Per l’esercizio pratico di oggi, ho analizzato su Wireshark “Cattura_U3_W1_L3.pcapng”.

Dall'analisi del traffico catturato, emerge chiaramente un **notevole numero di richieste TCP** (SYN) indirizzate a porte differenti sul sistema di destinazione. Questa situazione suscita la congettura di un'**eventuale attività di scansione in atto** da parte dell'host 192.168.200.100 diretta verso l'host target 192.168.200.150. La validità di questa ipotesi è rafforzata dalla presenza di risposte positive da parte del target, rappresentate da [SYN+ACK], che indicano l'apertura di alcune porte, e da risposte negative, segnalate come [RST+ACK], che indicano la chiusura di altre porte.

Al fine di mitigare questa potenziale minaccia, si consiglia di **implementare delle regole nel firewall del sistema di destinazione** per respingere le richieste in arrivo dall'host 192.168.200.100. Questa misura difensiva mirerebbe a limitare ulteriori tentativi di scansione da parte di quest'ultimo, fornendo così una barriera di protezione per le porte e i servizi in ascolto, riducendo al contempo il rischio di compromissione della sicurezza del sistema.