策等各个方面。更为重要的是如何将上述各方面问题有机地结合起来，形成计算机网络主机脆弱性评估规范流程及系统框架。

归纳起来，针对计算机网络脆弱性评估的研究主要包括：评估的目标、评估的标准、评估的规范流程、评估技术及评估模型、评估辅助决策。若更加具体地对每个方面进行研究，可能存在以下研究难点：

(1) 网络评估中脆弱性影响因素的提取，这不仅包括主机脆弱性因素，还包括网络脆弱性因素。

(2) 网络评估中量化评估指标的建立，依据不同算法从网络脆弱性因素中提取量化指标。

(3) 确定网络评估模式，建立网络评估框架。

(4) 对目标网络拓扑结构进行分析。

(5) 对目标网络主机的依赖关系进行分析。

(6) 通过对目标网络的评估，找出目标网络的脆弱结点及关键结点。

(7) 对目标网络进行路径分析。

(8) 充分考虑目标网络中的各种影响因素，建立合理的数学模型。

(9) 通过网络评估，形成评估辅助决策。

(10) 目前未知的其他难点。

实践表明，系统与网络的安全性取决于网络中最薄弱的环节。检测网络系统中的薄弱环节，最大限度地保证网络系统的安全，其中最为有效的方法就是定期对网络系统进行安全性分析，及时发现并改正系统和网络存在的脆弱性，并分析出现这些安全问题的原因，以及在整体上进行何种程度的改进。因此，作为这一切前提的网络脆弱性评估显得尤为重要。

而漏洞之间的关联性、网络主机之间的依赖性、网络服务的动态性及网络连接的复杂性决定了网络脆弱性评估是一项非常复杂的工作。

网络脆弱性分析架构如图 3-5 所示。网络脆弱性分析架构由几个方面构成，包括代

理(包含有监控器)、脆弱性分析机和主动防御机等,以及通信接口,也就是如图所示的事件交互层、脆弱性分析和重配置层。由代理控制的、监控特定的度量的子实体称为监控器。代理是中间体,只要度量发生显著改变,代理将产生事件,利用计算脆弱性系数 vc (vulnerability coefficient)的网络脆弱性分析算法,脆弱性分析机将从代理获取的事件做相关统计。根据在网络不同结构中得到的脆弱性系数,主动防御机通过脆弱性分析和重配置层依次在代理中设定策略。网络资源的动态重新配置使得攻击影响最小。其中,脆弱性度量是表示网络攻击事件中系统行为的特有的参数。脆弱性度量可以分为两类,也就是节点层次分析的度量以及流层次分析度量。

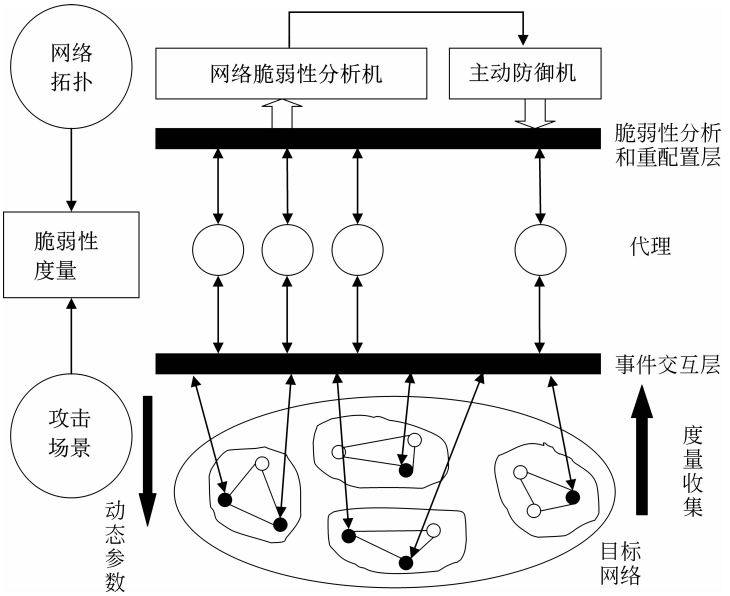

图 3-5　网络脆弱性分析架构

节点的度量包括 CPU 时间、现有的服务数量、缓冲的使用、文件系统的大小等。流的度量有已用带宽、连接的数量、各种协议(IP、ICMP、TCP 和 UDP)通信流速率、丢包率、连接利用率、服务队列长度等。被监控和检验的这些脆弱性度量量化了网络攻击的影响。

2. 网络脆弱性评估方法分类

以下介绍几种网络脆弱性的评估分析方法。

(1) 可生存性分析方法。生存性的中心思想是即使在入侵成功后,且系统的重要部分遭到损害或摧毁时,系统依然能够完成任务,并能及时修复被损坏的服务能力。图 3-6 为可存性网络分析方法模型。

图 3-6 描述分析方法的四个步骤：首先评估当前或待开发系统的目标任务和需求,得出步骤一中架构的定义形式和性能。在步骤二中,基于任务目标和系统失效的分析结果,确定基本的服务和设施,这些服务和设施的使用特征被映射到架构上,它们的执行是为了确定基本组件的构成,而这些组件对传输必要的服务和维持必要的设施必须有效。

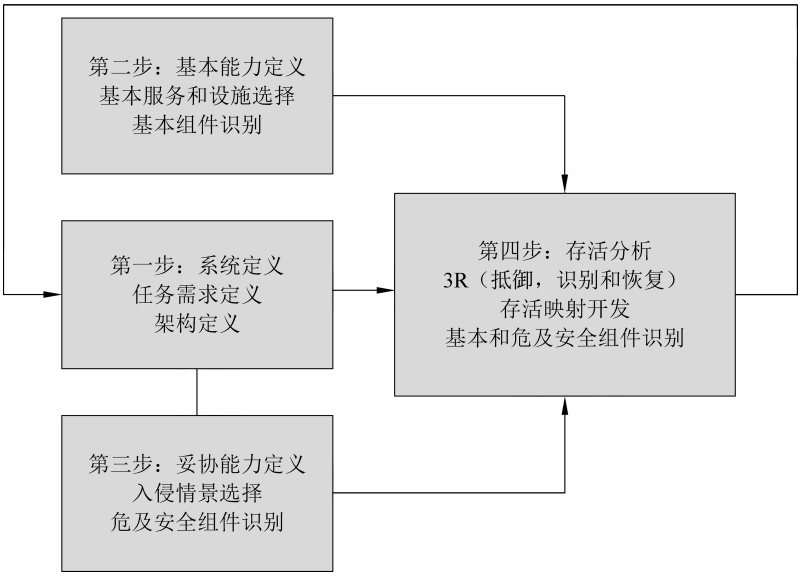

图 3-6　可生存性分析方法模型

在步骤三中，基于系统环境、风险及入侵可能性的评估，选择入侵情景。这些入侵情景同样被映射到架构中，其执行是为了确认相应妥协组件的组成，或入侵可能损害的组件。在步骤四中，将软场景（softspot）组件作为基本组件和妥协组件，基于步骤二和步骤三的结果，分析软场景组件及其支持抵御（Resistance）、识别（Recongnition）和恢复（Recovery）等主要存活性能的架构，此“3R”的分析概述为存活映射。采用矩阵表示映射，由每个入侵情景及其对应软场景、目前和推荐的 3R 架构策略组成。存活映射提供最初架构和系统需求反馈，结果通常形成成本-效益分析和存活改善的迭代过程。虽然本方法是为大规模分布式网络系统设计，但对其他的架构（例基于主机和实时系统）同样适用。

（2）基于连通性的网络脆弱性评估。若网络越容易断开（连通性越弱），则网络越脆弱，脆弱性越高；若网络连通性越强，则该网络脆弱性越低。如果不从网络连通性这个角度来考虑，而是从网络安全和网络攻击的角度来评估网络脆弱性，假设网络中存在的连接路径都不会断开，则连通性越强，存在攻击的路径越多，网络攻击成功的可能性越大，网络脆弱性越高；相反，网络的连通性越弱，攻击可选择路径越少，攻击成功率越低，网络脆弱性就越低。在评估网络脆弱性时，应该考虑网络的物理连接、网络系统漏洞以及网络入侵路径等多种因素。

（3）基于入侵路径的网络脆弱性评估。大多数网络入侵事件的发生是一个层次入侵的过程，真正的目标主机可能是难以直接攻破的，但与它相关的其他机器可能存在安全脆弱性，这往往是由于配置不当或存在不同程度的信任关系所造成，入侵者可以从薄弱环节入手，基于层次入侵的思想逐步提高自己的权限，最终达到控制目标机器的目的。该方法考虑网络的拓扑结构以及主机间的依赖关系，提出相关的算法对网络脆弱性进行一定的评估。其关键是对各种网络脆弱性因素的全面掌握与对评估算法准确性的严格要求。

（4）基于图的网络脆弱性评估。该方法提出了一个“攻击图”的概念，它可以用来发

现最可能成功的攻击路径，也可以用来模拟仿真各种攻击行为。攻击图中的结点包含信息有机器名、用户权限、用户能力等；边代表攻击者采取动作所引起的状态改变。产生攻击图需要3种类型的输入：攻击模板、网络配置及攻击者描述。其中，攻击模板描述了已知攻击的一般步骤，包括攻击所需条件；网络配置中包括机器类型、硬件类型、操作系统、用户描述、机器描述、网络描述等；攻击者描述包含攻击者的攻击能力描述。

(5) 基于代理(Agent)的网络脆弱性评估。该方法主要完成了两个任务：提出了一个网络脆弱性评估框架；提出了一些网络脆弱性评估度量。其中，网络脆弱性评估度量将网络中各结点的脆弱性度量分为两类：可计算度量和通信度量。可计算度量是指系统CPU状态、开发服务程序、内存使用情况以及文件系统信息等；通信度量是指带宽、连接数、网络协议、连接队列长度、丢包率及其他通信信息度量。利用脆弱性索引函数将相关的脆弱性度量结合在一起，形成脆弱性量化指标，以此表示该结点目前的连接状况。当实施网络攻击时，各个结点上的代理收集其脆弱性度量，并通过脆弱性索引函数计算脆弱性量化指标，系统通过对各个指标的分析此来对主机的安全状况进行评估。

3.3.3 评估网络脆弱性的准则

在评估时应遵循如下一些准则。

1. 标准性准则

评估方案的设计和具体实施都依据国内和国外的相关标准进行。

2. 可控性准则

评估过程和所使用的工具都具有可控性。评估所采用的工具都经过多次评估项目考验，或者是根据具体要求和组织的具体网络特点定制的，具有很好的可控性。

3. 整体性准则

评估从实际需求出发，而不是局限于网络、主机等单个的安全层面。整个服务涉及安全管理和业务运营以保障整体性和全面性。

4. 最小影响准则

评估工作应具备充分计划，不对或尽可能少地对现有网络的运行和正常工作产生影响。

3.4 信息系统安全风险的概念与评估

3.4.1 风险的基本概念

风险是指人们对未来行为的决策及客观条件的不确定性而导致的实际结果与预期结果之间偏离的程度。客观环境和条件的不确定性是风险的重要成因，风险的大小取决于实际结果与预测结果偏离的程度。风险因素、风险事故和损失是风险的三要素，风险的存在具有客观性和普遍性，风险的发生具有偶然性和必然性，风险还具有变动性。

3.4.2 信息系统安全风险的概念

信息系统的安全风险，是指由于系统存在的脆弱性，人为或自然的威胁导致安全事件

发生所造成的影响。

网络风险是指在互联网日益成为日常生活重要手段的过程中，因技术、管理及法律等方面的不确定性而造成的损失的不确定性。网络风险主要表现为以下几个方面：网络故障风险、媒体法律风险、安全性风险。其中安全性风险主要包括网络自身漏洞风险、网络攻击风险、安全管理风险等。

评估风险的两个关键因素包括威胁发生的可能性和威胁发生可能造成的影响。评估者根据威胁评估、弱点评估和现有的安全措施评估三者相结合，通过经验分析或定性分析的方法得出前者，后者一般从威胁对资产的影响的分析中得到。

威胁对资产的影响一般可以从其损害的资产的完整性、保密性、可用性等方面考虑；

(1) 完整性的损害，指对数据或系统造成了非授权改变，包括被窃取或其他有形损失。

(2) 保密性的损害，指被保护的资产遭到了未授权的泄露。

(3) 可用性的损害，指对授权的合法用户来说，资产部分或全部不可用。

通过以上三个方面的分析，将威胁对资产的影响映射到该威胁事件的发生对信息系统所在组织结构造成的社会影响，可以用客户信任度、经济损失等方面进行描述。明确威胁发生的可能性及其影响之后，可以通过风险分析矩阵来对风险的严重程度定级。

3.4.3　信息安全风险评估

信息安全风险评估，则是指依据国家有关信息安全技术标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程，它要评估信息系统的脆弱性、信息系统面临的攻击威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险。从而，尽可能地减少弱点，避免攻击，识别风险，保护信息系统的资产免受攻击侵害。

风险是与安全事件紧密相关的。识别风险就是分析潜在的安全事件对具体的信息系统是否存在发生的可能性，是否需要考虑和应对。构成风险的要素有4个：资产、威胁、弱点和安全措施。在识别了这4个要素之后，可以开始评估组织机构的风险。缺少其中一个关键因素，将无法形成风险。识别风险可以减少风险评估的工作量。风险是由威胁(威胁源和行为)、脆弱性和客体(资源)构成的。而威胁源是随机分布在各处的。威胁源必须利用脆弱性才能形成风险。存在风险就必定有脆弱性。在实际的风险分析中，以脆弱性作为风险分布分析的基础，结合威胁源的情况，就可以得到信息系统风险的分布状况。风险识别的核心工作是识别威胁源和脆弱性。对风险的描述可以借助场景叙述的方式来进行。所谓场景，就是威胁事件可能发生的情况。对威胁场景进行描述的同时，对风险进行评估，并确定风险的等级。

1. 威胁源的识别

威胁源包括黑客、内部误操作人员、内部恶意攻击人员、外部恶意攻击人员、商业间谍、国家(军事)间谍人员等。对信息系统威胁源的识别方法可以有信息系统分析、技术工具检测等。信息系统的分析指根据信息系统的特点，分析其可能引起哪些威胁源的关注

和面临哪些威胁源的威胁。入侵检测工具是专门用于检测信息系统是否受到攻击的工具。入侵检测的记录将反映出信息系统曾经遭受的网络攻击及攻击企图，并能记录攻击及攻击企图来自何处。操作系统及应用软件日志或专门的审计工具能记录下本地或通过网络所做的操作，可用于分析威胁源。

2. 脆弱性的识别

脆弱性识别是风险分析的核心内容。减少脆弱性能大大减轻信息安全的工作量。因此，脆弱性的发现技术和工具是信息安全研究的重点。目前，已经有很多对已知脆弱性（漏洞）检测发现与未知漏洞进行发掘的方法、技术手段和工具。

（1）漏洞扫描，对已知的漏洞进行扫描检测。漏洞扫描分为基于网络的漏洞扫描、基于主机的漏洞扫描、分布式漏洞扫描和数据库漏洞扫描。在国内，部分信息安全公司已经从比较单一的系统漏洞检测向应用软件缺陷扫描的方向扩展。

（2）Fuzz 测试（黑盒测试），通过构造可能导致程序出现问题的输入数据和其他各种尝试方式进行自动测试。

（3）源码审计（白盒测试），一系列的工具都能协助发现程序中的安全缺陷，例如最新版本的 C 语言编译器。信息系统中的很多应用程序是针对专门的业务定制的，没有通用的漏洞检测工具，因此也需要进行源码审计。

（4）交互式反汇编（Interactive Disassembler，IDA）（灰盒测试），与上面的源码审计非常类似，用于有软件但没有源码的情形。IDA 是一个非常强大的反汇编平台，能基于汇编码进行安全审计。

（5）动态跟踪分析，记录程序在不同条件下执行的全部和安全问题相关的操作（如文件操作），然后分析这些操作序列是否存在问题。

（6）补丁比较，提供商的软件出了问题通常都会在补丁中解决，通过对比补丁前后文件的源码（或反汇编码）就能了解到漏洞的具体细节。

以上手段中都需要通过人工参与分析来找到全面的流程覆盖路径。通过分析整个进程的运行来获得脆弱性信息，分析手法多种多样，有分析设计文档、分析源码、分析反汇编代码、动态调试程序等。

另外，入侵检测工具也能提供脆弱性的一些线索。

信息系统的脆弱性，除了以上的检测技术，还有针对特定技术和应用的脆弱性检测，特别是安全技术的脆弱性检测，如密码安全性、防火墙的安全性检测等。

密码协议分析，如 SSL 协议分析工具，由于是专用软件，因此市面上几乎没有合适的产品。作为安全研究人员实验用的工具有 SSL Dump、SSL Sniffer 等。其他一些协议分析仪或协议分析软件也部分集成了 SSL 协议解析模块。

异常检测是对信息系统功能的不正确设计、实现、配置和使用等异常情况的检测。

除了技术方面的脆弱性检测外，还有物理、硬件和管理方面的脆弱性检测。技术不是万能的，尤其在有人参与的信息系统中，人的行为可能导致技术的失效和误用。因此，管理在信息安全中也是极其重要的部分。而管理是否恰当和完善，是否得到有效实施，都需要通过管理的脆弱性检测得到识别。