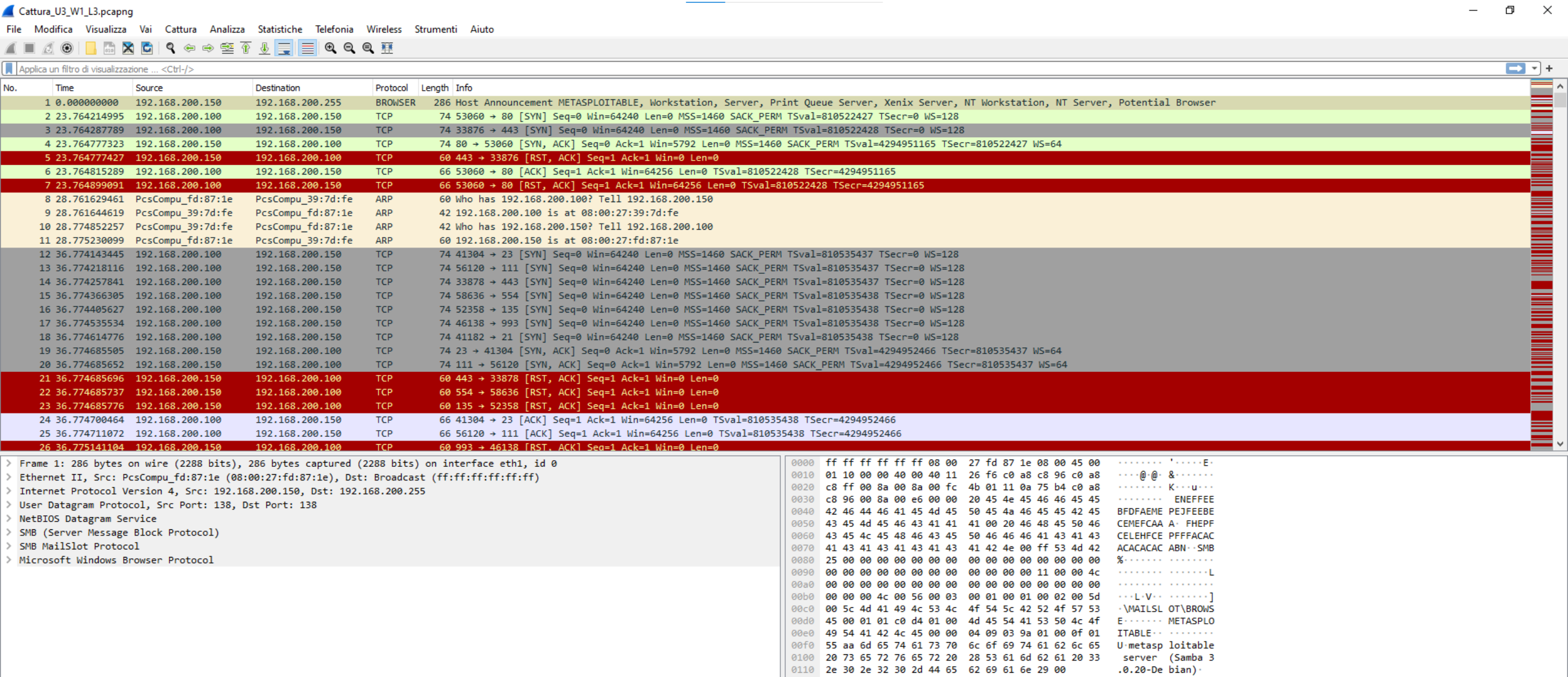
In questo esercizio bisogna riscontrare delle evidenze di un attacco in corso, ipotizzare i vettori di attacco ed infine capire che metodo utilizzare per contrastare e ridurre l'impatto di eventuali attacchi.
Possiamo subito notare svariate richieste TCP da parte dell'host che finisce in .100. Questo dovrebbe essere già un campanello d'allarme. Potrebbe essere un potenziale attacco DoS, ma investigando un po' più a fondo, la richiesta TCP sta avvenendo su più e più porte, facendoci pensare ad una probabile **scansione**.



Notando che la richiesta viene effettuata e droppata più e più volte, su porte diverse, possiamo decisamente confermare l'ipotesi di una scansione in corso.
Potremmo ovviare mettendo una policy/regola all'interno del firewall, che blocchi l'accesso a tutte le porte da parte di quell'indirizzo IP. E' comunque "good practice" chiudere l'accesso alle known ports dei servizi che non vengono utilizzati.