**课程名称** 计算机信息安全

**实验项目名称** 实验2 ARP攻击(Ettercap)

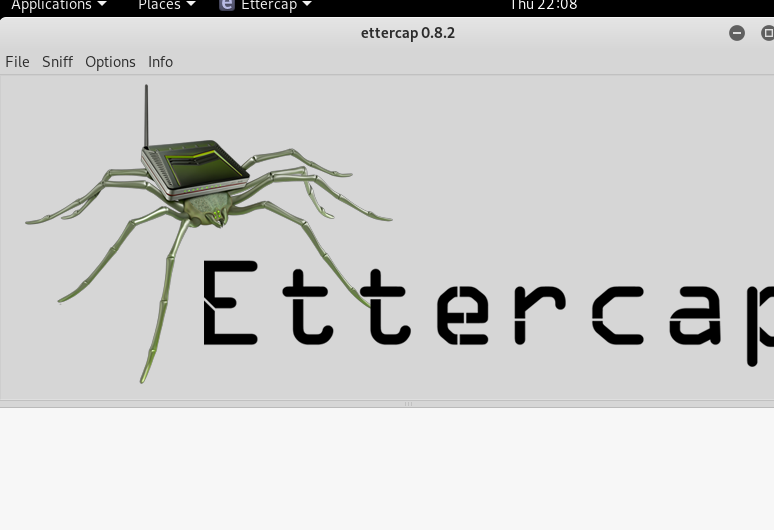
* **一、实验任务**
  1. 在Kali中使用Ettercap进行中间人攻击进行抓包破解
* **二、实验环境**
  1. Kali
  2. 使用工具ettercap
* **三、实验参考几个重要过程**

1. **启动ettercap (# ettercap -G)**
2. **设置抓包的选项(promisc Mode，Unified Sniffing)**
3. **Scan Host；Target1 选择攻击目标；Target2选择网关**
4. **ARP Poisoning**
5. **Start Sniffing**

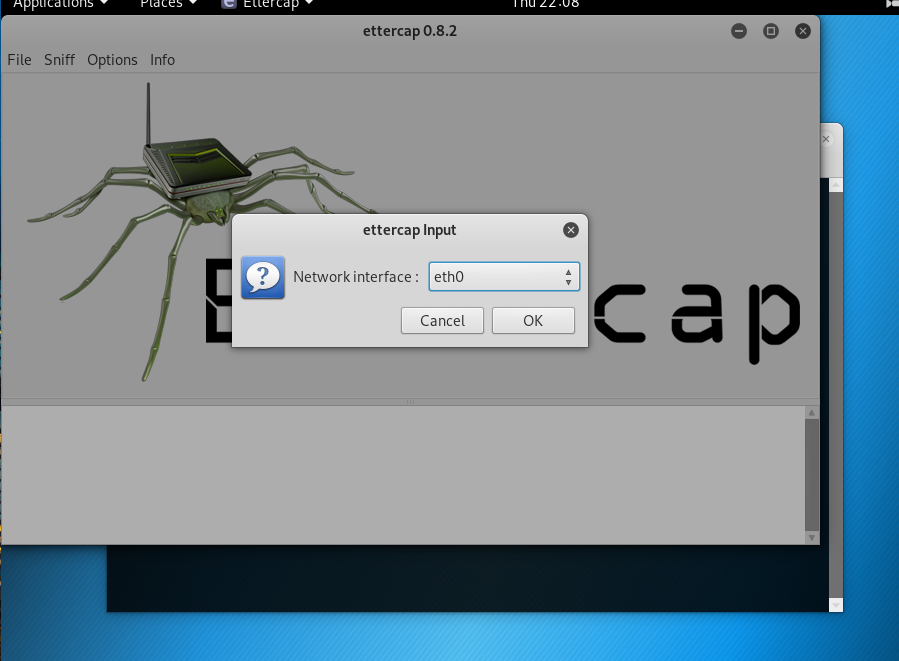
* **四、写下详细实验的步骤和实验心得**

root权限下打开ettercap -G （GTK+ GUI）

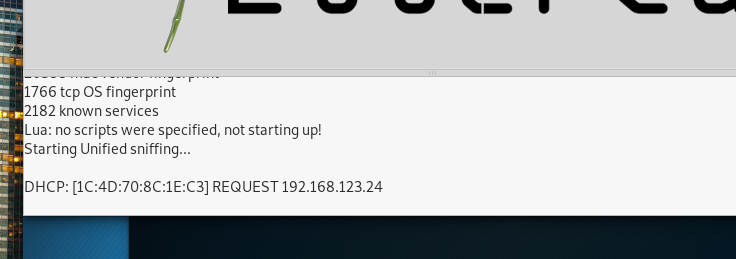
curses UI工作界面：

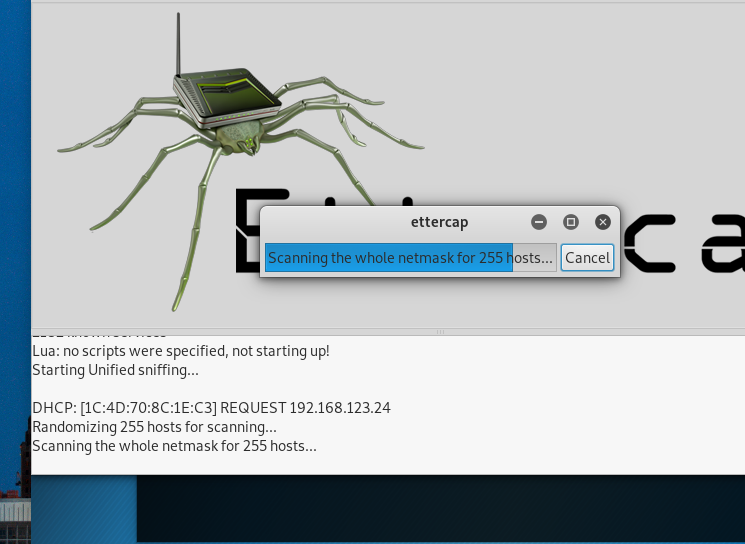


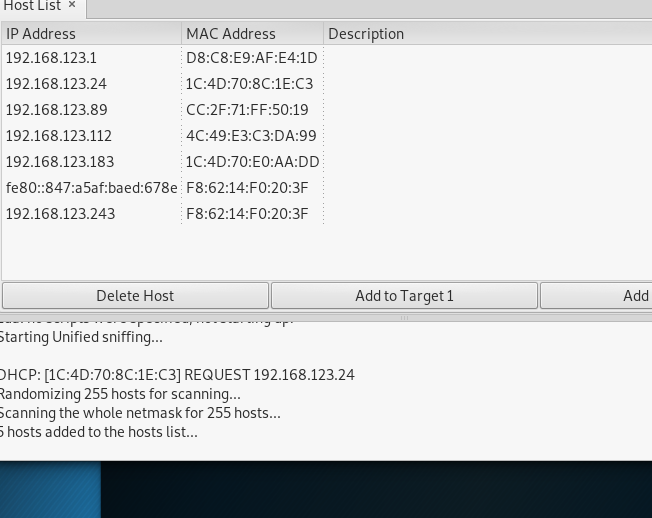
这里以GTK+ UI为例，打开ettercap之后，选择Sniff----Unified-sniffing，然后选择网卡：



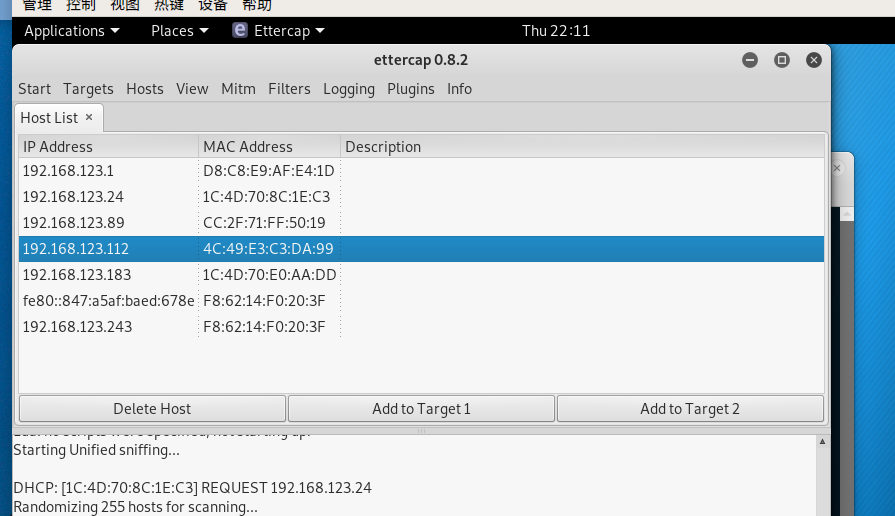
然后Hosts---Scan for hosts---Hosts list，此时可以看到目标主机ip

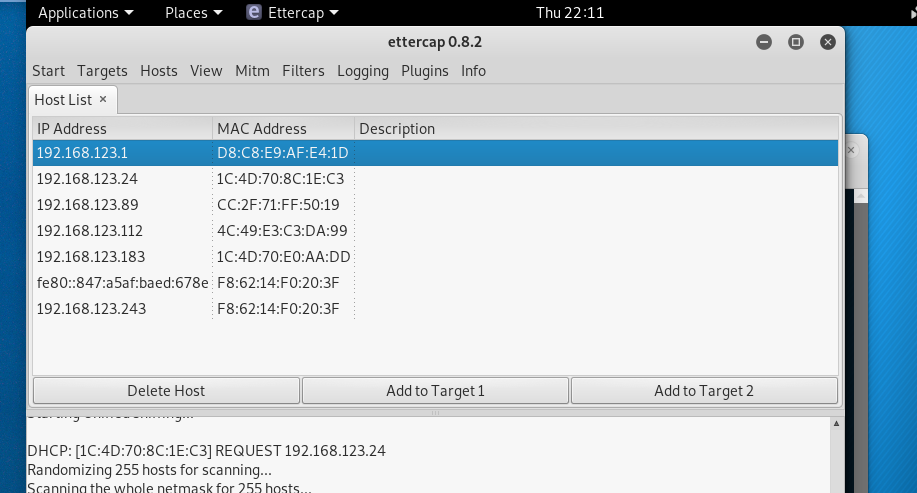






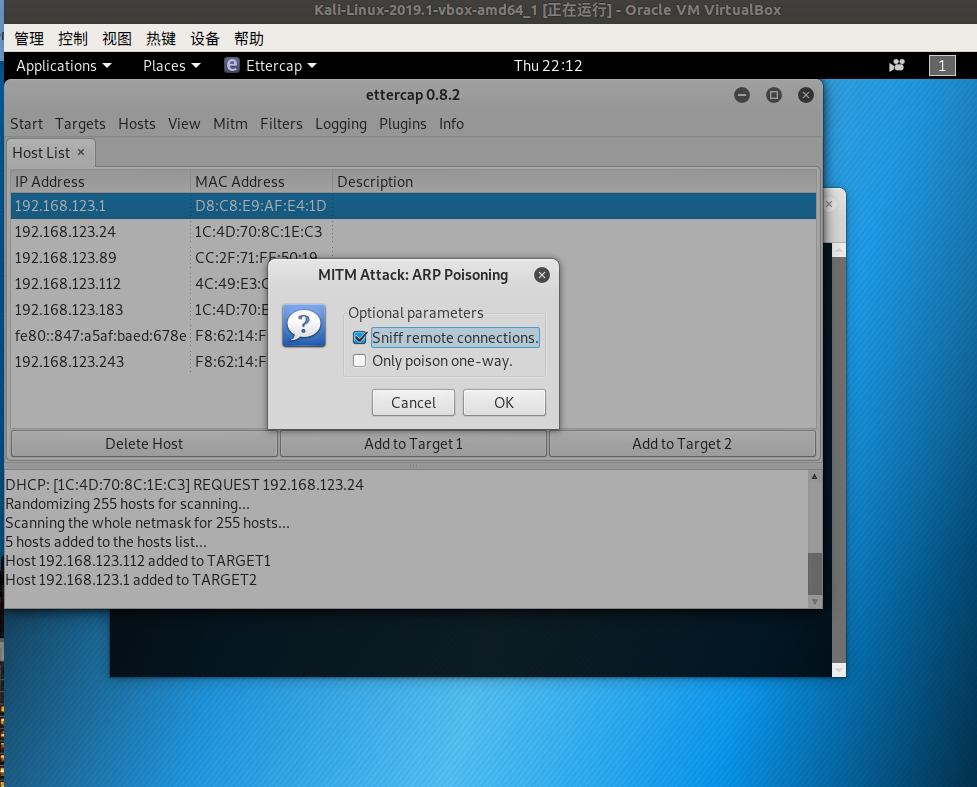
选定目标主机，然后点add to target 1,将目标主机添加到目标1;选定路由，点add to target 2,将路由添加到目标2：





如图，添加成功！

然后点mitm --- arp posoning ，勾选sniff remote connections：



之后start --- start sniffing开始监听～

点view -- connections开始查看连接：

