Windows安全性饱受质疑Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Windows_E5_AE_89_c100_644083.htm 网络时代，尽管外有杀毒厂商的日日监测预警，电脑自身也不乏安全软件的实时防护，但是我们反而更加地寝食难安，因为层出不穷地攻击事件意味着黑客们总能找到可攻克的大门 究竟是谁将我们的电脑暴露给了黑客？过去，我们是对操作系统又爱又恨，现在答案或许有了新解。 5月29日，美国总统奥巴马在公布的网络安全评估报告中指出，来自网络空间的威胁已成为美国面临的最严重的经济和军事威胁之一。此前，奥巴马在竞选期间曾一直强调网络安全对美国的重要性，在其就职不久，便要求对美国的网络安全状况展开为期60天的全面评估，以检查联邦政府部门保护机密信息和数据的措施。作为全球科技发展的前沿国家，奥巴马将网络安全提上政府议程之举再次表明全球网络安全形势已经极为严峻。 来自Sophos的《2009安全威胁报告》显示，每隔4.5秒就会有一个网页遭病毒感染。 据了解，一次成功的黑客攻击基本包含搜索、扫描、获得权限、保持连接、消除痕迹五个步骤。前期的搜索过程将是耗时最长的阶段，通过各种途径完成攻击的准备阶段，之后对攻击目标周边和内部网络设备进行扫描，如开放的端口、开放的应用服务、含操作系统在内的应用漏洞、保护性较差的数据传输等寻找潜在漏洞，以完成最终的攻击。 从上述攻击路径来看，应用服务、操作系统在内的应用都成为用户端面临的最主要的攻击途径。 此前，微软于4月8日发布的最新安全研究报告（该报告每半年发布一次）指出，2004年到2007年间，绝大

部分漏洞是来自于应用软件，并呈快速上升趋势（从88%增至94%），言外之意影响互联网安全的主要是来自应用软件，而非操作系统。 安全厂商很无奈 事实上，安全厂商也一直在积极做出技术和产品的改进，可面对新的网络环境，他们的努力却没有阻止安全问题的愈演愈烈之势。国家计算机网络应急技术处理协调中心监测，2008年接收到的网络安全事件报告中，拒绝服务攻击事件、垃圾邮件事件和病毒、蠕虫或木马问题尤为突出，与2007年相比，涨幅分别为165%、54.5%和20.6%。 对此，全球网络安全设备厂商美国飞塔（Fortinet）公司总裁谢青告诉《IT时代周刊》，早期的互联网安全是属于链接方面的安全，防火墙只是为防止黑客连接到公司内部。他指出，过去五到十年间，网络安全最大的威胁来自于病毒，来自于入侵检测或垃圾邮件等不良信息，而这些都是链接类防火墙挡不住的。此类防火墙只是为防止外面的链接，但传染的病毒和垃圾都是从用户周围的人传入。网络攻击方式的飞速变化让整个网络安全产业都在思考，“八年前，我们就在努力将网络安全防护往更上层发展，走向内容和应用层次。”谢青如是说。 但是，分析人士指出，包括Cisco、Juniper这些知名厂商在内，若将网络安全往更高层做，最需要解决的技术问题是如何将防火墙的处理速度尽量接近网络的速度，同时将功能尽量集中在同一个产品上，使用户及其管理更为方便。据悉，一般做链接式防火墙，大概需5～10倍的数据处理量。而如果将安全做到更高层，做到内容，做到防病毒，做到垃圾邮件等，实际上所处理的数据量，要比处理链接式防火墙的要求更高，一般需要20倍～50倍的处理能力，才能赶上路由器和交换机的处理速度。 不过，

从整个网络安全市场来看，统一威胁管理（UTM）正在快速取代防火墙，仅2008年全球UTM的销量就已经超过了防火墙。他认为，相比国外很多互联网应用较为广泛、比较先进的国家，中国市场其实还相对滞后，特别是防火墙市场比UTM市场还大许多。据悉，UTM较之防火墙的优势，就是它可以将病毒去掉，可以将入侵者去掉。“ 不能100%隔离，但对各类应用软件的防护至少可以做到60%以上。 ”谢青坦言。 操作系统非罪魁祸首 谈及操作系统的安全性，微软的Windows操作系统可谓饱受质疑。 2008年10月24日微软系统爆出的年度最大安全漏洞 (Microsoft 安全公告 MS08-067)让人记忆犹新。该问题涉及Windows2000/XP /Vista等桌面操作系统的绝大多数版本。借此漏洞，黑客可发动大规模远程攻击，实际效果可与“ 冲击波 ”、“ 震荡波 ”等病毒类似。微软当即也紧急发布了安全更新。据了解，因此漏洞存在于操作系统的远程过程调用模块（RPC），如用户的电脑收到了特制的RPC请求，则攻击者可绕过系统认证远程运行任意代码，很可能造成大规模蠕虫攻击。 百考试题获悉：依照微软的每月补丁周期（通常在每月第二周周二发布安全补丁）来看，今年3月份至5月份的安全公告数分别为3个、8个、1个，按照微软安全漏洞四级标准划分，严重级别的过半。 微软在“ 尽自己所能在安全方面做出努力 ”，也及时地发布安全漏洞公告和补丁，但绝大多数电脑用户对这位桌面霸主的举动并不领情，“ 出了任何事情第一反应就是微软系统不安全 ”一位媒体同行如是说。甚至连安全厂商卡巴斯基实验室创始人尤金卡巴斯基都如此断言：目前的电脑操作系统整体设计含有不安全的因素，使得恶意软件侵入操作系统变得非常容易。“ 其实

微软也是受害者。”微软大中华区战略安全架构师裔云天感慨地说。分析人士指出，其实每个软件都有漏洞，有些是要在使用过程中才能被发现，故有“补丁”一说。而操作系统因其使用人群范围广泛，即便不提开发时潜在的漏洞，黑客为攻击计算机也会不停寻找系统漏洞，以期乘虚而入。微软报告也表明，从2004年开始到2007年，操作系统的安全漏洞正在逐年下降，从12%降至6%。裔云天告诉《IT时代周刊》，“如果网络攻击是针对某款软件本身漏洞的，那么防火墙和杀毒软件都是无效的”，在他看来“其实防火墙和杀毒软件只能抵御一般攻击”，因为很多软件是特定的应用，防火墙并不能判别针对特定应用的攻击是采用哪一种。频频出现的安全厂商“误杀误报”事件恰巧也印证了微软的这个说法。既然防火墙和安全软件都不完全“靠谱”，操作系统也非罪魁祸首，黑客是从哪里乘虚而入的呢？“祸起”第三方软件 一份来自IBM安全组织的报告指出，前5大IT厂商，包括微软、IBM、思科、Oracle和Apple，总共的系统漏洞只占了所有漏洞的14%，而其他中小厂商出品的应用软件则占了86%。应用软件的安全性着实堪忧！“因为第三方软件在开发过程中只考虑功能本身，并没有把安全考虑进去，所以漏洞百出。”裔云天直言不讳。他指出，之所以漏洞百出还有客观的外在因素，中国很多中小型软件开发商，本身生存就非常困难，也很难将自己的开发人员输出进行安全培训，且国内也很少有开发方面的安全培训。事实也确如此，对大多数软件厂商而言，最大目的就是完成所开发软件的功能，其开发人员也没有安全方面的培训，即只是开发软件功能，而不是开发一个安全的软件。比如ERP财务软件，设计之初，鲜有开

发者会考虑到，当输入一个字串时，它是不是要检查是否有效，如百分比等等，因为黑客会对这个进行攻击；还有对输入长度进行检查，许多开发者并不会考虑这点，所以当他调用时就会产生安全隐患，但他并不知情。 前文微软报告还显示，在基于浏览器漏洞的攻击中，使用中文简体版本浏览器的用户位列被攻击对象的第二位，占25.6%；从2008年下半年开始，每月被Live Search检测到的挂马网页数量超过一百万，.CN 域名网站中有超过1%的网站被挂马。且冒牌安全软件呈现爆发趋势。所谓冒牌安全软件，是指在木马病毒盛行的情况下，用户会自主搜索一些免费的“ 安全软件 ”，而此时搜索引擎所列厂商很多都是伪装的安全厂商，自称安装后不会再有病毒侵入，以免费三个月等期限为诱饵，实际他们本身就是木马，欺骗用户安装。 鉴于互联网安全趋势正从操作系统转向应用软件，为在软件开发过程中确保其安全性和可靠性，微软耗费近7年时间建立起一套安全方法论“ 软件安全开发生命周期(SDL) ”。从安全教育、安全设计、到安全响应，在软件开发的每一个阶段都严把安全关，有效地降低安全漏洞和隐私问题的数量，以及残留漏洞的严重性。微软所开发的所有软件都必须经过这一方法论的监测，如果安全状况达不到标准，无论功能多么完备都不会被发布。据悉，SDL流程还将被用于帮助我国政府、合作伙伴、软件开发商改进第三方软件，最终建立端到端安全可信的互联网环境。 一方面系统提供商在为安全积极改进，同时，微软也认为，用户也要增强自我保护的习惯和知识，坚持使用正版软件，开启操作系统自动更新，便于他们第一时间发现问题自动帮助用户修复。 100Test 下载频道开通，各类考试题目直接下载。详