Kali：

以太网卡为eth0，

ip地址为192.168.1.102，

MAC地址为00:0c:29:6e:98:a6

靶机windows：

Ip：192.168.1.18

构造arp：

op: 值为1代表arp请求，值为2代表arp响应

hwsrc：发送方mac

psrc：发送方ip

hwdst：目标mac

pdst：目标ip

pkt = Ether(src=[1.102的MAC], dst=[1.18的Mac]) / ARP(1.102的MAC, 网关IP地址, hwdst=1.18MAC, pdst=1.18IP地址, op=2)

pkt = Ether( src = kali攻击机mac , dst = 靶机的mac ) / ARP( )

发送数据包：

Scapy是一个强大的交互式数据包处理程序（使用python编写）。它能够伪造或者解码大量的网络协议数据包，能够发送、捕捉、匹配请求和回复包等等。它可以很容易地处理一些典型操作，比如端口扫描，tracerouting，探测，单元 测试，攻击或网络发现

用scapy的send和sendp：

send()作用于第三层(从下往上数)网络层，所以我们可以用它来send(IP()/TCP())，但是不能send(Ether()/IP()/TCP())，sendp()才能发送第二层的协议,比如sendp(Ether()/IP()/TCP())

开始前，开启kali的ip转发：sysctl net.ipv4.ip\_forward=1

先打开一个终端，对目标靶机（192.168.1.18）欺骗，告诉它网关为（192.168.1.102）所在的地址：python arpDeceive.py –I eth0 –t 192.168.1.18 –m rep 192.168.1.102

再打开另一个终端，对网关进行欺骗，192.168.1.18对应的主机为192.168.1.102

防范arp：

在主机绑定网关MAC与IP地址为静态（默认为动态），命令：arp -s 网关IP 网关MAC

在网关绑定主机MAC与IP地址

使用ARP防火墙