高等院校网络空间安全专业实战化人才培养系列教材

郭启全　丛书主编

网络安全
事件处置与追踪溯源技术

吴云坤　郭启全　段晓光
裴智勇　刘　洋　李洪亮　张永印　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书共 9 章，围绕“网络空间安全导论”这一主题，系统介绍网络空间安全的事件处置和追踪溯源技术。其中，第 1 章概括性介绍网络安全与事件处置，包括网络空间安全事件处置的目的、作用、原则、方法、触发条件、内外协作和追踪溯源技术发展和主流技术等。第 2 章介绍网络安全事件分类与分级，包括网络安全事件的分类方法和类别，网络安全事件的分级，网络安全事件类别和级别的关联关系。第 3 章介绍网络安全事件处置流程和方法，包括事件处置的一般流程、准备阶段、检测阶段、抑制阶段、固证与溯源阶段、根除与恢复阶段、反制阶段、信息通报和预警阶段和事件原因分析与安全建设整改。第 4 章介绍事件处置的组织保障，包括基本框架、协调中心、决策中心、IT 技术支撑、业务线支撑、外部协调和事件处置组织能力建设。第 5 章介绍事件处置关键技术，包括网络安全事件发现关键技术、处置和分析常用工具及事件响应关键技术。第 6 章介绍追踪溯源技术，包括追踪溯源的网络技术基础，身份识别技术，身份隐藏技术，日志，溯源分析常用工具，威胁情报和入侵检测指标等内容。第 7 章介绍溯源分析的组织与方法，包括溯源分析的基本概念，痕迹采集与分析，历史轨迹溯源，网络空间测绘技术和公开信息采集等内容。第 8 章介绍常见安全事件响应处置及溯源方法，包括钓鱼邮件溯源、勒索病毒溯源、挖矿木马溯源、Webshell 溯源、恶意网站溯源、DDoS 溯源、扫描器溯源、APT 攻击溯源和流量劫持等内容。第 9 章介绍基于大数据的溯源分析，包括威胁数据的采集与汇聚、关联分析的原则与方法、大数据可视化分析技术、互联网威胁研判技术和告警降噪等内容。

本书是高等院校网络空间安全专业实战化人才培养系列教材之一，可作为网络空间安全专业的专业课教材，适合网络空间安全专业、信息安全专业以及相关专业的大学生、研究生系统学习，也适合各单位各部门从事网络安全工作者、科研机构和网络安全企业的研究人员阅读。

图书在版编目（CIP）数据

网络安全事件处置与追踪溯源技术 / 吴云坤等编著.
北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121
-50037-4

Ⅰ. TP393.08

中国国家版本馆CIP数据核字第2025S0N316号

责任编辑：潘　昕　　文字编辑：王腾可
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：787×1 092　1/16　印张：20　　字数：480千字
版　　次：2025年7月第1版
印　　次：2025年7月第1次印刷
定　　价：69.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）88254569，lyt@phei.com.cn。

高等院校网络空间安全专业
实战化人才培养系列教材

编委会

序 FOREWORD

在数字化智慧化高速发展的今天，网络和数据安全的重要性愈发凸显，直接关系到国家政治、经济、国防、文化、社会等各个领域的安全和发展。网络空间技术对抗能力是国家整体实力的重要方面，面对日益复杂的网络安全威胁和挑战，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”的思路，培养具有实战化能力的网络安全人才队伍，已成为国家重大战略需求。

一、培养网络安全实战化人才的根本目的

在网络安全“三化六防”（实战化、体系化、常态化；动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控）理念的指引下，网络安全业务越来越贴近实战。实战行动和实战措施都离不开实战化人才队伍的支撑。培养网络安全实战化人才的根本目的，在于培养一批既具备扎实的理论基础，又掌握高新技术和前沿技术、具备攻防技术对抗能力，还能灵活运用各种技术措施和手段，应对各种网络安全威胁的高素质实战化人才，打造“攻防兼备”和具有网络安全新质战斗力的队伍，支撑国家网络安全整体实战能力的提升。

二、培养网络安全实战化人才的重大意义

习近平总书记强调：“网络空间的竞争，归根结底是人才竞争”，“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。要建设网络强国，必须打造一支高素质的网络安全实战化人才队伍。我国网络安全人才特别是实战化人才严重缺乏，因此，破解难题，从网络安全保卫、保护、保障三个方面加强实战化人才教育训练，已成为国家重大战略需求。

当前，国家在加快推进数字化智慧化建设，本质是打造数字化生态，而数字化建设面临的最大威胁是网络攻击。与此同时，国家网络安全进入新时代，新时代网络安全最显著的特征是技术对抗。因此，新时代要求我们要树立新理念、采取新举措，从网络安全、数据安全、人工智能安全等方面，大力培养实战化人才队伍，加强“网络备战”，提升队伍的技术对抗和应急处突能力，有效应对新威胁和新技术带来的新挑战，为国家经济发展保驾护航。

三、构建新型网络安全实战化人才教育训练体系

为全面提升我国网络安全领域的实战化人才培养能力和水平，按照“理论支撑技术、技术支撑实战”的理念，创新高等院校及社会差异化实战人才培养的思路和方法，建立新型实战化人才教育训练体系。遵循“问题导向、实战引领、体系化设计、督办落实”四项原则，认真落实“制定实战型教育训练体系规划、建设实战型课程体系、建设实战型师资队伍、建设实战型系列教材、建设实战型实训环境、以实战行动提升实战能力、创新实战

型教育训练模式、加强指导和督办落实”八项重大措施，形成实战化人才培养的“四梁八柱”，有力提升网络安全人才队伍的新质战斗力。

四、精心打造高等院校网络空间安全专业实战化人才培养系列教材

在有关部门的大力支持下，具有 20 多年网络安全实战经验的资深专家统筹规划和整体设计，会同 20 多位部委、高等院校、科研机构、大型企业具有丰富实战经验和教学经验的专家学者，共同打造了 14 部技术先进、案例鲜活、贴近实战的高等院校网络空间安全专业实战化人才培养系列教材，由电子工业出版社出版，以期贡献给读者最高水平、最强实战的网络安全重要知识、核心技术和能力，满足高等院校和社会培养实战化人才的迫切需要。

网络安全实战化人才队伍培养是一项长期而艰巨的任务，按照教、训、战一体化原则，以国家战略为引领，以法规政策标准为遵循，以系统化措施为抓手，政府、高校、企业和社会各界应共同努力，加快推进我国网络安全实战化人才培养，为筑梦网络强国、护航中国式现代化贡献我们的智慧和力量！

郭启全

前言 PREFACE

近年来，国家级有组织的网络攻击活动日益猖獗，网络安全重大事件高发频发。2010 年，伊朗遭“震网”病毒攻击，其浓缩铀工厂内五分之一离心机报废；2013 年，美国希拉里个人邮件服务器遭攻击，美联邦调查局 2016 年重启调查希拉里“邮件门”事件，直接导致其竞选总统失败；2017 年，勒索病毒“永恒之蓝”在全球爆发，150 多个国家和地区网络系统遭攻击，众多机构网络瘫痪；2021 年，美国最大燃油管道公司遭勒索病毒攻击，致使燃油供应中断，部分地区进入国家紧急状态；2022 年俄乌冲突，双方实施网络战打击，并综合使用军事战、经济战、舆论战、信息战、情报战等手段，展现了国家间现代化战争的基本形态。全球网络安全重大事件爆发，一再给我们敲响警钟，网络安全事关国家安全、政权安全、经济安全、国防安全，以及企业运营安全和个人生命安全。

近年来，我国加快推进数字经济、数字政府、数字中国建设和数字化转型，本质是打造数字化生态，建设数字社会。然而，随着数字化建设的深入推进，网络攻击威胁日益凸显。一是数据大集中大流动大应用，客观上造成重要数据保护困难，而网络攻击却变得容易、快捷；二是外部网络攻击入侵活动明显增多，某些国家将我国作为主要战略对手，不断加速网络空间军事化进程，开展一系列攻防演习，研发突破性网络武器，长期对我国实施网络攻击渗透，严重威胁我国的国家安全；三是一些具有国家和地区背景的黑客组织，频繁对我国重要行业实施网络攻击，窃取情报和重要数据。国家级有组织的高级可持续威胁（APT）攻击、漏洞利用攻击、供应链攻击、勒索病毒攻击等活动日益猖獗，我国网络空间安全面临的外部威胁显著增大，给我国国家安全和数字化生态建设带来重大挑战。

进入新时代，网络安全最显著的特征是技术对抗，我们应树立新理念，采取新举措，立足有效应对大规模网络攻击，认真落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施。按照“打造一支攻防兼备的队伍、开展一组实战演习行动、建设一批网络与数据安全基地”这条主线，加强战略谋划和战术设计，建立完善网络安全综合防御体系，大力提升综合防御能力和技术对抗能力。从创新角度出发，按照“理论支撑技术、技术支撑实战”的理念，加强理论创新和技术突破，实施“挂图作战”；从“打造一支攻防兼备的队伍”出发，创新高等院校和企业差异化网络安全人才培养思路和方法，建立实战型人才教育训练体系，加强教育训练体系规划，强化课程体系、师资队伍、系列教材、实训环境建设和培养模式创新，培养网络安全实战型人才。

为了满足培养网络安全实战型人才需要，郭启全组织了具有丰富实战经验和教学经验的专家、学者，成立编委会，共同编著高等院校网络空间安全专业实战化人才培养系列教材，包括《网络安全保护制度与实施》《网络安全建设与运营》《网络空间安全技术》《商

用密码应用技术》《数据安全管理与技术》《人工智能安全治理与技术》《网络安全事件处置与追踪溯源技术》《网络安全检测评估技术与方法》《网络安全威胁情报分析与挖掘技术》《数字勘查与取证技术》《恶意代码分析与检测技术》《恶意代码分析与检测技术实验指导书》《漏洞挖掘与渗透测试技术》《网络空间安全导论》。丛书由郭启全统筹规划和整体设计，并对内容严格把关。

《网络安全事件处置与追踪溯源技术》共 9 章，主要介绍网络安全事件处置与追踪溯源的概念、事件分类与分级、事件处置流程和方法、事件处置的组织保障、事件处置关键技术、追踪溯源技术、溯源分析的组织与方法、常见安全事件响应处置及溯源方法、基于大数据的溯源分析，并给出了许多案例，以其培养读者的网络安全事件处置与追踪溯源技术能力。本书由吴云坤、段晓光等编著，具体章节编写者：第 1 章裴志勇，第 2 章段晓光，第 3 章李洪亮、段晓光，第 4 章裴智勇，第 5 章董旭、张永印、段晓光，第 6 章张永印 、段晓光，第 7 章段继平、董旭、段晓光，第 8 章张永印、汪列军，第 9 章董旭、黄鑫、邱喆彬、刘洋。

由于撰写时间紧迫，不足之处请读者批评指正。

作者

目录 CONTENTS

第 6 章

追踪溯源技术

第 1 章 概　述

本章主要介绍网络安全与事件处置、事件处置与追踪溯源、相关领域的技术发展、相关政策法规与标准，为网络安全事件处置和追踪溯源奠定基础。主要内容包括：网络安全事件处置的目标、作用、原则和方法，事件处置的触发条件，进行网络安全事件处置的协作方法，溯源分析的目的、作用和方法，追踪溯源的常用技术和相关领域的技术发展，我国网络安全事件的处置和处置方面的国家战略、法律法规、部门规章规范，以及国家发布的相关标准。

1.1 网络安全与事件处置

1.1.1 网络安全与网络安全事件

1. 网络安全的基本含义

《中华人民共和国网络安全法》（以下简称《网络安全法》）将网络安全的范围确定为网络运行安全和网络数据（含信息）安全，主要包括以下几方面。一是网络空间主权，包括国内管辖权、独立权、自卫权、依赖性主权；对境外攻击破坏行为的管辖权，包括防御防范网络攻击、惩治打击网络犯罪、外交制裁、冻结财产等手段。二是确立了国家网络安全等级保护制度。三是明确了关键信息基础设施保护，关键信息基础设施重要数据跨境传输要求。四是明确了网络运营者、网络产品和服务提供者的责任义务。五是保障网络信息安全和个人信息安全。六是采取监测预警与应急处置等重要措施。

网络安全包含五个属性：保密性、完整性、可用性、可控性和不可抵赖性。

（1）保密性，是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用，信息不泄露给非授权用户、实体或过程，或供其利用的特性。这些信息不仅包括国家机密，也包括企业和社会团体的商业机密和工作机密，还包括个人信息。人们在应用网络时很自然地要求网络能提供保密性服务，而被保密的信息既包括在网络中传输的信息，也包括存储在计算机系统中的信息。

（2）完整性，是指数据未经授权不能进行改变的特性。即信息在存储或传输过程中保

持不被修改、不被破坏和避免丢失的特性。数据的完整性保证计算机系统上的数据和信息处于一种完整和未受损害的状态，这就是说数据不会因为有意或无意的事件而被改变或丢失。除了数据本身不能被破坏外，数据的完整性还要求数据的来源具有正确性和可信性，也就是说需要首先验证数据是真实可信的，然后再检验数据是否被破坏。

（3）可用性，是指对信息或资源的使用期望，即可授权实体或用户访问并按要求使用信息的特性。简单地说，就是保证信息在需要时能为授权者所用，防止由于主客观因素造成的系统拒绝服务。例如，网络环境下的拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。数据不可用也可能是由软件缺陷造成的。

（4）可控性，是指人们对信息的传播路径、范围及其内容所具有的控制能力，即不允许不良内容通过公共网络进行传输，使信息在合法用户的有效掌控之中。

（5）不可抵赖性，也称不可否认性，是指在信息交换过程中，确信参与方的真实同一性，即所有参与者都不能否认和抵赖曾经完成的操作和承诺。简单地说，就是发送信息方不能否认发送过信息，信息的接收方不能否认接收过信息。利用信息源证据可以防止发信方否认已发送过信息，利用接收证据可以防止接收方事后否认已经接收到信息。

2. 网络安全的主要类型

网络安全由于不同的环境和应用而产生了不同的类型，主要有以下几种。

（1）系统安全。运行系统安全即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的消息造成破坏。避免由于电磁泄漏，产生信息泄露，干扰他人或受他人干扰。

（2）网络信息安全。网络上系统信息的安全，包括用户口令鉴别、用户存取权限控制、数据存取权限和方式的控制、安全审计、计算机病毒防治、数据加密等。

（3）信息传播安全。网络上信息传播安全，即信息传播过程和结果的安全，包括信息过滤等，侧重于防止和控制由于非法、有害的信息传播所产生的后果，避免公用网络上自由传输的信息失控。

（4）信息内容安全。网络上信息内容的安全，侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损用户合法权益的行为，其本质是保护用户的利益和隐私。

3. 网络安全事件的基本含义

危害网络系统、通信网络设施和数据安全的事件称为网络安全事件，包括网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、病毒传播等事件。事件的主体可能是自然界、系统自身故障、组织内部或外部的人、计算机病毒或蠕虫等。

根据《信息安全技术 网络安全事件分类分级指南》等国家有关标准规范，综合考虑网络安全事件的起因、威胁、攻击方式、损害后果等因素，将网络安全事件分为 10 类，包括恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等。按照事

件影响对象的重要程度、业务损失的严重程度和社会危害的严重程度三个要素，将网络安全事件分为 4 个级别，包括“特别重大事件、重大事件、较大事件和一般事件”，由高到低分别为一级、二级、三级和四级。详见第 2 章。

4. 网络安全事件的具体描述

（1）破坏保密性的安全事件。包括入侵网络系统并读取信息、搭线窃听、远程探测网络拓扑结构和计算机系统配置等。

（2）破坏完整性的安全事件。包括入侵网络系统并篡改数据、劫持网络连接并篡改或插入数据、安装木马和计算机病毒（修改文件或引导区）等。

（3）破坏可用性的安全事件。包括网络系统发送故障、拒绝服务攻击、消耗系统资源或网络带宽等。

（4）扫描。包括地址扫描和端口扫描等，为入侵网络系统寻找系统漏洞。

1.1.2　事件处置的目的和作用

事件处置，也称事件应急处置、应急响应，是指网络运营者针对因内部或外部因素触发特定形式的网络安全事件时，所采取的必要处置措施或应急行动。事件处置是网络安全工作中的重要组成部分，也是安全运营的重要环节，还是一种将人的主观能动性与技术方法、系统平台相结合的、动态的、持续的网络安全工作。

不存在完美无缺的网络系统，尤其在复杂系统中，不可避免地存在各种安全漏洞和隐患。因此，无论系统的前期建设和后期运营多么完善和精心，都难以避免在持续运行过程中发生各种网络安全事件。由于安全事件的发生是必然的，因此，在安全事件发生时，采取正确和迅速的响应措施是至关重要的。

1. 及时止损是事件处置的首要目标

事件的处置首要目标是“及时止损”，这意味着必须及时排除潜在和已知的安全风险，对各种来自内外部的攻击行为采取必要的反制措施，尽一切可能避免或减少损失。在处理安全事件时，必须保持冷静、理性，采取严谨的态度和有力的措施，以确保事件处置迅速、有效。

安全事件的触发并不必然导致实际的损失，只要能做到及时响应，仍有可能避免损失的产生。例如，及时发现系统存在的安全漏洞或网络入侵活动，使事件不能造成危害。如果能及时修补这些安全漏洞，并针对入侵活动采取有针对性的反制措施，就有可能避免系统破坏、数据外泄等实际损失产生。因此，应该对安全事件保持高度的警惕和重视，及时采取有效的应对措施，以最大程度地避免潜在的损失。

在遭遇安全事件并已对系统或网络运营者造成实质性损失时，首要任务是防止损失进一步扩大。例如，当一台主机感染勒索病毒时，应及时断开主机的网络连接，阻止病毒的进一步扩散。一旦网络安全事件对机构的正常生产和运营产生影响，首要任务是尽快恢复

生产和经营秩序以减少损失。

安全事件所造成的“损失”具有多重性。有些事件可以通过经济损失来进行量化，例如因停产停工给企业带来的直接经济损失。有些事件则会对涉事机构的声誉或信誉造成影响，例如网站被篡改、服务中断等。此外，还有一些事件在表面上看似并未给网络运营机构带来直接损失，但却可能给整个社会带来安全风险，进而使网络运营者承担法律责任或司法风险，例如重大的个人信息泄露事件，可能会导致网络诈骗的泛滥，涉事机构及关键责任人需要承担相应的法律责任。

2. 完善网络安全体系是事件处置的重要任务

若将事件处置视为单纯的应急救援行动，那么网络运营者必将陷入疲于奔命且无尽无休的“响应”循环之中。安全事件的每一次发生，都表明网络安全建设与运营过程中存在一定程度的漏洞或安全隐患，这些漏洞可能大小不一，也可能严重程度不同。同时，这些事件也暴露出网络内外部存在的客观安全威胁。如果在事件处置过程中，无法修补或改善这些安全漏洞及潜在风险，无法有效遏制甚至反击攻击者的攻击行动，那么即使暂时修复了受损的系统、恢复了中断的生产和经营活动，攻击者仍会再次发起新的攻击。许多机构之所以频繁遭受攻击，主要原因在于在事件处置过程中未能实现网络系统的完善、升级和加固。

此外，在应对安全事件过程中，对攻击路径进行深入分析、对攻击者特征进行细致研究、全面排查潜在安全风险，对于不断完善网络系统的安全建设至关重要。而开展这些分析工作的核心环节，是本书详细介绍的“追踪溯源”这一重要技术手段。

1.1.3 事件处置的原则与方法

网络安全运营实践表明，事件处置需要具备组织性、计划性、科学有序性。通常，事件处置应遵循以下四个原则。

1. 关口前移

早期的网络安全理念认为，防御是在攻击之后才出现的，即矛先于盾，攻先于防。这意味着在安全事件发生后才开始进行响应。如果没有出现威胁行为，那么响应行为也就不会产生；任何安全系统、技术或机制都只能防御已知的安全威胁，对于未知的安全威胁，尤其是针对系统 0-day 漏洞的攻击是无法防御的。然而，多年来的安全实践已经打破了这种传统观念。特别是在开展关键信息基础设施安全建设时，必须确保网络系统的安全建设具备应对新兴威胁和新式攻击手段的能力，并通过科学有效的事件处置化解安全风险。

在网络系统设计之初应充分考虑到未来的业务发展及可能面对的各种网络安全威胁风险，提前设计好各种防范和响应措施。只有这样，才可能在安全事件真正发生时，采取有效的响应行动。这种将安全攻防前置到网络系统规划设计阶段的思想被称为“关口前移”，即在攻击行动之前采取防守行动。

根据关口前移的原则，在网络系统的网络安全建设过程中，应充分考虑威胁发现能力和威胁响应能力的建设，以确保网络系统的安全性和稳定性。首先，在网络系统中设置并实施所需的安全监测措施，以确保运营者具有在安全事件发生的第一时间发现相关威胁的能力。及时发现威胁是有效处置安全事件的前提和基础，在实际应用中，常见的用于威胁监测的技术手段包括但不限于终端安全管控、边界安全防护、入侵监测、流量监测、态势感知等。其次，在网络系统中配置必要的安全策略和灾备措施，以便在发生安全事件时，运营者可以及时采取有效手段进行应对。例如，针对攻击源 IP 地址进行封堵，对被感染设备网段采取隔离等操作；在系统数据遭受破坏时，可以利用异地灾备系统进行数据恢复等操作。

2. 止损优先

事件处置的首要目标是及时止损，因此在事件处置过程中，应遵循“止损优先”的处置原则。一些机构在面临网络安全事件时，由于缺乏应急预案和事件处置经验，导致在犹豫不决中错失解决问题的最佳时机，从而产生损失。以下几种问题是比较常见的。

（1）在处理安全事件时，一些部门或责任人可能会因为害怕承担责任，而在事件影响范围尚小时，隐瞒不报，采取各种不当的“自救”或“掩盖”措施，从而错过了最佳的处理时机，导致事件扩大，甚至演变成大规模的危机。

（2）在安全事件发生后，有关部门推卸责任，导致应急处置工作不能及时开展。

（3）在面对潜在风险时存在侥幸心理，试图实施在线救援，未断开失陷的设备，导致感染区域扩大，最终造成业务中断。

（4）作为证据保全的一部分，应急响应团队需要在进行修复之前进行取证。这种做法可能导致业务遭受不必要的长时间中断。在实际情况中，尽管“固证留痕”是事件处置的重要内容之一，但当溯源、取证工作与止损目标发生冲突时，应将止损作为优先任务。

3. 组织有序

在应对安全事件时，必须保持有序的组织和流程，避免出现混乱无序、忙中出错的情况。首先，必须具备有效的组织架构和明确的岗位职责，以确保在安全事件发生时，有专门的人员进行报告、管理和指挥，所有相关部门都能紧密协作并服从统一指挥。其次，必须预先制定针对不同类型安全事件的应急预案，并定期进行应急演练，以便验证这些预案的执行效率和可靠性。只有通过科学的预设响应流程，才能确保在安全事件真正发生时，相关人员能够有序、有步骤地进行有效处置。此外，应该定期组织全员网络安全意识教育和事件应急业务培训，对于特殊岗位还应开展有针对性的教育训练，以确保员工在遇到各类突发网络安全事件时，能够清楚了解如何上报安全事件并第一时间采取科学有效的处置措施。

4. 固证留痕

在网络安全事件处置过程中，固证留痕是指在条件允许的情况下，应尽可能保留或备份各类系统日志和网络安全日志，并尽可能保护好攻击者留下的“犯罪现场”，保留关键

证据，为追踪溯源和取证提供支持。

为确保固证留痕工作的顺利进行，前期相应的准备工作是不可或缺的。只有在安全设备和安全措施已全面部署到位的情况下，才有可能对网络攻击行为进行相对全面的记录。单纯依赖操作系统或 IT 系统的自带日志功能，往往无法保留全面的攻击证据。

前文提到“固证留痕”的优先级低于“及时止损”，因此不能因追求证据的留存而影响到系统的止损。然而，在实际操作中，网络运营人员因缺乏专业指导，往往会不经意地破坏“犯罪现场”。例如，当某一设备受到威胁时，只需将其断网以隔离风险，不会对网络系统运行造成影响，但为了迅速解决问题，选择对设备进行杀毒操作或将硬盘格式化并重装系统，导致该设备的所有日志被清除，无法进行后续的溯源分析。

1.1.4 事件处置的触发条件

通常，网络安全事件的发生是事件处置的启动条件。然而，从实际经验来看，安全事件并不总是具体的攻击事件。以下列举了一些常见的事件处置启动条件。

1. 系统失陷且有明显表象

这是最为严重的触发条件。一旦网络系统出现明显的网络攻击迹象，意味着攻击者已成功入侵系统。常见的现象包括感染勒索软件，导致系统屏幕被篡改或收到勒索信；感染挖矿木马，使得 CPU 占用率长时间高达 100%；网站或服务器遭受拒绝服务攻击（DDoS 攻击）而无法访问；网站和设备页面被明显篡改；安全软件或设备发出大量告警等。这些均为系统失陷的表象。

2. 生产系统出现大面积异常

尽管生产系统的异常并不一定由网络攻击事件引发，但对于高度数字化的系统，一旦出现大面积异常，通常可以认定为网络安全事件，或至少需要启动网络安全事件处置预案。在此情况下，网络安全部门应积极开展异常排查。根据实践，即使是员工误操作或违规操作导致的诸如断网、拒绝访问、设备异常、系统访问异常等问题，也都应纳入可启动网络安全事件处置的范畴。

3. 外部机构发布安全通报

安全通报是由特定安全机构（例如公安网警、各级网络与信息安全通报中心、CERT 等机构）向相关单位发送的具有针对性的安全事件告警信息。这种通报也是事件处置的重要触发条件，尤其对于关键信息基础设施运营者来说，安全通报可能成为他们最常见、最重要的响应触发原因。

安全通报通常由三个主要来源提供信息：网信、公安等网络安全主管机构，行业监管机构或行业协会，以及国家漏洞库或第三方漏洞平台。其中，第三方漏洞平台是由企业或民间组织建立的漏洞收集平台，它们在收到“白帽子”提交的安全漏洞报告后，会以安全通报的形式将漏洞信息报送给涉事机构。这些通报信息通常包含有关漏洞的详细信息，以

及建议采取的措施和修复方案，以帮助相关机构及时修复和防止潜在的安全威胁。

安全通告通常涵盖一些重要且普遍的安全问题，其中包括：网络安全漏洞、违法交易行为、违规外部链接以及攻击性的信息等。这些问题的出现，不仅可能对个人与企业的网络安全造成威胁，还可能对整个网络环境的安全稳定产生消极影响。其中安全事件有以下几种。

（1）黑产交易信息，是指涉事机构内部数据可能作为在黑市上被交易的信息。

（2）非法外联行为，是指机构内部设备存在与已知“黑 IP 地址”进行通信的行为。一般来说，只有失陷的设备才会向攻击者的服务器传递信息。非法外联行为的出现，意味着已经有内部设备失陷。

（3）攻击舆情信息，是指在某些比较活跃的黑客论坛或黑产交流平台上出现的，针对特定机构、特定系统或特定平台的攻击威胁信息，如漏洞信息、后门信息、攻击计划等。

在一般情况下，涉事机构在接到安全通报后，如能及时采取措施，可以有效防止风险扩散；若未能及时处理，不仅可能加剧风险扩散，还可能面临攻击威胁。

4. 威胁情报收到特定信息

某些机构会自行采购安全机构的威胁情报服务，以加强自身的安全防范。当机构收到的威胁信息内容与该机构的网络安全工作有直接关联时，应当及时触发事件处置，采取相应的措施以防范和应对潜在的安全威胁。例如，当发现某个新出现的恶意样本曾经在机构内网中出现过，或者某个恶意组织正在针对机构所在行业发起针对性的网络攻击等情况，都应当立即采取行动，防止可能的危害。

需要指出的是，威胁情报的信息往往比安全通报更加具体和详细，有些甚至可以直接用于安全设备的威胁检测。这些威胁情报是通过技术手段或安全服务供应商自主获取的，属于机构内部安全建设与运营的一部分，与安全通报有着本质的区别。因此，在处理和应对威胁情报时，需要采取果断措施。

5. 安全防护系统发出告警信息

安全设备和防御系统在机构内部发出告警信息，这些告警信息虽然小但频繁发生，每条信息都暗示着一种潜在的安全风险。实际上，通过安全运营手段逐步减少或消除告警信息的过程，就是逐渐消除潜在安全威胁的过程。对于安全运营工作相对成熟的机构来说，处理告警信息应有具体的规范和清晰的流程。然而，许多机构在完成前期网络安全建设后，对网络安全运营工作持轻视态度，对大量的告警信息长期忽视，这导致所有的安全防御措施都无法发挥应有的作用，最终可能导致重大安全事故发生。因此，及时、有效地处理告警信息是维护网络安全不可或缺的一环。

6. 内部巡检发现潜在隐患

机构内部巡检是安全运营工作中不可或缺的一部分，既包括日常的例行巡检，也涵盖了针对特定需求的专项巡检，例如针对勒索病毒防护的暴露面巡检、灾备措施巡检等。通过科学的安全巡检工作，可以提前发现潜在风险和隐藏的安全隐患，这些被检测出的风险和隐患同样属于安全事件，需要启动相应的事件处置机制。

7. 内部员工报告安全事件

员工上报也是触发事件处置的重要条件。在某些情况下，员工可能会收到钓鱼邮件或发现办公电脑出现异常，向 IT 或安全部门主动上报这些问题。另外，一些安全意识较强且具备一定安全技能的员工还可能会主动发现内部系统的安全隐患，并向机构信息化部门或网络安全部门反馈。因此，机构应充分重视员工主动报告的安全事件，确保员工上报安全事件的渠道畅通。

1.1.5 事件处置的内外协作

网络安全事件处置并非是单一部门的独立行动，需要跨部门协作方可完成。若协作不力，将导致事件处理效率降低，安全隐患无法彻底清除，甚至可能引发额外损失。在网络安全事件应对过程中，组织协作通常涉及以下环节：从统一指挥到技术实施、从 IT 保障到关联业务、从供应链到外部客户、从应急服务到监管上报。这些环节在事件处置中发挥着重要作用，以确保机构能够高效地应对网络安全事件。

1. 从统一指挥到技术实施

网络安全部门或信息化部门通常是应急响应的指挥协调机构。在组织架构上，其上级是公司领导层和专家顾问组，对于重要问题，需要将情况上报给领导层进行决策。其下级是提供技术支撑的运营团队，负责实施应急响应所需的具体技术操作。在网络安全或信息化部门之下，通常还有一支实施团队，负责执行具体的应急响应任务。这支团队需要具备专业的技术知识和技能，能够根据事件性质和应急预案，迅速采取相应的技术措施，如隔离攻击、恢复系统、查杀病毒等。此外，网络安全部门或信息化部门还需要与各个业务部门保持紧密联系，确保应急响应过程中的协作顺畅。在事件发生时，各部门需要快速协同、共同应对，以最快的速度恢复业务系统的正常运行。

在事件处置过程中，网络安全部门或信息化部门还需要及时汇总和分析事件信息，为领导层提供准确的事件进展和应对措施。这需要该部门具备高效的信息收集、分析和报告能力，以便领导层能够全面了解事件情况并做出科学决策。

2. 从 IT 保障到关联业务

对于事件处置，通常需要 IT 部门各个环节的保障和支持，这些环节包括网络运营、机房管理、软件开发、设备维护等。此外，所有可能受到安全事件影响的业务部门也需要根据事件处理的最新进展来制定各自的响应计划。为了保障生产经营秩序，IT、安全和业务团队之间的紧密协作至关重要。业务部门的参与对于事件的快速、高效处理有着不可替代的作用。安全部门通过与业务部门紧密合作，可以更好地了解业务需求和流程，从而更好地调整安全策略和措施。

3. 从供应链到外部客户

在网络安全事件处置中，产业链上下游的协作具有极其重要的地位。当安全事件涉及

机构外部的供应商或者需要外部技术支持时，机构通常无法单独完成事件的处置，因此需要与各 IT 和安全供应商积极合作以共同应对。此外，如果安全事件有可能影响到产业链的下游机构、机构的客户或服务对象时，机构应当及时向外部业务关联方同步关键信息和处置进度，共同制定应对策略，以最大程度地减少对客户或服务对象的影响并提供援助。

4. 从应急服务到监管上报

在面临重大网络安全事件或机构内部人员专业能力不足时，向专业的网络安全应急响应服务平台寻求帮助，或向提供长期网络安全服务的安全企业求助是最佳的选择。将专业的工作交给专业的人来处理，特别是关键信息基础设施发生安全事件，并且该事件已经对社会或公共利益产生重大影响时，安全事件的处置不再仅仅是机构内部的事情。此时，需要立即上报给网信、公安等网络安全主管部门，在必要情况下，可以申请主管机构协助处理并协调外部资源提供援助。

1.2 事件响应与追踪溯源

1.2.1 追踪溯源的目的与作用

追踪溯源，也称为溯源分析，是指对网络攻击进行源头追踪和定位的行为。网络攻击追踪溯源，一般指追踪网络攻击源头、溯源攻击者的过程，即寻找网络攻击的发起者或源头。在早期，追踪溯源工作主要是以找到攻击源头为目标，特别是确定攻击者在物理空间中的具体位置。这种做法的最终目的是抓到攻击者，从而打击网络犯罪活动。

随着网络攻防技术的持续发展和各种身份隐藏技术、僵尸网络技术的广泛应用，网络安全工作人员逐渐认识到，在许多情况下，实现“顺着网线抓坏人”的目标是相当困难的，甚至可以说是不可行的。更重要的是，在网络犯罪产业化和国际化的大背景下，以及 APT（Advanced Persistent Threat，高级持续性威胁）攻击频繁发生的环境中，即使投入大量的资源和人力，对某一次特定的网络攻击事件实现了物理空间的“精准定位”，但受限于法律执法权范围，这对于打击网络犯罪或反制网络战活动的实际意义并不大，因为根本无法抓捕这些网络攻击者。

然而，这并不能否定追踪溯源工作的价值。在网络安全工作的实践中，人们发现，溯源分析的技术和方法对于网络安全建设至少具有两个方面的重要积极意义。首先，通过还原犯罪现场，复原攻击者的攻击路径，可以让防守方能够从攻击者的视角发现系统建设和运营过程中存在的安全漏洞。其次，通过对攻击者攻击手法、攻击特征、攻击武器等分析，以及对攻击者身份的研判，可以帮助防守方制定有效的防御方案，动态优化防御策略，从而大幅度降低攻击的安全威胁。

因此，追踪溯源和溯源分析，已不再局限于传统的对攻击者在网络空间或物理空间定位，而是广泛运用于网络安全事件的处置过程中，涵盖了对事件的起源、演化过程和相关

责任人（或组织）的确定过程，包括但不限于对攻击者攻击手法、攻击路径的还原，对攻击者的研判和画像等相关工作。

追踪溯源的主要目标主要体现在以下三个方面：一是通过深入溯源分析，及时发现并识别网络系统存在的安全漏洞和隐患，为机构提升网络安全建设与运营水平提供参考依据；二是借助溯源分析成果，深入了解攻击者的手法和特点，为机构动态调整和优化防御策略提供重要参考依据；三是通过溯源分析，尽可能收集并掌握攻击者或责任人的相关信息，为后续打击和追究相关人员的法律责任提供关键线索和证据。

1.2.2 内部溯源与外部溯源

根据溯源目标和范围的不同，追踪溯源工作通常分为两个阶段：内部溯源和外部溯源。

1. 内部溯源

内部溯源是指当发生特定安全事件时，在内部网络环境中，对攻击者的攻击路径、手法及范围等进行回溯的过程。主要目的是从攻击者视角发现系统安全漏洞，为外部溯源提供重要支持。内部溯源的基本任务：一是确认失陷范围和攻击范围，以便确定受到影响的系统和数据范围；二是确认攻击路径，以便了解攻击者是如何进入系统的，并追踪其活动；三是确认互联网侧攻击 IP 地址，以便确定攻击的来源和相关联的 IP 地址；四是确认攻击工具和攻击手法，以便更好地理解攻击的性质和攻击者的意图。

（1）确认失陷范围和攻击范围

失陷范围是指被攻击者成功攻入的网络设备、系统账号、数据库资源等内部资源的总和。成功攻击的标志包括获得系统权限、盗取账号密码、投放木马病毒程序、窃取数据、篡改系统等。确定失陷范围是进行溯源分析的基础和起点，需要对失陷范围进行修复和加强安全防护。

失陷范围是攻击范围的子集。在渗透型攻击中，攻击者会尝试对多个目标同时发起攻击，有时甚至使用批量自动化攻击手段。未成功攻破的目标不属于失陷范围，但属于攻击范围，如图 1.1 所示。确定攻击范围较为复杂，其意义在于明确潜在安全风险并完善对攻击者的特征描述。

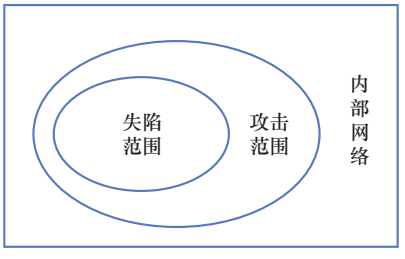

图 1.1　失陷范围与攻击范围之间的关系

（2）确认攻击路径

攻击路径是指攻击者从网络入侵的突破口开始，直至完成所有攻击活动，在内部网络

中依次访问的所有节点连接而成的拓扑结构。确认攻击路径是内部溯源的核心任务之一，也是发现内部网络安全建设和运营漏洞的关键步骤。在大多数情况下，攻击路径呈现树形结构，即攻击者每控制一个新的内网节点，就会以此节点为跳板，通过横向移动攻击内网的其他节点，如图 1.2 所示。

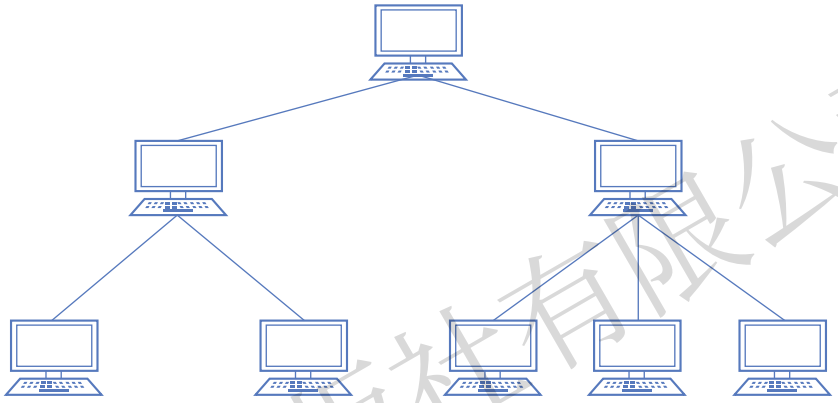

图 1.2　攻击路径树状结构

（3）确认互联网侧攻击 IP 地址

内部溯源的一项关键任务是识别攻击者在互联网侧的攻击 IP 地址。尽管该攻击 IP 地址可能是攻击者通过代理节点隐藏身份后的 IP 地址，但这依然是进行外部溯源的起点和必要条件之一。

（4）确认攻击工具和攻击手法

攻击工具是指攻击者在攻击过程中所使用的各种黑客工具、木马程序及浏览器等。攻击手法多种多样，其中比较常见的包括：暴力破解、钓鱼邮件、钓鱼社交、网页挂马、漏洞利用、漏洞扫描、外插 U 盘等。确认攻击工具和攻击手法有助于分析内网漏洞，并为外部溯源提供重要依据。然而，确认攻击工具和攻击手法需要一定的专业安全知识，建议在专业人员的指导下完成。

2. 外部溯源

外部溯源是指对攻击者的网络资产进行全面梳理，对其意图和身份进行深入研究和分析的过程。外部溯源是在内部溯源的基础上，进一步拓展对攻击者的分析，以便更加有效地指导防御策略的制定和实施。同时为打击网络犯罪、追踪攻击者提供线索和依据。需要强调的是，尽管溯源分析和电子取证技术存在一定的技术交叉，但不论是内部溯源还是外部溯源，都无法取代电子取证。在计算机系统的取证过程中，需要遵循一定的“程序保障”，才能确保电子证据在法律上的有效性。而一般的溯源过程并不能保证其溯源结果在法律上具有有效性。外部溯源工作的基本任务如下。

（1）对攻击者的网络资产梳理

攻击者的网络资产是指攻击者发动网络攻击所使用的各种网络资源，包括但不限于

域名、IP 地址、主机、代理等。其中，攻击者建立的网站或 C2 服务器（也称为 C&C 服务器）是最为关键的网络资产，这些资产是攻击者与内部网络失陷设备进行通信的关键环节，往往包含攻击者的一些关键特征信息。这些网络资产对于攻击者的成功攻击至关重要，因此对于网络安全防御来说，识别这些资产是至关重要的。

仅对某一起网络安全事件中的攻击者网络资产进行孤立梳理，不足以实现对攻击者特征的有效研究与判断。为了对攻击者特征进行准确研判，需要在“安全大数据”的基础上，将溯源过程中发现的攻击者网络资产与所有攻击者的“网络资产库”进行比对，才有可能确定本次安全事件与历史上其他安全事件是否存在确定的关联性。例如，截获了攻击者使用的 5 个网络资产，其中 4 个没有任何不良记录，但 1 个资产曾出现在某个非法组织的网络资产清单中，表明此次安全事件可能与该非法组织存在内在联系。如果发现内部设备与该组织的其他网络资产有过通信行为，这意味着发现了之前未知的内网失陷设备。结合该组织的所有网络资产和行为特征，可以更准确、更详细地描述攻击者的特征，并采取有效的防范措施来应对该非法组织的网络攻击。

（2）攻击者的历史活动分析

虽然一次攻击活动留下的线索有限，但是如果能将已知的攻击者的历史活动进行梳理，聚合所有信息，包括攻击者何时何地、使用何种工具对何种网络系统进行了何种操作，产生了何种后果等，就有可能绘制出一张相对清晰且完整的“攻击者画像”。历史活动不仅涵盖攻击活动，也包括攻击者在系统中进行的所有“合规操作”。所谓“合规操作”，是指未引发任何安全警报，也无任何显著攻击特征的操作行为。

在实施最终攻击之前，攻击者会进行大量的探测活动，包括从外部进行探测和在目标系统内部进行横向移动，以确定对目标进行攻击的可行性。这些探测活动大多数情况下不会引发安全告警，也不会产生明显的破坏现象，因此极不易被察觉。例如，攻击者可能会多次访问某个机构的门户网站，尝试注册并登录一个新的用户账号，点击系统的某项功能按钮等。同样，攻击者在完成攻击后可能会清理自己的攻击痕迹，而这些清理动作也不会引发任何安全告警。然而，当已经确定某个攻击者与某起安全事件存在关联时，该攻击者在系统中进行的所有操作都应被记录和分析，只有这样，才能完整地复现整个攻击过程。

在实际工作中，分析人员应关注安全告警和典型攻击活动，同时也不能忽视攻击者进行的“合法操作”。尽管这些操作可能没有典型攻击特征且未触发任何告警信息，但仍然可能是攻击者行为的一部分。因此，分析人员应该全面分析攻击者的行为模式，以更好地防范和应对潜在的安全威胁。

（3）攻击者的画像与研判

外部溯源的最终目标在于锁定攻击者以及攻击者的物理空间位置。首先对攻击者进行定性分析，对其资产特征、行为特征、攻击手段等加以描述，之后对其具体的身份、背景、动机进行研判，结合社交平台的情报收集或线下取证手段，才能最终锁定攻击者。有时即使无法锁定具体的攻击者，无法从根本上铲除攻击源，集合溯源分析中获得的攻击者情报，仍然能够有效地帮助防守方优化防守策略，提升防护能力和水平。

1.3 追踪溯源技术发展和主流技术

1.3.1 早期追踪溯源关注点

2004 年，以 Cohen D 为代表的研究团队［C3s Inc，位于美国加利福尼亚州洛杉矶市，研究项目为高级研究与开发活动（Advanced Research and Development Activity，ARDA）中的攻击归因领域］将网络攻击追踪溯源划分为四个级别：追踪溯源攻击主机、追踪溯源攻击控制主机、追踪溯源攻击者、追踪溯源攻击组织机构。在第一层上主要使用 Input Debugging、Itrace、PPM、DPM、SPIE 等网络数据包层面的技术方法；在第二层上主要使用内部监测、日志分析、网络流分析、事件处置分析等技术；在第三层上主要使用自然语言文档总结分析、Email 分析、聊天记录分析、攻击代码分析、键盘信息分析等技术；在第四层上，主要依托攻击组织机构的攻击特征、方法进行分析。

2018 年 9 月，美国国家情报总监办公室发布的《网络溯源指南（A Guide to Cyber Attribution）》备忘录指出，“所有行动都会留下痕迹”，溯源分析就是使用这些信息，结合对之前已知恶意入侵事件及所有工具和手段的了解，尝试追溯攻击源头。总而言之，溯源的首要任务是深入了解攻击事件的来龙去脉，包括攻击方式、攻击路径以及攻击者的身份等信息。在明确了这些基本情况之后，需要进一步分析和评估攻击的影响、严重性以及相应的应对策略。这个过程需要回答的核心问题是：谁应该对这次攻击负责？为什么会发生这次攻击？

1.3.2 追踪溯源技术的发展

技术手段是进行溯源的重要基础。一些主流的技术模型和框架，如“钻石”模型、MICTIC 框架（Malware, Infrastructure, Control Server, Telemetry, Intelligence, Cui Bono）和 ATT&CK 框架（Adversarial Tactics, Techniques, and Common Knowledge），已经在获取攻击者的工具、技巧和流程（TTPs）等信息方面日趋完善和标准化。

另一种具有代表性的研究方法则是根据不同的攻击场景，将网络攻击追踪溯源划分为虚假 IP 追踪、Botnet 追踪、匿名网络追踪、跳板追踪和局域追踪 5 类问题，并将解决这 5 类问题的技术方法归纳为 4 种类型，包标记、流水印、日志记录和渗透测试。

（1）包标记方法。主要包括 Itrace[1]（ICMP Traceback）、PPM[2]（Probabilistic Packet

1　iTrace：使用 ICMP 回溯消息进行数据包路径表征和线路跟踪，在转发数据包时，路由器可以以较低的概率生成发送到目的地的回溯消息。通过路径上来自足够多路由器的足够多的回溯消息，可以确定流量源和路径。

2　PPM：概率数据包标记，在数据包通过互联网遍历路由器时对其进行概率标记，使用路由器的 IP 地址或数据包到达路由器所经过的路径边缘来标记数据包。

Marking，概率数据包标记）、DPM[1]（Deterministic Packet Marking，确定性数据包标记）技术，作为网络数据包层面的追踪溯源方法。这种方法难以应对复杂的以 APT 为代表的网络攻击。

（2）流水印技术。不需要修改协议，也适用于加密流量，甚至可以用来追踪溯源一些以匿名网络为跳板的网络攻击，但是流水印技术需要大量匿名网络基础设施的支持，因而不易实施，同时在技术上要保证水印检测的准确率也有一定难度。

（3）日志记录技术。是一种被动追踪溯源方法，存在所记录的信息有限、可能被攻击者篡改的问题。

（4）渗透测试技术。可以为网络攻击的追踪溯源提供关键突破，但技术难度大，并且存在合法性方面的问题。

从技术细节来看，现有技术手段以被动追踪溯源技术为主，缺少主动获取追踪溯源关键信息方面的研究。网络攻击的隐蔽性和匿名性也符合“木桶原理”，因此，追踪溯源的突破往往取决于少量的关键线索。被动追踪溯源收集到的是攻击者有意或无意泄露的信息，线索质量难以满足溯源方的预期。需要结合主动溯源进行主动出击，在司法允许的范围内，结合陷阱、诱捕、欺骗和软硬件特性利用等方法，同时在攻击目标和攻击者两端获取高质量的关键溯源线索。

从系统性来看，各类追踪溯源技术往往存在独立使用、各自为战的问题，而缺少定向网络攻击追踪溯源的整体模型研究。模型研究作为基础性工作，可以有效整合现有策略、资源和技术手段，并可应用于网络和系统的各个层面上，形成面向追踪溯源的纵深化防御体系。

总体来看，现有研究成果大多面向非定向网络攻击，而缺少专门面向定向网络攻击追踪溯源的理论和技术的研究。定向网络攻击是应用和业务层面上而非网络层面上的攻击，更具隐蔽性、匿名性、持久性和复杂性，追踪溯源的难度更大。现有的定向网络攻击溯源技术在应对类似 APT 等频繁使用跳板主机、跳板网络和公共网络服务的网络攻击时，追踪溯源能力有限。同时，定向网络攻击使用的攻击工具和攻击方法，也和非定向网络攻击有着显著的区别。因此，在定向网络攻击追踪溯源理论和技术方面，需要进一步的创新。

1.3.3 主流的网络攻击追踪溯源技术

主流网络攻击追踪溯源技术包含威胁情报、Web 客户端追踪技术、网络欺骗技术等。

1. 威胁情报

为了准确高效地追踪溯源网络攻击，工业界提出了威胁情报（Threat Intelligence）这一概念。Gartner 曾给出了比较通用的威胁情报定义：威胁情报是一种基于证据的知识，

1 DPM：确定性数据包标记，通过对 IP 地址进行编码（例如 Hash）存入数据包的 ID 字段中，跟踪和识别不同来源的数据包的一种方法，以及基于 DPM 发展出的 DREM、DDPM 方法。

包括威胁相关的上下文信息、威胁所使用的方法机制、威胁指标、攻击影响以及应对建议等。威胁情报描述了现存的或者即将出现的针对资产的威胁或危险，并可以用于通知受害一方针对威胁或危险采取应对措施。在后续章节中有详细介绍。

2013 年，David J. Bianco 在总结 IOC（威胁指标，Indicator of Compromise）类型及其攻防对抗价值的基础上，建立了威胁情报价值金字塔模型，该模型揭示了防御者追踪溯源到不同的威胁指标时，会导致攻击者付出的代价不同。各国的 CERT、防病毒机构、安全服务机构、非政府安全组织等纷纷建立了各自的在线威胁情报平台，提供查询和分析服务，可以查看安全预警公告、漏洞公告、威胁通知等，帮助网络运营者追踪溯源网络攻击。

威胁情报在网络攻击追踪溯源方面的优势在于其具备海量多来源知识库以及情报的共享机制。这些情报可以为追踪溯源提供有力支撑。具体来说，防御者可以将已掌握的溯源线索输入给威胁情报分析系统，后者通过关联和挖掘，不断拓展线索的边界，并输出大量与已知线索存在关联的新线索。如何利用威胁情报自动化追踪溯源是近年来学术界和工业界研究的热点话题。

2. Web 客户端追踪技术

主要是指用户使用客户端（通常是指浏览器）访问 Web 网站时，Web 服务器通过一系列手段对用户客户端进行标记和识别，进而关联和分析用户行为的技术。基于浏览器及插件存储机制（如 Cookie）的 Web 追踪，是该领域最早使用也是最广为人知的技术。随着前端技术的发展，许多新的 Web 追踪机制应运而生。近年来，有研究者提出使用指纹技术跨网站追踪浏览器用户的方法。

（1）Cookie 追踪

Cookie 同步是指用户访问 A 网站时，该网站通过页面跳转等方式将用户的 Cookie 发送到 B 网站，使得 B 网站获取到用户在 A 网站的用户隐私信息。

用户可以通过清空浏览器缓存等方式，清除已保存的 Cookie，Evercookie 将 Cookie 通过多种机制保存到系统多个地方，如果用户删除其中某几处的 Cookie，Evercookie 仍然可以恢复 Cookie，如果用户开启了本地共享，Evercookie 甚至可以跨浏览器传播。

（2）浏览器指纹

① 基本指纹。是任何浏览器都具有的特征标识，比如硬件类型、操作系统、用户代理、系统字体、语言、屏幕分辨率、浏览器插件、浏览器扩展、浏览器设置、时区差等众多信息。

② 高级指纹。是基于 HTML5 的方法，包括 Canvas 指纹、AudioContext 指纹等。Canvas 是 HTML5 中动态绘图的标签，每个浏览器生成不一样的图案。AudioContext 生成与 Canvas 类似的指纹，前者是音频，后者是图片。

③ 硬件指纹。主要通过检测硬件模块获取信息，作为对基于软件的指纹的补充，主要的硬件模块有：时钟频率、摄像头、声卡/麦克风、移动传感器、GPS、电池等。

④ 综合指纹。采用单一指纹有可能会出现碰撞问题，可以将上述基本指纹和高级指纹综合起来，计算哈希值作为综合指纹，降低碰撞率。

⑤ 跨浏览器指纹。上述指纹都是基于浏览器进行的，同一台电脑的不同浏览器具有不同的指纹信息，这样造成的结果是，当同一用户使用同一台电脑的不同浏览器时，服务方收集到的浏览器指纹信息不同，无法将该用户进行唯一性识别，进而无法有效分析该用户的行为。跨浏览器的浏览器指纹，依赖于浏览器与操作系统和硬件底层进行交互进而分析计算出指纹，这种指纹对于同一台电脑的不同浏览器也是相同的。

（3）Web RTC

Web RTC（网页实时通信，Web Real Time Communication），是一个支持网页浏览器进行实时语音对话或视频对话的 API，功能是让浏览器可以实时获取和交换视频、音频和数据。基于 Web RTC 的实时通讯功能，可以获取客户端的 IP 地址，包括本地内网地址和公网地址。

Web 客户端追踪技术在网络攻击中扮演着重要角色，不仅是攻击者探测信息的重要平台，还是投递攻击载荷的重要通道。浏览器指纹在溯源方面的一个重要应用场景便是跨网站追踪：攻击者同时拥有一个已公开的身份和一个未公开的身份，虽然两个身份访问了不同的网站，但可以提取到相同的浏览器指纹，就可以通过指纹关联来溯源攻击者的真实身份。

3. 网络欺骗技术

网络欺骗技术由蜜罐技术演化而来，其基本含义是，使用骗局或者假动作来阻挠或者推翻攻击者的认知过程，扰乱攻击者的自动化工具，延迟或阻断攻击者的活动；通过使用虚假的响应、蓄意的混淆，以及假动作、误导等行为达到“欺骗”的目的。

网络欺骗技术主要包括欺骗环境构建和蜜饵部署。欺骗环境构建依赖于虚拟化技术和蜜罐技术，前者主要目的是模拟真实内网，构建一个包括主机和网络拓扑的高仿真欺骗基础环境；后者则是在欺骗环境中部署包括大量仿真业务的应用级蜜罐群。蜜饵部署主要是在可能的攻击路径上放置虚假的诱骗信息，如代码注释、数字证书、Robots 文件、管理员密码、SSH 密钥、VPN 密钥、邮箱口令、ARP 记录、DNS 记录等，从而诱使攻击者进入可控的欺骗环境。网络欺骗技术在网络攻击追踪溯源方面的作用与优势如下。

（1）发现网络攻击。这是追踪溯源的前提。网络欺骗通过部署虚假环境和蜜饵，吸引和误导攻击者，一旦这些正常用户难以触及的资源被访问，则表明网络极有可能正在被攻击。

（2）粘住网络攻击。为溯源网络攻击赢得时间。防御者通过欺骗手段将网络攻击逐步吸引至虚假的欺骗环境，可以消耗攻击者的时间、精力和资源，减少其攻击重要真实系统的可能，还能够大量暴露其 TTPs，从而为防御者采取针对性的防御策略争取缓冲空间，以及为溯源反制赢得主动。

（3）威慑攻击者。如果攻击者意识到自己已落入欺骗陷阱，这本身对其就是一种巨大

的心理威慑，同时攻击行为已被发现、攻击线索可能已经暴露，全给攻击者造成威慑。此外，攻击者长期处于欺骗环境的监视之下，防御者有充足的时间和空间部署工具、设置机关，开展网络攻击追踪溯源工作，从而进行反制和威慑。

1.3.4　如何应用网络攻击追踪溯源技术

网络攻击的追踪溯源是一门综合性技术，包括战略、战术、谋略、工具、装备、人员、能力、保障等内容。没有单纯的技术方法可以程式化、计算、量化或全自动实现溯源，无论这种技术是简单的还是复杂的。高质量的溯源取决于各种技巧、工具以及组织文化。

未来网络攻击追踪溯源可能会以一种“自相矛盾”的方式进行演变。一方面，溯源工作正变得愈发便捷。更加完善的入侵检测系统能够实时发现攻击行为，并能更快地调取更多数据以进行分析。构建更强大的网络防护体系将增加攻击行为的成本，消除不确定因素，并节约资源以更好地识别高级攻击。随着网络犯罪活动的增多，这将推动许多国家执法部门之间的合作，使得国与国之间的间谍行为更难以隐藏。另一方面，溯源工作也面临着更大的挑战。攻击者能够从公开的错误中吸取经验教训，这使得追踪溯源行动变得更加困难。随着强加密技术的广泛应用，取证工作也面临着更多难题，这进一步限制了大规模数据的收集。

习　题

1．网络安全的基本属性包含哪些内容？
2．网络安全的主要类型有哪些？
3．网络安全事件的基本含义是什么？
4．事件处置的基本含义是什么？其首要目标和任务是什么？
5．事件处置有哪些基本原则？
6．触发事件处置有哪些条件？
7．追踪溯源的基本含义是什么？
8．追踪溯源的主要目标是什么？
9．简述内部和外部溯源的主要目的。
10．简述主流的网络攻击追踪溯源技术。