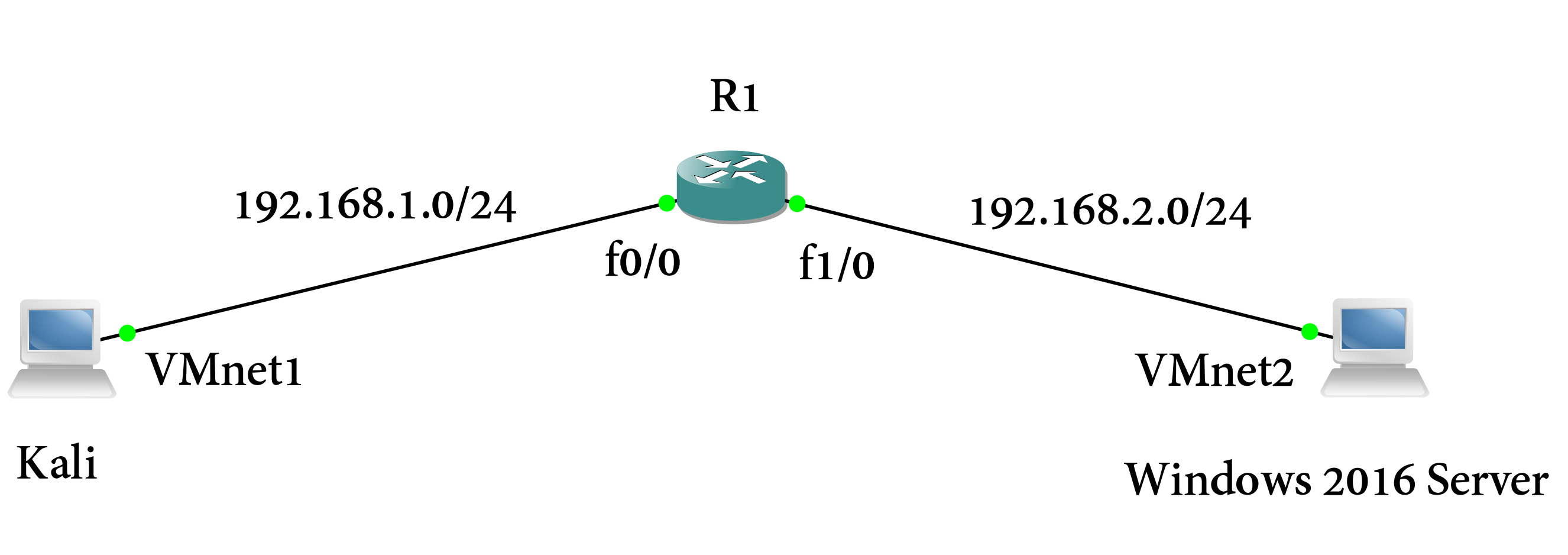
TCP Flood攻击与UDP Flood攻击

本实验方法一定不要用来攻击公网的服务器，仅能在自己的虚拟机里进行操作！不然可能构成违法行为，大家一定注意！

1. 实验环境搭建：

一台Kali Linux攻击主机、一台Windows 2016 Server、GNS3镜像路由器。Kali Linux使用hping3命令进行攻击



1. 实验内容

（1）TCP Flood攻击

1.在Kali Linux上使用以下命令打开文件，设置Kali Linux的IP地址参数：

vim /etc/network/interfaces

在源文件内容（回环地址loopback默认设置）下面添加以下内容后保存退出：

auto eth0

iface eth0 inet static

address IP地址

netmask 子网掩码

gateway 网关IP地址

输入以下指令关闭网络

ifdown eth0

输入以下指令开启网络

ifup eth0

检查当前网络的IP地址参数是否变为修改好的地址（ifconfig查看IP地址和子网掩码, route -n查看网关）

2.在Windows 2016上使用以下命令设置IP地址参数

netsh interface ip set address “Ethernet0”static IP地址 子网掩码 网关IP地址

通过Win键🡪服务器管理器，创建一个Web服务器并开启该服务器功能

3.在Kali Linux上使用自带命令hping3通过以下指令攻击Windows 2016 Server

hping3 -S（表示SYN Flood攻击） -c 包数量 –-flood（表示以最快速度发送包，并且不显示回复） -d 每个包中数据长度 -w 窗口长度 -p 目标端口号 --rand-source（表示以随机的IP地址发送流量）

4.在GNS3上服务器侧网段上打开Wireshark抓包，分析抓取的TCP Flood流量的过程，并通过改变hping3命令的参数，观察攻击报文的相应变化。

5.在Kali Linux上打开浏览器，以http访问Windows 2016 Server，在攻击时看看能否成功访问网页。打开多个终端模拟器对服务器进行攻击，调整hping3的参数，观察以怎样的参数进行攻击时就无法访问浏览器内容了。（注意每次实验清除浏览器缓存）

（2）UDP Flood攻击

1.以TCP Flood攻击平台为基础，在Windows 2016 Server上通过以下方式添加DNS服务器

服务器管理器🡪管理🡪添加角色和功能🡪下一步🡪…🡪下一步🡪勾选DNS服务器🡪下一步🡪…🡪下一步🡪完成即可。按下Win键，在Windows管理工具里面找到新添加的DNS服务器，选中服务器的下拉条，右键“正向查找区域”，点击“新建区域”，单击“下一步”并选中“主要区域”再点击“下一步”，输入区域名称“cybersecurity.com”，并一直点击“下一步”直至完成。在“正向查找区域”下拉条中右击刚刚添加的区域，点击“新建主机A或AAAA”，在名称处填写“www”，并在IP地址处填写一个合法的IP地址作为该域名的解析地址，并单击“添加主机”。这样就创建了DNS服务器上www.cybersecurity.com到其IP地址的映射关系。

2.开启一台Windows10主机，修改其IP地址为192.168.1.0/24网段的地址，网关为192.168.1.254，首选DNS地址为192.168.2.0/24网段的Windows2016服务器IP地址。

3.通过以下指令观察能否解析出www.cybersecurity.com的IP地址

nslookup www.cybersecurity.com

此时打开Wireshark抓取该过程的UDP报文并分析该报文，都有哪些字段，数据段包含哪些内容。

4.通过Kali Linux的hping3工具用以下指令攻击Windows2016服务器

hping3 --udp --rand-source -p 53 -d 100 --flood 目标服务器的IP地址

该过程打开真实机上的Wireshark抓取192.168.2.0/24网段的流量，观察并分析攻击时发送的UDP包的特征。

5.在Windows10上通过nslookup指令解析刚才的域名，看能否解调出来。如果仍可以解析出IP地址，则再开启新的root终端进行刚才指令的攻击，记录开启多少个终端即可使Windows10无法解析域名。