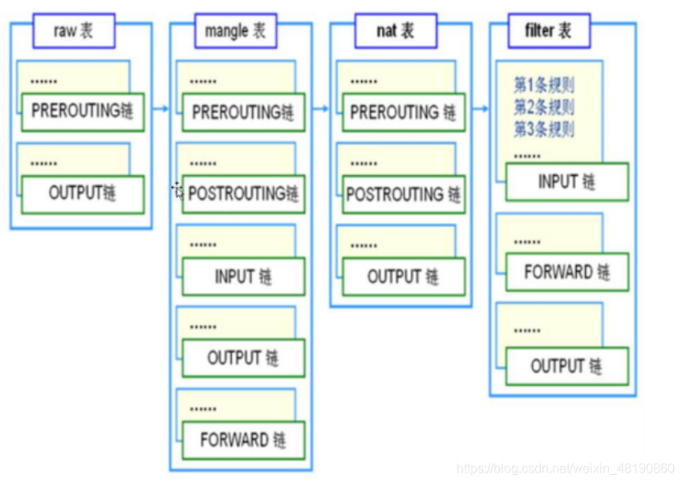
LUNIX防火墙部署与配置：

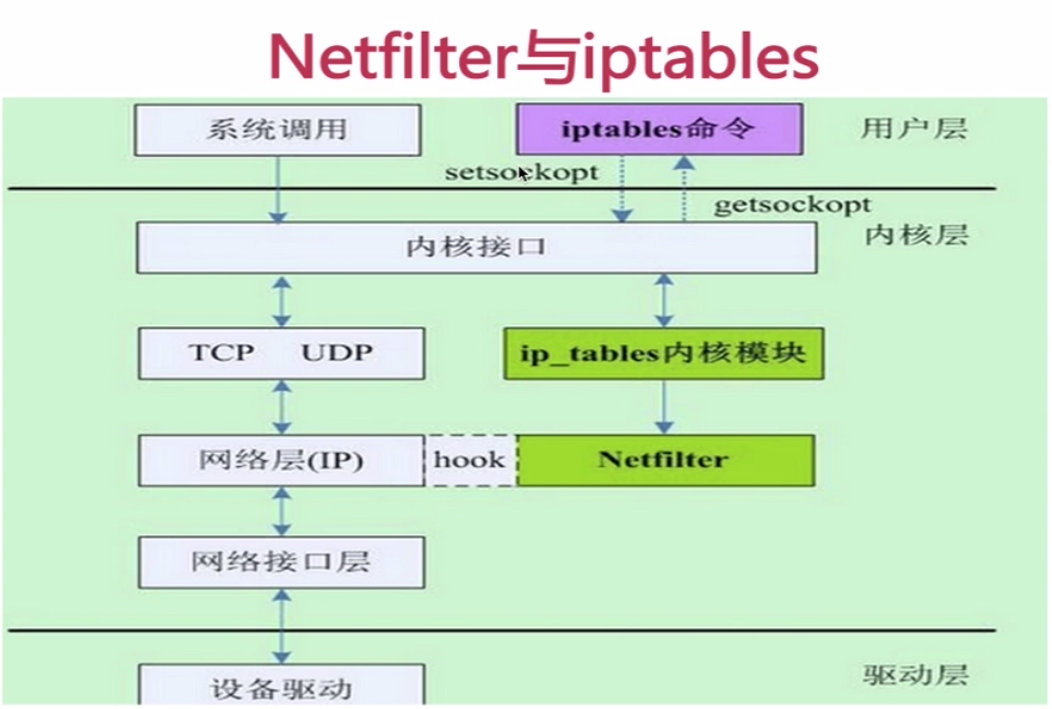
iptable防火墙属于包过滤防火墙，在网络层工作，针对ip数据包进行工作，工作内容为包内的ip地址，端口等的处理，其由iptable和netfilter组成，前者用于管理lunix防火墙的命令程序，通常是“用户态”下的，后者是防火墙的内部结构，是“内核态”下的。

firewalld iptables：

iptables由四表五链和用户在链中的写入的规则组成，四表包括：raw表（决定是否对数据包进行追踪）mangle表（对数据包进行标记）nat表（修改数据包ip地址，端口等信息）filter表（决定是否放行数据包）；五链包括：input链（处理进入包）output链（处理响应包和应答包）forward链（处理转发数据包，实现不同网段之间的通信）preouting链（在包做路由选择前，先对比此链的规则）postrouting链（选择后应用此链规则）。

netfilter：

采用模块化设计，具有良好的可扩容性,提供扩展各种网络服务的结构化底层框架，可以在网络堆栈中的数据包遍历过程中的各个点注册回调并对数据包执行各种操作，比如对数据包进行过滤，地址或者端口转换等，这些netfilter钩子为内核模块提供基础结构，这些模块注册回调以执行netfilter子系统的各种任务。



实验：

1. 安装虚拟机，使用vmware，使用kali lunix2023.1版本



1. 提高权限：

输入whoami，会返回自己的用户名，然后输入sudo -i，获得root权限



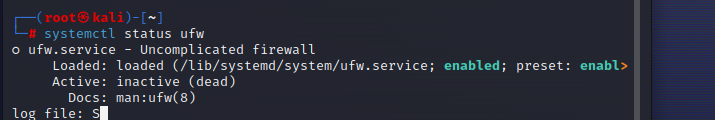
1. 安装防火墙

输入apt-get install ufw



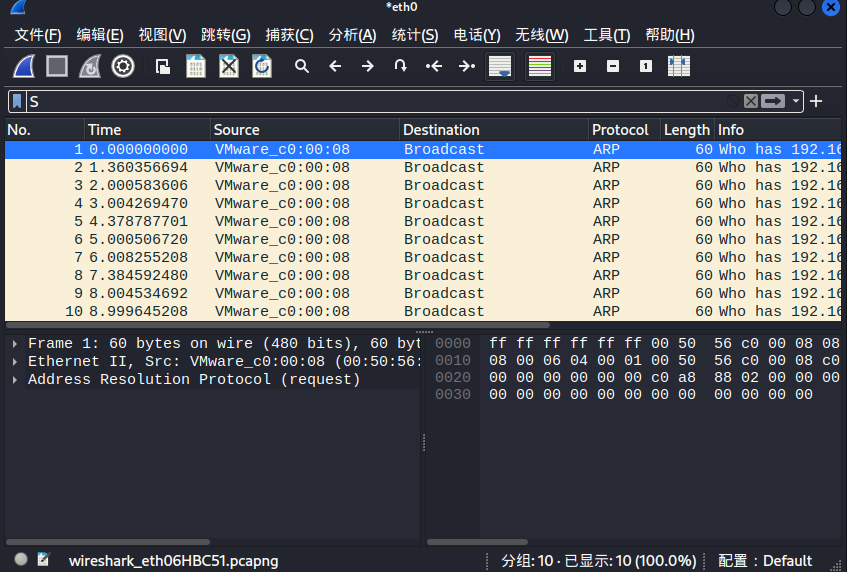
4查看防火墙状态：

输入systemctl status ufw



防火墙目前是“不复杂的”，状态为dead，防火墙现在没有开启

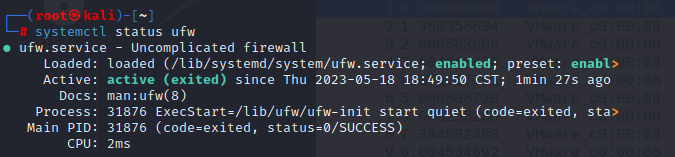
1. wireshark第一次抓包

抓的到东西

1. 开启防火墙

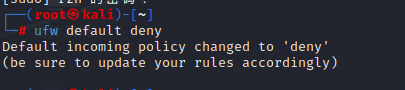
同样在root权限下输入systemctl start ufw

再次检查防火墙状态，防火墙状态变为active



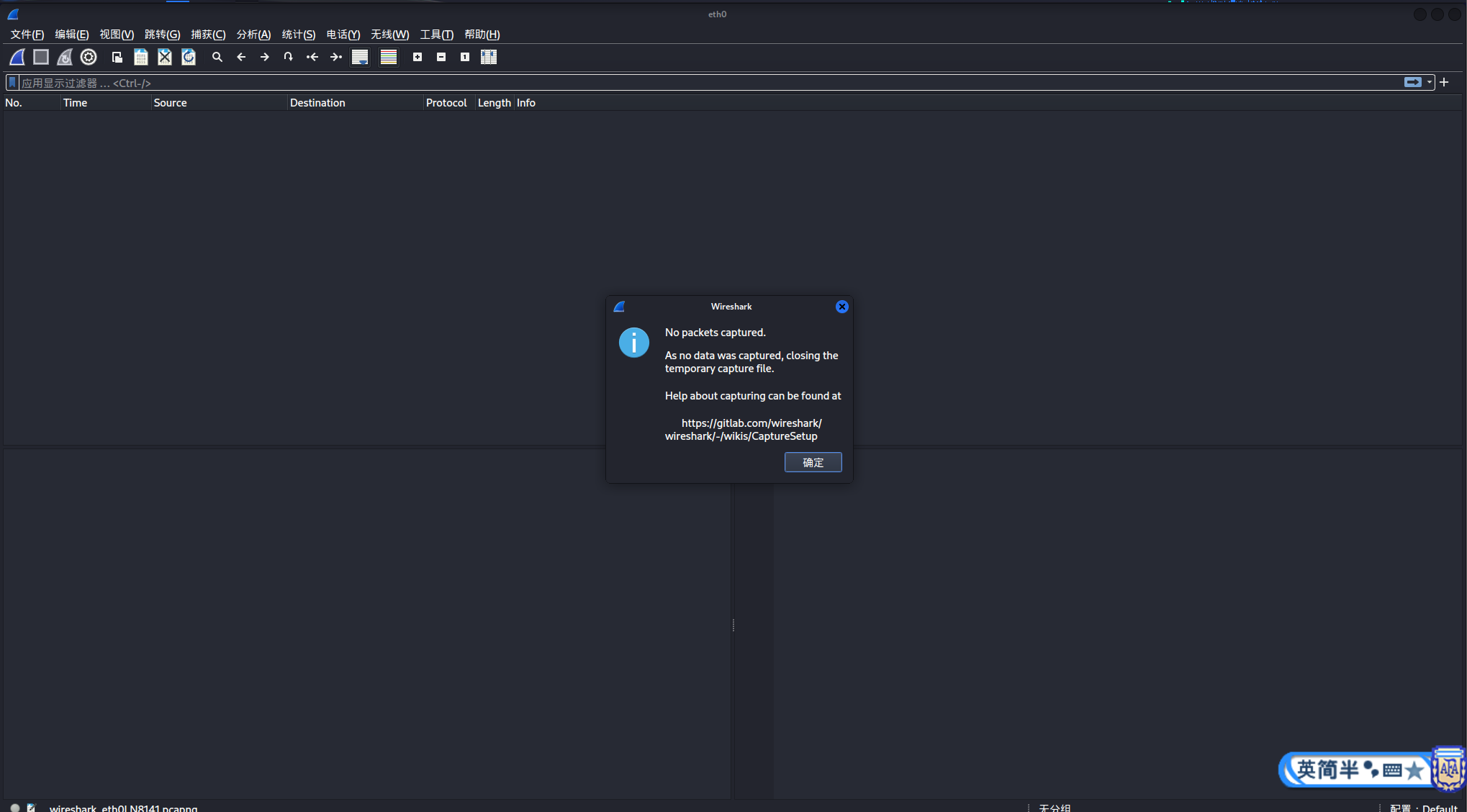
1. 阻止所有服务

输入ufw default deny



1. 再次打开wireshark，无法有效抓包





1. 其他防火墙相关

systemctl enable firewalld.service开机启用防火墙

systemctl disable firewalld.service开机禁用防火墙

systemctl stop firewalld关闭防火墙

firewall-cmd—state查看防火墙状态

firewall-cmd—reload重新加载配置

firewall-cmd—list -ports查看开放的端口

firewall-cmd—zone=public—add-port=9200/tcp—permanent开启防火墙端口