

安全知识当今最流行网络攻击六大趋势 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/454/2021_2022__E5_AE_89_E5_85_A8_E7_9F_A5_E8_c98_454829.htm 在最近几年里，网络攻击技术和攻击工具有了新的发展趋势，使借助Internet运行业务的机构面临着前所未有的风险，本文将对网络攻击的新动向进行分析，使读者能够认识、评估，并减小这些风险。

趋势一：自动化程度和攻击速度提高 攻击工具的自动化水平不断提高。自动攻击一般涉及四个阶段，在每个阶段都出现了新变化。扫描可能的受害者。自1997年起，广泛的扫描变见惯。目前，扫描工具利用更先进的扫描模式来改善扫描效果和提高扫描速度。损害脆弱的系统。以前，安全漏洞只在广泛的扫描完成后才被加以利用。而现在攻击工具利用这些安全漏洞作为扫描活动的一部分，从而加快了攻击的传播速度。传播攻击。在2000年之前，攻击工具需要人来发动新一轮攻击。目前，攻击工具可以自己发动新一轮攻击。像红色代码和尼姆达这类工具能够自我传播，在不到18个小时内就达到全球饱和点。攻击工具的协调管理。随着分布式攻击工具的出现，攻击者可以管理和协调分布在许多Internet系统上的大量已部署的攻击工具。目前，分布式攻击工具能够更有效地发动拒绝服务攻击，扫描潜在的受害者，危害存在安全隐患的系统。

趋势二：攻击工具越来越复杂 攻击工具开发者正在利用更先进的技术武装攻击工具。与以前相比，攻击工具的特征更难发现，更难利用特征进行检测。攻击工具具有三个特点：反侦破，攻击者采用隐蔽攻击工具特性的技术，这使安全专家分析新攻击工具和了解新攻击行为所花费的时

间增多.动态行为，早期的攻击工具是以单一确定的顺序执行攻击步骤，今天的自动攻击工具可以根据随机选择、预先定义的决策路径或通过入侵者直接管理，来变化它们的模式和行为.攻击工具的成熟性，与早期的攻击工具不同，目前攻击工具可以通过升级或更换工具的一部分迅速变化，发动迅速变化的攻击，且在每一次攻击中会出现多种不同形态的攻击工具。此外，攻击工具越来越普遍地被开发为可在多种操作系统平台上执行。许多常见攻击工具使用IRC或HTTP(超文本传输协议)等协议，从入侵者那里向受攻击的计算机发送数据或命令，使得人们将攻击特性与正常、合法的网络传输流区别开变得越来越困难。趋势三：发现安全漏洞越来越快 新发现的安全漏洞每年都要增加一倍，管理人员不断用最新的补丁修补这些漏洞，而且每年都会发现安全漏洞的新类型。入侵者经常能够在厂商修补这些漏洞前发现攻击目标。趋势四：越来越高的防火墙渗透率 防火墙是人们用来防范入侵者的主要保护措施。但是越来越多的攻击技术可以绕过防火墙，例如，IPP(Internet打印协议)和WebDAV(基于Web的分布式创作与翻译)都可以被攻击者利用来绕过防火墙。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