1. 实验项目名称：

拒绝服务攻击kali（kali渗透攻击课程中第五个实验）

1. 实验原理：
2. 拒绝服务攻击(Dos)

常见的DOS攻击都会包含用额外通信请求来形成流向目标的洪水。这些过载会导致资源无法响应合理的网络请求，或是显著的降低响应的速度。Dos攻击可以针对系统资源、配置信息、状态信息等能对系统运行造成危害的所有操作。该攻击工具的一个最基本特点是，它仅需要对加密密钥进行重新请求，而加密密钥被用来在服务器端和客户端创建高达1000的并行连接。因此，任何一台SSL服务器在这种工具面前都失去了免疫，包括Web服务器、电子邮件服务器等。漏洞存在于协议的renegotiation过程中，renegotiation被用于浏览器到服务器之间的验证。网站可以在不启用renegotiation进程的情况下使用HTTPS，但研究人员指出很多网站仍然默认启用renegotiation。

2) Dos攻击分类：

基于带宽的攻击：包括UDP洪水、ICMP洪水和其它基于欺骗数据包的洪水，其目的在于耗尽受害者站点的带宽。

协议攻击：利用网络协议的漏洞进行攻击，如ARP、DDOS、TCP半连接、SYN洪水攻击

等。这些协议本身都是正常的，但是用在不正常的地方就成了病毒了。

应用层攻击：利用合法网络数据来使web服务崩溃

1. 实验目的：

使用thc-ssl-dos工具攻击目标网站,使目标网站无法正常访问

1. 实验器材（设备、虚拟机名称）：

Kali操作机IP：192.168.1.2，目标机IP：192.168.1.3

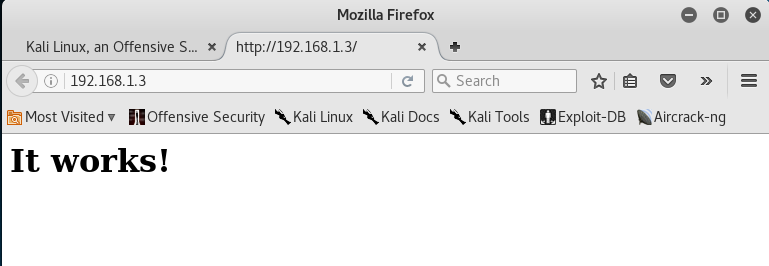
1. 实验步骤：

1.攻击目标网站

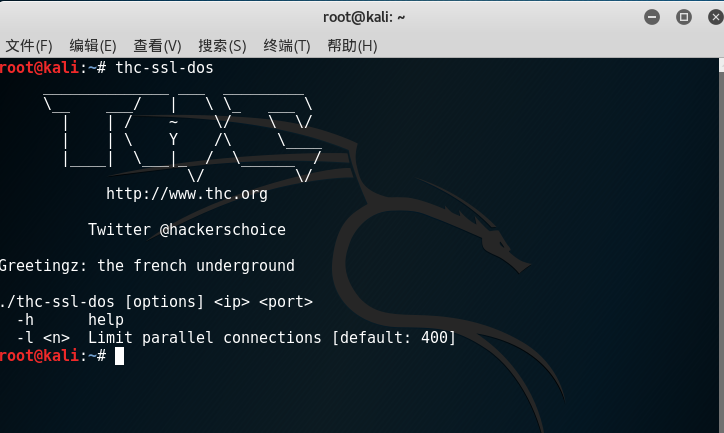
1.1 单击桌面空白处，右键菜单选择“打开终端”。



1.2 在浏览器输入192.168.1.3，网站正常。



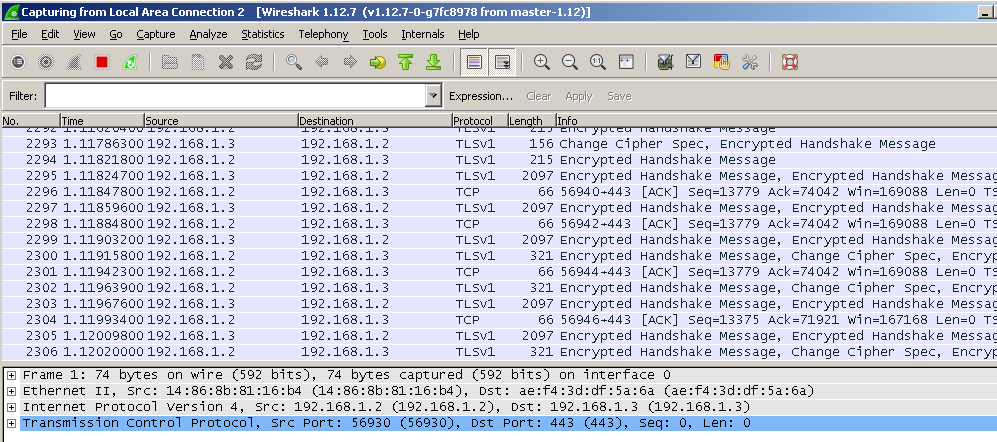
1.3 在终端中输入命令“thc-ssl-dos”。



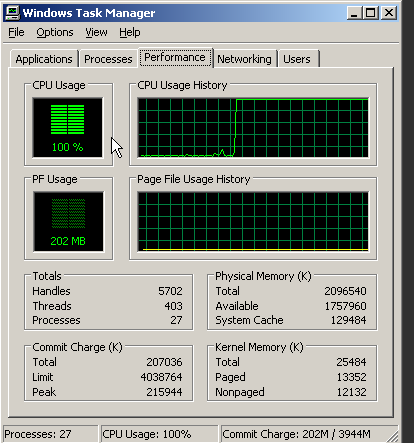
1.4 在终端输入命令：thc-ssl-dos -l 15 192.168.1.3 443 –accept,对目标主机443端口建立100条连接进行泛洪攻击，l参数越大，目标主机资源消耗越大（因实验环境限制，l参数不用超过15，否则目标主机死机）。



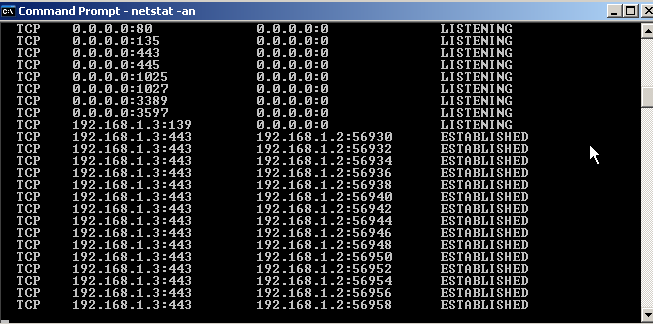
1.5 进入目标主机，打开wireshark软件，开始抓包。从抓包可见当客户端连接到服务器端正常握手后，客户端重复发起握手，进行循环攻击。



1.6 在目标主机打开任务管理器，发现CPU利用率100%。



1.7 在目标主机的命令行输入netstat -an，这条命令是在windows下查看自己的电脑系统正在使用哪些端口，以分辨有没有非法的侵入，查看一下连接，发现大量攻击机和目标机连接



1. 实验结果及分析：
2. 总结及心得体会：