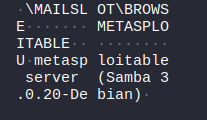
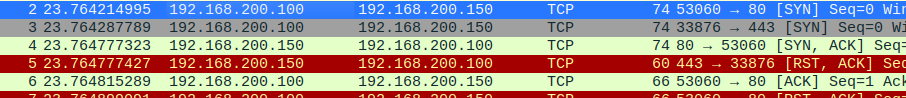
#### Analisi pacchetti con wireshark

Possiamo subito notare che l’host 150 (in questo caso METASPLOITABLE) fa un avviso in broadcast



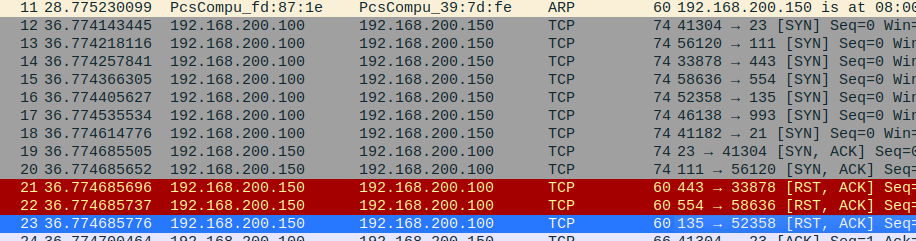
Possiamo vedere il server di samba

Poi notiamo che avviene una connessione alla porta 80 del server dal host 100



Vediamo che viene completata la triple hand shake

Andando avanti nella cattura notiamo un altra cosa interessante

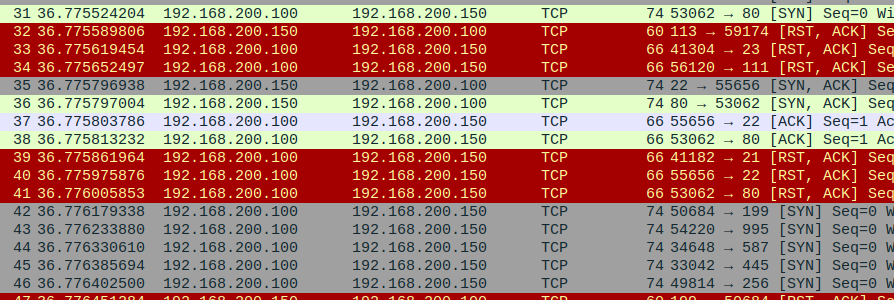


Una serie di richieste di syn dal host 100 al 150 su varie porte, potrebbe essere uno scan con nmap, vediamo che sotto è stata completata la connessione anche su queste porte

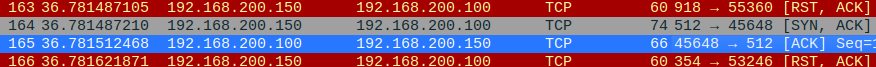


Possiamo ipotizzare che lo scan sia -sT

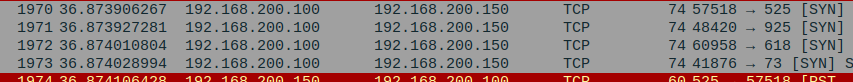
Notiamo che viene rifatta la connessione alla porta 80



Notiamo per esempio alcune porte che rispondono

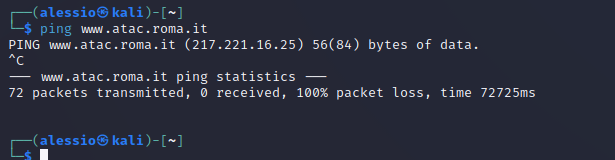


Le richieste sono quasi 2000 in poco tempo, è in questo caso quasi certo che si tratti di uno scan delle porte, vista la randomicità è probabilmente nmap



Una possibilità per ridurre il rischio di questi attacchi è filtrare le porte con il firewall facendo in modo che i ping vengano bloccati su tutte le porte che non vogliamo vengano raggiunte per eventuali servizi pubblici

#### Bonus



La pagina in questo momento non risponde, però possiamo comunque vedere il suo indirizzo ip grazie al dns