**实验三、DDOS攻击**

**一、实验目的**

理解分布式拒绝服务（DDoS:Distributed Denial of Service）攻击的原理， 通过模拟拒绝服务（DoS）攻击了解网络攻击的防御措施。

**二、实验内容**

Windows操作系统

了解ping命令

通过ping命令实现拒绝服务攻击

**三、实验步骤**

1.Windows 操作系统

Windows操作系统通过TCP/IP协议进行通信传输，它是在网络的使用中的最基本的通信协议。TCP/IP传输协议对互联网中各部分进行通信的标准和方法进行了规定。并且，TCP/IP传输协议是保证网络数据信息及时、完整传输的两个重要的协议。TCP/IP传输协议四层体系结构:应用层、传输层、网络层、数据链路层。

2.了解ping命令

PING 因特网包探索器,用于测试网络连接量的程序。

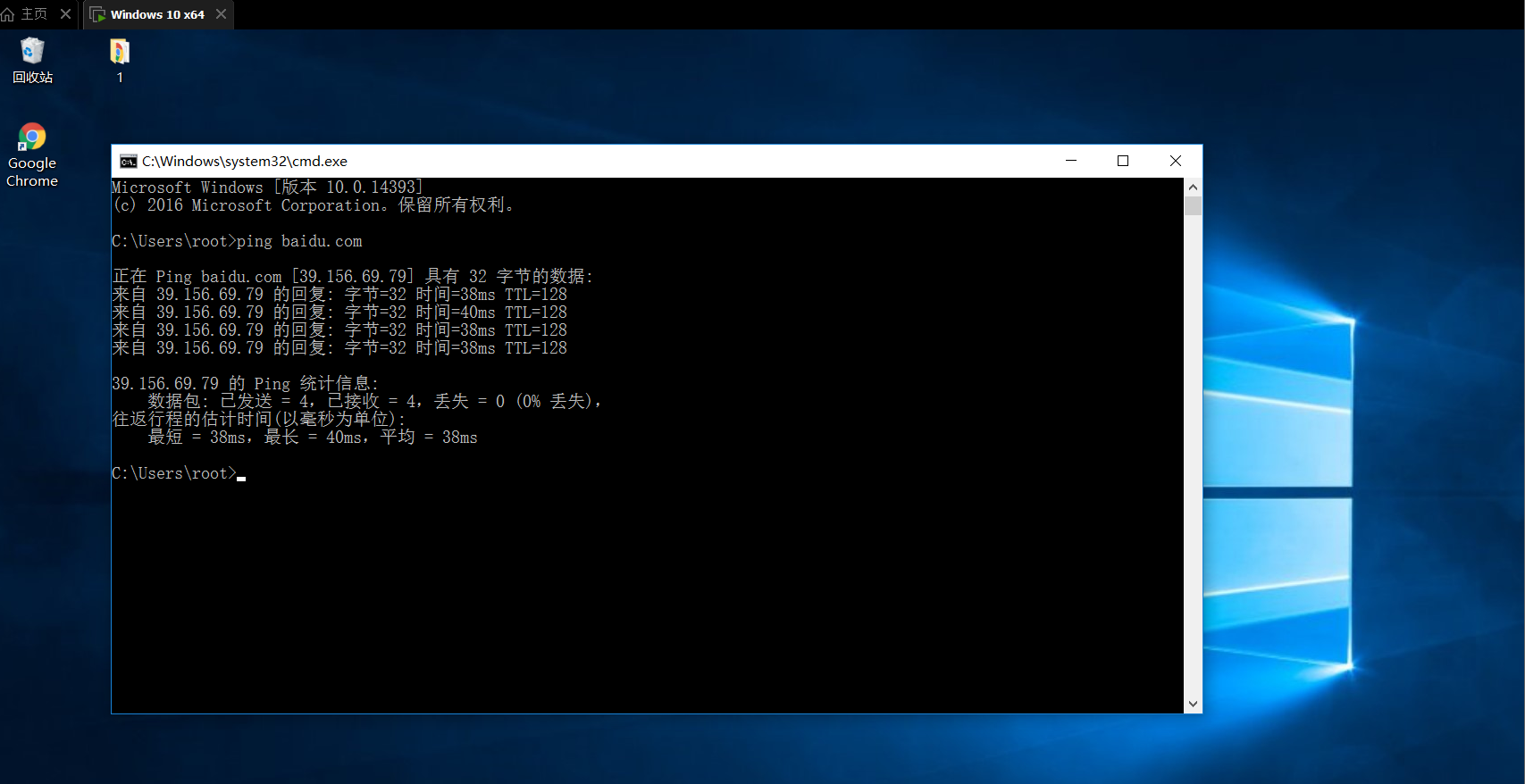
ping是工TCP/IP网络体系结构中应用层的一个服务命令,主要是向特定的目的主机发送请求报文,测试目的站是否可达及了解其有关状态。可通过ping命令进行DOS拒绝服务攻击。单一的DOS攻击一般是采用一对一方式的，利用网络协议和操作系统的一些缺陷，采用欺骗和伪装的策略来进行网络攻击，使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。



3. 通过ping命令实现拒绝服务攻击

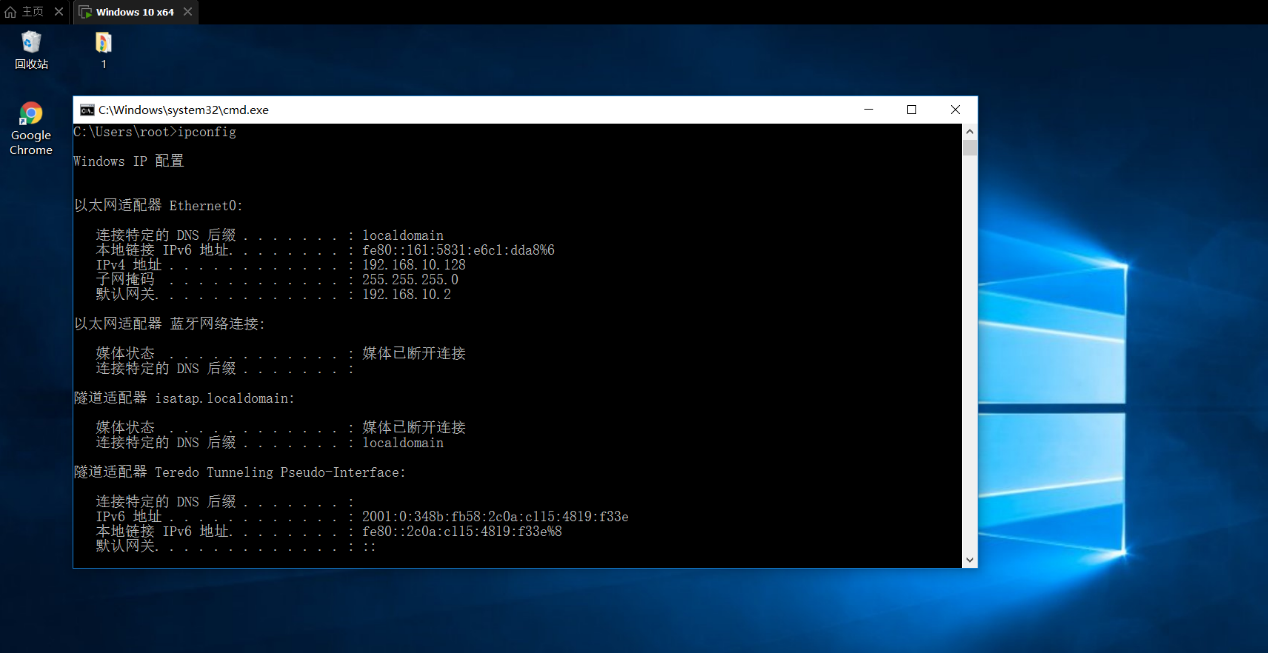
(1).检测网络是否连通

ping baidu.com



网络连通

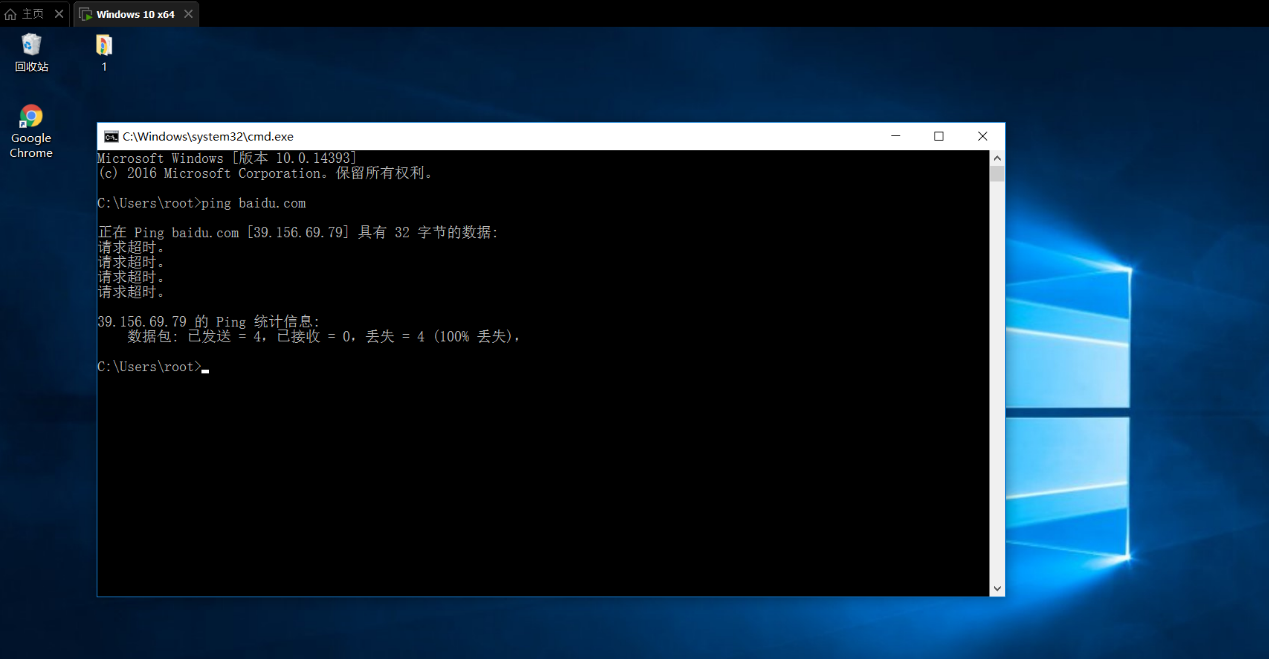
(2).查看IP地址, 并通过ping命令进行DOS攻击



在另一Windows操作系统上(同一网段下)执行

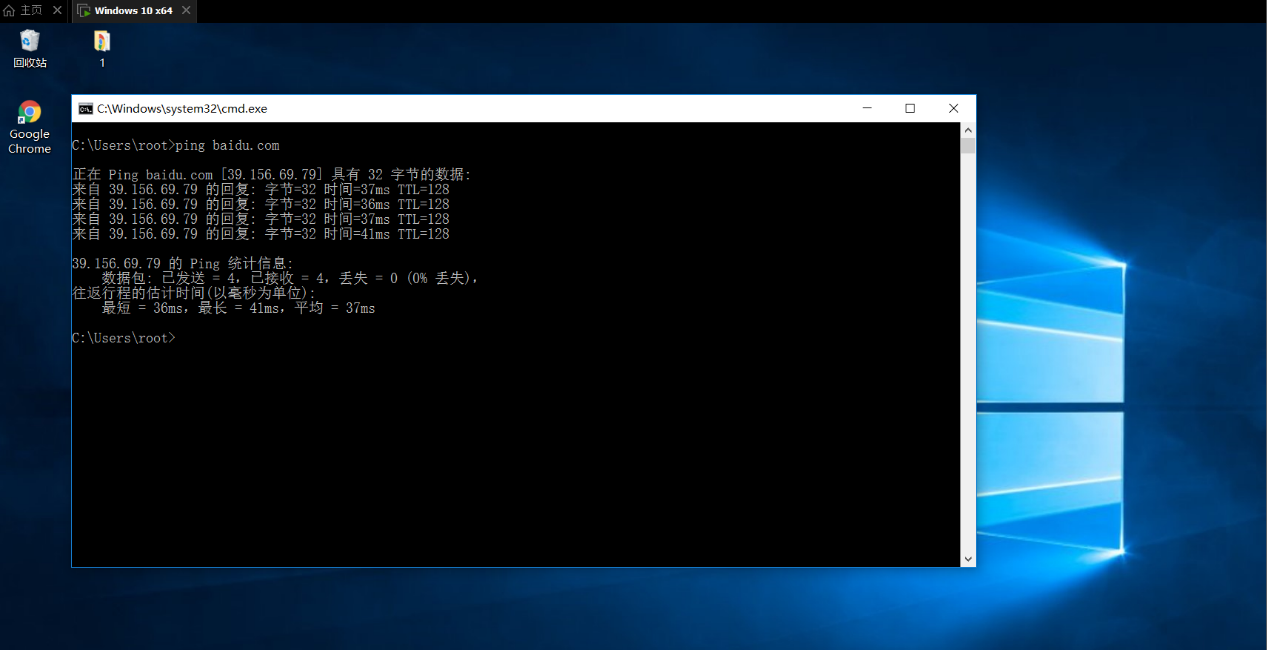
ping 192.168.10.128 -l 65500 -t 命令

(3).检测被攻击系统是否可上网



无法ping 通baidu.com

(4).停止 dos 攻击



网络恢复正常

DOS攻击实验成功

**四、实验结果**

通过ping命令进行DOS拒绝服务攻击使得目标机无法上网,

停止ping命令后目标及网络状态恢复

DOS攻击实验成功。

**五、写出本次实验的实验心得**

1.了解了DDOS攻击原理

分布式拒绝服务攻击原理分布式拒绝服务攻击DDoS是一种基于DoS的特殊形式的拒绝服务攻击，是一种分布的、协同的大规模攻击方式,与DoS攻击由单台主机发起攻击相比较，分布式拒绝服务攻击DDoS是借助数百、甚至数千台被入侵后安装了攻击进程的主机同时发起的集团行为。一个完整的DDoS攻击体系由攻击者、主控端、代理端和攻击目标四部分组成。主控端和代理端分别用于控制和实际发起攻击，其中主控端只发布命令而不参与实际的攻击，代理端发出DDoS的实际攻击包。对于主控端和代理端的计算机，攻击者有控制权或者部分控制权。在攻击过程中会利用各种手段隐藏自己不被别人发现。真正的攻击者一旦将攻击的命令传送到主控端，攻击者就可以关闭或离开网络。而由主控端将命令发布到各个代理主机上。这样攻击者可以逃避追踪。每一个攻击代理主机都会向目标主机发送大量的服务请求数据包，这些数据包经过伪装，无法识别它的来源，而且这些数据包所请求的服务往往要消耗大量的系统资源，造成目标主机无法为用户提供正常服务。甚至导致系统崩溃。

2.了解到一些防御网络攻击的措施

如:针对DDOS攻击

(1)定期扫描

定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清理。骨干节点的计算机因为具有较高的带宽，是黑客利用的最佳位置，因此对这些主机本身加强主机安全是非常重要的。并且连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就变得更加重要。

(2)在骨干节点配置防火墙

防火墙本身能抵御DdoS攻击和其他一些攻击。在发现受到攻击的时候，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。当然导向的这些牺牲主机可以选择不重要的，或者是linux以及unix等漏洞少和天生防范攻击优秀的系统。

(3)充分利用网络设备保护网络资源

(4)过滤不必要的服务和端口

滤不必要的服务和端口，即在路由器上过滤假IP ……只开放服务端口成为很多服务器的流行做法，例如WWW服务器那么只开放80而将其他所有端口关闭或在防火墙上做阻止策略。

3.了解了不同网络协议,学会了更多计算机网络知识;

4.体会到进行实际实验操作对于计算机学习的重要性;

5.在计算机专业学习过程中要扎实基础,深刻了解背后原理提高网络防御能力。