学术前沿：无线网络安全性的研究 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/467/2021_2022__E5_AD_A6_E6_9C_AF_E5_89_8D_E6_c67_467977.htm 一、无线网络常见的攻击和弱点 无线网络可能受到的攻击分为两类，一类是关于网络访问控制、数据机密性保护和数据完整性保护进行的攻击。这类攻击在有线环境下也会发生；另一类则是由无线介质本身的特性决定的，基于无线通信网络设计、部署和维护的独特方式而进行的攻击。 1 WEP中存在的弱点 IEEE（Institute ofElectrical and Electronics Engineers，电气与电子工程师学会）制定的802.11标准最早是在1999年发布的，它描述了WLAN（Wireless Local Area Network，无线局域网）和WMAN（Wireless Metropolitan Area Network，无线城域网）的MAC（Medium Access Control，介质访问控制）和物理层的规范。为了防止出现无线网络用户偶然窃听的情况和提供与有线网络中功能等效的安全措施，IEEE引入了WEP（Wired Equivalent Privacy，有线等价保密）算法。和许多新技术一样，最初设计的WEP被人们发现了许多严重的弱点。专家们利用已经发现的弱点，攻破了WEP声称具有的所有安全控制功能。总的来说，WEP存在如下弱点： 1）整体设计：在无线环境中，不使用保密措施是具有很大风险的，但WEP协议只是802.11设备实现的一个可选项。 2） 加密算法：WEP中的IV（Initialization Vector，初始化向量）由于位数太短和初始化复位设计，容易出现重用现象，从而被人破解密钥。而对用于进行流加密的RC4算法，在其头256个字节数据中的密钥存在弱点，目前还没有任何一种实现方案修正了

这个缺陷。此外用于对明文进行完整性校验的CRC（Cyclic Redundancv Check，循环冗余校验）只能确保数据正确传输，并不能保证其未被修改，冈而并不是安全的 校验码。 3）密钥管理：802.11标准指出， WEP使用的密钥需要接受一个外部密钥管理系统的控制。通过外部控制。可以减少Iv的冲突数量，使得无线网络难以攻破。但问题在于这个过程形式非常复杂，并且需要手工操作。因而很多网络的部署者更倾向于使用缺省的WEP密钥，这使黑客为破解密钥所作的工作量大大减少了。另一些高级的解决方案需要使用额外资源，如RADIUS和Cisco的LEAP，其花费是很昂贵的。 4）用户行为：许多用户都不会改变缺省的配置选项，这令黑客很容易推断出或猜出密钥。 2 执行搜索 NetStumbler 是第一个被广泛用来发现无线网络的软件。据统计，有超过50%的无线网络是不使用加密功能的。通常即使加密功能处于活动状态，AP（wireless Access Point，无线基站）广播信息中仍然包括许多可以用来推断出WEP密钥的明文信息，如网络名称、SSID（Secure Set Identife ，安全集标识符）等。 3 窃听、截取和监听 窃听是指偷听流经网络的计算机通信的电子形式。它是以被动和无法觉察的方式人侵检测设备的。即使网络不对外广播网络信息，只要能够发现任何明文信息，攻击者仍然可以使用一些网络工具，如Eth real 和TCPDump来监听和分析通信量，从而识别出可以破坏的信息。使用虚拟专用网、SSL（Secure Sockets Lave 安全套接字层）和SSH（Secure Shel1）有助于防止无线拦截。 4 欺骗和非授权访问 因为TCP，IP（Transmission Control Protocol，Internet Protocol，传输控制协议，网际协议）的设计原因，几乎无法防止MAC／IP地址

欺骗。只有通过静态定义MAC地址表才能防止这种类型的攻击。但是，因为巨大的管理负担，这种方案很少被采用。只有通过智能事件记录和监控日志才可以对付已经出现过的欺骗。当试图连接到网络上的时候，简单地通过让另外一个节点重新向AP提交身份验证请求就可以很容易地欺骗无线网身份验证。许多无线设备提供商允许终端用户通过使用设备附带的配置工具，重新定义网卡的 MAC地址。使用外部双因子身份验证，如RADIUS或SecurID，可以防止非授权用户访问无线网及其连接的资源，并且在实现的时候，应该对需要经过强验证才能访问资源的访问进行严格的限制。 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