六、web与无线渗透

（三）无线网络攻击

1. 无线网络安全性简介

无线组网是当今市场上最流行、发展最快的技术之一。从家庭网络到企业级的无线网络，人们都在急切地利用无线组网带来自由和便利。虽然无线组网很方便，但它的部署并不总是安全的。不安全的无线网络不仅在家庭组网中出现，就是在一些大型企业中也屡见不鲜。正是由于存在这个不安全部署的问题，人们才会请渗透测试人员找出无线网络中存在的漏洞。

新的无线标准 802.11n：在当今各种无线局域网技术交织的战国时代，WLAN、蓝牙、HomeRF、UWB 等竞相绽放，但 IEEE802.11 系列的 WLAN 是应用最广泛的。自从 1997 年 IEEE802.11 标准实施以来，先后有 802.11b、802.11a、802.11g、802.11e、802.11f、802.11h、802.11i、802.11j 等标准制定或者酝酿，

在传输速率方面，802.11n 可以将 WLAN 的传输速率由目前 802.11a 及 802.11g 提供的 54Mbps 提高到 108Mbps，甚至高达 500Mbps。

六、web与无线渗透

（三）无线网络攻击

1. 无线网络安全性简介

尽管无线网络在建立组网通信方便提供了极大的便利性，并提供了用户的可移动能力，但它却面临着比较大的安全风险。恶意黑客能够很轻易地检测到无线网络并获取对网络的访问。尽管已经采取了几种方法来增强无线网络的安全性，但绝大多数措施都很不足，可以很容易地被破解。因此，作为企业来说，应该将无线网络与单位中的关键网络相隔离，并且仅仅将无线网络用于非敏感信息的传输，如互联网访问。

每个无线网络都有一个识别名称，称为无线网络名称（Network Name）或服务设置标识符（Service Set Identifier，SSID）。所有无线路由器或无线访问点，都有自身的无线网络名称，而且所有无线网络的客户端，都必须提供与之对应的无线网络名称，方能成功建立连接。

在 IEEE 建立无线 802.11 标准时，并没有忘记安全问题。它提出的安全标准是有线等效协议（Wired Equivalent Privacy，WEP），顾名思义，它试图提供与有线网络相同级别的安全保护。WEP 在客户端和访问点之间使用了相同的共享密钥，这个共享密钥由 RC4 算法使用，来加密客户端和访问点之间的所有流量。

六、web与无线渗透

（三）无线网络攻击

1. 无线网络安全性简介

我们对 WEP 的安全性缺陷做一番总结：静态 WEP 密钥可靠性、可管理性不佳；应答式验证机制容易被攻击者监听；RC4 加密技术存在大量可被攻击者利用的漏洞；ICV 检验算法容易被破解修改。利用这些缺陷，有经验的入侵者甚至可以在 15 分钟内就完成入侵过程，早在 2001 年，AT&T 的两名员工和一名莱斯大学的普通学生仅仅使用市面上出售的无线客户端设备就成功破解了 WEP 加密机制，该体系脆弱的安全性可见一斑。

对无线网络访问点的寻找非常简单：

在开放网络中，AP 广播其管理信标来公告其 SSID，以及建立关联的其他参数，如所支持的速度、信号强度等，通常每 100 毫秒广播一次。客户端侦听这些信标，之后，客户端在想建立关联时，它就发出关联请求。AP 使用关联响应进行应答，其过程如图 11-5 所示。

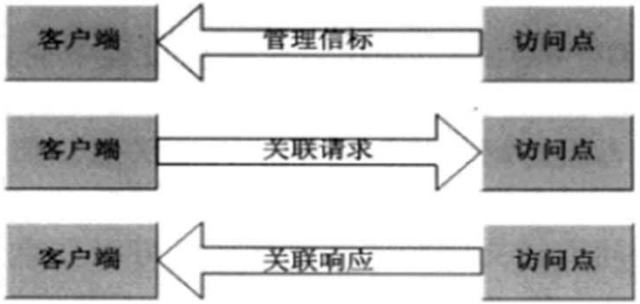

图 11-5　802.11 协议开放网络关联

六、web与无线渗透

（三）无线网络攻击

2. 无线网络渗透攻击-密码破解 Fern Wifi Cracker

python编写的一款无线网络破解测试工具，提供了GUI界面，操作方便

使用步骤：
steup 1： select interface　#选择网卡
steup 2： click to scan for all ...　#扫
steup 3： click to wep or wpa ...　#选
steup 4： 选择要破解的网络
steup 5 : attack　#开始破解 wpa wpa2

六、web与无线渗透

（三）无线网络攻击

3. 无线网络渗透攻击-信息劫持

因为无线AP相当于用户手机与互联网的桥梁，它处于中间位置，所以可以自由的实施中间人攻击，获取用户信息、密码。

实验任务：利用SET辅助完成DNS劫持，然后克隆一个网站，将用户访问该网站的请求转向攻击平台。

步骤：

- 安装dhcp3-server，配置/etc/default/dhcp3-server ->at0
- 配置set中ettercap的选项 路径 interface=at0
- ⑩ 配置dns欺骗的域名/usr/local/share/dsniff/dnsspoof.hosts www.discuz.net
- 启动set，选择 8 Wireless Access Point Attack Vector，创建linksys访问点
- 手机连接linksys，访问www.discuz.net，看是否被解析到10.0.0.1

- 在set中返回到2 Website Attack Vectors -》3 Credential Harvester Attack Method-》创建克隆站点用来欺骗真实的网站（修改网站的跳转信息）
- 再次用手机访问www.discuz.net，观察是否能获取到用户输入的帐号和密码
- echo "1" > /proc/sys/net/ipv4/ip_forward（开启访问外部网络）

六、web与无线渗透

（三）无线网络攻击

3. 无线网络渗透攻击-信息劫持

因为无线AP相当于用户手机与互联网的桥梁，它处于中间位置，所以可以自由的实施中间人攻击，获取用户信息、密码。

实验任务：利用SET辅助完成DNS劫持，然后克隆一个网站，将用户访问该网站的请求转向攻击平台。

步骤：

- 上述攻击过程还可以使用ettercap或者网络嗅探工具进行，不需要执行set攻击
- 将需要用户进行登录的代码放入/var/www下，启动apache
- 开启wireshark进行抓包即可