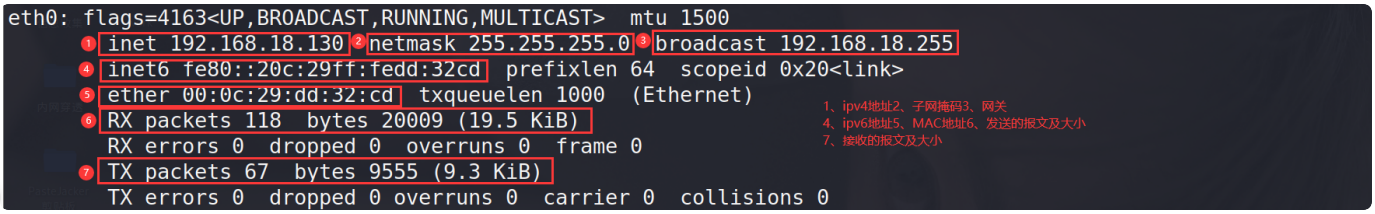
三、分析和管理网络

Linux黑客基础-18-分析和管理网络-01-网络信息查看和IP地址临时更改

Analyzing Networks with ifconfig （使用ifconfig查看和分析网络（状态））



eth0---第一块有线网卡

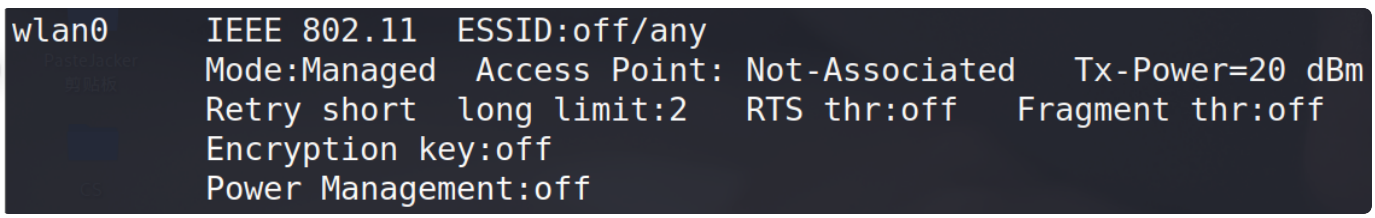
wlan0---第一块无线网卡

ifconfig -a（查看所有的接口）包括活动的和不活动的

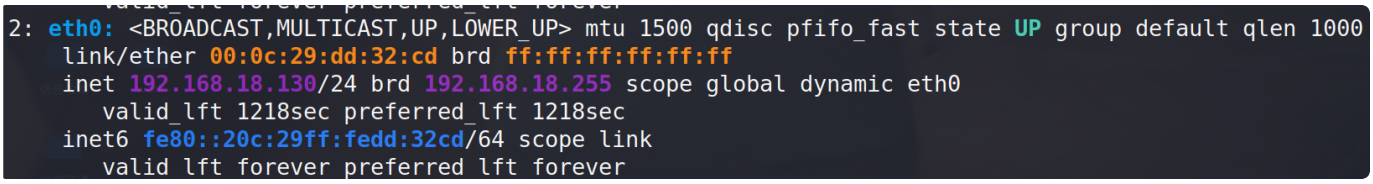
ifconfig eth0 down （停用eth0这块网卡）

ifconfig eth0 up （启用eth0这块网卡）

Checking Wireless Network Devices with iwconfig （使用iwconfig检测无线网卡）



ip address show(查看ip地址)



Changing Your IP Address 修改你的IP地址

1、临时更改

ifconfig eth0 192.168.18.131 //使用的是默认子网掩码

场景：排错、调试网络的时候

ifconfig eth0 10.1.1.1 netmask 255.0.0.0 broadcast 10.1.1.255 //指定ip地址的时候指定子网掩码及网关

Linux黑客基础–19–在Kali中连接无线网络

1、先在笔记本中使用这个无线网卡连接wifi

2、在虚拟机中添加USB控制器，连接到虚拟机中

3、查看网络接口

ifconfig –a 查看所有接口

4、如果无线网卡没有up使用ifconfig wlan0 up 启用这个无线网卡

5、使用iwconfig收集无线网卡的信息

wlan0 IEEE 802.11 ESSID:off/any

Mode:Managed Access Point: Not–Associated Tx–Power=20 dBm

Retry short long limit:2 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

连接之后

wlan0　　IEEE 802.11 ESSID:"QICHEBOLI"

Mode:Managed Frequency:2.457 GHz Access Point: D4:B7:09:96:33:72

Bit Rate=1 Mb/s　Tx-Power=30 dBm

Retry short long limit:2　RTS thr:off　Fragment thr:off

Encryption key:off

Power Management:off

Link Quality=37/70 Signal level=-73 dBm

Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0

Tx excessive retries:0 Invalid misc:32　Missed beacon:0

PS：

（1） IEEE 802.11 无线网络的标准

802.11　a/b/g/n

支持2，4GHZ和5GHZ，理论带宽最高600Mbps

（2）ESSID wifi的标识

（3） Access Point（AP：无线接入点）: D4:B7:09:96:33:72

（4）Mode:Managed 无线网卡的模式

Managed---客户端模式，连接wifi通常使用的模式

在破解无线密码时，我们需要使用到混杂模式(promiscuous mode)。在这种模式下网卡处于嗅探状态（被称为Passive状态，被动状态）

6、连接指定的wifi

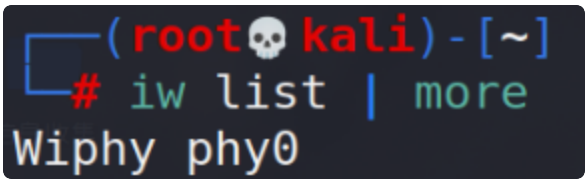
通过图形化的网络连接管理界面（简单推荐）

前提：NetworkManager服务要开启（服务名称区分大小写）

systemctl status NetworkManager　服务是开机自启动的

2、在kali中查看无线网卡是否可以用于无线攻击

iw–list　查看无线网卡支持的模式



Supported interface modes:

* IBSS

* managed

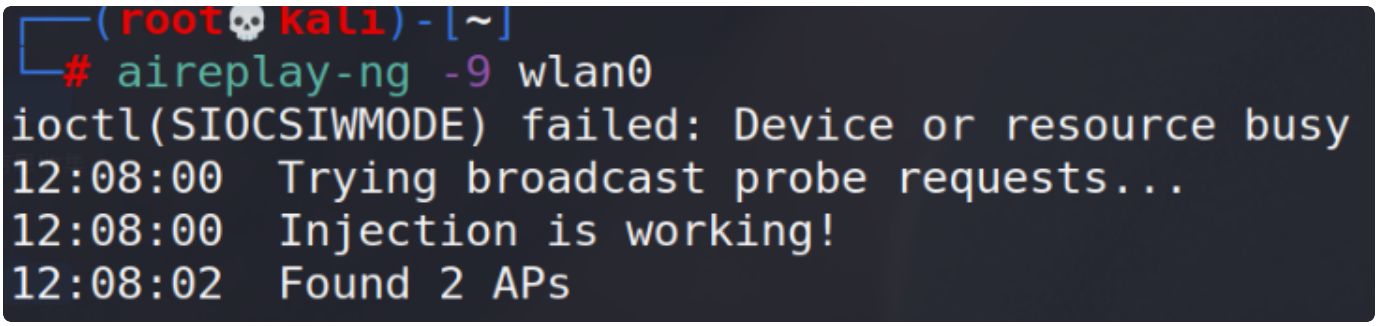
* AP（有）

* AP/VLAN

* monitor（有）

* mesh point

aireplay–ng –9 wlan0　查看是否支持数据包的注入功能



ioctl(SIOCSIWMODE) failed: Device or resource busy

12:08:00 Trying broadcast probe requests...

12:08:00 Injection is working!　（支持）

12:08:02 Found 2 APs

Linux黑客基础-20-分析和管理网络-02-更改MAC地址

MAC地址欺骗

MAC地址（物理地址）是全球唯一的，48位，16进制表示

00:12:0e:e5:f9:75

（防范角度）通常被用作一种安全措施，以防止黑客进入网络——或追踪他们

（攻击角度）更改你的MAC地址来伪装成一个不同的MAC地址使得上述安全措施无效和显得微不足道

这是一项非常有用的绕过网络访问控制技术。

ncpa.cpl--网络连接

arp协议--把IP地址解析成MAC地址

arp -a 查看arp缓存

arp -d删除arp缓存

arp -d 192.168.1.146 删除指定条目

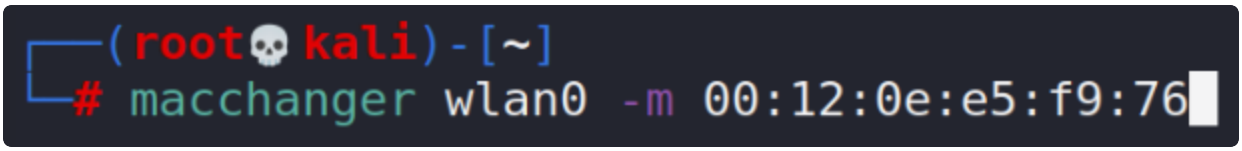
ifconfig wlan0 hw ether 00:12:0e:e5:f9:76 修改MAC地址

```
┌──(root💀kali)-[~]
└─# ifconfig wlan0 hw ether 00:12:0e:e5:f9:76
```

macchanger -s wlan0 查看MAC地址

```
┌──(root💀kali)-[~]
└─# macchanger -s wlan0
Current MAC:   00:12:0e:e5:f9:75 (AboCom)
Permanent MAC: 00:12:0e:e5:f9:75 (AboCom)
```

macchanger wlan0 –m 00:12:0e:e5:f9:76　修改MAC地址



Linux黑客基础–21–分析和管理网络–03–DHCP客户端工具–dhclient

DHCP协议–– 动态主机配置协议

Server：UDP/67

　　Linux下DHCP的服务进程（daemon，在后台运行）进程––dhcpd

Client：UDP/68

DHCP 服务器为子网上的所有机器分配 IP 地址，并在随时维护将 IP地址分配给哪台机器的日志文件。这使得它成为取证分析人员在攻击后追踪黑客的绝佳资源。出于这个原因，了解 DHCP 服务器的工作原理对一名黑客很有用。

Linux下DHCP客户端调试工具––dhclient

–r　释放（release）正在使用的IP地址

dhclient wlan0　获取新的地址

Linux黑客基础–22–分析和管理网络–04–配置网络地址

网络参数的配置

IP地址/掩码　ifconfig eth0　或　ip a

网关（默认–default 路由）ip route show　（ip r）

DNS（nameserver ，名称服务器） cat /etc/resolv.conf

192.168.X.Y

（1）手工方式

方法1：图形化的网络管理器

依赖的服务：NetworkManager

Wired 有线

Wireless 无线

192.168.195.102/24

192.168.195.2

223.6.6.6

更改之后

把启用连网（复选框）取消再选中

方法2：修改网卡的配置文件（掌握）

Centos（/etc/sysconfig/network-scripts/ifcfg-**）

/etc/network/interfaces

Step01: 把NetworkManager服务关闭并设置为开机不启动

systemctl stop NetworkManager //关闭

systemctl disable NetworkManager //禁用

systemctl status NetworkManager //状态

Step02: 编辑/etc/network/interfaces

PS：推荐man interfaces

auto eth0 //启动时激活网卡

iface eth0 inet static //接口为eth0,地址指派方式为静态（static，手工方式）

//dhcp

address 192.168.195.76/24 //IP地址

gateway 192.168.195.2 //网关

Step03 重启networking服务

systemctl restart networking

14.2 DNS的修改 Changing Your DNS Server

/etc/resolv.conf

修改方法1 vi直接编辑

search qwfy.cn　//搜索域

nameserver 8.8.8.8　//DNS服务器

nameserver

nameserver

修改方法2****

echo "nameserver 223.6.6.6" >/etc/resolv.conf

修改方法3

sed –i 's/nameserver 223.6.6.6/nameserver 8.8.8.8/' /etc/resolv.conf

sed 是非交互式的文本编辑器

–i　对原始文件内容进行修改

's/old/new/'　查找替换，把old替换成new

Linux黑客基础–23–分析和管理网络–05–使用dig工具获取DNS信息

Manipulating the Domain Name System–––维护DNS

黑客可以使用DNS从目标处收集信息

1）包含目标名称服务器（将目标名称转换成 IP 地址的服务器）的 IP地址（A记录）

2）目标邮件服务器（MX记录）

3）潜在的所有子域名和 IP 地址

（1）Examining DNS with dig

1）dig hackers-arise.com ns

2）dig hackers-arise.com mx

向系统默认的DNS服务器查询

3）dig hackers-arise.com mx @223.6.6.6

向指定的DNS服务器223.6.6.6查询

4）dig qq.com any @223.6.6.6

向指定DNS服务器查询qq.com域中任意记录类型

5） dig +noall +answer mail.163.com any

6）dig +noall +answer -x 220.181.14.161

-x 反向查询

（2）nslookup

nslookup qq.com -type=any 8.8.8.8

向指定DNS服务器查询qq.com域中任意记录类型

apt install dsniff

15.2. Mapping Your Own IP Addresses

映射你的IP地址

Linux :/etc/hosts

Windows: C:\Windows\System32\drivers\etc\hosts

作用：完成主机名到IP地址的映射

解析的优先级会比DNS要高

1）屏蔽一些不良网站

2）加快上网访问的速度

3）防止DNS劫持（DNS欺骗）

格式：

一行代表一条记录

IP地址　主机名1　主机名2　……

利用dnsspoof劫持用户的流量