ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术 网络攻击定义及描述规范

Information security technology — Specifications of definition and description for network attack

（征求意见稿）

(2017-5-1)

XXXX－XX－XX 发布　　－XX－XX

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分 标准结构与编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会提出。

本标准由全国信息安全标准化技术委员会归口。

本标准主要起草单位：北京大学软件与微电子学院、中国电子技术标准化研究院、中国科学院软件研究所

本标准主要起草人：

引　言

近年来，随着网络应用的普及和迅猛发展，网络攻击也日渐增多，攻击的方法更加先进和复杂，攻击的形式更是多种多样，无孔不入，对网络安全造成了严重威胁。

网络攻击涉及多方面的问题，包括网络攻击的界定、网络攻击涉及的角色、网络攻击的目的、网络攻击的分级和分类、网络攻击的过程、网络攻击的关键技术、网络攻击常用的方法、网络攻击后果的评估等内容。为了增强网络安全保障，面对网络攻击各个层面的挑战，应当对网络攻击进行准确的定义和描述，为抵御网络攻击夯实基础。

本标准适用于规范网络攻击的定义与描述、网络攻击的过程与关键技术、评估网络攻击的效果。

信息安全技术　网络攻击定义及描述规范

1　范围

本标准给出了网络攻击的定义、描述、典型过程、关键技术和效果评估。

本标准适用于规范网络攻击的定义与描述、网络攻击的过程与关键技术、评估网络攻击的效果。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.8－2001 信息技术　词汇　第8部分：安全

GB/T 25069－2010　信息安全技术　术语

GB/T 25068.3–2010 信息技术 安全技术 IT网络安全　第3部分：使用安全网关的网间通信安全保护

3　术语和定义

GB/T 5271.8－2001、GB/T 25069－2010和GB/T 25068.3－2010界定的术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069－2010中的术语和定义。

3.1　安全级别　security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精确地控制对数据的访问。

［GB/T 25069－2010，定义2.2.1.6］

3.2　访问控制［列］表　access control list

由主体以及主体对客体的访问权限所组成的列表。

［GB/T 25069－2010，定义2.2.1.43］

3.3　逻辑炸弹　logic bomb

一种恶性逻辑程序，当被某个特定的系统条件触发时，造成对数据处理系统的损害。

［GB/T 25069－2010，定义 2.2.1.87］

3.4　（特洛伊）木马　Trojan horse

一种表面无害的程序，它包含恶性逻辑程序，可导致未授权地收集、伪造或破坏数据。

［GB/T 25069－2010，定义2.1.37］

4　网络攻击的定义

4.1 攻击的定义

在IT系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能（包括窃取数据）的尝试。

4.2 网络攻击的定义

通过计算机、路由器等网络设备，利用网络中存在的漏洞和安全缺陷实施的一种行为，其目的在于窃取、修改、破坏网络中存储和传输的信息；或延缓、中断网络服务；或破坏、摧毁、控制网络基础设施。

5 网络攻击的描述

本标准采用下述5维方法对网络攻击进行描述，如图1所示：

a) 网络攻击涉及的角色
b) 网络攻击的分类
c) 网络攻击的典型过程
d) 网络攻击的关键技术
e) 网络攻击后果的评估

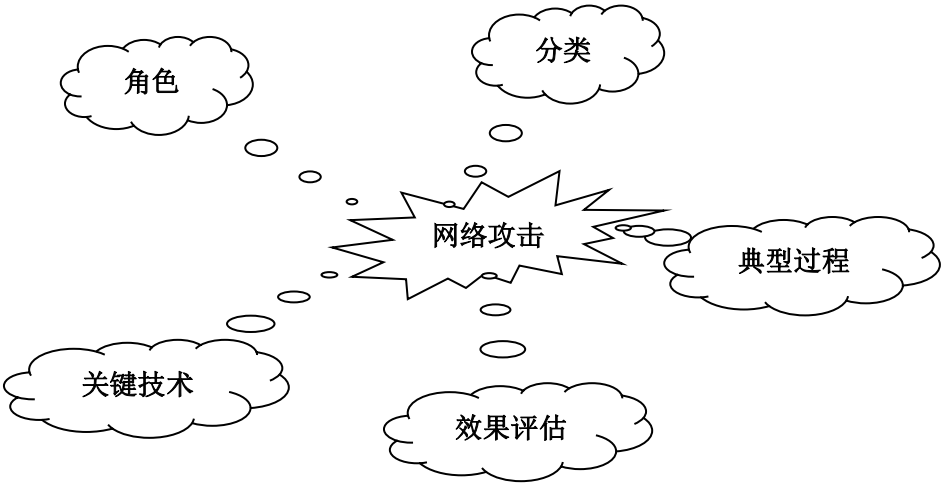

图1 网络攻击的5维描述

5.1 网络攻击涉及的角色

网络攻击中涉及到的角色包括5类：

a) 攻击者
b) 受害者
c) 监控者
d) 服务提供者
e) 宽带提供者

5.1.1 网络攻击者角色

故意利用网络安全的脆弱性，以窃取或泄露信息系统或网络中的资源为目的，危及信息系统或网络资源可用性的任何人/组织。

5.1.2 网络攻击的受害者角色

在网络攻击的活动中，信息、资源或财产被侵害的一方。

5.1.3 网络监控者角色

对网络运行和服务进行监视和控制，对网络上的活动、行为或资产进行监视和控制的人/组织。

5.1.4 网络服务提供者角色

为网络运行和服务提供基础设施、信息和中介、接入等技术服务的网络服务商和非营利组织。[1]
网络服务提供者包括因特网服务提供商ISP和为ISP提供主干服务的网络服务提供商NSP。

- NSP：
  提供用于因特网接入服务的基础设施，为ISP提供主干服务、WEB用户服务等。
- ISP：
  提供互联网服务，可分为网络硬件服务提供者和网络软件服务提供者。前者包括网络接入服务提供者和网络信息存储空间提供者，后者包括网络内容提供者和网络技术服务提供者。

5.1.5 网络带宽提供者角色

为网络服务提供带宽的组织。

5.2 网络攻击分类

本标准采用五维网络攻击分类法，对网络攻击分别按攻击对象、攻击方式、漏洞利用、攻击后果和严重程度进行分类。

5.2.1 攻击名称

攻击名称是对网络攻击的归类性描述。攻击名称可以代表一类攻击的描述，或表征一次攻击。

5.2.2 第 1 维：攻击对象

网络攻击按照攻击对象可以分为两大类：硬件和软件。

攻击对象	子级别1	子级别2	子级别3	子级别4
硬件	计算机 传输链路	存储设备 …… 网络设备 物理设备	硬盘 U盘 光盘 …… 路由器 交换机 网关 集线器 网络布线 …… 键盘 监控器	

1) [1] http://www.sipo.gov.cn/yl/2011/201102/t20110222_580220.html 网络服务提供者侵权行为探讨 中华人民共和国国家知识产权局.

			……	
软件	操作系统	Windows 系列	Windows 7 Windows 10 ……	
		Unix 系列	Linux FreeBSD ……	Redhat linux 6.0 10.1
		MacOS 系列	MacOS X ……	
		……		
	应用	服务器	数据库 电子邮件 网站	 IIS
		用户	办公软件 ……	Microsoft Word
		……		
	网络	协议	传输层协议	TCP/IP协议
		……	……	

5.2.3 第 2 维：攻击方式

网络攻击方式可以通过下表进行描述：

攻击方式	子级别1	子级别2
病毒	文件感染型病毒 系统/引导记录感染型病毒	
蠕虫	Macro Mass mailing Network aware ……	
缓冲区溢出	堆 栈	
拒绝服务	Host-based Network-based	资源hogs Crashers …… TCP flodding UDP flooding ICMP flooding ……

	……	
网络攻击	Distributed Spoofing Session hijacking Wireless attacks Web application attacks ……	WEP cracking Cross site scripting Parameter tampering Cookie poisoning Database attacks Hidden field manipulation
物理攻击	Basic Energy weapon ……	HERF LERF EMP

5.2.4 第 3 维：漏洞利用

漏洞利用可以通过下表进行描述：

漏洞类别	**子级别1**	**子级别2**
软件bug	缓冲区溢出 意料外的联合使用问题 未对输入内容进行预期检查 Race-conditions ……	
系统配置不当	使用默认配置 未关闭多余端口 使用临时端口 ……	
口令失窃	使用弱口令 字典攻击 蛮力攻击 ……	口令长度过短 口令复杂度过低 利用用户名字典数据库 利用口令字典数据库 ……
嗅探未加密通讯数据	共享介质 服务器嗅探 远程嗅探 ……	
设计存在缺陷	TCP/IP协议的缺陷 ……	

系统攻击	远程攻击 内部攻击 ……	

5.2.5 第 4 维：攻击后果

网络攻击后果可以通过下表进行描述：

攻击后果	子级别1	子级别2
非法控制	非法侵占系统 非法使用硬件 ……	
数据泄露	敏感数据泄露 关键代码泄露 个人隐私泄露 ……	
数据篡改	数据修改 数据增加 数据删除 ……	
拒绝服务	拒绝服务 分布式拒绝服务 ……	
设备故障	终端故障 …… 传输链路故障 ……	计算机节点故障 …… 路由器、交换机故障 ……

5.2.6 第 5 维：严重程度

网络攻击的严重程度可以通过下表进行表征：

严重程度	子级别1	子级别2
第一级	损害公民、法人和其他组织的合法权益	损害公民的合法权益 损害法人的合法权益 损害其他组织的合法权益
第二级	严重损害公民、法人和其他组织的合法权益 损害社会秩序和公共利益	严重损害公民的合法权益 严重损害法人的合法权益 严重损害其他组织的合法权益 损害社会秩序 损害公共利益
第三级	严重损害社会秩序和公共利益 损害国家安全	严重损害社会秩序 严重损害公共利益
第四级	对社会秩序和公共利益造成特别严重损害	对社会秩序造成特别严重损害 对公共利益造成特别严重损害

	严重损害国家安全	
第五级	对国家安全造成特别严重的损害	

5.2.7 网络攻击分类的举例

攻击名称	攻击对象	攻击方式	漏洞利用	攻击后果	严重程度
Blaster	WindowNT 4.0, XP, 2000, Server 2003	网络感知型蠕虫	CAN-2003-0325	TCP包flooding DOS	
Chernobyl	Window 95, 98	文件感染型病毒		信息破坏	
Code Red	IIS 4, 5, 6.0 beta	网络感知型蠕虫	CVE-2001-0500	栈缓冲区溢出；TCP包flooding DOS	
Ramen	RedHat 6.2, 7.0	网络感知型蠕虫	CVE-2000-0573 CVE-2000-0666 CVE-2000-0917	主机型DOS; UDP和TCP包flooding DOS	
Slammer	SQL Server 2000	网络感知型蠕虫	CAN-2002-0649	栈缓冲区溢出；UDP包flooding	
Sobig.F	Email 客户端	Mass-mailing蠕虫	配置	木马	
Trojaned Wuarchive FTPD	Unix系列	木马		破坏	

5.3 网络攻击的典型过程

网络攻击的典型过程如图2所示：

a) 攻击源的隐藏
b) 信息搜集判断
c) 选择入侵方式
d) 提升系统权限
e) 安装系统后门
f) 清除入侵记录

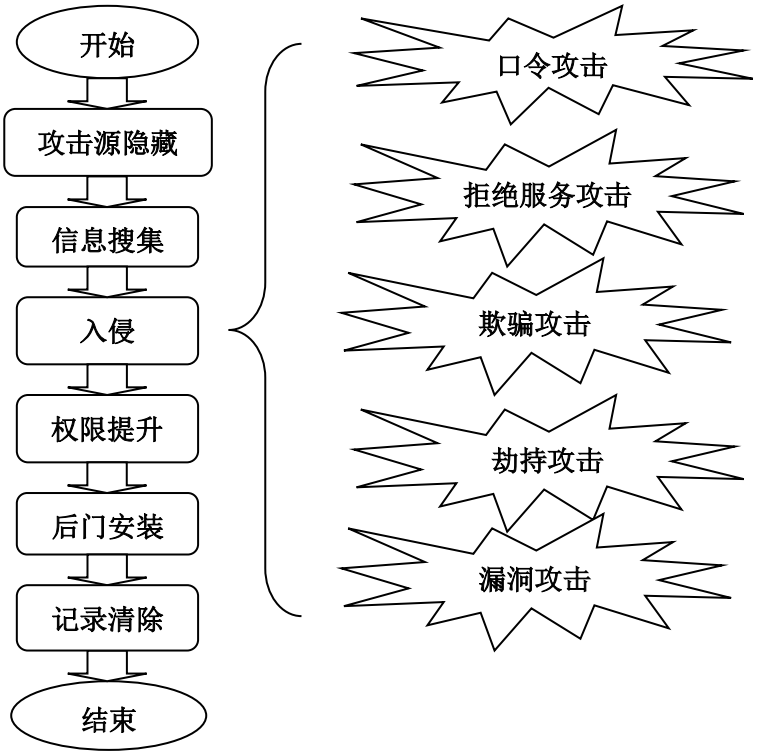

图 2 网络攻击的典型过程

5.3.1 攻击源的隐藏

通过各种方式隐藏攻击来源，逃避溯源软件的追踪。

5.3.2 信息搜集判断

在对目标对象实施网络攻击前，攻击者查看攻击环境、搜集目标环境的各种相关信息，为实施网络攻击进行准备。

典型的信息搜集判断过程如下：

a) 获得基本信息
b) 标识网络的地址范围
c) 标识活动的机器
d) 标识开放端口和入口点
e) 获取操作系统类型和机器端口对应的服务
f) 制定网络攻击蓝图

常用的信息搜集工具有：

a) Ping、fping、ping sweep
b) ARP探测
c) Finger
d) Whois
e) DNS/nslookup
f) 搜索引擎

g) telnet

5.3.2.1 获得基本信息

基本信息包括目标网络的IP地址、域名信息等。

5.3.2.2 标识网络的地址范围

标识目标网络的地址范围或子网掩码，明确攻击范围。

5.3.2.3 标识活动的机器

标识目标网络中活动的服务器和终端，明确攻击对象。

5.3.2.4 标识开放端口和入口点

通过端口扫描标识开放端口和入口点。端口扫描的分类如图3所示：

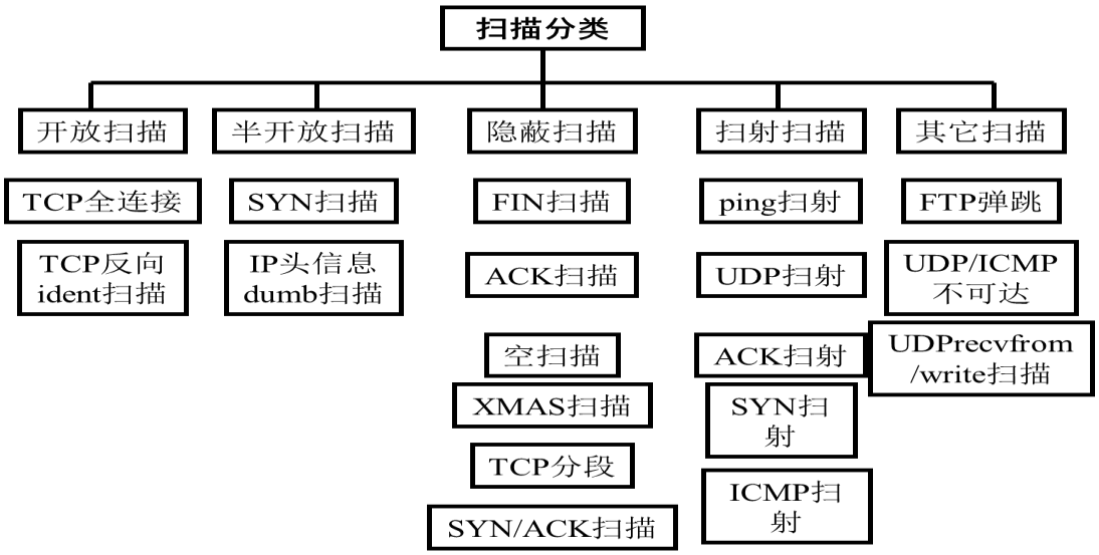

图3 端口扫描的分类

常见的端口扫描工具有：

a) Nmap
b) Xscan
c) SuperScan
d) Shadow Security Scanner
e) MS06040Scanner

5.3.2.5 获取操作系统类型和机器端口对应的服务

获取操作系统的类型和机器端口对应的服务，为实施网络攻击奠定基础。

5.3.2.6 制定网络攻击蓝图

在画出尽可能完整的目标网络拓扑图的基础上，制定网络攻击蓝图。

5.3.3 选择入侵方式

根据搜集到的信息进行判断后，选取适当的入侵方式对目标网络实施攻击，包括但不限于以下入侵方式：

a) 口令攻击
b) 拒绝服务攻击
c) 欺骗攻击
d) 劫持攻击
e) 漏洞利用攻击

5.3.3.1 口令攻击

攻击者通过信息搜集判断，获取了目标网络中的用户名、开放服务，操用系统类型等关键信息，就可以开始实施口令攻击。

口令攻击的类型包括但不限于：

a) 字典攻击。逐一尝试攻击者定义的词典中的单词或短语的攻击方式。
b) 蛮力攻击。逐一尝试字母、数字、特殊字符所有可能组合的攻击方式。
c) 组合攻击。字典攻击和蛮力攻击的组合。
d) 其他类型的攻击，例如社会工程学攻击。

5.3.3.2 拒绝服务攻击

拒绝服务攻击的目标有下面两类：

a) 消耗目标服务器的可用资源。致使目标服务器忙于应付大量非法和无用的连接请求，耗尽服务器所有的资源，致使服务器对正常的请求无法进行及时响应，形成服务中断。

b) 消耗网络的有效带宽。攻击者通过发送大量有用或无用的数据包，占用全部带宽，使合法的用户请求无法通过链路抵达服务器；服务器对合法请求的响应也无法返回给用户，形成服务中断。

通常，拒绝服务攻击可以分为拒绝服务攻击(DOS)和分布式拒绝服务攻击(DDOS)两类。

常见的DoS和DDOS攻击方式包括但不限于：

a) IP Spoofing
b) Land
c) Smurf
d) Fraggle
e) Win Nuke
f) SYN Flood
g) ICMP Flood
h) UDP Flood
i) ICMP重定向报文
j) ICMP报文不可达
k) TearDrop
l) CPU Hog
m) RPC Locator

5.3.3.3 欺骗攻击

攻击者通过欺骗方式，获取目标网络用户的重要信息，或获取目标用户的信任。常见的欺骗攻击包括但不限于：

a) IP欺骗。伪装成其他计算机的IP地址，获得信息或特权。

b) 电子邮件欺骗。例如，伪造发送方地址进行欺骗，获取信任或得到敏感信息。

c) WEB欺骗。例如，基于网站的欺骗。

5.3.3.4 劫持攻击

攻击者通过劫持服务器与用户之间的通信，实施网络攻击，包括但不限于：

a) 会话劫持攻击。例如，在共享网段中A和B站点的正常通信被攻击者C截获后，C冒充B与A进行会话，获取信任或敏感信息。

b) 包劫持攻击。例如，攻击者通过包截取工具，获得用户账户密码等敏感信息。

c) 域名劫持攻击。例如，攻击者使一个域名指向一个由攻击者控制的服务器。

5.3.3.5 漏洞利用攻击

常见的漏洞利用攻击包括但不限于：

a) 利用CGI漏洞的攻击。

b) 利用FTP等协议漏洞的攻击。

c) 利用服务程序漏洞的攻击。

d) 缓冲区溢出攻击。

5.3.4 提升攻击权限

攻击权限一步或逐步提升包括但不限于：

a) 本地用户获得非授权读权限。

b) 本地用户获得非授权写权限。

c) 远程用户获得非授权账号信息。

d) 远程用户获得特权文件的读权限。

e) 远程用户获得特权文件的写权限。

f) 远程用户获得系统管理员权限。

5.3.5 安装系统后门

后门指攻击者再次进入网络的隐蔽通道。如果攻击者获取了系统的存取权限，建立后门就相对容易；如果没有获取相应的系统权限，攻击者需通过木马实现后门。

5.3.6 清除入侵记录

攻击者通过各种方法清除入侵记录隐藏攻击痕迹，包括但不限于：

a) 清除所有的日志文件或修改/删除日志文件中与攻击相关的记录。

b) 修改相关文件的信息。攻击者通过修改相关文件中的某些信息，例如时间和文件长度信息，隐藏攻击痕迹。

c) 将文件、目录或共享设备的属性设置为隐藏。

d) 重命名文件。例如，攻击者将他的文件名修改为类似于系统文件名。

e) 清除网络上存在的攻击痕迹。

5.4 网络攻击的关键技术

网络攻击的关键技术包括但不限于以下几种，各种技术之间可以是包含关系。通常，攻击者会采用多种攻击技术组合的方法进行网络攻击。

5.4.1 获取口令

如5.3.3.1所述，口令攻击的类型包括但不限于：字典攻击、蛮力攻击、组合攻击和社会工程学攻击等。通常，攻击者用下述方法窃取口令：

a) 通过网络监听获得用户口令。尽管这种方法有一定局限性，但攻击者常常能够成功获得他所在网段的所有用户账号和口令；

b) 如果已知目标用户的账号，通过字典攻击等方法破解用户口令。这种方法不受网段限制，但耗时较长；

c) 如果已知服务器上的用户口令文件，例如Linux系统的Shadow文件，通过字典攻击等方法破解用户口令。

通过系统中的缺省账户或弱口令进行攻击，往往容易攻击成功。

5.4.2 安装木马程序

攻击者通过安装木马程序达到各种网络攻击的目的，例如攻击完成后可以方便地再次进入目标网络、通过木马程序消除入侵痕迹等。

5.4.3 WWW 欺骗

WWW欺骗有多种方式，都与网站访问相关。攻击者伪装为合法网页，在网页上提供虚假信息，实施网络攻击。例如，钓鱼网站仿冒真实网站的URL地址和页面内容，或利用真实网站的漏洞插入有害的HTML代码，获取用户的银行/信用卡账号等敏感信息。

5.4.4 电子邮件攻击

电子邮件攻击包括但不限于：

a) 电子邮件轰炸，即邮件炸弹，指用伪造的IP地址和电子邮件地址不断向同一信箱发送垃圾邮件，致使无法正常收/发/处理电子邮件。

b) 电子邮件欺骗。攻击者伪装为系统管理员，例如使用与系统管理员相同的邮件地址，进行各种欺骗性攻击。例如，给目标用户发送邮件要求用户修改口令，或在看似正常的附件中加载病毒或其他木马程序。只要目标用户按照邮件提示进行操作，攻击者就可以对目标系统实施攻击。

5.4.5 通过一个节点攻击其他节点

攻击者以某一台可以控制的终端或服务器为跳板，攻击网络中的其他服务器或终端。

5.4.6 网络监听

攻击者通过监听网络通信，获取攻击者所需的相关信息，为后续攻击奠定基础。

5.4.7 挖掘系统漏洞

攻击者通过各种方法挖掘网络协议、服务器和操作系统等的漏洞，为后续攻击进行准备。

5.4.8 窃取特权

通过各种木马程序和漏洞利用提升攻击权限，直至获得目标网络的部分或完全控制权。

5.4.9 零日攻击

零日漏洞指未经标识的漏洞，攻击者可以利用该漏洞进行攻击，即零日攻击。该名称的由来是，该

漏洞没有公开报道，使程序拥有者只有“零日”打补丁或提供减轻/消除该漏洞影响的方法。

5.4.10 高级持续性攻击（APT）

高级持续性攻击(APT)指为了商业或政治利益针对特定实体（如组织、国家等）进行一系列秘密和连续攻击的过程。“高级”指攻击方法先进复杂；“持续”指攻击者连续监控目标对象，并从目标对象不断提取敏感信息。

5.5 网络攻击后果的评估

5.5.1 信息泄露

攻击者实施网络攻击后获得目标系统中的敏感信息，例如敏感的文本文件、多媒体文件和关键程序代码。

5.5.2 拒绝服务

攻击者实施网络攻击后，致使一种或多种网络功能失效、网络服务延缓或中断。

5.5.3 代码执行

攻击者获得目标系统的代码执行权限，以本地或远程方式执行自己嵌入的代码，达到恶意的攻击目的。

5.5.4 权限提升

没有任何权限的攻击者获得目标网络中的某种权限或某些权限；或拥有较少或较低权限的攻击者获得目标网络中较多或较高的权限。