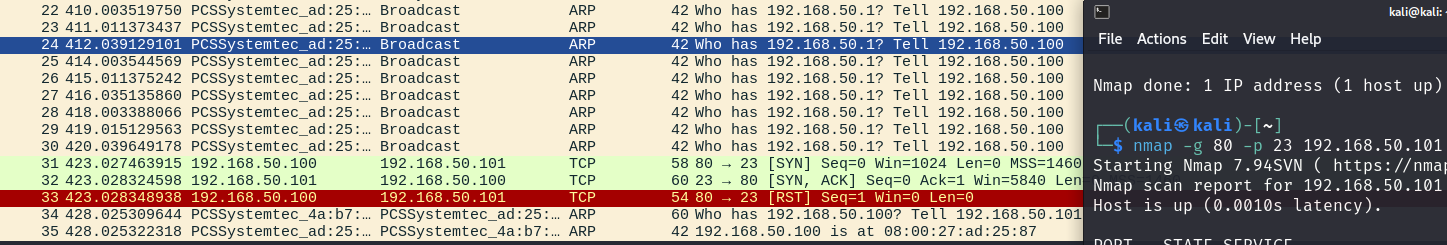
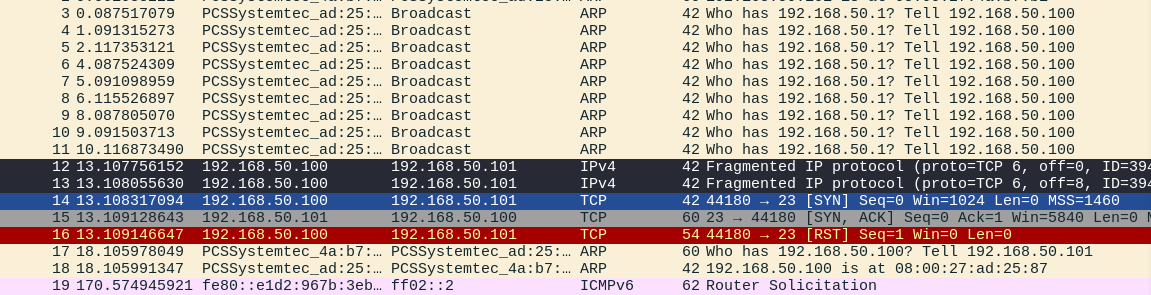
Il comando -g permette di specificare una porta di origine (80) per i pacchetti inviati durante la scansione. In questo caso verso la porta 23. Cercando ho letto che alcuni firewall permettono traffico solo da porte considerate sicure, come **53** (DNS) o **80** (HTTP). E che questo metodo di camuffa può essere utile per verificare il comportamento di un sistema target rispetto a specifiche porte di origine.

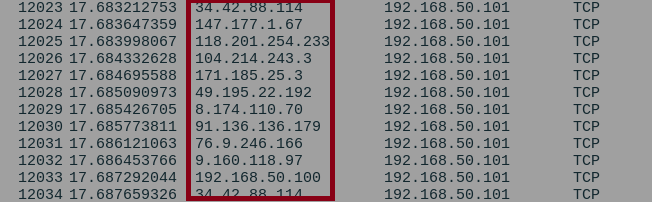


Il comando -f abilita l'uso di pacchetti frammentati durante la scansione. Cercando ho letto che questo è un metodo utilizzato per cercare di eludere i firewall, IDS o altri dispositivi di sicurezza che analizzano il traffico.



Utilizzando il comando -h acceso al menu informazioni, vediamo che il comando -D è nella stessa sezione” EVASIONE FIREWALL/ID E SPOFING” del comando -g e -f. Cercando ho letto che il comando -D consente di eseguire una scansione utilizzando indirizzi IP esca (decoy) per mascherare l'indirizzo IP sorgente

Comando utilizzato: nmap -D RND:10 192.168.50.101 = In questo caso ho creato automaticamente 10 IP esca



-p u:53,t:200

Il commando -p fa intendere che la scansione riguarda le porte di rete, ma i comandi dopo non esistono. Se lo scopo era scansionare la porta 53 e 200 il comando corretto è -p 53,200