从新手到高手

黑客入门与网络安全实用手册
安全技术全新升级

黑客攻防与无线安全

从新手到高手（超值版）

网络安全技术联盟 编著

一线网络安全技术联盟倾心打造
海量王牌资源超值赠送

- 超值赠送1 同步微视频
- 超值赠送2 精美教学PPT课件
- 超值赠送3 CDlinux系统文件包
- 超值赠送4 Kali虚拟机镜像文件
- 超值赠送5 无线密码的字典文件
- 超值赠送6 黑客工具（107个）速查电子书
- 超值赠送7 常用黑客命令（160个）速查电子书
- 超值赠送8 180页常见故障维修电子书
- 超值赠送9 Windows 10系统使用和防护技巧电子书
- 超值赠送10 8大经典密码破解工具电子书
- 超值赠送11 加密与解密技术快速入门小白电子书
- 超值赠送12 网站入侵与黑客脚本编程电子书
- 超值赠送13 黑客命令全方位详解电子书

清华大学出版社

从新手到高手

黑客攻防与无线安全

从新手到高手（超值版）

网络安全技术联盟 编著

清华大学出版社
北京

内容简介

本书在剖析用户进行黑客防御中迫切需要用到或迫切想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的无线攻击。全书共分为14章，包括：无线网络快速入门、无线网络攻防必备知识、搭建无线测试系统Kali Linux、熟悉无线网络安全测试平台——Kali Linux系统的基本操作、组建无线安全网络、数据帧的结构与加密原理、无线网络的安全分析工具、无线路由器的密码安全策略、无线网络中的虚拟AP技术、从无线网络渗透内网、扫描无线网络中的主机、无线网络中主机漏洞的安全防护、加固无线网络的大门、无线局域网的安全防护等内容。

本书内容丰富，图文并茂，深入浅出，同时本书还赠送超多资源，包括本书同步微视频、精美教学PPT课件、CDlinux系统文件包、Kali虚拟机镜像文件、无线密码的字典文件以及8本电子书，帮助读者掌握无线安全方方面面的知识。由于赠送资源比较多，本书前言部分对资源包的内容会做详细说明。本书不仅适合网络安全从业人员及网络管理员，而且适合广大网络爱好者，也可作为大、中专院校相关专业的参考书。

图书在版编目(CIP)数据

黑客攻防与无线安全从新手到高手：超值版 / 网络安全技术联盟编著. —北京：清华大学出版社，2019
（从新手到高手）
ISBN 978-7-302-52767-1

Ⅰ①黑… Ⅱ. ①网… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2019）第071021号

责任编辑：张　敏
封面设计：杨玉兰
责任校对：胡伟民
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，　http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**19.75　　**字　　数：**495千字
版　　次：2019年9月第1版　　**印　　次：**2019年9月第1次印刷
定　　价：69.80元

产品编号：074935-01

Preface

前 言

目前，无线网络安全问题日益突出。“工欲善其事必先利其器”，只有选择合适的攻防工具，才能起到事半功倍的作用。本书除了讲解有线端的攻防策略外，还把目前市场上流行的无线攻防等热点融入书中。

本书特色

知识丰富全面：涵盖了所有黑客攻防知识点，由浅入深地介绍黑客攻防方面的技能。

图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式便于读者在学习中直观、清晰地看到操作的过程以及效果，从而能更快地理解和掌握。

案例丰富：把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧，贴心周到：本书对读者在学习过程中可能遇到的疑难问题以“提示”的形式进行说明，以免读者在学习过程中走弯路。

本书赠送资源

- 同步微视频。
- 精美教学PPT课件。
- CDlinux系统文件包。
- Kali虚拟机镜像文件。
- 无线密码的字典文件。
- 黑客工具（107个）速查电子书。
- 常用黑客命令（160个）速查电子书。
- 180页常见故障维修电子书。
- Windows 10系统使用和防护技巧电子书。
- 8大经典密码破解工具电子书。
- 加密与解密技术快速入门小白电子书。
- 网站入侵与黑客脚本编程电子书。
- 黑客命令全方位详解电子书。

读者可扫描右方二维码获取本书赠送资源。

精美教学PPT课件

电子书

CDlinux系统文件包

Kali虚拟机镜像文件

无线密码的字典文件

读者对象

本书不仅适合网络安全从业人员及网络管理员，而且适合广大网络爱好者，也可作为大、中专院校相关专业的参考书。

写作团队

本书由长期研究网络安全的网络安全技术联盟编著，另外还有王秀英、王英英、刘玉萍、刘尧、王朵朵、王攀登、王婷婷、张芳、李小威、王猛、王维维、李佳康、王秀荣、王天护、皮素芹等人参与了编写工作。在编写过程中，编者们尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可通过电子邮件zhangmin2@tup.tsinghua.edu.cn与我们联系。

编　者

Contents
目 录

第1章　无线网络快速入门

无线网络，特别是无线局域网给我们的生活带来了极大的方便，为我们提供了无处不在的、高带宽的网络服务，但是，由于无线信道特有的性质，使得无线网络连接具有不稳定性，且容易受到黑客的攻击，从而大大影响了服务质量，本章介绍一些有关无线网络的基础常识。

1.1　什么是无线网络

无线网络（Wireless network）是采用无线通信技术实现的网络，与有线网络的用途十分类似，最大的不同在于传输媒介的不同，一般来说，无线网络可以分为狭义无线网络和广义无线网络两种。

1.1.1　狭义无线网络

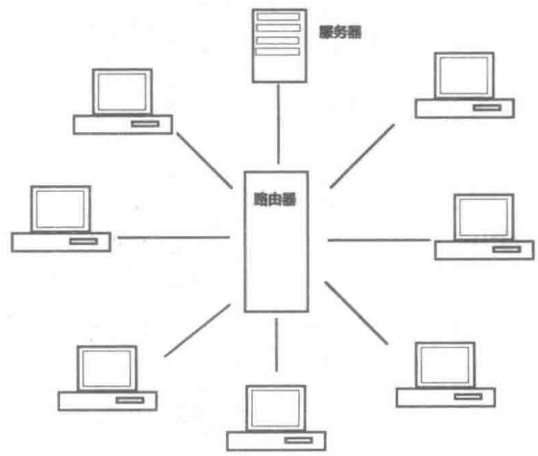
狭义无线网络就是我们常说的无线局域网，是基于802.11b/g/n标准的WLAN无线局域网，具有可移动性、安装简单、高灵活性和高扩展能力等特点，作为对传统有线网络的延伸，这种无线网络在许多特殊环境中得到了广泛地应用，如企业内部、学校内部、家庭等。这种网络的缺点是覆盖范围小，使用距离在5~30m内。

随着无线数据网络解决方案的不断推出，全球WiFi设备迅猛增长，相信在不久的将来，“不论在任何时间、任何地点都可以轻松上网”这一目标就会被实现，下面介绍一些有关无线网络的概念

1. 无线网络的起源

无线网络的起源，可以追溯到第二次世界大战期间，当时美军采用无线电信号作资料的传输，他们研发出了一套无线电传输技术，并且采用相当高强度的加密技术。当时美军和盟军都广泛使用这项技术。

无线电传输技术让许多学者得到了灵感，在1971年时，夏威夷大学（University of Hawaii）的研究员创造了第一个基于封包式技术的无线电通信网络，被称作ALOHNET网络，这可以算是相当早期的无线局域网络（WLAN）了。最早的WLAN包括了7台计算机，它们采用双向星型拓扑（bi-directional star topology），横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛（Oahu Island）上，从那时开始，无线网络可说是正式诞生了。下图为一个星型拓扑结构示意图。



2. IEEE 802.11标准

IEEE 802.11标准第一个版本发表于1997年，其中定义了介质访问接入控制层（MAC层）和物理层。物理层定义了工作在2.4GHz的ISM频段上的两种无线调频方式和一种红外传输的方式，总数据传输速

率设计为2Mb/s。两个设备之间的通信可以以自由直接（ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

对于无线网络重要发展标准，用户有必要了解一下IEEE 802.11标准的发展过程，具体内容见下表。

表　802.11标准的发展史

标　准	说　明
IEEE 802.11	1997年，原始标准（2Mb/s，工作在2.4GHz）
IEEE 802.11a	1999年，物理层补充（54Mb/s，工作在5GHz）
IEEE 802.11b	1999年，物理层补充（11Mb/s工作在2.4GHz）
IEEE 802.11c	符合802.1D的媒体接入控制层桥接（MAC Layer Bridging）
IEEE 802.11d	根据各国无线电规定做的调整
IEEE 802.11e	对服务等级（Quality of Service,QoS）的支持
IEEE 802.11f	基站的互连性（IAPP,Inter-Access Point Protocol），2006年2月被IEEE批准撤销
IEEE 802.11g	2003年，物理层补充（54Mb/s，工作在2.4GHz）
IEEE 802.11h	2004年，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz频段）
IEEE 802.11i	2004年，无线网络的安全方面的补充
IEEE 802.11n	2009年9月通过正式标准，WLAN的传输速率由802.11a及802.11g提供的54Mb/s、108Mb/s，提高至350Mb/s甚至高达475Mb/s
IEEE 802.11p	2010年，这个协定主要用在车用电子的无线通信上

目前，无线网络及设备主要使用的是IEEE 802.llb/g/n标准，尤其以IEEE 802.llg最为普及，不过IEEE 802.lln正在以飞快的速度赶超。

除了上面的IEEE标准，另外有一个被称为IEEE 802.11b+的技术，通过PBCC技术（packet binary convolutional code）在IEEE 802.11b（2.4GHz频段）基础上提供22Mb/s的数据传输速率。但这事实上并不是一个IEEE的公开标准，而是一项产权私有的技术。

3. WiFi联盟

WiFi联盟成立于1999年，是一家全球及非营利性的行业协会，拥有几百家企业会员，致力解决符合IEEE 802.11标准的产品的生产和设备兼容性问题，从而推动无线局域网产业的发展，以增强移动无线、便携、移动和家用设备的用户体验为目标。自2003年3月WiFi联盟开展此项认证以来，已经有超过4000多种产品获得了WiFi GERTIFIED指定认证标志，有力地推动了WiFi产品和服务在消费者市场和企业市场两方面的全面开展。

WiFi联盟认证标志就是无线技术支持的象征，被广泛应用在智能手机、平板计算机、笔记本计算机和各种便携式设备上。

4. 无线网络的组成

无线网络由以下几个部分组成。

（1）站点（Station）。网络最基本的组成部分，通常指的就是无线客户端。

（2）基本服务单元（Basic Service Set，BSS）。网络最基本的服务单元。最简单的服务单元可以只由两个无线客户端组成，客户端可以动态地连接（Associate）到基本

服务单元中。

（3）分配系统（Distribution System，DS）。分配系统用于连接不同的基本服务单元，分配系统使用的媒介逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，例如同一个无线频道。

（4）接入点（Access Point，AP）。无线接入点既有普通有线接入点的能力，又有接入到上一层网络的能力。其实AP和无线路由器是有区别的，相比来说，无线路由器的功能更多，不过在基本功能方面，两者并无实质性的区别，所以在实际应用中，都会将无线路由器称为AP。

（5）扩展服务单元（Extended Service Set，ESS）。由分配系统和基本服务单元组合而成。这种组合是逻辑上的，并非物理上的，不同的基本服务单元有可能在地理位置上相差甚远。分配系统也可以使用各种各样的技术。

（6）关口（Portal）。用于将无线局域网和有线局域网或其他网络联系起来，是一个逻辑成分。

以上组成部分使用了3种媒介，站点使用的无线媒介，分配系统使用的媒介，以及和无线局域网集成一起的其他局域网使用的媒介，物理上它们可能相互重叠。IEEE 802.11只负责在站点使用的无线媒介上寻找地址，分配系统和其他局域网的寻址不属于无线局域网的范围。

5. 无线网络的运行原理

要想建立一个有效运行的无线网络，首先需要至少一个AP，如无线路由器，然后是至少一个无线客户端，即装有无线网卡的便携式设备，如计算机、手机、平板计算机等。硬件准备完成后，AP每100ms将SSID信号封包广播一次，无线客户端可以借此决定是否要和这一个SSID的AP连接，使用者还可以设定要连接到哪一个SSID。这就好比用户使用智能手机连接周边的WiFi一样，可以有选择地进行连接。不过，WiFi系统总是对客户端开放其连接标准，并支持漫游，这是WiFi的优点。

1.1.2　广义无线网络

广义无线网络主要包含3个方面，分别是WPAN、WLAN和WWAN，下面分别进行介绍

1. WPAN

WPAN（Wireless Personal Area Network，无线个人局域网通信技术）即常说的无线个人局域网。无线个人局域网（WPAN）是一种采用无线连接的个人局域网。它被用在诸如电话、计算机、附属设备以及小范围（个人局域网的工作范围一般是在10m以内）内的数字助理设备之间的通信。

无线个人局域网（WPAN）是一种与无线广域网（WWAN）、无线局域网（WLAN）并列但覆盖范围相对较小的无线网络。在网络构成上，WPAN位于整个网络链的末端，用于实现同一地点终端与终端间的连接，如连接手机和蓝牙耳机等，WPAN设备具有价格便宜、体积小、易操作和功耗低等优点。

支持无线个人局域网的技术包括：蓝牙、ZigBee、超频波段（UWB）、IrDA、HomeRF等，其中蓝牙技术在无线个人局域网中使用最广泛，下面就来介绍几种主要的技术。

- 蓝牙（Bluetooth）：蓝牙是一种短距离无线通信技术，它可以用于在较小的范围内通过无线连接的方式实现固定设备或移动设备之间的网络互联，从而在各种数字设备之间实现灵活、安全、低动耗、低成本的语音和数据通信。

蓝牙技术的一般有效通信范围为10m，

强的可以达到100m左右，其最高速率可达1Mb/s。其传输使用的功耗很低，广泛应用于无线设备，如平板计算机、手机、智能电话等领域。下图为一个智能手机的蓝牙设置界面，在其中可以开启与关闭蓝牙。

- IrDA（红外）：IrDA是红外数据组织（Infrared Data Association）的简称，目前广泛采用的IrDA红外连接技术就是由该组织提出的，到目前为止，全球采用IrDA技术的设备超过了5000万部。

IrDA技术的主要特点有：利用红外传输数据，无须专门申请特定频段的使用执照；设备体积小、功率低；由于采用点到点的连接方式，数据传输受到的干扰较小，数据传输速率高，可达lGb/s。但存在一定的技术缺陷，如受视距影响其传输距离短、要求通信设备的位置固定、其点对点的传输连接无法灵活地组成网络等。

2. WLAN

WLAN（Wireless Local Area Networks，无线局域网）即上面所说的“狭义无线网络”，具体请参考上面狭义无线网络的内容。

3. WWAN

WWAN（Wireless Wide Area Network，无线广域网通信技术）即常说的无线广域网。WWAN技术是使得笔记本计算机或者其他的设备装置在蜂窝网络覆盖范围内可以在任何地方连接到互联网。目前全球的无线广域网络主要采用GSM及CDMA技术，其他还有3G或者4G等技术。

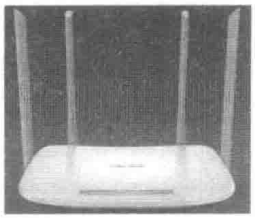
简单地说，WWAN指的就是通过通信设备和通信网络来上网，不管是以前的GSM、EDGE和CDMA，还是现在的3G、4G网络，只要用计算机中的PC卡装SIM卡，或者把手机连在笔记本计算机上当作Modem连网，都叫WWAN。

1.2 认识无线路由器

无线路由器是应用于用户上网、带有无线覆盖功能的路由器，它和有线路由器的作用是一样的，唯一的不同就是无线路由器的顶部或者尾部多了一个或者几个天线，其作用就是提供无线网络的支持。除此以外，其他无论是外观，或者是内在配置页面都和同款型的有线路由器一模一样。

市面上每一个厂商的无线产品都有自己的特点，下图为美版思科Linksys WRT1900AC双频无线路由器，该路由器具有4个天线，支持用户根据需要对天线进行拆卸和换装，非常方便。另外，该路由器支持802.11b/g协议，其特点是使用多个无线来分工进行无线数据的接收与发送。

目前，市场占有率比较高的无线路由器是TP-LINK，其性价比比较高。下图为TP-LINK千兆无线路由器，具有高速双核、覆盖更远、家长控制、一键禁用等功能。



为方便大家选购无线路由器，下面把目前市面上常见的无线设备厂商列举出来，包括厂商名称、官方网站以及个人建议等信息见下表。

表　常见无线路由器

厂商名称	官方网站	个人建议
Linksys（领势）	www.linksys.com/cn/	价格昂贵，性能好
D-LINK（友讯）	www.dlink.com.cn	性价比不错，性能稳定
TP-LINK（普联）	www.tp-link.com.cn	性价比较高，市场占有率较高
Netgear（网件）	www.netgear.com.cn	价格比较贵，性能不错
ASUS（华硕）	www.asus.com.cn	不太稳定，价格适中
Tenda（腾达）	www.tenda.com.cn	性价比较高，性能稳定
MERCURY（水星）	www.mercurycom.com.cn	价格较高，性能比较稳定

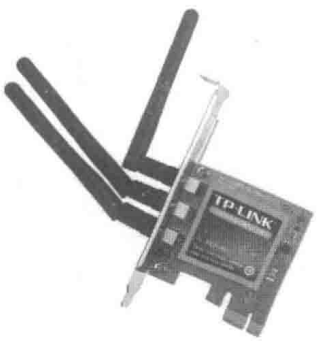
1.3　了解无线网卡

对于初次接触无线网络的用户来说，无线网卡与无线上网卡是有些迷惑的，本节就来介绍什么是无线网卡，什么是无线上网卡。

1.3.1　无线网卡

无线网卡是终端无线网络设备，是不通过有线连接，采用无线信号进行数据传输的终端，有时也被称为WiFi卡，根据接口类型的不同，主要有PCMCIA无线网卡、PCI无线网卡、Mini-PCI无线网卡、USB无线网卡、CF/SD无线网卡几类。

PCI无线网卡：主要用于台式计算机中，下图为TP-LINK出品的PCI无线网卡。



PCMCIA无线网卡：主要用于笔记本计算机中，下图为Linksys出品的PCMCIA无线网卡。

USB无线网卡：这种网卡不管是台式机用户还是笔记本用户，只要安装了驱动程序，都可以使用，下图为LB-LINK出品的USB无线网卡。