

2006指导安全专家惊曝NAC方案漏洞 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/61/2021_2022_2006_E6_8C_87_E5_AF_BC_c40_61824.htm 在今年于美国拉斯维加斯召开的Black Hat会议上，来自Insightix的安全专家Ofir Arkin等认为现阶段的NAC解决方案存在漏洞，可让黑客轻易绕过NAC的保护，进入企业网络，进行攻击。而思科一位高层则表示对于厂商来说，任何产品都需要一个很长的过程才可能完善，才可能提供全面的安全解决方案。Ofir认为来自于如思科、微软、赛门铁克等公司提出的现阶段NAC解决方案都不同程度地存在漏洞。比如说，靠DHCP代理服务器利用对IP地址分配的过程强制执行安全策略的NAC解决方案，无法对配置静态IP地址的计算机进行控制。而像思科那种利用交换机实现NAC解决方案的做法，由于需要思科交换机来支持，如果企业混合使用不同厂家的路由交换设备的，黑客可以找到不能被NAC管理的交换机，利用MAC地址的欺骗手段，冒充已经经过认证的计算机，在网络里进行攻击。另外，对于不支持802.1x协议的设备来说，也不能实现良好的控制。另一位安全专家Marc Maiffrete说，有报道说一些反病毒软件产品存在安全漏洞，这样黑客可以利用反病毒软件、Web或者其他程序的漏洞，让被感染的系统看上去已经被打满了补丁、更新了病毒库，从而对网络造成安全危害。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