计算机网络原理第三次作业

> 计64 翁家翌 2016011446

ICMPv4 协议辅助 IPv4 协议进行网络操作被广泛使用。经网上查找，黑客可以利用 ICMPv4 如下的特性发起攻击:

1. DDOS：利用 ICMPv4 协议里面定义的 `echo request` 和 `reply` 两条指令。由于 `reply` 报文具有较高的转发优先级，黑客可用肉鸡发送大量 `echo request` 到被攻击站点，使其花费大量时间处理这些报文，占用系统资源而无法处理其他类型的包，从而造成拒绝服务攻击。此外黑客还能够伪造 IP 地址，向被攻击者所在的某个子网发送 `echo request` 请求，大量的 `reply` 会占满受害者带宽，从而达到 DDOS 效果。
2. ping of death (POD)：早期操作系统为每个 IP 包预留的封包大小为 65535 字节，如果超出该范围则会造成数组越界，引发异常。通过路由器实验二，修改 IP 包的大小和偏移是一件非常容易的事情。所以只要构造/转发并修改几个值就能做到。
3. ICMP Redirect Attack：类似 ARP 攻击能够修改路由表来修改流向转发路径，达成中间人攻击效果。ICMP 重定向报文能为主机指明一个更好的路由，黑客通过伪造 ICMP Redirect 报文将受害者数据包重定向至自己机器上截获流量之后再进行转发。