电子商务应对黑客攻击的八大技术动态电子商务师考试 PDF 转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_645147.htm 电子商务和电子政务迅猛发展，黑客攻击的频率和强度有增无减。今天我们所面临的网络威胁，早已不仅仅是早期出现的那些攻击手段，如病毒、木马、间谍软件与网络监听、口令攻击、漏洞攻击等。黑客攻击技术近年来的最新动态是什么？ 硬件安全 利用硬件的黑客技术虽然报道不多，但它的的确确出现了：在BIOS芯片中植入病毒木马，让目前的防火墙、防毒软件都失效. 针对主机板上的电磁辐射进行信息获取的技术……仅仅使用软件非法侵入的方式可能已经落伍，新时期的黑客技术应包括破解硬件本身。前几年微软公司曾经对硬件黑客侵犯其Xbox设备的行为采取法律与技术措施。索尼公司的PS2游戏机也成为一些专门修改芯片的黑客目标，其核心技术Sony的记忆棒被破解。美国苹果公司新推出的iPhone 3Gs的加密系统也被硬件黑客破解，造成磁盘文件数据可以被实时偷走。 逆向工程 逆向工程是指对软件执行码直接进行分析，可被看做是“ 开发周期的逆行 ”。实际应用中逆向工程主要分成两种情况：第一种，软件的源代码可用，但描述文档不再适用或者丢失；第二种，软件没有可用的源代码，任何能找到它的源代码的努力都被称为逆向工程。软件的逆向工程实现方法有：通过观察信息交换进行分析、使用反汇编器进行反汇编和使用反编译器进行反编译等。黑客则利用反逆向工程的方法保护自己的恶意代码。 社会工程学 社会工程学定位在计算机信息安全工作链的一个最脆弱的环节，即“ 人 ”这个环节上。“

人”这个环节在整个信息安全体系中是非常重要的，这一点信息安全的脆弱性是普遍存在的，它不会因为系统平台、软件、网络或者是设备的新旧等因素不相同而有所差异。无论是在物理上，还是在虚拟的信息系统上，任何一个可以访问系统某个部分的人都有可能构成潜在的安全风险与威胁。任何细微的信息都可能会被黑客用做“补给资料”来运用，使其得到其他的信息。 0day 在计算机领域中，0day通常是指没有公布补丁的漏洞，或者是还没有被漏洞发现者公布出来的漏洞利用工具。一般，带有0day名字的黑客软件指的是软件公布时对应的漏洞还没有打补丁。0day漏洞的利用程序对于网络安全具有巨大威胁，因此0day不但是黑客的最爱，掌握多少0day也成为评价黑客技术水平的一个重要参数。 Rootkit Rootkit已被大多数的防毒软件归类为具危害性的恶意软件。Rootkit是攻击者用来隐藏自己的踪迹和保留root访问权限的工具。通常，攻击者通过远程攻击获得root访问权限，或者首先采用密码猜测或者密码强制破译的方式获得系统的访问权限，进入系统后，再通过某些安全漏洞获得系统的root权限。攻击者会在侵入的主机中安装rootkit，并经常通过rootkit的后门来检查系统是否有其他的用户登录，如果只有攻击者登录，攻击者就开始着手清理日志中的有关信息。攻击者通过rootkit的嗅探器获得其他系统的用户和密码之后，就会利用这些信息侵入其他的系统。 痕迹销毁与反取证 计算机取证将犯罪者留在计算机中的“痕迹”作为证据提供给法庭。可以用做计算机取证的信息源很多，如系统日志、防火墙与入侵检测系统的工作记录、反病毒软件日志、系统审计记录、网络监控流量、电子邮件、操作系统文件、数据库文件和操

作记录、硬盘交换分区、软件设置参数和文件、完成特定功能的脚本文件、Web浏览器数据缓冲、书签、历史记录或会话日志、实时聊天记录等。随着计算机取证技术的发展和取证工具的广泛使用，黑客在入侵过程中越来越多地使用痕迹销毁技术和反取证技术，以对抗调查人员的取证分析。因此，取证与反取证往往形成矛与盾的关系，成为黑客攻击技术与反黑客技术较量的技术制高点之一。 利用虚拟机实施攻击近些年更多的攻击者倾向于在虚拟机环境中进行攻击，这是由于虚拟机可模拟多种系统平台，造成了攻击主机系统与位置的隐蔽性。黑客可通过快速卸载或简单删除等方式来逃避一般的搜查追踪。当前各黑客网站都有虚拟机安装和使用的详细教学资料，并且认为虚拟机相关知识是黑客重要的基本知识之一。因此，今后一旦发生类似于“ 熊猫烧香 ”事件时，黑客完全可能改用虚拟机作案，然后立即关闭虚拟机系统并删除该虚拟机文件夹。调查人员必须首先发现该机器上的虚拟机痕迹，再从中寻找黑客制造病毒并进行传播的证据，这项工作往往变得异常复杂，需要特殊的技术和工具。 无线入侵 无线通信包括手机、卫星电视、无线局域网、无线传感网络、红外、蓝牙、RFID等，它们在人们的日常工作生活中扮演着越来越重要的角色。无线通信在给人们带来很大便利的同时，也带来了很多安全隐患：一方面，针对无线通信的窃听和恶意代码能获取用户的通信内容、侵犯用户的隐私权.另一方面，入侵者可以通过这些无线通信技术，进一步接入网络的核心部分。无线通信极大扩展了网络的边界，使得网络接入的控制变得复杂起来，黑客通过无线入侵往往能起到事半功倍的效果。 无锡石中剑国际网络高峰论坛将召开 为了

遏制日益扩张的黑客经济产业链的恶性发展，推动我国网络高手与国际同行的直接交流，由民间发起、无锡高科技园区支持的（无锡）石中剑国际网络高峰论坛将于今年11月6～8日在江苏无锡召开。会议为期三天，将有国内外特邀高手的精彩演讲与讨论、专题分组研讨和比赛交流等各种形式的活动。本次活动的国外特邀嘉宾很多都是经常出入黑帽大会的常客，下面先简要做一些介绍： Jayson E. Street，2006年度《时代周刊》提名人物，，现任美国顶级安全学院（SANS学院）顾问； Joe McCray，在美国几所知名大学任教，同时开设自己的安全培训班； Iftach Ian Amit，原来在Finjan安全公司工作，从事研究和项目开发十几年，对全球IT地下产业犯罪有专门的深入研究. Jordan Wiens，DEFCON黑客大会夺旗比赛冠军； 来自英国的Adam Laurie，无线技术牛人，使用一部诺基亚手机、一台笔记本电脑，仅用12分钟就破解了英国的新身份证； Mohammad Hluchan，语言天才，可以说八种语言、写五种语言，关注网络恐怖和极端势力研究。 巴西黑客Rodrigo Branco，可以搞高难度的负载均衡攻防； Steve Topletz，严肃的律师、优雅的艺术家，同时具有黑客的身份。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com