



中华人民共和国国家标准

GB/T 37027—2025

代替 GB/T 37027—2018

网络安全技术 网络攻击和网络攻击事件判定准则

Cybersecurity technology—Criteria for determining network attack and
network attack incident

2025-02-28 发布

2025-09-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 描述信息要素 2

 5.1 网络攻击 2

 5.2 网络攻击事件 2

6 判定条件 3

 6.1 判定概述 3

 6.2 网络攻击的判定条件 4

 6.3 网络攻击事件的判定条件 6

7 计数方法 7

 7.1 计数概述 7

 7.2 网络攻击的计数 7

 7.3 网络攻击事件计数 7

附录 A（资料性） 典型攻击对象类型 10

附录 B（资料性） 典型网络攻击过程 12

附录 C（资料性） 网络攻击和网络攻击事件的典型判定方法 14

附录 D（资料性） 网络攻击和网络攻击事件概述 15

附录 E（资料性） 描述网络攻击和网络攻击事件的信息要素和计数示例 16

参考文献 18

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 37027—2018《信息安全技术 网络攻击定义及描述规范》，与 GB/T 37027—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了网络攻击的定义(见 3.1, 2018 年版的 3.1)；
- b) 增加了网络攻击事件的定义(见 3.2)；
- c) 更改了“网络攻击”中“攻击技术手段”“安全漏洞类型”的描述(见 5.1, 2018 年版的 6.2、6.3)；
- d) 增加了网络攻击事件的信息描述(见 5.2)；
- e) 增加了网络攻击的判定条件(见 6.2)；
- f) 增加了网络攻击事件的判定条件(见 6.3)；
- g) 增加了网络攻击的计数方法(见 7.2)；
- h) 增加了网络攻击事件的计数方法(见 7.3)。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心北京分中心、中国电子技术标准化研究院、中国移动通信集团有限公司、启明星辰信息技术集团股份有限公司、安天科技集团股份有限公司、北京长亭科技有限公司、国家工业信息安全发展研究中心、国能数智科技开发(北京)有限公司、郑州信大捷安信息技术股份有限公司、北京天融信网络安全技术有限公司、国家信息中心(国家电子政务外网管理中心)、中国信息通信研究院、广东省信息安全测评中心、中科信息安全共性技术国家工程研究中心有限公司、杭州安恒信息技术股份有限公司、北京升鑫网络科技有限公司、奇安信科技集团股份有限公司、中国电子信息产业集团有限公司第六研究所、北京时代新威信息技术有限公司、江苏君立华域信息安全技术股份有限公司、北京中测安华科技有限公司、中电科网络安全科技股份有限公司、北京神州绿盟科技有限公司、三六零数字安全科技集团有限公司、杭州迪普科技股份有限公司、公安部第三研究所、国家计算机网络应急技术处理协调中心黑龙江分中心、长安通信科技有限责任公司。

本文件主要起草人：严寒冰、饶毓、郭晶、陈亮、赵彦、周莹莹、卢卫、徐剑、吕志泉、韩志辉、温森浩、王惠莅、朱雪峰、徐雅丽、李一鸣、邱勤、杨天识、刘佳男、杨坤、张晓菲、牛月坤、刘为华、安高峰、闫桂勋、董航、甄茁、胡建勋、陈彦羽、卞建超、刘勇、赵云龙、王连强、金建军、严默默、曹旭博、肖岩军、耿贵宁、刘吉林、陶源、刘琨、张洛什。

本文件及其所代替文件的历次版本发布情况为：

- 2018 年首次发布为 GB/T 37027—2018；
- 本次为第一次修订。

引 言

近年来,随着网络应用的普及和迅猛发展,网络攻击的方法和形式复杂与多变,对网络安全造成了严重威胁。

网络攻击和网络攻击事件的判定涉及多方面因素,包括:网络攻击和网络攻击事件的区别;网络攻击和网络攻击事件的界定和分类;网络攻击及网络攻击事件涉及的角色、过程、关键技术、后果评估;各类网络攻击的和网络攻击事件的判定及计数方法等内容。随着网络攻击和网络攻击事件的日益增多,当前各组织对网络攻击、网络攻击事件判定和计数方法不统一,导致各组织判定和统计网络攻击出现较大差异,难以有效实现网络攻击态势的共享和准确感知。因此,需对网络攻击和网络攻击事件进行更加准确的定义、描述,给出统一分类、判定及统计准则,为抵御网络攻击夯实基础,提升网络攻击态势的感知效果,增强网络安全保障能力。



网络安全技术

网络攻击和网络攻击事件判定准则

1 范围

本文件确立了网络攻击和网络攻击事件的描述信息要素、判定和计数的方法。

本文件适用于指导组织开展网络攻击和网络攻击事件的监测分析、态势感知、信息报送等活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 20986—2023 信息安全技术 网络安全事件分类分级指南

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 20986—2023、GB/T 30279—2020 界定的以及下列术语和定义适用于本文件。

3.1

网络攻击 network attack

通过信息网络技术和各种手段,利用网络中存在的安全漏洞和安全缺陷针对网络实施干扰、控制、破坏等影响网络正常运行状态,以及针对网络数据实施窃取、滥用、篡改、损毁等危害数据安全的行为。

3.2

网络攻击事件 network attack incident

网络攻击(3.1)造成或潜在造成业务损失或危害的安全事件。

4 缩略语

下列缩略语适用于本文件。

APT:高级可持续威胁攻击(advanced persistent threat)

ARP:地址解析协议(address resolution protocol)

AS:自治系统(autonomous system)

BGP:边界网关协议(border gateway protocol)

DNS:域名系统(domain name system)

HTTP:超文本传输协议(hypertext transfer protocol)

IOC:失陷指标(indicators of compromise)

IP:互联网协议(internet protocol)

WLAN:无线局域网(wireless local area network)

5 描述信息要素

5.1 网络攻击

描述网络攻击的基本信息要素见表 1。

表 1 描述网络攻击的基本信息要素

信息要素	描述
标识号	每次网络攻击应具有唯一标识号
攻击对象	被实施网络攻击的客体信息,如被攻击设备的 IP 地址、域名,或具体的某个网络设备或者信息系统名称等
攻击对象类型	攻击对象的类型描述,可参考附录 A
攻击源	实施网络攻击的主体信息,包括攻击者身份(如攻击组织名、网络身份标识)、攻击资源(如攻击者使用的直接攻击 IP、真实攻击 IP、控制域名)等
攻击技术手段	网络攻击使用的技术手段,包括网络扫描探测、网络钓鱼、漏洞利用、后门利用、后门植入、凭据攻击、信号干扰、拒绝服务、网页篡改、暗链植入、域名劫持、域名转嫁、DNS 污染、WLAN 劫持、流量劫持、BGP 劫持、广播欺诈、失陷主机、其他,共 19 类
攻击时间	攻击发生的时间点或时间范围
注: GB/T 20986—2023 中的供应链攻击事件、APT 攻击事件一般是综合使用上述攻击技术手段的网络攻击事件,因此不在攻击技术手段中单独设置相应的类别。见附录 D 相关描述。	

描述网络攻击的扩展信息要素见表 2。

表 2 描述网络攻击的扩展信息要素

信息要素	描述
网络攻击名称	反映网络攻击特征的命名
安全漏洞	攻击过程中所利用的网络或系统的安全漏洞或安全缺陷
安全漏洞类型	安全漏洞的类型,按 GB/T 30279—2020 的规定
攻击源详细信息	攻击源的详细信息,包括国内/国外、组织内部/组织外部等
攻击阶段	攻击所处的阶段,可参考附录 B
攻击详细信息	详细描述攻击行为、手法或过程等
判定方法	判定网络攻击所使用的方法,见附录 C
其他信息	可根据需要增加一个或多个其他信息要素

5.2 网络攻击事件

描述网络攻击事件的基本信息要素见表 3。

表 3 描述网络攻击事件的基本信息要素

信息要素	描述
标识号	每个网络攻击事件应具有唯一标识号
事件时间	攻击事件发生的时间点或者时间范围
事件类型	网络攻击事件的类型,按 GB/T 20986—2023 及 D.2 的规定
攻击对象	同表 1“攻击对象”
攻击对象类型	同表 1“攻击对象类型”
攻击源	同表 1“攻击源”
事件影响	网络攻击事件已造成或潜在造成的影响,包括影响对象的重要程度、业务损失的具体情况、危害具体情况等

描述网络攻击事件的扩展信息要素见表 4。

表 4 描述网络攻击事件的扩展信息要素

信息要素	描述
网络攻击事件名称	反映网络攻击事件特征的命名
事件分级	网络攻击事件的分级描述,按 GB/T 20986—2023 的规定,包括特别重大事件(一级)、重大事件(二级)、较大事件(三级)、一般事件(四级)
事件详细信息	详细描述网络攻击事件的行为、手法或过程等
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
安全漏洞类型	安全漏洞的类型,按 GB/T 30279—2020 的规定
攻击源详细信息	攻击源的详细信息,包括国内/国外、组织内部/组织外部等
攻击动机	可能的攻击动机,如政治、经济、兴趣、炫耀等
判定方法	判定网络攻击事件所使用的方法,见附录 C
相关网络攻击的标识	提供与本起网络攻击事件相关的 1 个或者多个网络攻击的标识号
其他信息	可根据需要增加一个或多个其他信息要素

6 判定条件

6.1 判定概述

网络攻击和网络攻击事件的判定,指在一个判定时间段内,结合判定方法(见附录 D),识别出不同的网络攻击和网络攻击事件。在判定的过程中,如果命中了相关的判定条件,则可以认为识别出了相应的网络攻击或网络攻击事件。



6.2 网络攻击的判定条件

6.2.1 网络扫描探测攻击

存在下列情况之一,判定发生网络扫描探测攻击:

- a) 一定时间范围内,针对端口、路径、配置等的网络请求数量超出正常阈值范围,或网络请求内容存在遍历性和构造性;
- b) 网络流量或设备/系统/软件日志中包含网络扫描软件的特征,如 HTTP 头部中的 UA 和 Cookie 字段中包含某类网络扫描软件所特有的字符串特征。

6.2.2 网络钓鱼攻击

当通过网络传播的信息(如网页、网络邮件、软件、文件、图片等)具有欺诈性、伪造性,且存在诱使访问者提交重要数据、个人信息,或下载恶意软件,或通过扫描二维码转账等方式获取经济利益等情况时,判定发生网络钓鱼攻击。

6.2.3 漏洞利用攻击

存在下列情况之一,判定发生漏洞利用攻击:

- a) 网络流量或设备/系统/软件日志中包含典型漏洞利用攻击包的字符串特征;
- b) 网络流量或设备/系统/软件日志中包含漏洞利用工具的特征,如 HTTP 头部中的 UA 和 Cookie 字段中包含相关字符串特征。

6.2.4 后门利用攻击

存在下列情况之一,判定发生后门利用攻击:

- a) 网络流量或设备/系统/软件日志中包含后门利用攻击包的特征,如存在后门利用工具或者代码的特征;
- b) 网络、应用或操作系统中包含后门利用的痕迹,如存在网页后门执行文件,或者存在后门账户的登录行为等。

6.2.5 后门植入攻击

存在下列情况之一的,判定发生后门植入攻击:

- a) 网络流量或设备/系统/软件日志中包含后门植入攻击包的特征,如存在后门植入工具或者代码的特征;
- b) 网络、应用或操作系统中包含后门植入的痕迹,如检测发现存在可使攻击者获取更大权限的后门文件,或存在某被植入的后门账户。

6.2.6 凭据攻击

存在下列情况之一,判定发生凭据攻击:

- a) 网络流量或者业务系统日志中包含攻击者在短时间内进行凭据枚举猜解的行为特征,如 SSH、RDP 等网络登录多次失败超过设定的阈值,WEB 系统登录失败超过设定的阈值;
- b) 攻击者存在识别解析凭据信息的行为,如账号密码破解,证书窃取等;
- c) 识别发现存在诱导将凭据信息提交给攻击者的恶意链接或文件;
- d) 发现凭据遗失或者被窃取的情况,如通过开源情况发现暗网等论坛存在企业证书、账号密码的售卖行为。

6.2.7 信号干扰攻击

存在下列情况之一,判定发生信号干扰攻击:

- a) 通过检测发现未授权的干扰源;
- b) 通过检测发现利用已授权信号源干扰其他信号源的行为;
- c) 通过检测与正常设备行为不一致的迹象,如未经授权的无线电发射器的存在,可以发现潜在的信号干扰攻击;
- d) 通过监测邻近通信链路的质量变化和异常行为。

6.2.8 拒绝服务攻击

存在下列情况之一,判定发生拒绝服务攻击:

- a) 网络流量中包含拒绝服务攻击的指令特征;
- b) 网络或信息系统的流入流量或访问量超过设定的阈值;
- c) 网络流量符合拒绝服务攻击的特定协议类型与代码、速率和报文长度特征。

注: 设定或者自学习网络和信息系统的正常流量或正常访问量的阈值,并与实际流量、访问量进行比对。针对不同网络和信息系统可以依据其重要程度设定不同的检测阈值。

6.2.9 网页篡改攻击

存在网页源代码及内容被非授权恶意更改的情况时,判定发生网页篡改攻击。

6.2.10 暗链植入攻击

存在下列情况之一,判定发生暗链植入攻击:

- a) 发现存在未经授权的或异常的链接,指向恶意网站、下载恶意软件的链接或其他恶意资源;
- b) 发现安全日志和监测出现异常行为,网站或应用程序文件被修改。

6.2.11 域名劫持攻击

当域名的解析结果被非域名所有者指向非预期的 IP 地址的情况时,判定发生域名劫持攻击。

6.2.12 域名转嫁攻击

当域名的解析结果被域名所有者指向了不属于所有者或者利益相关方所拥有的 IP 地址情况时,判定发生域名转嫁攻击。

6.2.13 DNS 污染攻击

当网络中存在错误的 DNS 数据包,把域名的解析结果指向不正确的 IP 地址时,判定发生 DNS 污染攻击。

6.2.14 WLAN 劫持攻击

存在下列情况之一,判定发生 WLAN 劫持攻击:

- a) 无线网络大量的数据流量被重定向到未知的目标,或数据包被篡改,或通信被中断;
- b) 频繁断连且超出设定阈值,或连接到未知的或可疑的无线网络;
- c) 出现未经授权的无线接入点,频繁地信道切换且超出设定阈值。

6.2.15 流量劫持攻击

存在下列情况之一,判定发生流量劫持攻击:

- a) 实际流入流量与对端发出流量存在差别;
- b) 实际流出流量与到达对端流量存在差别。

6.2.16 BGP 劫持攻击

存在下列情况之一,判定发生 BGP 劫持攻击:

- a) 检测发现攻击者发送污染包劫持路径的行为,如使用伪造或篡改等手段污染 BGP 边界网关协议的路由数据,欺骗其他 AS 将流量引向攻击者指定的 AS,出现请求内容与响应结果不对称,响应时间增大的现象;
- b) 检测发现攻击者已经劫持了路径,并将流量引向其指定的 AS,如检测发现 AS 实际网络通信路由路径与合理的网络路由通信路径存在差别。

6.2.17 广播欺诈攻击

存在下列情况之一,判定发生广播欺诈。

- a) ARP 表中 IP 地址与 MAC 地址的映射与正常情况不一致或存在重复映射。
- b) 网络中的数据流量和通信模式发现大量的冲突通信、数据包丢失、通信中断等异常情况。
- c) 频繁地发送 ARP 请求且超出设定阈值,或自动更新 ARP 表,或重置网络接口等。

6.2.18 失陷主机攻击

存在下列情况之一,判定发生失陷主机攻击:

- a) 被控设备对外发送心跳包、控制指令响应包或开启非授权服务;
- b) 被控设备中包含具有远程控制功能的恶意代码或者相关感染痕迹,例如特洛伊木马文件等。

6.2.19 其他网络攻击

采取其他攻击技术手段的网络攻击行为。

6.3 网络攻击事件的判定条件

判定网络攻击事件需同时满足两个条件:一是已判定单个或多个相关的网络攻击;二是已判定的网络攻击造成或潜在造成业务损失或危害。

- a) 针对 6.2 所列网络攻击,如存在已判定的使用相应攻击技术手段的网络攻击,且网络攻击造成或潜在造成业务损失或危害,则判定发生相应类型的网络攻击事件。
- b) 针对供应链攻击事件,通过分析相关攻击行为,如确认攻击方通过利用合法软件产品或网络服务的供应链中的脆弱性来实现其攻击意图,则判定发生供应链攻击事件。
- c) 针对 APT 攻击事件,存在下列一种或者多种情况,则判定发生 APT 攻击事件:
 - 1) 网络攻击中的 IOC 或者技战术属于已知 APT 组织;
 - 2) 攻击活动存在针对性、持久性和高隐蔽性,且攻击对象是重要信息系统或高价值个人,且攻击目的是窃取情报、破坏或者潜伏等待指令。

7 计数方法

7.1 计数概述

网络攻击和网络攻击事件的计数,是指在判定单次网络攻击、单个网络攻击事件的基础上,对多个网络攻击和网络攻击事件进行计数。

多次或者多个网络攻击和网络攻击事件,如果具有相同的信息要素,则可以进行加合统计。

如果包含的信息要素的数量和类型不同,可代表不同范围内的网络攻击或者网络攻击事件。

计数的结果,需要给计数的时间段、计数方法的简要描述,以及所得出的计数次数或者个数。计数的示例见附录 E。

7.2 网络攻击的计数

7.2.1 单次网络攻击

单次网络攻击指在一个时间点或一段时间范围内,依据 6.2 判定的网络攻击。

7.2.2 网络攻击的计数方法

网络攻击的计数指在一个计数时间段内,对包含某些信息要素的单次网络攻击进行加和,得到的网络攻击的次数。

网络攻击的典型计数方法包括以下方法。

- a) 使用某类技术手段的网络攻击计数:对信息要素中包含某类技术手段的单次网络攻击进行统计。
- b) 某个攻击对象遭受的使用某类技术手段的网络攻击计数:对信息要素中同时包含某个攻击对象、某类技术手段的单次网络攻击进行统计。
- c) 某个攻击源对某个攻击对象使用某类技术手段的网络攻击计数:对信息要素中同时包含某个攻击源、某个攻击对象、某类技术手段的单次网络攻击进行统计。

7.2.3 多个网络攻击计数结果的合并计算条件

多个网络攻击计数结果满足可比较或可累加条件时可合并计算。

满足以下条件的多个网络攻击计数结果可进行比较:多个网络攻击计数结果是使用完全相同的网络攻击判定条件、网络攻击计数方法得到的。

满足以下条件的多个网络攻击计数结果可进行累加:多个网络攻击计数结果是使用完全相同的网络攻击判定条件、网络攻击计数方法得到的,且不存在单次网络攻击被重复计数的情况。

除上述情况外,多个网络攻击计数结果不宜进行合并计算。

7.3 网络攻击事件计数

7.3.1 单个网络攻击事件

单个网络攻击事件指在一个判定时间段内,依据 6.2 判定的相关网络行为,需要具有一个或多个相同信息要素,相同信息要素见表 5。即在一个判定时间段,具有表 5 中相同信息要素的网络攻击即为一个网络攻击事件。

一个判定时间段一般为一个自然日,或者一个持续的攻击时间段,也可依据判定的实际情况设定。

表 5 单个网络攻击事件中包括的相关网络攻击具有的共同信息要素

网络攻击事件类型	单个网络攻击事件中包括的相关网络攻击具有的共同信息要素 (以下均指一个判定时间段内)	单个网络攻击事件的典型情况 (以下均指一个判定时间段内)
网络扫描探测事件	攻击源、攻击对象	一个攻击对象遭受一个攻击源的网络扫描探测攻击
网络钓鱼事件	攻击源	一个具有网络钓鱼功能的、可访问的钓鱼链接或文档
漏洞利用事件	攻击源、攻击对象	一个攻击源单次或多次成功利用一个攻击对象的漏洞
后门利用事件	攻击源、攻击对象	一个攻击源单次或多次成功利用一个攻击对象的后门
后门植入事件	攻击源、攻击对象	一个攻击源向一个攻击对象单次或多次成功植入后门
凭据攻击事件	攻击源、攻击对象	一个攻击源向一个攻击对象发起单次或多次凭据攻击,并成功获取正确的凭据
信号干扰事件	攻击对象	一个设备(如通信设备、雷达系统、导航设备等)遭受信号干扰攻击的影响
拒绝服务事件	攻击对象	一个攻击对象的业务遭受拒绝服务攻击的影响
网页篡改事件	攻击对象	一个网页的内容被单次或多次成功篡改
暗链植入事件	攻击对象	一个网页被成功植入单个或多个暗链
域名劫持事件	攻击对象	一个域名被单次或多次成功劫持
域名转嫁事件	攻击对象	一个域名被单次或多次成功转嫁
DNS 污染事件	攻击对象	一个域名遭受单次或多次 DNS 污染
WLAN 劫持事件	攻击对象	一个无线局域网遭受 WLAN 劫持攻击的影响
流量劫持事件	攻击对象	一个攻击对象被单次或多次成功流量劫持
BGP 劫持攻击事件	攻击对象	一个攻击对象遭受 BGP 劫持攻击的影响
广播欺诈事件	攻击对象	一个局域网遭受广播欺诈攻击的影响
失陷主机事件	攻击源、攻击对象	一个攻击对象被一个攻击源成功远程控制
供应链攻击事件	攻击对象	一个攻击对象发生供应链攻击事件
APT 事件	攻击源、攻击对象	一个攻击源对一个攻击对象的 APT 攻击事件
其他网络攻击事件	宜根据具体情况确定	根据具体情况确定

7.3.2 网络攻击事件的计数方法

网络攻击事件的计数指在一个计数时间段内,对包含某些信息要素的单个网络攻击事件进行加和,得到网络攻击事件的个数。

网络攻击事件的典型计数方法包括以下方法。

- a) 某类网络攻击事件计数:对信息要素中包含某类网络攻击事件的单个网络攻击事件进行统计。

- b) 某个攻击对象遭受的某类网络攻击事件计数:对信息要素中同时包含某个攻击对象、某类网络攻击事件的单个网络攻击事件进行统计。
- c) 某个攻击源针对某个攻击对象的某类网络攻击事件计数:对信息要素中同时包含某个攻击源、某个攻击对象、某类网络攻击事件的单个网络攻击事件进行统计。

7.3.3 多个网络攻击事件计数结果的合并计算条件

多个网络攻击事件计数结果满足可比较或可累加条件时可合并计算。

- a) 可比较:使用完全相同的网络攻击事件判定条件、网络攻击事件计数方法得到的多个网络攻击事件计数结果。
- b) 可累加:使用完全相同的网络攻击判定事件条件、网络攻击事件计数方法得到的,且不存在单个网络攻击事件被重复计数的多个网络攻击事件计数结果。

除上述情况外,多个网络攻击事件计数结果不宜进行合并计算。


附 录 A
(资料性)
典型攻击对象类型

典型攻击对象类型如表 A.1 所示。

表 A.1 攻击对象类型表

一级分类	二级分类	说明
计算机	移动终端	如智能手机、平板(Pad)等
	PC	个人电脑,如台式机、笔记本等
	服务器	为客户端提供特定应用服务的计算机系统
	其他	
工控设备	SCADA	数据采集与监视控制系统
	PLC	可编程逻辑控制器
	DCS	分布式控制系统
	其他	
网络设备	路由器	基于路由协议机制和算法选择路径或路由,建立和控制不同网络间数据流的网络设备
	交换机	利用内部交换机制来提供连通性的设备
	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	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 系列	
	Android 系列	
	其他	
服务软件	数据库服务	包括关系型和非关系型数据库,对存放在库中的数据进行统一管理和处理等,并对外提供服务访问接口
	电子邮件服务	包括支持 POP3 协议、IMAP 协议、SMTP 协议等的 email 服务端
	FTP 服务	文件传输服务,包括服务端的文件浏览、下载、上传等
	Web 服务	支持处理浏览器等 Web 客户端的请求并返回相应处理结果,也可以放置网站、数据文件,供 Web 客户端浏览、下载
	远程管理连接服务	支持用户远程访问和控制计算机,例如 SSH 服务、Telnet 服务、RDP 服务、VNC 服务等

表 A.1 攻击对象类型表（续）

一级分类	二级分类	说明
中间件	中间件	提供系统软件和应用软件之间连接的软件,以便软件各部件之间的沟通,特别是应用软件对于系统软件的集中的逻辑,如 COM、CORBA、Tomcat、Weblogic、JBoss、TongWeb
	其他	
用户软件	办公软件	如文档编辑、图表编辑类工具软件等 
	社交软件	通过网络来实现社会交往目的的软件
	支付软件	直接支持金融支付功能的软件
	其他	
网络基础设施	电信网	包括固网和移动通信网(如 3G、4G 和 5G 等)
	DNS	域名服务设施
	云计算平台	IaaS/PaaS/SaaS 类型的云计算平台
	CA	证书颁发机构
	其他	

附 录 B

(资料性)

典型网络攻击过程

B.1 概述

网络攻击的典型过程如图 B.1 所示。

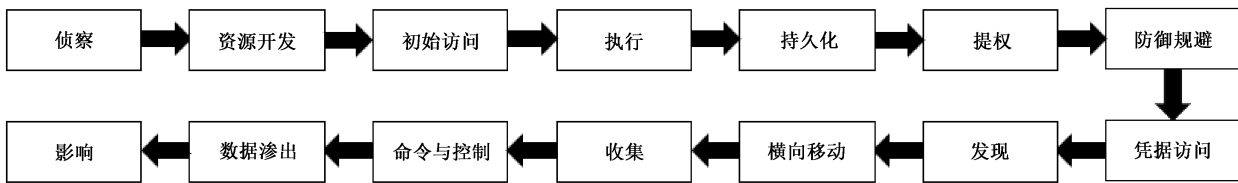


图 B.1 网络攻击的典型过程

B.2 侦察

在实施网络攻击前,攻击者通过主动或被动信息收集技术,收集可以用来规划未来攻击行动的信息,包括受害组织信息、基础设施信息、人员详细情况信息等,攻击者能够利用收集的信息为实施网络攻击进行准备,为全生命周期其他阶段提供帮助。

B.3 资源开发

根据收集到的详细信息,攻击者通过创建、购买或破坏/窃取可用于支持目标定位的资源的技术,建立可用于支持行动的资源,包括基础架构、受害者账户等资源,攻击者能够利用开发的资源为全生命周期其他阶段提供帮助。

B.4 初始访问

攻击者通过使用鱼叉式网络钓鱼、利用 Web 服务器上漏洞等技术在目标网络中获得初始立足点。通过初始访问获得的立足点能够允许攻击者在目标网络中继续访问或攻击。

B.5 执行

攻击者在本地或远程系统上控制恶意代码执行,执行恶意代码技术通常与网络搜索、窃取数据等其他策略的技术结合使用。例如,攻击者使用远程访问工具来运行执行远程系统发现的 PowerShell 脚本等。

B.6 持久化

攻击者通过使用当出现重启、更改凭证、其他可能切断其访问的情况时,在中断期间保持对目标系统访问的技术,保障攻击者立足点。

B.7 提权

攻击者利用系统漏洞、错误配置等,在目标系统或网络上获得更高级别权限;通过提升权限,攻击者才能达成更多目的。提权技术通常与持久化技术重叠。



B.8 防御规避

攻击者利用卸载/禁用安全软件、混淆/加密数据和脚本等技术,以及通过利用受信任进程隐藏/伪装恶意软件等,避免在入侵目标网络过程中被发现。

B.9 凭证访问

攻击者通过键盘记录、凭证转储等技术窃取账户名和密码等。攻击者利用合法凭证访问目标系统,难以被发现,并提供了创建更多账户以帮助实现攻击对象的机会。

B.10 发现

攻击者搜索其可以控制的内容以及切入点周围的内容,获取有关系统和内部网络的知识,帮助在行动之前观察目标环境并确定行动方向。

B.11 横向移动

攻击者利用进入和控制网络远程系统的技术搜索整个网络以找到最终目标,攻击者可能会安装自己的远程控制工具,也可能将合法凭证与本机网络和操作系统工具一起使用来完成横向移动。

B.12 收集

攻击者利用收集信息相关技术在目标网络中收集其感兴趣的数据,收集目标源包括各种驱动器类型、浏览器、音频、视频和电子邮件等,收集方式包括截图、键盘输入等。

B.13 命令与控制

攻击者利用网络通信技术与受感染的系统通信并对其进行控制,通常攻击者会尝试模仿正常的预期流量以避免被发现,以及根据目标网络结构和防御情况建立具有隐蔽功能的命令和控制。

B.14 数据渗出

攻击者收集到目标数据后,通常采用压缩、加密等方式将数据打包以避免在渗出数据时被发现。从目标网络渗出数据技术包括通过命令和控制通道或备用通道传输数据、对传输设置大小限制等。

B.15 影响

攻击者利用破坏、篡改数据等技术,通过操纵业务和操作流程来破坏网络可用性 or 损害完整性,攻击者使用相关技术实现最终目的或为机密数据泄露提供掩护。

附 录 C

(资料性)

网络攻击和网络攻击事件的典型判定方法

C.1 网络攻击的典型判定方法

网络或信息系统运营者、安全厂商、行业主管机构、监管机构等可使用以下方法中的一种或者多种判定网络攻击。

- a) 通过在网络安全设备或软件系统中发现和判定网络攻击的行为。如在流量监测设备中发现典型的漏洞利用攻击包特征,进而可判定发现漏洞利用攻击。网络安全设备或软件系统包括但不限于防火墙、入侵检测设备、入侵防御设备、流量分析设备、蜜罐、APT 检测设备、日志审计设备等。
- b) 通过人工查看分析终端主机、交换机、服务器、软件等设备的日志、状态等信息,结合正常操作规律,对信息进行主观分析,从而发现和判定网络攻击。
- c) 通过威胁信息共享或者其他外部途径,从个人或组织处获取关于网络攻击的判定条件或者其他关联线索,从而判定网络攻击行为。

C.2 网络攻击事件的典型判定方法

网络或信息系统运营者、安全厂商、行业主管机构、监管机构等可使用如下方法中的一种或者多种判定网络攻击事件:

- a) 首先判定网络攻击,然后确认网络攻击已造成或潜在造成业务损失或危害;
 - b) 首先确认业务损失或危害已发生或潜在发生,然后判定造成业务损失或危害的网络攻击。
- 存在下列一种或者多种情况,可确认业务损失或危害已发生或潜在发生:
- a) 网络安全设备或软件系统判定网络攻击已经成功;
 - b) 通过对终端、交换机等设备取证分析,确认存在非授权的操作行为;
 - c) 通过受害方核实或外部线索佐证,确认业务损失或危害已发生或潜在发生。

附 录 D

(资料性)

网络攻击和网络攻击事件概述

D.1 网络攻击

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侦察、资源开发、初始访问、执行、持久化、提权、防御规避、凭证访问、发现、横向移动、收集、命令与控制、数据渗出、影响等步骤。典型网络攻击过程的详细描述参见附录 B。

从生存周期角度看,一次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、应用或操作系统的脆弱性,未经授权试图访问系统的数据、功能或其他受限的范围,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) 网络攻击检测防御者: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、接入等技术服务的服务商和非营利组织,如云服务提供商、电信运营商等。

D.2 络网攻击事件

网络攻击事件是指网络攻击者通过网络攻击对网络攻击受害者造成或潜在造成业务损失或危害的安全事件。

网络攻击事件可从事件的攻击技术手段、攻击危害、攻击者的意图等方式进行分类。

GB/T 20986—2023 中,定义了 21 类网络攻击事件。其中供应链攻击事件和 APT 攻击事件两类,主要从攻击的危害、攻击者的意图角度进行分类,其他 19 类主要从攻击技术进行分类,可作为“网络攻击”技术手段的分类,也即可作为“网络攻击”的分类。

附 录 E
(资料性)

描述网络攻击和网络攻击事件的信息要素和计数示例

E.1 网络攻击的信息描述和计数示例

假设攻击源 2.2.2.2 在 2024 年 1 月 1 日对 1.1.1.1 发起后门利用攻击,依据附录 A 所属判定方法,产生多条攻击描述记录。表 E.1 是 1 次网络后门利用攻击的信息要素描述示例。

表 E.1 1 次网络攻击的信息要素描述示例

信息要素	信息要素类型	典型值举例
标识号	基本信息要素	2024010100000001
攻击对象		1.1.1.1
攻击对象类型		服务器
攻击源		2.2.2.2
攻击技术手段		后门利用攻击
攻击时间		2024 年 1 月 1 日 1 时 2 分 3 秒
网络攻击名称	扩展信息要素	网络后门连接
安全漏洞		* * * * 服务器存在命令注入漏洞
安全漏洞类型		命令注入漏洞
攻击源详细信息		疑似国外 * * 网络攻击组织
攻击阶段		执行
攻击详细信息		2024 年 1 月 1 日 1 时 2 分 3 秒,攻击者使用 2.2.2.2 的 IP 连接位于服务器 1.1.1.1 上的后门,执行相关操作
判定方法		人工查看分析服务器上的日志,发现存在后门利用攻击
其他信息		无

在 2024 年 1 月 1 日统计周期内,攻击源 2.2.2.2 对 1.1.1.1 发起的网络攻击次数可通过对 2024 年 1 月 1 日涉及的网络攻击信息要素中,同时包含攻击源 2.2.2.2、攻击对象 1.1.1.1,且攻击技术手段为“后门利用攻击”的相关网络攻击记录条数得到。假设相关攻击记录涉及网络攻击标识号为包含 2024012800000001 在内的 1 000 个标识号,则 2024 年 1 月 1 日攻击源 2.2.2.2 对 1.1.1.1 发起的后门利用攻击为 1 000 次。

E.2 网络攻击事件的信息描述和计数示例

假设通过分析,表 E.1 网络攻击造成了危害,可以判定为“后门利用攻击事件”,则可进行如表 E.2 网络攻击事件描述。

表 E.2 描述单个网络攻击事件的信息要素描述示例

信息要素	信息要素类型	描述
标识号	基本信息要素	Incident-2024010100000001
事件时间		2024 年 1 月 1 日 1 时 2 分 3 秒至 4 时 5 分 6 秒
事件类型		后门利用攻击事件
攻击对象		1.1.1.1
攻击对象类型		服务器
攻击源		2.2.2.2
事件影响		攻击者成功连接了位于服务器上的后门,获取了相关权限,并执行相关操作,存在巨大网络安全威胁
网络攻击事件名称	扩展信息要素	网络后门连接及代码执行
事件分级		一般事件(四级)
事件详细信息		2024 年 1 月 1 日 1 时 2 分 3 秒至 4 时 5 分 6 秒,攻击者使用 2.2.2.2 的 IP 成功连接位于服务器 1.1.1.1 上的后门,执行相关操作,对服务器造成了运行危害
安全漏洞		**** 服务器存在命令注入漏洞
安全漏洞类型		命令注入漏洞
攻击源详细信息		疑似国外**网络攻击组织
攻击动机		疑似经济利益驱动
判定方法		判定发生网络攻击且攻击对象已确认受到危害
相关网络攻击的标识		包括 2024010100000001 在内的等 1 000 个网络攻击标识号
其他信息		无

单个后门利用攻击事件的典型情况是“多个涉及的相关网络攻击具有相同的攻击源、攻击对象”,也就是说以上 2024012800000001 在内的 1 000 个网络标识号所涉及的 1 000 次网络攻击,可以合并为 1 个网络攻击事件。如果在 1 个统计周期内,多条网络攻击记录中的攻击源都为 2.2.2.2,但攻击对象不同,则可以通过将涉及的记录按照攻击对象 IP 个数进行统计,进而得到攻击源 2.2.2.2 在此统计周期内的攻击事件个数。

参 考 文 献

- [1] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全
 - [2] GB/T 7408—2023 日期和时间 信息交换表示法 第1部分:基本原则
 - [3] GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分:事件管理原理
 - [4] GB/T 20985.2—2020 信息技术 安全技术 信息安全事件管理 第2部分:事件响应规划和准备指南
 - [5] GB/T 25068.3—2022 信息技术 安全技术 网络安全 第3部分:面向网络接入场景的威胁、设计技术和控制
 - [6] GB/T 25069—2022 信息安全技术 术语
-

