ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37027—2018

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

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
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 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位: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、中国科学院信息工程研究所、上海众人网络安全技术有限公司、蓝盾信息安全技术有限公司、北京永信至诚科技股份有限公司、北京奇安信科技有限公司、国家计算机网络与信息安全管理中心、北京神州绿盟信息安全科技股份有限公司、国云科技股份有限公司、北京时代新威信息技术有限公司、启明星辰信息技术集团股份有限公司、贵州省公共大数据重点实验室、海南大学信息科学技术学院、重庆邮电大学网络空间安全与信息法学院、沈阳东软系统集成有限公司、阿里云计算有限公司、北京天际友盟信息技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、黑龙江省网络空间研究中心、百度在线网络技术(北京)有限公司、北京鼎普科技股份有限公司。

本标准主要起草人:卿斯汉、刘贤刚、叶润国、胡影、王利明、谈剑峰、鲍旭华、蔡晶晶、季统凯、李雪莹、徐震、吴汉炜、周由胜、陈驰、张大江、吕志泉、严寒冰、杨辰钟、韩炜、李佳、杨大路、翟湛鹏、罗锋盈、王新杰、彭长根、马杰、路娜、孙建坡、李文瑾、陈景妹、谢安明、徐雨晴、王希忠、方舟、王海洋、周启明、沈晴霓、文伟平、张泉、孙松儿、吴槟、姜伟鹏。

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。面对网络攻击各个层面的挑战，对网络攻击进行准确的定义和描述，增强网络安全保障，为抵御网络攻击夯实基础。

信息安全技术　网络攻击定义及描述规范

1　范围

本标准界定了网络攻击的定义、属性特征和多维度描述方法。

本标准适用于网络运营者进行网络建设、运维和管理时对安全的设计与评估。

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 7408—2005　数据元和交换格式　信息交换　日期和时间表示法

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

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 5271.8—2001、GB/T 25069—2010和GB/T 25068.3—2010界定的以及下列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 5271.8—2001、GB/T 25069—2010、GB/T 25068.3—2010中的某些术语和定义。

3.1

网络攻击　network attack

通过计算机、路由器等计算资源和网络资源，利用网络中存在的漏洞和安全缺陷实施的一种行为。

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

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]

3.4

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]

3.5

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]

注：本标准简称“木马”。

3.6

欺骗 spoofing

假冒成合法的资源或用户。

[GB/T 25068.3—2010，定义 3.21]

3.7

威胁 threat

一种潜在的计算机安全违规。

[GB/T 5271.8—2001，定义 08.05.04]

3.8

高级持续性威胁 advanced persistent threat

精通复杂技术的攻击者利用多种攻击方式对特定目标进行长期持续性网络攻击。

4 缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁（Advanced Persistent Threat）

DoS：拒绝服务攻击（Denial of Service）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

WWW：万维网（World Wide Web）

5 网络攻击概述

网络攻击为利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击。网络攻击具有动态和迭代性，随着攻击过程的进行，攻击者对目标的掌握和控制程度不断深入，可实施的攻击面越大，可能造成的安全影响也越大。根据网络攻击实施步骤的粗细层次及复杂程度，网络攻击又可分为单步攻击和组合攻击。单步攻击是具有独立的、不可分割的攻击目的的简单网络攻击，组合攻击是单步攻击按照一定逻辑关系或时空顺序进行组合的复杂网络攻击。通常情况下，一个典型的复杂网络攻击过程包括信息收集、攻击工具研发、攻击工具投放、脆弱性利用、后门安装、命令与控制、攻击目标达成等 7 个步骤。典型、多步骤网络攻击过程的详细描述参见附录 A。

网络攻击具有多个属性特征，主要包括：

a) 攻击源：发动网络攻击的源，它可能为组织、团体或个人。

b) 攻击对象：遭受网络攻击并可能导致损失的目标对象。

c) 攻击方式：攻击过程中采用的方法或技术，体现网络攻击的原理和细节。网络攻击的关键技术参见附录 B。

d) 安全漏洞：攻击过程中所利用的网络或系统的安全脆弱性或弱点。

e) 攻击后果：攻击实施后对目标环境和攻击对象所造成的影响和结果。

网络攻击各属性特征之间的关系如图 1 所示，其组合关系的分类示例参见附录 C。

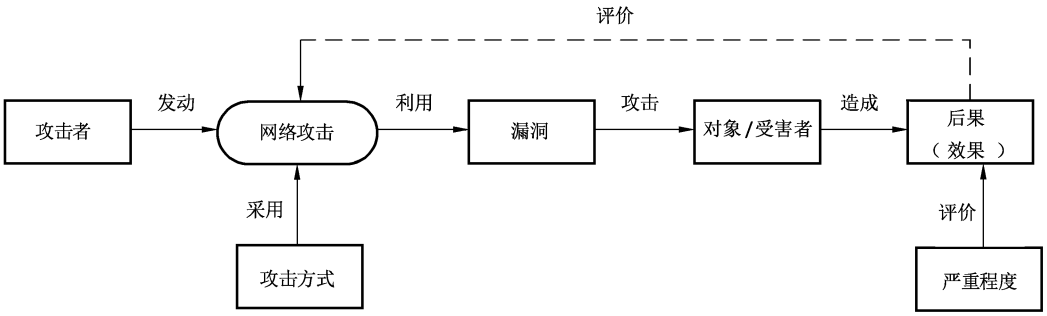

图 1　网络攻击各属性特征的关系

从生命周期角度看，一次成功的网络攻击涉及的角色（包括参与者和利益相关者）包括 4 类：

a）　网络攻击者：利用网络安全的脆弱性，以破坏、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个人或组织，如某黑客组织。

b）　网络攻击受害者：在网络攻击的活动中，信息、资源或财产受到侵害的一方，如某互联网应用提供商。

c）　网络攻击检测者：对网络运行和服务、网络活动进行监视和控制，具有对网络攻击进行安全防护职责的组织。

d）　网络服务提供者：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，如云服务提供商、电信运营商等。

本标准从多个维度对网络攻击进行描述，并提供一种网络攻击统计方法，以方便实现对网络攻击的统一标识，以及对上报的网络攻击事件的多维度自动化统计。

6　网络攻击多维度描述

6.1　第 1 维分类：攻击对象

攻击对象是网络攻击的具体攻击目标，并在攻击成功后可能带来信息泄露、数据篡改、系统不可用等安全影响。一次网络攻击存在一个或多个攻击对象。可以按照攻击对象对网络攻击进行分类描述，如表 1 所示。

表 1　攻击对象分类表

子级别 1	子级别 2	说　明
计算机	移动终端	如智能手机、Pad、上网本等
	PC	个人电脑：包含台式机、笔记本等
	服务器	在计算机网络中为用户提供服务的专用设备
	其他	
工控设备	SCADA	SCADA 是数据采集与监视控制系统
	PLC	PLC 是可编程逻辑控制器
	DCS	分布式控制系统
	其他	

表 1（续）

子级别 1	子级别 2	说　明
网络设备	路由器	具有路由功能的网络设备
	交换机	
	网关	除路由器、交换机之外的其他网关类产品，如防火墙等
	集线器	集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上
	其他	
操作系统	Windows 系列	
	Unix 系列	
	MacOS 系列	
	IOS	
	Android 系列	
	其他	如 AIX、VMware 等
服务器软件	数据库	如 sqlserver、mysql、oracle、db2、sybase、postgreSQL 等
	电子邮件	如 Exchange、foxmail、gmail 等
	中间件	如 COM、CORBA、J2EE、Docker、tomcat、weblogic、jboss 等
	FTP 服务器	如 Vsftpd、FileZilla、Serv-U、Xlight 等
	Web 软件	如 IIS、apache、struts、ngix、CMS 等
	其他	
用户软件	办公软件	如 Microsoft Word、WPS、OpenOffice、Adobe PDF 等
	社交软件	如 weibo、facebook、twitter 等
	聊天工具	如 weixin、qq 等
	其他	
网络基础设施	云计算	IaaS/PaaS/SaaS 类型的云计算平台
	物联网	如智能网关、智能摄像头、智能家电，摄像头，车联网设备等
	电信网	如 3G、4G 和 5G 网络等
	DNS	如 BIND 等
	CA	如金融 CA、政务 CA 等
	其他	

6.2　第 2 维分类：攻击方式

网络攻击者在对攻击对象实施网络攻击时，会使用各种类型的攻击方式，以实现攻击目标。可以按照攻击方式对网络攻击进行分类描述，如表 2 所示。

表 2　攻击方式分类表

子级别 1	子级别 2	说明
拒绝服务	基于主机	如源 hogs、Crashers 等
	基于网络	如 P Spoofing、SYN Flood、ACK Flood、UDP Flood、ICMP Flood、IGMP Flood、HTTP Flood、HTTPS Flood、DNS Request Flood、DNS Response Flood、SIP Flood、NTP REFLECTION FLOOD 等
信息收集	网络结构	如地址扫描、端口扫描、反响映射、慢速扫描、体系结构探测、DNS 域转换、Finger 服务、LDAP 服务等
	系统和应用服务	如操作系统扫描、体系结构探测、系统服务扫描、访问控制[列]表扫描、应用扫描、漏洞扫描等
	业务信息	如业务信息收集等
代码利用	二进制代码攻击	如缓冲区溢出、数据库攻击等
	WEB 应用攻击	如命令注入、sql 注入、SSRF、CSRF、Cookie poisoning、路径穿越、信息泄露、webshell 等
	应用安全	如口令猜测、暴力破解、提高攻击者的安全级别等
	恶意样本	如木马、病毒、逻辑炸弹、勒索软件、后门等
	信道攻击	如拦截、中间人攻击、协议操作、流量注入、通信阻碍等
消息欺骗	网络协议电子欺骗	如 IP 欺骗、ARP 缓存欺骗、DNS 高速缓存污染等
	电子邮件	如伪造/污染电子邮件等
	应用数据	如网络钓鱼(phishing)攻击等
物理攻击	物理安全旁路	如取下电池绕过 BIOS 口令、绕过控制设备直接访问存储、旁路密码芯片等
	物理窃取	如偷窃计算机、令牌等
	物理破坏设备或组件	如破坏计算机、网络交换机等
硬件攻击	硬件完整性攻击	如破坏硬件锁、硬件完整性检查机制等
	插入恶意逻辑	如更新恶意固件、植入硬件木马、插入恶意控制代码等

6.3　第 3 维分类:漏洞利用

网络攻击者在对攻击对象实施成功的网络攻击时,必定利用了攻击对象的某种类型安全漏洞。可以按照安全漏洞对网络攻击进行分类描述,如表 3 所示。

表 3　安全漏洞分类表

子级别 1	子级别 2	说明
软件 bug	缓冲区溢出	主要通过向程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，造成程序崩溃或使程序转而执行其他指令
	格式串问题	如在 printf 类调用中没有正确使用格式串参数，使攻击者可以控制格式串的内容，从而操纵 printf 调用越界访问内存
	释放后重用	主要源于对象的引用计数操作失当，导致对象被非预期地释放后重用。进程在后续操作那些已经被污染的对象时执行攻击者的指令
	二次释放	主要源于代码中涉及内存使用和释放的操作逻辑失当，使同一个堆缓冲区可以被反复释放，最终导致可以执行任意指令
	意料外的联合使用	主要通过对程序不同层输入不同的内容，联合使用这些输入达到攻击目的
	文件操作的顺序和锁定	如未正确处理对同一文件的读/改/写的操作顺序，造成攻击者可以对某些重要文件进行篡改
	其他	
系统配置不当	使用存在缺陷的默认配置	如在新安装系统时不修改默认配置，而该默认配置存在安全缺陷
	未关闭多余端口	未关闭没有使用的端口，使攻击者可以利用该端口进行攻击
	使用临时端口	开启临时端口，使攻击者可以利用该端口进行攻击
	使用弱口令	使用“123456”“admin”“password”等容易被猜测到的口令
	使用空口令	不设置口令或口令为空
	不安全的信任关系	如由于信任关系，一旦攻破了信任群中的某一个机器，其他机器就存在被攻击的风险
	其他	
设计缺陷	通信协议缺陷	如 TCP/IP 协议的设计缺陷，使攻击者可以提升权限
	算法设计缺陷	如加密算法的设计缺陷，使攻击者容易解密
	绕过安全机制	如可以绕过认证机制，使攻击者可以不用认证即取得授权
	其他	
输入验证	SQL 注入	未充分对攻击者提交给数据库的参数进行检查过滤，导致数据库信息泄露或执行相关命令
	跨站脚本执行	未充分对攻击者提交给网站的数据进行检查过滤，导致攻击者可以将恶意代码发送给其他用户
	文件攻击	如传入的文件名未经过合理的校验，或者校检被绕过，从而操作意料之外的文件，导致文件泄露甚至恶意代码注入
	命令注入	系统命令调用和执行的函数在接收攻击者的参数输入时未进行充分检查过滤，导致执行攻击者指定的命令
	目录遍历	未充分对攻击者输入的数据进行检查过滤，使攻击者可以构造一些特殊字符，访问允许位置以外的文件
	其他	

6.4 第4维分类:攻击后果

一次成功的网络攻击会对攻击对象导致不同的攻击后果。可以按照攻击后果对网络攻击进行分类描述,如表4所示。

表4 攻击后果分类表

子级别1	子级别2	说明
网络故障	网络中断	网络中断,无法进行正常通信
	服务质量下降	网络服务质量下降,可用下降百分比进行描述
通信异常	协议规范失效	改变网络协议规范,如ARP欺骗、ARP病毒、ping of death攻击、泪滴攻击等
	传输路径改变	发送伪造路由信息,造成传输路径改变
	内容修改	在网络数据中插入数据包,改变原有传输数据内容;破坏网站与客户间传输数据的完整性和保密性
内容窃取	网络嗅探	通过嗅探、截获等方式获取网络数据、窃听通信双方间的有用信息、捕捉和篡改通信双方的通信数据等
配置变更	设备被黑	通过修改网络设备的访问规则、路由条目等,造成网络规划变更或非法访问
设备故障	物理损坏	设备无法使用和恢复,如cpu、内存、硬盘等物理损坏
	可恢复损坏	设备暂时无法使用,但可通过设备重启等方式进行恢复
	功能异常	设备虽然可以使用,但个别功能报错或运行异常
非法侵入	—	未经授权对系统进行访问;在系统中置入木马、病毒等;收集、阻断、降级或破坏信息系统或其中的信息
非法占用	资源无效占用	计算资源、存储资源的无效使用
	资源私有占用	计算资源、存储资源的私有使用
权限提升	—	通过缺陷和漏洞利用、缓冲区溢出等攻击方法提升访问权限
应用故障	服务异常	通过漏洞利用、代码挖掘等手段,改变应用的正常功能
	服务中断	受到拒绝服务攻击、邮件炸弹、C&C等攻击时应用系统服务出现中断
信息泄露	账号异常	如账号被盗、密码被暴力破解、账号滥用、多地异常登录等
	数据泄露	数据内容泄露、文档泄露、程序过程泄露、加密方式泄露等;收集敏感数据但不篡改数据内容
信息篡改	密码篡改	如修改密码、证书等
	内容篡改	内存修改、混淆;文件内容增加、修改;数据库记录变更等
数据丢失	—	如文件删除、数据条目删除、数据库删除、配置清除等
信息泛滥	—	发送大量不属于非正常业务的数据,如垃圾邮件、广告信息等
信息展示	—	通过技术手段使被攻击者主动或被动访问指定的信息内容,在网络上进行传播

6.5 第5维分类:严重程度

严重程度用于反映网络攻击的严重性,可以定性或定量表示。网络攻击的严重程度可通过多个攻击属性综合评价获得,例如从攻击后果影响和攻击可利用程度两方面进行评价,也可考虑时间、环境对

网络攻击的影响综合判断获得。可以按照攻击后果对网络攻击进行分类描述，如表5所示。

表5　攻击严重程度分类表

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 对国家安全造成损害	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 对国家安全造成严重的损害	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
第五级	对国家安全造成特别严重的损害	

7　网络攻击统计项

7.1　统计项

网络攻击的统计项如图2所示，包括必选的统计项和可选的统计项。在图2中，必选的统计项以实线框表示，可选的统计项以虚线框表示。

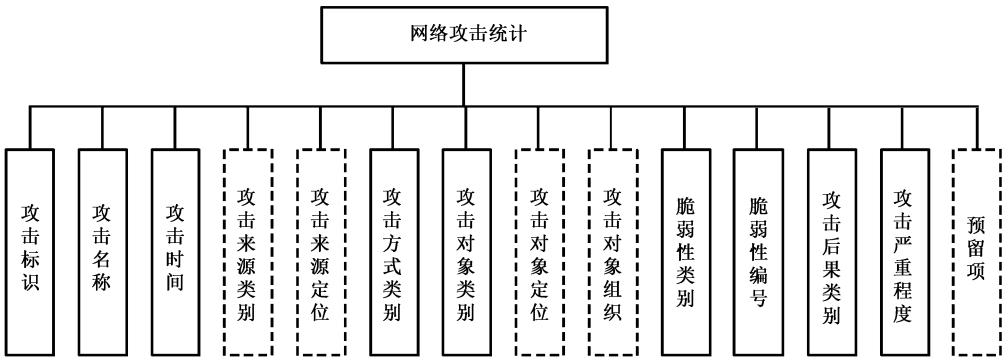

图2　网络攻击的统计项

7.2　攻击标识

唯一标识每一个攻击事件，并在全局范围内具有唯一性。

7.3　攻击名称

攻击方式的名称，如“利用Edge漏洞的缓冲区溢出攻击”。

7.4 攻击时间

攻击发生的具体时间，格式采用 GB/T 7408—2005 中的完全表示法的扩展模式。

7.5 攻击来源类别（可选）

攻击来源指利用网络安全的脆弱性，以破坏、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个人、组织或国家。本字段用于描述攻击来源的个人、组织或国家名称。

7.6 攻击来源定位（可选）

与定位攻击来源相关的信息，例如 IP 地址、域名、AS 号等。

7.7 攻击方式类别

攻击方式的类别，其分类描述参见 6.2 和表 2。

7.8 攻击对象类别

受到攻击的对象类别，其分类描述参见 6.1 和表 1。

7.9 攻击对象定位（可选）

与定位攻击对象相关的信息，例如 IP 地址、域名、AS 号等。

7.10 攻击对象组织（可选）

遭受攻击的人员、组织或国家名称。

7.11 脆弱性类别

攻击所利用的脆弱性类别。其分类描述参见 6.3 和表 3。

7.12 脆弱性编号

攻击所利用的脆弱性编号，包括国内漏洞库编号和国际漏洞库标号，如 CVE2017-11888。

7.13 攻击后果类别

攻击造成的后果类别。其分类描述参见 6.4 和表 4。

7.14 攻击严重程度

攻击的严重程度可以定性或定量表示。其分类描述参见 6.5 和表 5。

7.15 预留项

根据实际工作需要，可以增加 1 个或多个预留项。可以为空，即用占位符表示；也可以为攻击报送单位的名称或代码；也可以为其他相关统计信息或备注等。

附 录 A
（资料性附录）
典型网络攻击过程

A.1 概述

网络攻击的典型过程如图 A.1 所示。

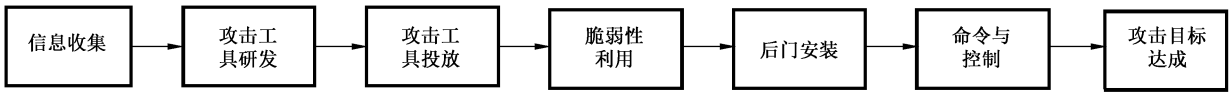

图 A.1 典型网络的攻击过程

A.2 信息收集

在实施网络攻击前，攻击者通过技术手段或社会工程学方法，收集目标系统的各种有关信息，包括外部环境信息、目标系统的配置信息和网络情况、相关人员的邮件及社交关系等。在这个阶段，攻击者会充分、详细地收集各种相关信息，以发现漏洞和脆弱性，为实施网络攻击进行准备。

A.3 攻击工具研发

根据收集到的详尽信息，攻击者确定入侵目标系统的最佳途径，针对性地研制攻击工具，并进行测试验证。最常见的攻击工具是客户端应用程序的数据文件，如带有漏洞利用代码的 pdf 文件或 office 文件。

A.4 攻击工具投放

将攻击工具投放到目标系统上。最常见的三种投放方式是电子邮件附件、网站挂马和移动存储介质。

A.5 脆弱性利用

攻击工具被投放到目标系统后，在目标系统中触发攻击代码运行。大多数情况下，利用目标系统的应用程序漏洞或操作系统漏洞来触发执行，也可利用社会工程学方法或系统的机制来触发执行，从而实施网络攻击。

A.6 后门安装

当攻陷目标系统以后，在目标系统上安装远程访问木马、后门等，使攻击者能够长期控制目标系统。后门是指攻击者再次进入目标系统的隐蔽通道；如果攻击者获取了目标系统的存取权限，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。大部分的恶意软件在这个阶段

安装。

A.7 命令与控制

攻击者一旦控制目标系统并安装了后门，会控制目标系统与攻击者建立的命令与控制服务器进行通信，以便长期控制目标系统。

A.8 攻击目标达成

攻击者采取行动对目标系统实施攻击，实现攻击目标。常见的攻击目标包括三类：1)窃取数据，从目标系统中收集、加密并传送信息；2)破坏数据，或者破坏系统；3)将目标系统当做跳板，进一步攻击其他系统扩大战果。

附 录 B
（资料性附录）
网络攻击关键技术

B.1 概述

网络攻击关键技术包括但不限于 B.2～B.11 中的几种，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。

B.2 获取口令

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。

B.3 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。

B.4 Web 欺骗

Web 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。

B.5 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。

B.6 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。

B.7 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。

B.8 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。

B.9 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。

B.10 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。

B.11 高级持续性威胁攻击

高级持续性威胁攻击（APT 攻击）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。

附 录 C
（资料性附录）
网络攻击分类示例

网络攻击分类示例如表 C.1 所示。

表 C.1 网络攻击分类示例

攻击名称	攻击对象	攻击方式	漏洞利用	攻击后果	严重程度
HTTP_Microsoft_Windows_Edge_安全漏洞[CVE-2017-11888]	Edge 浏览器（软件/用户软件/桌面软件/Edge/AAA/1.1.1.1）补充字段（受害者组织名称、IP 地址）	远程代码执行（代码利用/二进制代码攻击）	（软件 bug/缓冲区溢出）补充字段：CVE 编号 CVE-2017-11888	数据泄露/应用故障	第一级
HTTP_SQL 错误信息泄露	数据库	信息泄露		可能会泄露服务器端敏感信息，从而利用它们进行下一步攻击	第一级
HTTP _ 木马 _ Win32.Pony_连接	Window 系统所有版本	有害程序		窃取浏览器、Email、FTP 等各种客户端保存的账号	第二级
HTTP _ IIS6.0 _ WebDAV 远程代码执行漏洞	IIS 6.0 及以下	远程代码执行	CVE-2017-7269	通过微软 IIS 6.0 的 WebDAV 服务的 ScStoragePathFromUrl 函数缓存区溢出漏洞，攻击者以“If:＜http://”开始的较长 header 头的 PROPFIND 请求执行任意代码	第二级
DDoS 攻击	网络资源	泛洪攻击	N/A	应用故障/服务中断	第二级
HTTP _ Struts2 _ S2-045/S2-046 远程命令执行攻击	Apache struts2	远程代码执行	CVE-2017-5638	Struts 2.3.5-Struts 2.3.31，Struts 2.5-Struts 2.5.10 版本存在严重的漏洞，在使用 Jakarta 插件处理文件上传操作时可能导致远程代码执行漏洞	第三级

表 C.1（续）

攻击名称	攻击对象	攻击方式	漏洞利用	攻击后果	严重程度
TCP_NSA_EternalBlue_（永恒之蓝）_SMB 远程代码执行漏洞[MS17-010]	Window 系统所有版本	获取权限 代码执行	CVE-2017-0144 CVE-2017-0147	栈缓冲区溢出； 攻击者可以利用 smb 服务获取目标主机的管理员权限	第三级
Stuxnet	伊朗核设施	工控系统蠕虫	MS10-046 MS10-061 MS08-067 ……	破坏离心机运转	第四级

参 考 文 献

[1] GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范

[2] 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.http://www.sipo.gov.cn/yl/2011/201102/t20110222 580220.html