ICMP重定向攻击

1.使用一台Kali Linux攻击一台Windows 10。

2.将Kali Linux和Windows 10都设置为net或桥接模式，使他们可以正常上网，并且在同一个网段中，且彼此能够ping通。

3.使用Kali下载netwox工具包。

4.查看Kali Linux的IP地址，查看Windows 10的IP地址和其网关IP地址，在Kali Linux上使用以下命令攻击Windows 10

netwox 86 -g 重定向到的新网关的IP地址（Kali攻击机的IP地址） -i 受攻击主机的**网关**的IP地址

5.在Windows 10上使用Wireshark抓取流量，观察并分析Kali Linux攻击产生的ICMP重定向报文，配合抓取的报文阐述整个攻击原理。

6.在Windows 10上访问Internet，看看是否能上网。如果把netwox里面的命令中-i 及后面的内容删除，观察此时是否能上网，说明了什么？如果把netwox命令中的-g指定的ip地址改为一个不在该网段中的虚假ip地址，观察此时能否上网，说明了什么？

7.在Kali Linux能够攻击成功时，观察Wireshark抓取的ICMP重定向报文，思考理论上有没有办法识别出ICMP重定向攻击报文。（与正常的ICMP重定向报文做对比，写出思路即可，不用实现）

8.结合课程内容，或上网查询防御ICMP重定向攻击的方法。在虚拟机中试试看使用该方法时能否成功阻止ICMP重定向攻击。