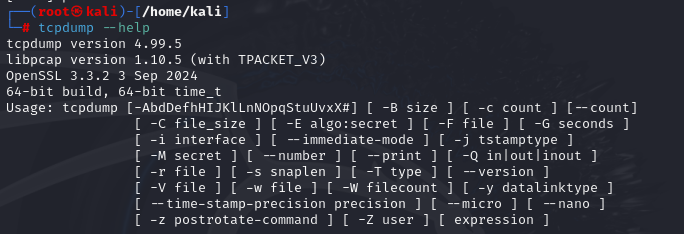
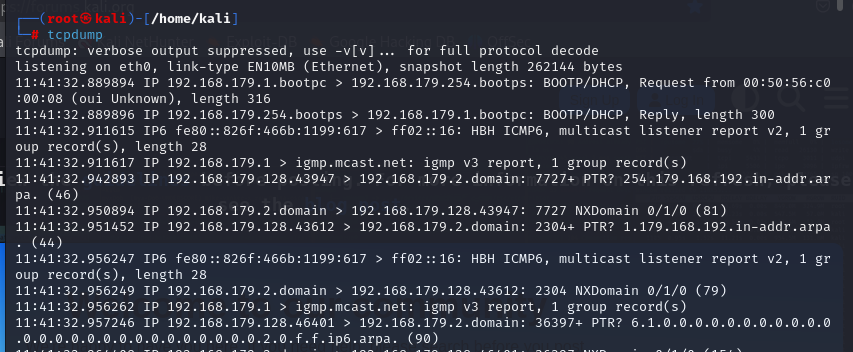
# Network monitoring(TCP dump)

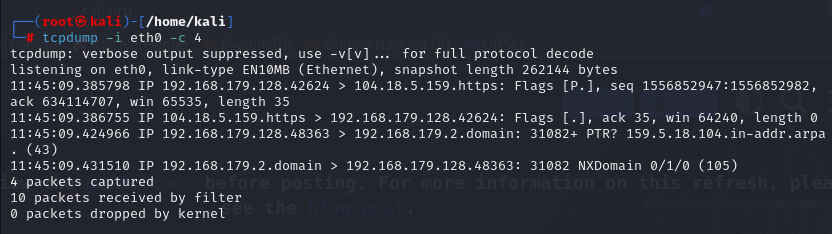
## Tcpdump –help



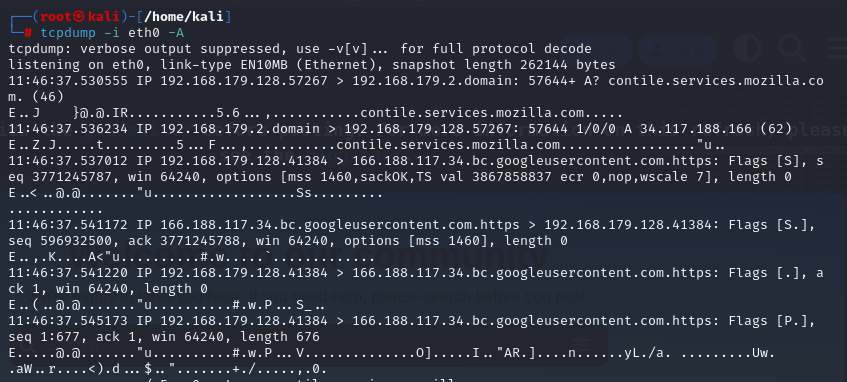
## Capture packets of current network



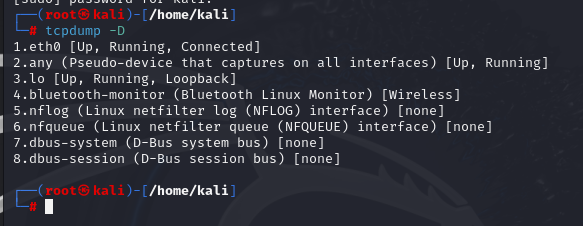
## Capture 4 packets from specific network interface



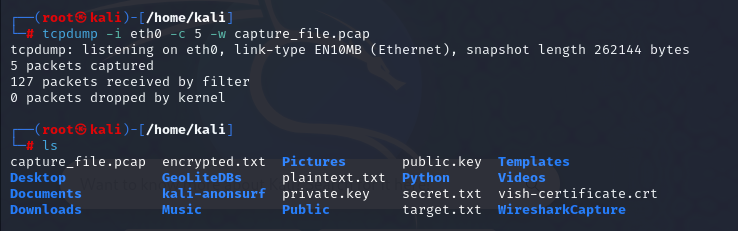
## Capture in ASCII format



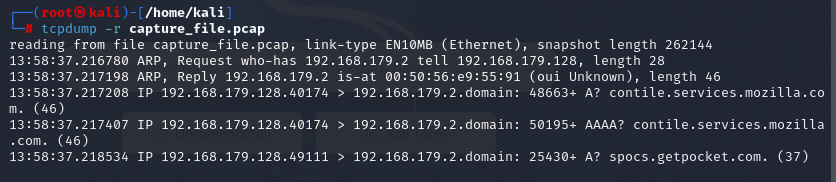
## Show available network interfaces



## Save captured packets into pcap file

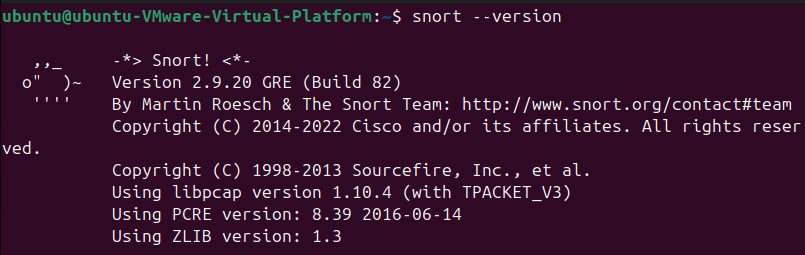


## Read from captured pcap file

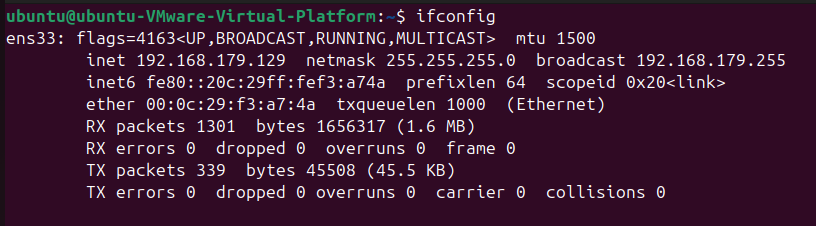


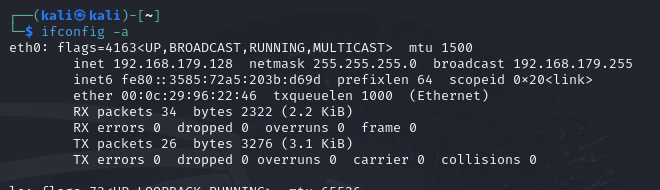
# Snort

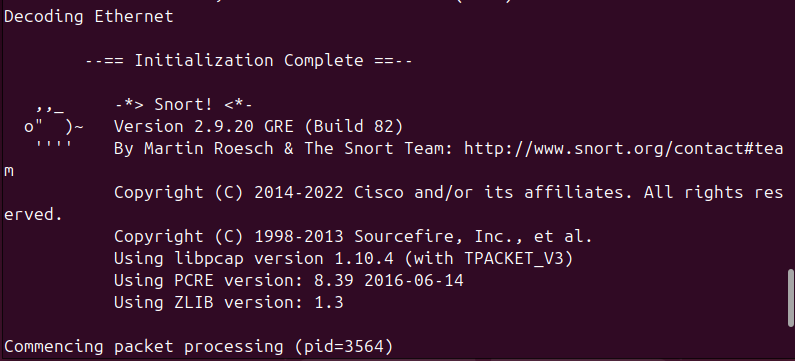
## Installation and snort version



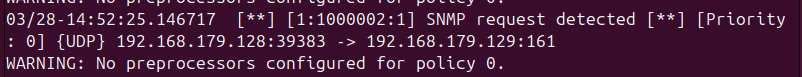
## Start snort, show IP addresses of target machine and attacker machine

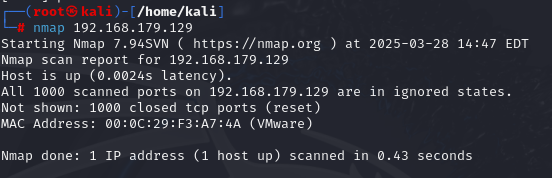




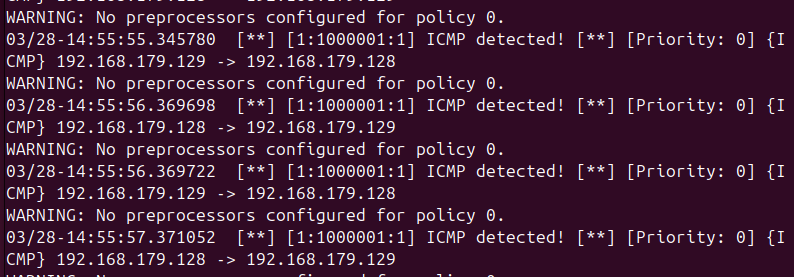


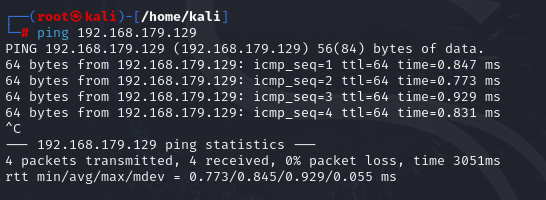
## Send SNMP message and detect it



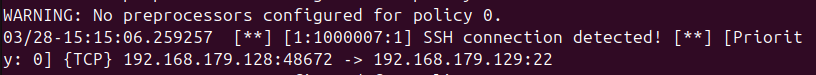


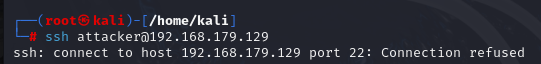
## Send ICMP message and detect



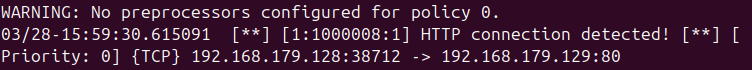


## Add SSH rule, and detect





## Add HTTP rule, and detect





## 2 sub, Show local.rules file for snort

