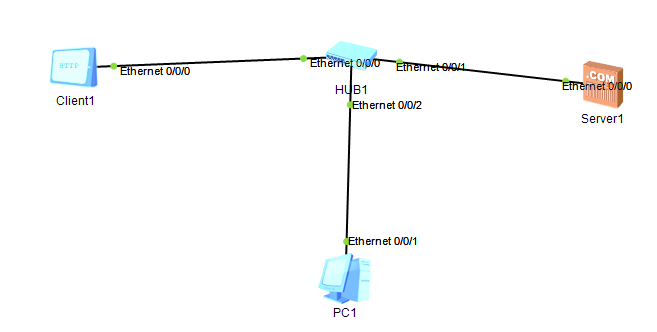
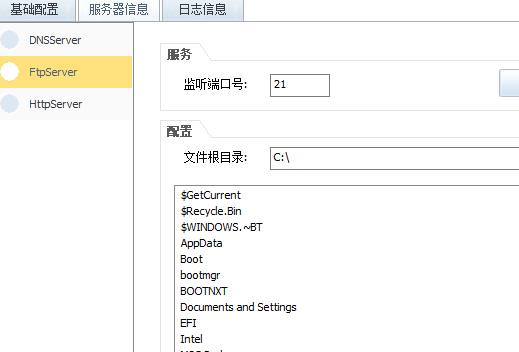
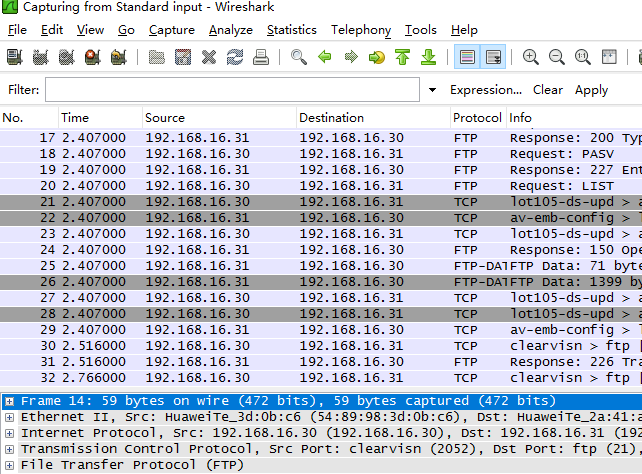
**Hub集线器环境抓取密码**

ensp抓取密码

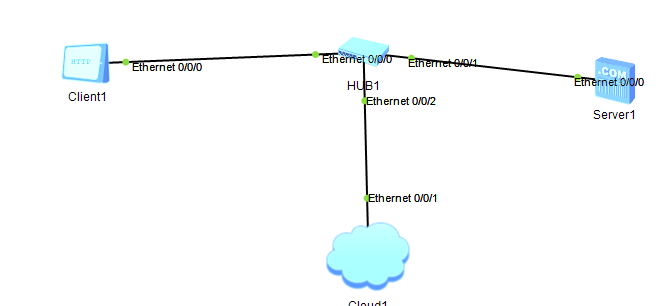




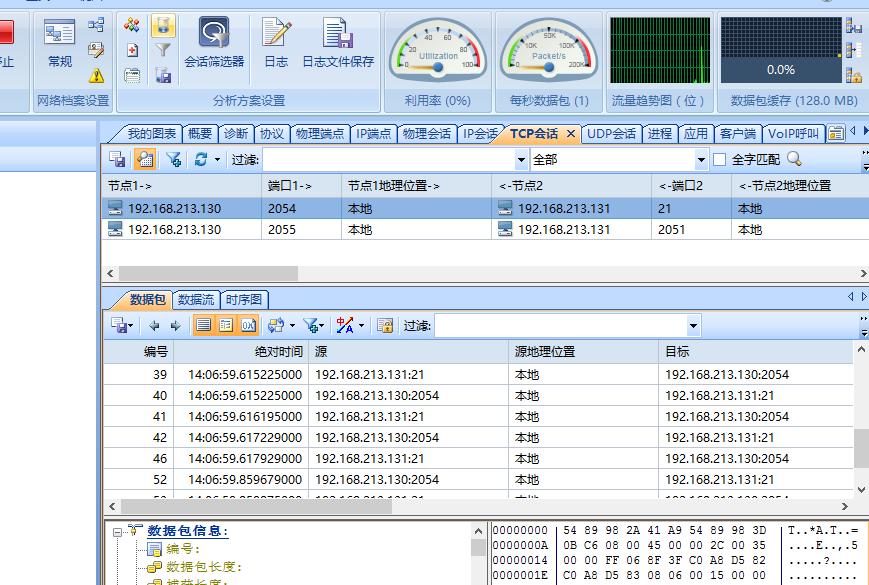


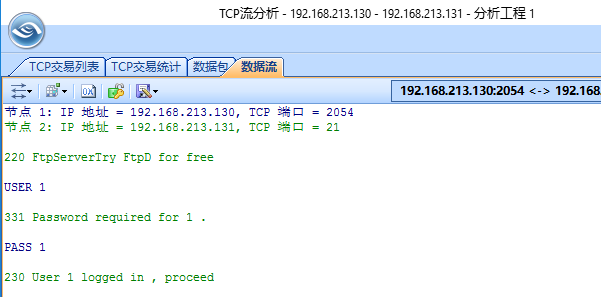


**物理机环境抓取密码**

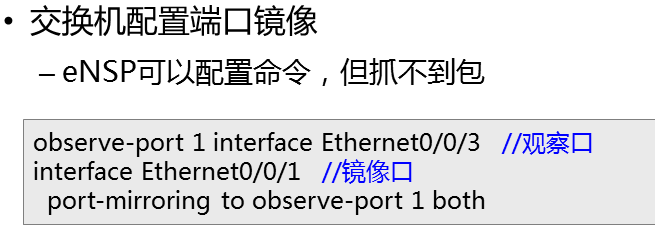




。

**交换机环境抓取密码**

如果抓取不到，需要设置端口为port link-type access

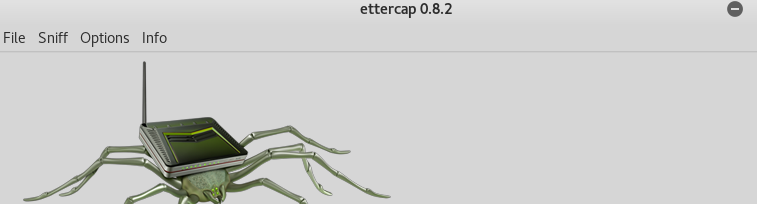




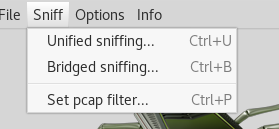
**ARP欺骗抓取密码**

中间人攻击的原理：MITM攻击就是攻击者伪装自己，然后拦截其他计算机的网络通信数据，并进行篡改和窃取，而通信双方毫不知情。

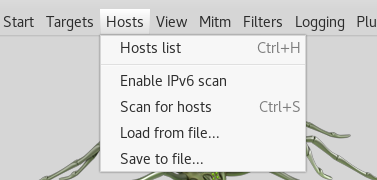
常见的方法有ARP欺骗、DNS欺骗



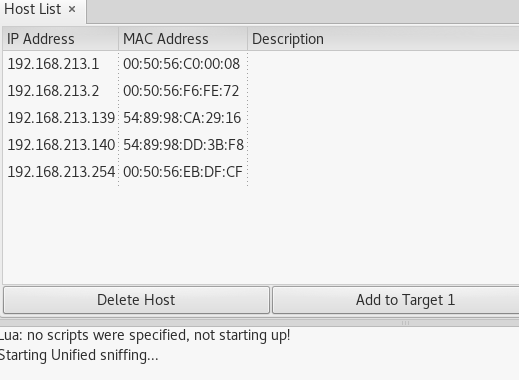
选择unified sniffing（统一嗅探）



选择scan for hosts



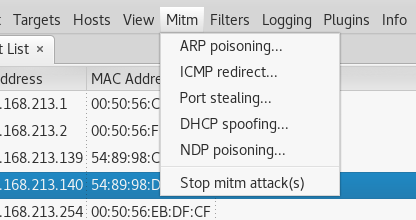
选择并查看host list

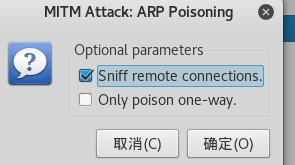


添加地址



选择ARP poisoning参数





获取密码



防范

绑定IP/MAC：以管理员身份运行netsh interface ipv4 show interface



Netsh –c ii add ne 17 192.168.19.200 54-89-98-8c-06-8e

Netsh –c ii del ne 17

查看网卡编号netsh i i sh in

将网卡设备与远端的设备MAC进行绑定netsh –c i i add ne 编号 远端设备IP 远端设备MAC