Analizzando le tabelle del traffico salvate da Wireshark si puo' dedurre che la scansione e' stata effettuata dall'attaccante con l'IP 192.168.200.100 e che le macchine comunicano nella stessa rete interna tramite un dispositivo router/switch di cui conosciamo quindi l'indirizzo di broadcast 192.168.200.255,osserviamo di fatto i protocolli TCP ed ARP sostenuti.
Osserviamo dati ottenuti come SACK_PERM tra le prime richieste riconducibile ad un three handshake(SYN,SYN,ACK),la connessione ACK fallisce...
Le prime porte prese di mira sono 80,443,mentre l'attaccante comunica dalle porte 5360,33876.
Il dato "who has 192.168.200.100? tell 192.168.200.150" ci suggerisce invece che l'attaccante sta cercando di fare il ping tra le macchine tramite una richiesta ARP cosi da rincodurre indirizzo IP ad MAC.
Nonostante i primi tentavi falliti successivamente l'attaccante riuscira' ad mettersi in ascolto sulle porte.