防范非法入侵的技术措施 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/62/2021_2022__E9_98_B2_E8_8C_83_E9_9D_9E_E6_c40_62213.htm 防范非法入侵的技术措施 防范黑客的技术措施根据所选用的硬软件产品的不同，可以分为七类：即网络安全检测设备、访问设备、测览器/服务器软件、证书、商业软件，防火墙和安全工具包/软件。1. 网络安全检测设备预防为主是防范黑客的基本指导思想。网络安全检测设备主要用来对访问者进行监督控制，一旦发现有异常情况，马上采取应对措施，防止非法入侵者进一步攻击。2. 访问设备访问设备方法是通过给访问者提供智能卡，通过智能卡的信息来控制用户使用。非法入侵者如想入侵就必须防止类似的访问设备，这增加了非法入侵者的入侵难度。3. 防火墙 防火墙是目前保证网络安全的必备的安全软件，它通过对访问者进行过滤，可以使系统限定什么人在什么条件下可以进人自己网络系统。非法入侵时，就必须采用IP地址欺骗技术才能进人系统，但增加了入侵的难度。4. 安全工具包安全工具包主要是提供一些信息加密和保证系统安全的软件开发系统。用户可以在这些安全工具包的基础上进行二次开发，开发自己的安全系统。如RSA的BSAFE是“ 最畅销的通用密码工具包 ”。BSAFE支持RSA、DES、Triple DES、RC2、RC4和其他密码技术。Terisa的系统也提供一种比较高级的客户机和服务器工具包。该工具包可使开发商实现安全的通信系统集成，如SSL和SHTTP等。对黑客的防护是一项系统性的长期工作。要真正保护系统的安全，防止非法入侵者、加强系统的监控和使用必要的安全系统是非常关键的。

要完全杜绝黑客的入侵，从技术上是很难完全解决的，但可以增加"黑客"非法入侵的难度。因此，解决黑客问题还需要全社会关注，建立完善的监控体系和严厉的法律惩罚体系，才是解决问题的出路。