刑事司法科学与治理
Criminal Justice Science & Governance
2022 年 第 3 卷 第 2 期

面向网络攻击的电子数据取证方法研究 *

李 杨[1] 夏 萌[2]

1．铁道警察学院，郑州；
2．中南财经政法大学，武汉

摘 要 | 近年来，网络攻击事件高发，严重危害我国信息网络安全，且网络攻击朝着自动化、智能化方向发展，漏洞发现和利用速度越来越快、防火墙渗透率越来越高、安全威胁不对称性增加、对网络基础设施破坏越来越大，这些都给网络空间安全带来极大威胁。网络攻击者在实施网络攻击时，常采用各种技术手段隐藏自己以对抗追踪，给网络攻击案件侦破带来巨大挑战。本文对常见网络攻击行为的特点进行了总结，并针对不同网络攻击行为进行了分析研究，提出相应的网络取证方法，对于网络攻击案件的侦查取证具有重要意义和价值。

关键词 | 网络攻击；电子数据；取证方法；分析研究

一、引言

近年来，网络安全风险不断增加，如“随着区块链技术的广泛应用，借助数字货币实现匿名转账的新型勒索邮件攻击逐渐兴起”和“不断发生的包括医疗信息、账户凭证、公司电子邮件和企业内部敏感数据泄露的数据泄露事件”等，给网络空间安全带来极大威胁。网络攻击者在实施网络攻击时，常采用各种技术手段隐藏自己以对抗追踪，如采用虚假IP地址、网络跳板、僵尸网络、匿名网络等技术。网络取证是一种对网络攻击的事后追责手段[1]，通过对网络流量等进行取证分析，将生成的电子数据证据用于诉讼活动，从而实现对各类网络违法犯罪活动的事后追责。网络攻击案件频频发生，为了能在日后筑起牢固的网络安全防线，办案人员与调查人员必须具有一定的网络取证分析能力，利用获取到的网络入侵线索总结出不同类型网络攻击案件的特征和相应的取证对策，并基于此进行多次网络靶场练习，增强应对网络安全突发事件的组织指挥、整体协作、应急处置能力和水平，进一步完善网络安全事件应急处置机制。网络取证主要针对的是网

*基金项目：中央高校基本科研业务经费项目（2022TJBKY027，2021TJJBKY023）；铁道警察学院教改项目（JY2021010，JY2021Z10）。

［1］刘雪花，丁丽萍，郑涛，等．面向网络取证的网络攻击追踪溯源技术分析［J］．软件学报，2021，32（1）：194–217.

络数据流、系统日志等，一旦发现网络活动存在异常行为，便会自动记录网络上的犯罪证据，并阻止入侵破坏的进一步发生。网络攻击案件发生后，为了防止电子数据证据被破坏，通常需要尽快进行勘验侦查，尽最大可能在有限范围内最大化获取有效的电子数据证据，形成完整“证据链”，也为追踪犯罪嫌疑人提供有利、可靠的证据线索。因此，针对不同类型的网络攻击案件总结出不同的网络取证方法和防御对策，对于预防和阻止网络攻击类案件的发生、提升侦查人员的办案效率具有重要意义。

在国外，网络取证技术发展较早，早在 20 世纪 90 年代就创立了“国际计算机证据组织”，建立了较为完善的法律原则和电子取证规范。现如今取证过程的模型有基本过程模型（BPM）、事件响应过程模型（IRPM）、法律执行过程模型（LEPM）、过程抽象模型（APM）等，取证工具有 Encase（GUIDANCE）、DIBS（美国计算机取证与司法鉴定公司）、Flight Server（Vogon）等。在国内，早期一些互联网安全领域的专家学者为了帮助公安机关侦破案件，开始利用计算机多媒体设备从网络通信会话和电子设备中捕获、分析和梳理能够证明犯罪事实的电子数据证据，以达到将进行网络攻击的犯罪嫌疑人缉拿归案的目的。传统的网络攻击取证技术多采用基本过程模型，将已知的攻击证据作为证据来源，主要强调从电子数据中提取证据，但更主要的是强调攻击行为发生后，将网络恢复到初始状态。如杨天识等人提出了一种主动取证技术[1]，即创建一个具有与真实服务器相同内存和存储的蜜罐虚拟机，利用 OpenFlow 来把控网络流量，从而将虚拟系统与真实的服务器断绝开来。当某个访客发送正常请求来访问服务器时，交换设备会将访客的访问请求链接到真实的服务器中；当某个访客被 IDS 标识为可疑攻击者时，交换设备会再一次重新计算路由路径，将可疑攻击者的访问请求链接到之前制定好的虚拟蜜罐服务器中。肖应君等人计划并设计了一种基于探测识别的网络取证系统，该系统包含了入侵识别、模拟服务、网络跟踪、日志上传等模块，当恶意攻击者准备对目标网络采取破坏措施时，该网络取证系统能够自动识别出网络攻击的类型是什么，同时采取相对应的网络取证手段，还能对这一网络犯罪过程进行监测、控制。吴丰盛则提出了多模光纤网络异常入侵信号提纯取证方法，通过建立网络信号传输模型，利用时间序列重构方法检测出网络异常入侵信号，并提取其时频谱特征量。在此基础上，结合经验模态分解法分离网络异常入侵信号特征信息，根据其收敛性将分离后的入侵信号输入到降噪滤波器中，完成入侵信号提纯处理，实现网络异常入侵取证。以上通过不同的方法实现了对典型网络攻击的取证，但依然存在对攻击、入侵行为的检查不全面、对恶意攻击行为相似度分辨准确性较差的问题[1]。

本文将从网络攻击行为的特点、在网络节点中留存的数据等角度出发，针对不同的网络攻击行为进行分析归纳，提出适合于不同类型网络攻击的取证方法，做到精准识别、快速阻止、有效提取，规范和优化公安机关处理网络攻击案件时的应对措施和使用技术，加大案件的侦办力度，提高案件侦破效率。

二、网络攻击的特点分析

随着互联网的广泛普及和蓬勃发展，人们可以通过网络上的各种教程来进行网络攻击，有时候甚至不需要掌握很多的高端技术，按照他人提供的演示实例即可完成相应的入侵攻击，并且近年来网络攻击已经演化为一门综合性的学科，这也得益于互联网的飞速发展，使得网络空间安全面临着难以预估的挑战。网络攻击正在朝着自动化、智能化、漏洞发现和利用速度越来越快、防火墙渗透率越来越高、安全威胁不对称性增加、对网络基础设施破坏越来越大的趋势发展，给网络空间安全带来极大的威胁。

（一）网络攻击趋于自动化

网络攻击的自动化体现在四个阶段：在扫描阶段，攻击者使用各种新出现的扫描技术来推动扫描工具的发展，同时利用更高级的扫描手段来达到提升速度、提高质量、改善效果的目的。在渗透控制阶段，一些类似于邮件植入、文件植入的传统植入方式已经不再具有之前那样良好的效果，因为现在的人们大都在自己的计算机上安装有防火墙和各种

[1] 高菲．分布式异构网络恶意攻击取证及预警方法研究［J］．计算技术与自动化，2021，40（1）：184–188.

先进的杀毒软件，有效阻碍了上述植入方式的进行。随之出现的先进的隐藏远程植入方式，如基于数字水印远程植入方式、基于 DLL（动态链接库）和远程线程插入的植入技术，能够成功躲避防病毒软件的检测，将受控端程序植入到目的计算机中。在传播攻击阶段，以往的攻击方式是需要操作者手动启动，而现在随着科技的进步则逐渐演变为攻击工具的自动启动，根本无须再依靠人工操控。在攻击工具协调管理阶段，DDOS 攻击广泛进入大众视野，各种分布式拒绝服务攻击工具盛行，恶意攻击者能够通过控制大量“肉机”来轻易达到调控攻击工具的目的，使大量计算机受到不同程度的破坏，互联网安全面临着不容小觑的挑战。

（二）网络攻击迈向智能化

现如今，各种智能化的网络攻击工具不断出现，即便是技术水平一般的人员都可以对计算机信息系统展开一定程度的网络攻击，更不用说是技术高超、具备系统化知识的人员。安全人员若想要成功阻碍攻击者实施的攻击破坏，就需要了解对方将要采取的技术手段和攻击类型是什么，才能制定相应的对策来对抗网络攻击，做到对症下药，以达到事半功倍的效果。目前攻击工具的开发设计者正在使用与现实更加适应的思维模式和技术手段来打磨升级这些攻击工具，攻击工具较之前的隐蔽性更强，同时朝着更加智能化的方向发展，一大部分攻击工具已经具备了反侦破、智能动态行为、攻击工具变异等特点。

（三）漏洞的发现和利用速度越来越快

可以毫不夸张地说，安全漏洞几乎在所有的计算机操作系统和应用程序中普遍存在，绝对是危害网络安全至关重要的因素。现如今，新发现的各种操作系统与网络安全漏洞每年都要增加一倍数量之多，网络安全管理员需要不断利用最新的补丁修补相应的漏洞。但攻击者往往能够抢在厂商发布漏洞补丁之前，发现这些未修补的漏洞并发起攻击，对网络空间安全造成极大的危害。

（四）防火墙的渗透率越来越高

架设防火墙一直以来都是单位和个人用于阻挡网络攻击的重要防范措施。但是，攻击者也一直都在研究如何能够避开防火墙阻挡的绕开手段。从他们攻击防火墙的过程来看，大致分为两种：第一种方法是探测识别目标网络上安装的防火墙系统是哪一种，找出该种防火墙存在的服务漏洞，对其展开攻击。第二种方法是采用欺骗技术绕过防火墙的身份认证环节，进而对内部网络实施攻击。

（五）安全威胁的不对称性在增加

互联网安全处于牵一发而动全身的状态，意思就是存在于互联网上的每一台计算机受到危害后都会间接影响到全球互联网上其他所有计算机的安全。随着网络攻击水平的大幅度提升，攻击者可以较为容易地入侵那些相对不太安全的计算机系统，这给攻击者带来很多可乘之机，使其抓住漏洞，进而对其他计算机系统展开新一轮的攻击破坏，由此下去，安全威胁的不对称性将持续增大。

（六）对网络基础设施的破坏越来越大

互联网的普及使得依托于互联网的各项服务越来越便利，用户会更多地选择通过网上服务来处理日常生活、工作中的事务，基于此攻击者一旦攻击互联网上的关键基础设施，其造成的影响便会是破坏性的。对于互联网关键基础设施实施的攻击，常用的手段主要有欺骗攻击、ARP 欺骗、电子邮件欺骗、DNS 攻击、Web 攻击等，攻击者一旦得手，这些网络基础设施的恢复将会十分困难。

三、网络取证概述

网络取证与传统的电子数据取证具有一定的区别，网络取证的对象主要是网络设备、网络数据流，以及发现、提取、分析与处理使用网络服务设备中的网络数据，在事件发生前或者发生中进行，网络取证可以监测并识别到入侵行为发生的异常数据流从而及时作出响应。而计算机取证是在事件发生后对涉及案件的计算机系统及设备展开具体的侦查取证工作。网络取证的最终目的是形成“证据链”，它的过程通常都是环环相扣的，前一个阶段的完成会为后一个阶段奠定基础、做好铺垫，提供一定的数据信息，后一个阶段的取证结果往往会使前一个阶段的取证结果得到印证。网络取证的每一个阶段都是相互联系的，这就需要这些信息相互关联，主要由关联分析引擎实现。

然而，受传统电子数据取证理念的影响，网络取证发展相对较缓慢，同时也存在一定的困难。我国的信息安全观念立足于被动防护的层面，倾向采

用密码、防火墙、杀毒软件等防御措施来保证信息安全，更多的关注于正常提供服务，针对网络攻击的取证大多在事件发生后进行，导致取证难度加大且已经造成了一定损失；同时，网络取证相关的法律法规目前不够完善，取证流程和操作规范尚存在一定不足；反取证技术发展迅速，也给网络取证带来了前所未有的挑战。

针对当前网络取证面临的困难，网络取证应围绕网络设备节点，针对不同网络攻击类型，开展端到端的数据分析，进而形成完整的证据链。随着移动电子设备的发展，新型通信手段的升级换代，网络取证也要与时俱进，针对不同设备研发出相应的恶意数据挖掘分析工具，形成有效的监管和取证手段。针对网络攻击的特点模式，要扩大网络取证的人员主体范围，加强企业与执法部门的合作，对网络数据进行有效监管。同时，开发系统化的取证工具，朝着综合型的方向发展，与人工智能、大数据、物联网、云计算等新型技术深度融合，更好地获得电子数据之间的相关性，来证明犯罪事实，给案件定性。

四、针对不同网络攻击的取证方法

（一）欺骗攻击与取证方法

欺骗攻击实质上就是一种冒充身份通过认证以骗取信任的攻击方式。攻击者针对认证机制的缺陷，将自己伪装成可信任方，从而与受害者进行交流，最终攫取信息或是展开进一步攻击。常见的欺骗攻击有：IP 欺骗、ARP 欺骗、电子邮件欺骗、DNS 欺骗、Web 欺骗[1]。

对于 IP 欺骗，大多数路由器有内置的欺骗过滤器，如果一个来自外网的数据包，声称来源于本单位的网络内部，就可以非常肯定它是假冒的数据包，应该丢弃，这种类型的过滤叫作入口过滤，它保护单位的网络不成为欺骗攻击的受害者。另一种过滤类型是出口过滤，用于阻止有人使用内网的计算机向其他的站点发起攻击。路由器必须检查向外的数据包，确信源地址是来自本单位局域网的一个地址，如果不是，这说明有人正使用假冒地址向另一个网络发起攻击，这个数据包应该被丢弃；对于 ARP 欺骗，如果知道正确的网关 MAC 地址，而通过 ARP-a 命令看到的网关 MAC 与正确的网关 MAC 地址不同，可以肯定这个虚假的网关 MAC 就是攻击主机的 MAC。使用嗅探软件抓包发现的大量以网关 IP 地址发送的 ARP 响应包，包中所指定的 MAC 地址就是攻击主机的 MAC 地址；对于电子邮件欺骗，可以查看完整的电子邮件头。头信息中的 Received 或 Message-ID 等域信息都很有用，大多数邮件系统允许用户查看信息从源地址到目的地址经过的所有主机，这不仅指出了是否有人欺骗了电子邮件，而且指出了这个信息的来源。有时，电子邮件用户不允许查看头信息，可检查包含原始信息的 ASCII 文件，因为头信息可能是假冒的；对于 DNS 欺骗，攻击者不能替换缓存中已经存在的记录，并且 DNS 欺骗的有效时间是与缓存中记录的 TTL 相关的，一旦超过缓存有效时间，除非重新构造缓存记录，否则 DNS 欺骗自动失效；对于 Web 欺骗，有两种方法可以找出正在发生的 URL 重定向，其一是配置网络浏览器使它总能显示当前的 URL，其二是检查源代码。

（二）拒绝服务攻击与取证方法

DoS 攻击通常是利用传输协议的漏洞、系统存在的派漏洞、服务的漏洞，对目标系统发起大规模的进攻，用超出目标处理能力的海量数据包消耗可用系统资源、带宽资源等或造成程序缓冲区溢出错误，致使其无法处理合法用户的正常请求，无法提供正常服务，最终致使网络服务瘫痪，甚至引起系统死机。这是破坏项攻击目标正常运行的一种“损人不利己”的攻击手段。最常见的 DoS 攻击行为有网络带宽攻击和连通性攻击。

在使用入侵检测系统对这类攻击进行监测时，除了注意检测 DoS 工具的特征字符串、默认端口、默认口令等信息外，还应该着眼于观察分析 DoS 攻击发生时网络通信的普遍特征。根据 DoS 攻击导致的网络通信异常现象在入侵检测系统中建立相应规则，能够更早地检测出 DoS 攻击。

（三）缓冲区溢出攻击与取证方法

缓冲区溢出攻击的目的在于扰乱工作在某些特权状态下的程序，使攻击者取得程序的控制权，借

[1] 韩琦，翁腾飞，葛继科，等. 网络安全技术课程中的思政教育融入方法 [J]. 办公自动化，2021，26（1）：13-14.

机提高自己的权限，控制整个主机。一般来说，攻击者要实现缓冲区溢出攻击，必须完成两个任务，一是在程序的地址空间里安排适当的代码；二是通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。

当程序的执行流程已经被重定向到攻击者的恶意代码时，这时仍然可以采取一定的措施阻止攻击代码的执行。通过设置被攻击程序的数据段地址空间的属性为不可执行，使得攻击者不可能执行植入被攻击程序缓冲区的代码，从而避免攻击，这种技术被称为非执行的缓冲区技术。事实上，很多老的 UNIX 系统都是这样设计的，设置缓冲区最初的目的就是用来存放数据而不是可执行代码，但是近来的 UNIX 和 Windows 系统为了便捷地实现更好的性能和功能，往往允许在数据段中放入可执行代码，所以为了保证程序的兼容性，人们不可能使得所有程序的数据段不可执行，不过，可以设定堆栈数据段不可执行，因为几乎没有任何程序会在堆栈中存放代码，这样就可以最大限度地保证程序的兼容性。

（四）Web 攻击与取证方法

OWASP 调查发现，对 Web 应用危害较大的安全问题主要有：未验证参数、访问控制缺陷、账户及会话管理缺陷、跨站脚本漏洞、缓冲区溢出、命令注入漏洞、错误处理问题、远程管理漏洞、Web 服务器及应用服务器配置不当等问题。

分析前台网站服务器的配置文件，找到网站服务文件所在的目录（Document Root）和全部代码。通过分析网站服务器文件的配置，找出网站数据库类型、IP 地址以及数据库的访向用户名、密码等，导出数据库中的所有数据。利用仿真的方式或者使用提取的网站代码和数据库构建模拟网站服务器，注意需要设置同样的主机名、数据库连接关系等。使用同样的方式导出后台管理服务器的代码和数据库中的所有数据，并搭建后台仿真或模拟网站[1]。通过登录前台界面，模拟用户操作行为，确定与之相关联的网站程序和模块。通过登录后台管理界面，确定并分析后台管理数据。综合分析网站数据，查清网站结构、人员组织架构、涉案资金流转等情况。

（五）木马攻击与取证方法

从本质上说，木马程序基本都是客户端与服务端的组合形式。一般情况下，网络攻击者使用木马程序进行网络攻击的过程为：将木马植入到目标计算机系统后，通过一定的方式将自己很好地隐藏起来，自动运行程序才能不被用户轻易发现，最后，木马可以完成一些攻击者想要实现的功能。

如果怀疑一个系统被植入了木马，我们的第一要务应该是检查该系统确定是否真的被植入了木马。扫描端口是检测木马的常用方法，大部分的木马服务端会在系统中监听某个端口，因此通过查看系统上开启了哪些端口能有效地发现远程控制木马的踪迹；[2]还可以通过检查系统进程的方式，虽然现在也有一些技术使木马进程不显示在进程管理器中，不过绝大多数的木马在运行期都会在系统中生成进程。因此，检查进程列表是一种非常有效的发现木马踪迹的方法；检查 ini 文件、注册表和服务，为使木马自动运行，大部分的木马都会把自己登记在开机启动的程序当中，这样才能在计算机开机后自动加载。也有少数木马采用文件绑定的方式，将木马与特定的可执行文件进行绑定，木马随着这个文件的运行而自动运行；监视网络通信，一些特殊的木马程序使用 ICMP 协议通信，被控端不需要打开任何监听端口，也无须反向连接，更不会有什么已经建立的固定连接，这使得 netstat 或 fport 等工具很难发挥作用。对付这种木马，除了检查可疑进程之外，还可以通过嗅探器软件（也称 sniffer 软件）监视网络通信来发现可疑情况。

五、结语

网络技术的发展给社会带来便利的同时，也带来了巨大的安全威胁，世界各国对网络安全的重视程度也日益提升，受俄乌战争的影响，网络攻击成为现代社会的热点问题，加强对网络攻击

---

［1］吕江鸿．网络涉枪犯罪的法律规制研究［D］．西安：西北大学，2015.

［2］刘录敬．浅析网络黑客的攻击手段及防范措施［C］//Proceedings of 2010 Asia-Pacific Conference on Information Network and Digital Content Security（2010APCID）．Scientific Research Publishing，2010：225-230.

行为的分析，提高网络安全是当前的重中之重。目前网络在社会各个领域中的应用越来越广泛，电子商务、移动通信、移动支付、网上银行、智能家居等，针对网络的攻击越来越频繁，具有传播速度快、影响范围广、造成损失巨大特征的恶意攻击不断出现，因此加强对网络攻击的取证研究，获取其攻击行为，提前了解可能会发生的入侵攻击具有重要的意义。本文针对目前常见的网络攻击行为的特点进行了描述，并根据其特点进行了取证方法的总结，对于网络攻击案件的侦破与取证具有重要意义，对于减少网络攻击事件发生、提高网络安全性具有重要价值。

（责任编辑：汪　川）

Research on Electronic Data Forensics Method for Network Attack

Li Yang[1]　Xia Meng[2]

1. Railway Police College, Zhengzhou;
2. Zhongnan University of Economics and Law, Wuhan

Abstract: In recent years, the high incidence of network attacks has seriously endangered China's information network security, and network attacks are developing towards automation and intelligence. The speed of vulnerability discovery and utilization is faster and faster, the firewall penetration is higher and higher, the security threat asymmetry is increased, and the damage to the network infrastructure is greater and greater, which poses a great threat to the security of cyberspace. When network attackers implement network attacks, they often use various technical means to hide themselves against tracking, which brings great challenges to the detection of network attack cases. This paper summarizes the characteristics of common network attacks, analyzes the characteristics of common network attacks and the electronic data generated, and analyzes different network attacks, and puts forward corresponding network forensics methods. It is of great significance and value for the investigation and evidence collection of network attack cases.

Key words: Network attack; Electronic data; Forensic methods; Analysis and research