主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

本期规划

- 7　介绍无线网络基础知识
- 8　破解 WEP 加密方式
- 9　 实战演练 1
- 10 穿插其他知识
- 11 破解 WPA 加密方法
- 12 穿插其他知识
- 13 实战演练 2
- 14 抓包分析
- 15 拓展与总结

本周主题

- 无线基础知识扫盲
- 常用无线网络设备
- WEP/WPA 基础
- 实验环境搭建

无线基础知识扫盲

- 狭义无线网络
- 广义无线网络
- 常见术语
- 无线安全与 Hacking 技术的发展

狭义无线网络

标准	备注
802.11	1997年，原始标准（2Mbit/s，2.4GHz频道）
802.11a	1999年，物理层补充（54Mbit/s，5GHz频道）
802.11b	1999年，物理层补充（11Mbit/s，2.4GHz频道）
802.11c	符合802.1D的媒体接入控制层（MAC）桥接（MAC Layer Bridging）
802.11d	根据各国无线电规定做的调整
802.11e	对服务等级（Quality of Service，QoS）的支持
802.11f	基站的互连性（Interoperability）
802.11g	物理层补充（54Mbit/s，2.4GHz频道）
802.11h	无线覆盖半径的调整，室内（indoor）和室外（outdoor）通道（5GHz频段）
802.11i	安全和鉴权（Authentification）方面的补充
802.11n	导入多重输入输出（MIMO）和40Mbit通道宽度（HT40）技术，基本上是802.11a/g的延伸版

广义无线网络

- WPAN
- WLAN
- WWAN

	WPAN	WLAN	WWAN
Standards	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Speed	< 3 Mbps	1-540 Mbps	10-384 Kbps
Range	Short	Medium	Long
Applications	Peer-to-Peer device to device	Home, small business and enterprise networks	PDAs, mobile phones, cellular access

常见术语

- SSID
- WAP
- AP
- WEP
- WPA
- WiFi-Mesh

无线安全与 Hacking 技术的发展

常见无线设备

- 无线路由器
- 无线网卡 / 无线上网卡
- 走近天线（全向 / 定向天线）

WEP/WPA 基础

- WEP 简介
- WPA 简介

搭建实验环境

- 介绍无线网卡
- 介绍操作系统
- 搭建方案

无线网卡

芯片类型	品牌	型号	接口类型	支持频率	备注
Atheros	TP-LINK	TL-WN510G TL-WN610G	PCMCIA	802.11b/g	重点推荐，在 Windows 及 Linux 下十分稳定
PrismGT	Linksys	WUSB54G	USB	802.11b/g	带延长线，笔者最早购买的一款，效果还不错
Broadcom	Linksys	WPC54G	PCMCIA	802.11b/g	在 Windows 下工作稳定
Ralink	ASUS	WL-167G	USB	802.11b/g	在注入攻击时效率不高，个别时候会出现卡死情况
Ralink	IPTime	IP-G200U（新版型号为 G054U-A）	USB	802.11b/g	带延长线，注入攻击时间稍长，但效果不错，很稳定，重点推荐
Ralink	WiFiCity	IDU-2850UG（俗称：卡王）	USB	802.11b/g	在注入攻击时效率一般，但能够获取到远距离 AP 信号，适合探测
Ralink	G-Sky	GS-27USB（俗称：卡皇）	USB	802.11b/g	在注入攻击时效率一般，但能够获取到远距离 AP 信号，适合探测

关于大功率无线网卡

操作系统

- 本期教学使用 Kali linux
- 当然还有其他各种“小众”的系统
- 本期教学使用的软件： Aircrack-ng 套件

环境搭建

- VM 虚拟机 + 外接 usb 网卡
- U盘的Kail linux Live CD

下期预告

- 了解 WEP 加密方法，并破解

Thank you