TCP SYN、UDP、ICMP之DOS攻击

1. 实验背景

DoS攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃。

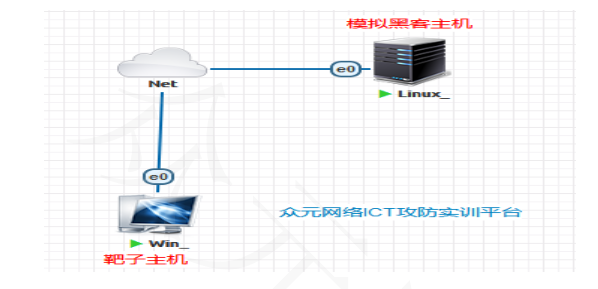
1. 实验设备

1、一台靶机windows主机

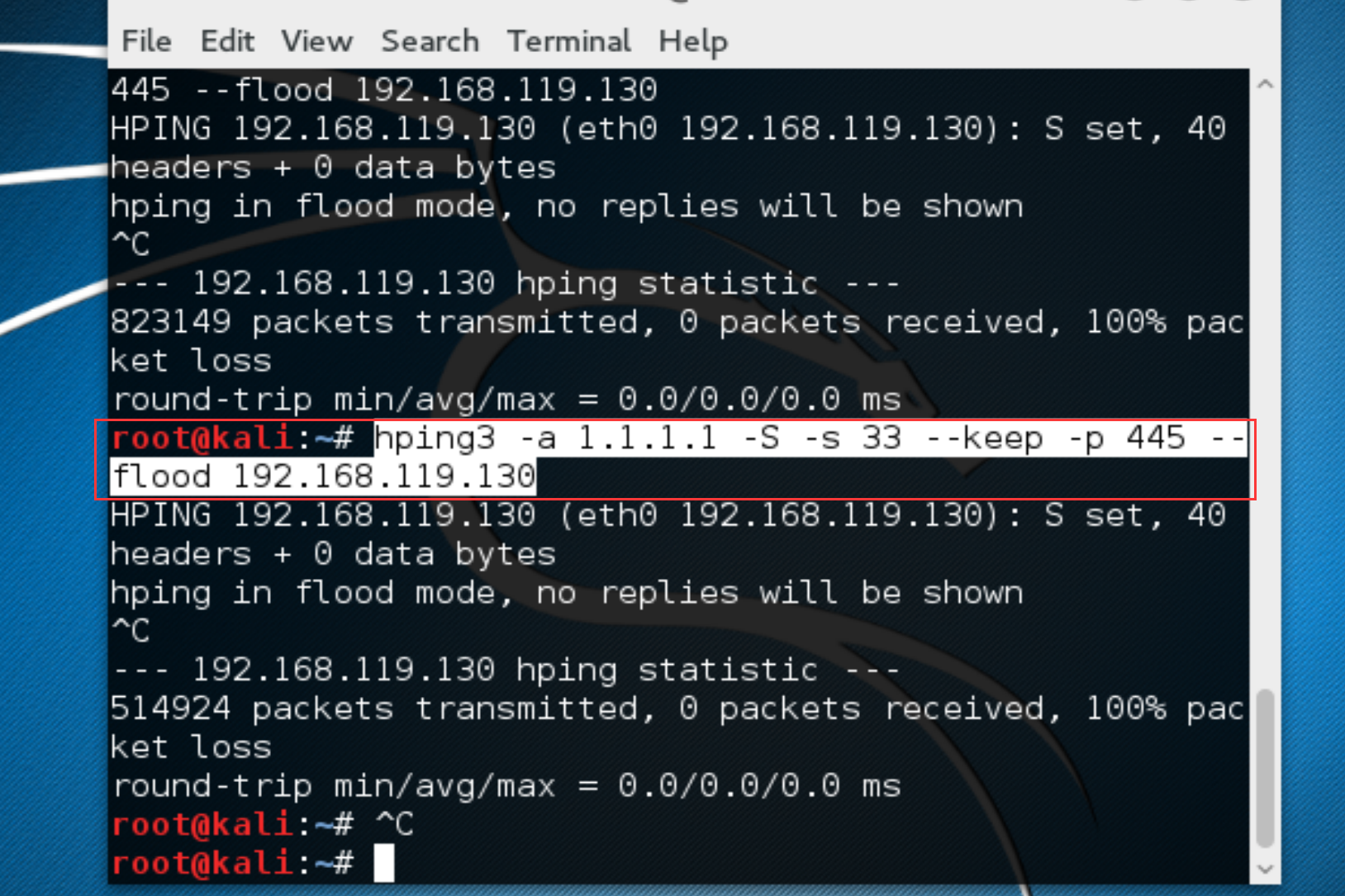
2、增加一个网络net:cloud0

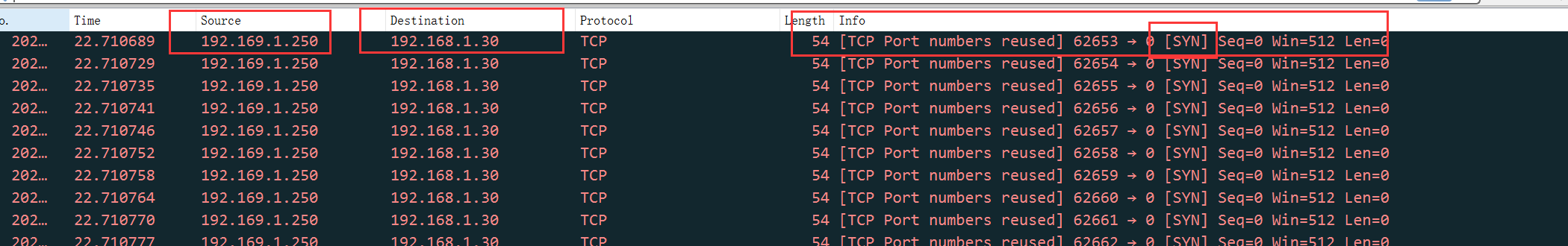
3、一台模拟黑客主机kali

1. 实验拓扑图



1. 实验步骤
2. **kali主机向靶子机（192.168.119.130）发送大量的TCP SYN置1的报文，使得靶子机系统奔溃。**

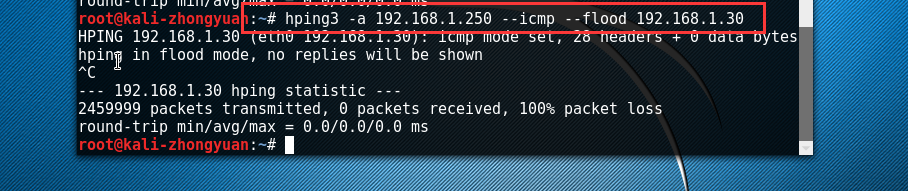


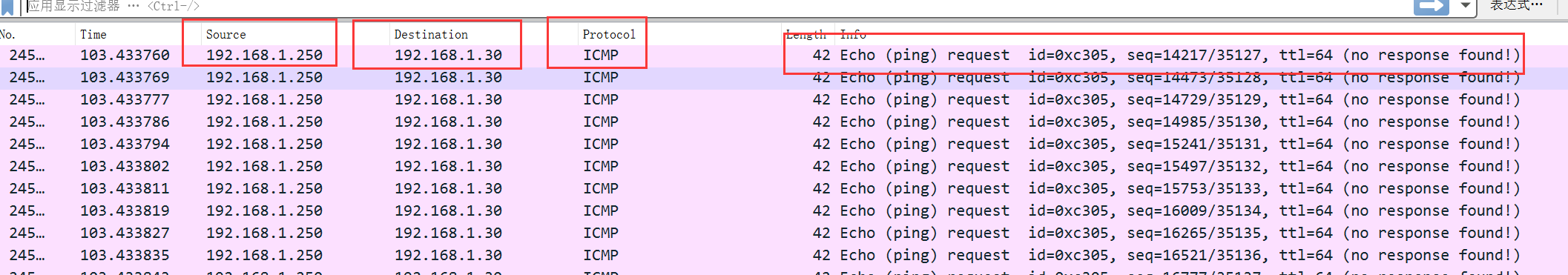


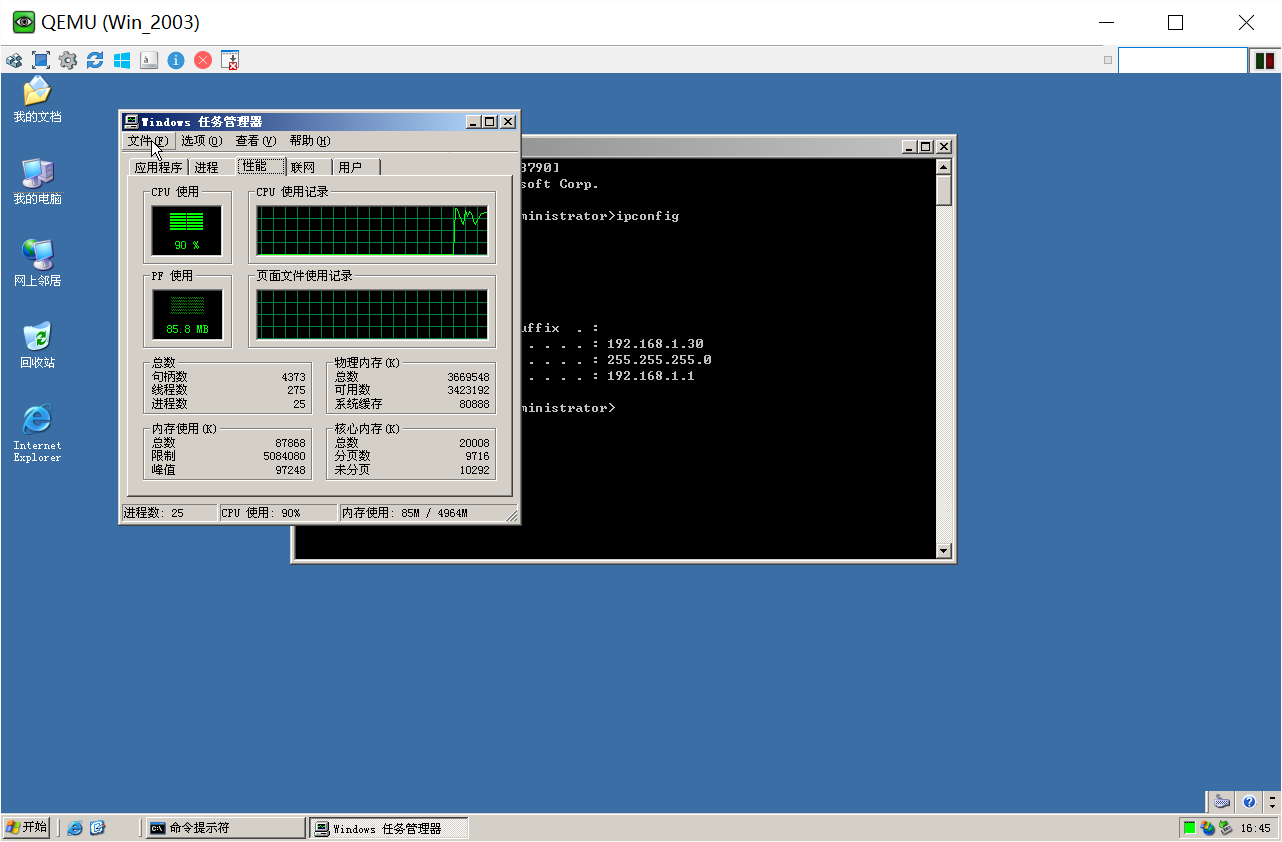
分析：由上图可知靶子机收到大量的TCP SYN的报文，但是此时源ip

为1.1.1.1，此ip并不是真正的kali的ip，因此有效的隐藏了kali的ip地址

**2、kali主机伪造源ip向靶子机（192.168.1.30）发送大量的icmp包，使得靶子机系统奔溃。**

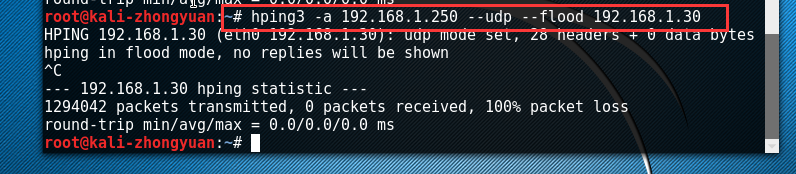


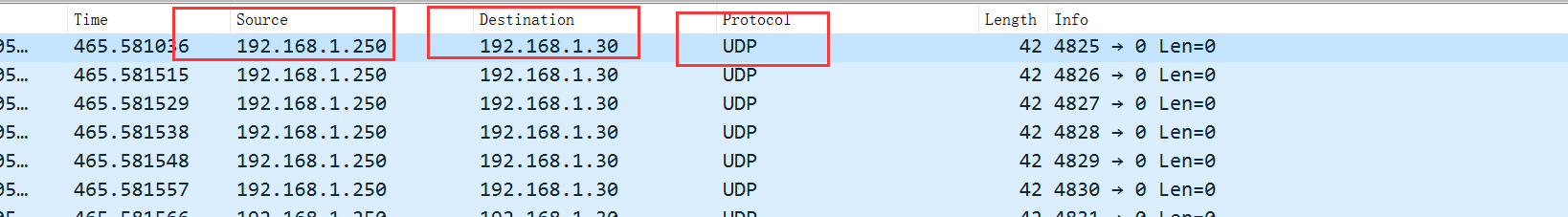




分析：由上图可知，靶子机收到大量的icmp数据包，消耗系统内存，cpu占用到达接近100%，且源ip是伪装的，看不到黑客主机的ip。

**3、kali主机伪造源ip向靶子机（192.168.1.30）发送大量的udp包，使得靶子机系统奔溃。**





分析：由上图可知，靶子机收到大量的udp数据包，消耗系统内存，c且源ip是伪装的，看不到黑客主机的ip。

总结：dos攻击的目的是为了消耗目的主机的系统资源、内存、cpu等，最后让目的主机奔溃，宕机。Dos攻击的方式有很多种，例如：TCP SYN、UDP、ICMP、泪滴攻击等等。