Linux操作系统下应急响应流程与步骤 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022_Linux_E6_93_8D_E4_BD_c103_145032.htm 进入21世纪的信息时代以来，随着计算机网络技术的进步，给人们的生活带来很大的便利。然而在人们越来越依赖网络的同时，网络安全形势日趋严峻，大规模互联网攻击事件频繁发生。如2000年Yahoo等网站遭到大规模拒绝服务攻击，2001年爆发了红色代码等蠕虫事件，2002年全球的根域名服务器遭到大规模拒绝服务攻击，2003年又爆发了SQL Slammer等蠕虫事件，其间还频繁发生着网页篡改和黑客竞赛等安全事件。与此同时，我国的广大互联网使用者还只是刚刚充分享受到互联网的乐趣，网民的整体安全意识薄弱，技术水平很低，加上国家在网络安全方面的法律法规不健全，与互联网攻击相应的法律法规的制定明显滞后。另外在组织体系以及协调机制方面都存在很多不和谐不规范的地方，为此加强国内的网络安全建设是一件紧急迫切的任务。 在常见的安全保障模型中，有一个很著名的PDR模型，其中“ P ”是protection（防护），“ D ”是detection（检测），“ R ”是 response（响应），安全保障的主要操作环节被分为防护、检测、响应这几个主要部分。其中应急响应是安全保障工作中一个非常重要的环节。由于在防护和检测环节，通常比较成熟的应用都是针对已知特征来识别的，因此应急响应可以弥补前面各环节的不足的必要部分：在攻击和防御的对抗中，攻击方通常掌握着主动性和主观能动性，而防御方只有应急响应这个环节可能具备能够和攻击方相抗衡的智能。 我们先来介绍一下应急响应的基本

概念和基本内容。英文中紧急响应有两种表示法，即Emergency Response和Incident Response，其含义是指安全技术人员在遇到突发事件后所采取的措施和行动。而突发事件则是指影响一个系统正常工作的情况。这里的系统包括主机范畴内的问题，也包括网络范畴内的问题，例如黑客入侵、信息窃取、拒绝服务攻击、网络流量异常等。一般来讲，在攻击开始以后，如果能够做到在系统被攻克之前发现攻击并进行有效的应对处理，使得攻击不能奏效或被化解，则可以说实现了安全。可见，是否能够做到及时发现和快速响应是实现安全的关键。 在现实生活中应急响应这个环节往往没有得到用户真正的重视。用户总是觉得已经投入了很多购置了全套的设备，不能理解为什么还要不断地支出一笔似乎看不到回报的费用。可是实际上现实经验越来越证明，缺少了高质量的应急响应，整个安全保障环节就好比一个上了大锁的监视系统但是却没有配备保卫人员的住所，攻击者总是可以想办法进入住所的。 应急响应通常需要达到的目标首先是要确认或排除突发事件的发生。在实际的工作中，用户大量的报警被发现是“ 虚惊一场 ”。用户可能把各种由于其他原因导致的异常现象都归咎于受到某种攻击所带来的结果。在一个案例中，有一个用户甚至用绝对肯定的口气说，他能够感觉到有人在他的计算机没有任何接口连入网络的情况下，被别人通过电源线实施了监控。从网管的角度来看，经常会面临各种流量异常的情况，其中有时候只是网络中用户应用情况的反映，而有时候确是网络中正在发生某种大量的攻击行为造成的。 应急响应的第一项任务就是要尽快恢复系统或网络的正常运转。在有些情况下，用户最关心的是多长时间能

恢复正常，因为系统或网络的中断是带来损失的主要方面。这时候应急工作的一个首要任务就是尽快使一切能够相对正常地运行。 应急响应的第二项任务就是要使系统和网络操作所遭受的破坏最小化。通过收集积累准确的数据资料，获取和管理有关证据。在应急的过程中注意记录和保留有关的原始数据资料，为下一阶段的分析和处理提供准确可信的资料。 最后应急响应要提供准确的分析统计报告和有价值的建议。在响应工作结束时提交的分析。 应急响应的主要阶段 我国在应急响应方面的起步较晚，按照国外有关材料的总结，通常把应急响应分成几个阶段的工作，即准备、事件检测、抑制、根除、恢复、报告等阶段。 