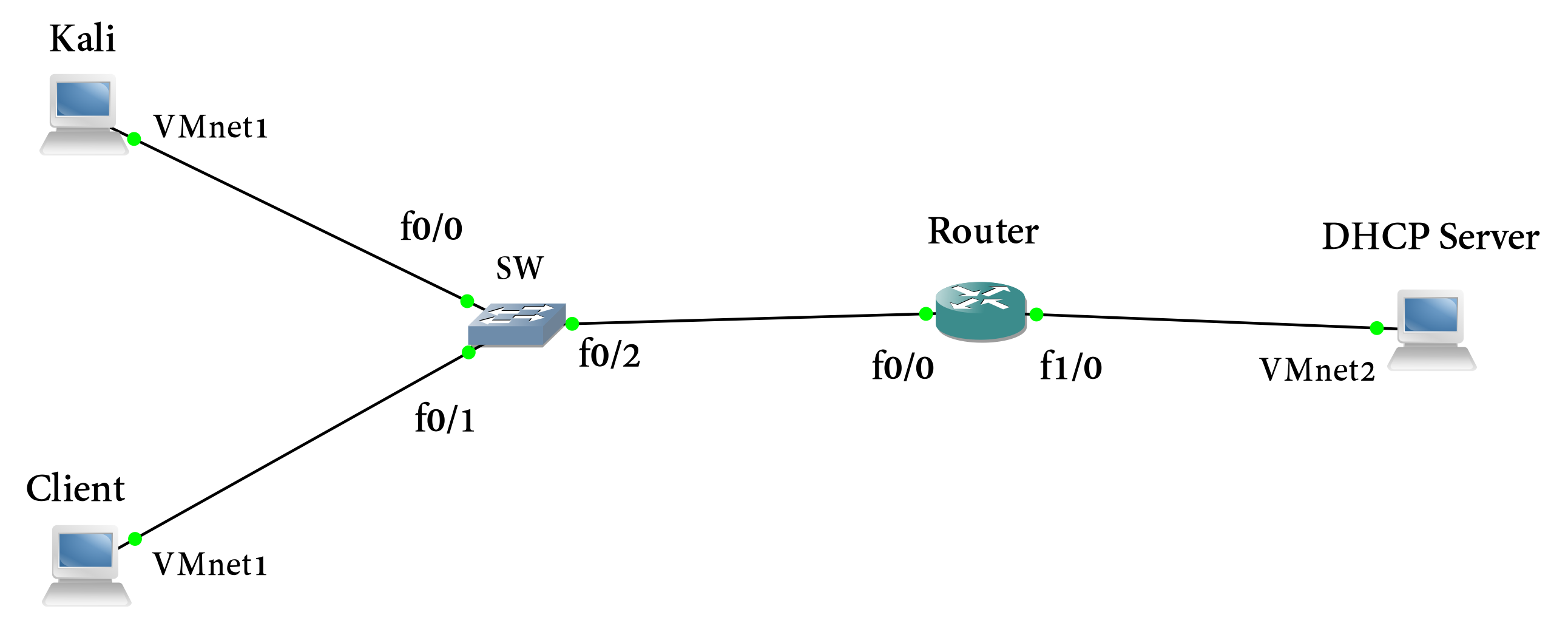
DHCP欺骗

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

实验环境搭建：

一台Kali Linux攻击主机、一台Windows 10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）部署DHCP服务器

1.选择Windows 2016 Server为仅主机模式的VMnet2网段，用以下命令配置Windows 2016 Server的IP地址

netsh interface ipv4 set address “Ethernet0(即虚拟机网卡名称)” static IP地址 子网掩码 网关IP地址

2.通过以下方式在Windows 2016 Server上添加DHCP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DHCP服务器🡪下一步🡪…🡪下一步🡪完成即可。在服务器管理器页面右上角通知（黄色感叹号）处点击完成DHCP服务器配置。按下Win键，在Windows管理工具里面找到新添加的DHCP服务器，在下拉条里面右键“ipv4”点击出现的“新建作用域”。在新建作用域向导里面单击“下一步”，填写第一个作用域（一般是DHCP服务器所在的网段）的名称（随便写），之后点击“下一步”。填写起始IP地址和结束IP地址（可随意填写，因为实验环境中该网段没有主机）。通过下一步🡪下一步🡪“否，稍后配置这些选项”🡪下一步🡪完成，完成对第一个作用域的配置。其中租期的时间可以设置长一些。右击ipv4下的作用域，点击“激活”使该配置生效。

3.通过相似的方法设置Kali Linux与Windows 10侧网段（VMnet1）的作用域。只不过在结束之前选择“是，我想现在配置这些选项”，再点击“下一步”。添加网关的IP地址为实验环境中路由器的f0/0端口的IP地址，点击“下一步”。DNS稍后设置，再点击“下一步”直至结束。随后右击新配好的作用域下的“作用域选项”，选中DNS选项，在下面的IP地址栏中输入一个DNS服务器IP地址（虚假的真实的都可以，因为没有连接互联网）。在验证不通过后选择强制使用。

4.在Vmware的虚拟网编辑器中，将VMnet1中的“使用本地DHCP服务将IP地址分配给虚拟机”选项勾除。在Windows 10的网络适配器中把ipv4更改为自动获取IP地址和自动获取DNS服务器。抓取GNS3上路由器左侧的链路的流量。在Windows 10的cmd上输入以下指令释放自己本身的IP地址参数

ipconfig /release

然后输入

Ipconfig /renew

尝试获取IP地址。观察分析此时抓取到的报文，并观察Windows 10此时能否获取IP地址。

5.在GNS3中的镜像路由器上为f0/0端口配置中继，使用以下命令

conf t

int f0/0

ip helper-address 中继到f0/0的IP地址（即服务器IP地址）

抓取GNS3路由器右侧链路的流量。禁用并开启Windows 10上的Ethernet0网卡，观察此时Windows 10能否获取到IP地址，并分析路由器左侧和右侧的dhcp报文。

6.打开一台Kali Linux，使用桥接模式，下载yersinia工具。随后配置其IP地址为VMnet1网段的IP地址，网关IP地址为路由器f0/0端口的IP地址。用ping命令验证网络之间的连通性。

7.开启抓取GNS3路由器两侧和Kali Linux连接的链路的报文。使用以下命令以图形化界面打开yersinia

yersinia -G

点击“launch attack”，选择sending discover packet。观察此时网络中抓取的DHCP discover攻击报文的形式。此时在Windows 2016 Server中右击“作用域”选择“显示统计信息”，观察该作用域当前分配的IP地址的情况。

8.在Windows 10上使用

ipconfig /release

释放已分配的IP地址。然后在Kali Linux上点击“List Attacks”并关闭当前DHCP攻击流量。然后点击“Launch Attack”，选择“creating DHCP rogue server”。在弹出的窗口中填写攻击参数，服务器地址为Kali的IP地址，Start IP和End IP写为非VMnet1中的IP地址，使Kali给Windows 10分配到IP地址不规范。其他参数可以随意自行填写，最终点击确定。在Windows 10上使用

ipconfig /renew

命令重新获取IP地址。观察分配到的IP地址的形式，并在抓取的报文中找到以上操作的DHCP报文信息。

9.结束以上实验后，让Kali Linux使用桥接模式并可以正常上网。此时让Kali用以上的实验方式发送DHCP discover攻击真实机所连接的无线网络（**一定要是自己的宿舍的路由器提供的无线网络，不要直接连接4G等公共网络，否则可能构成违法行为**），观察是否能使得连接该网络的设备无法上网。