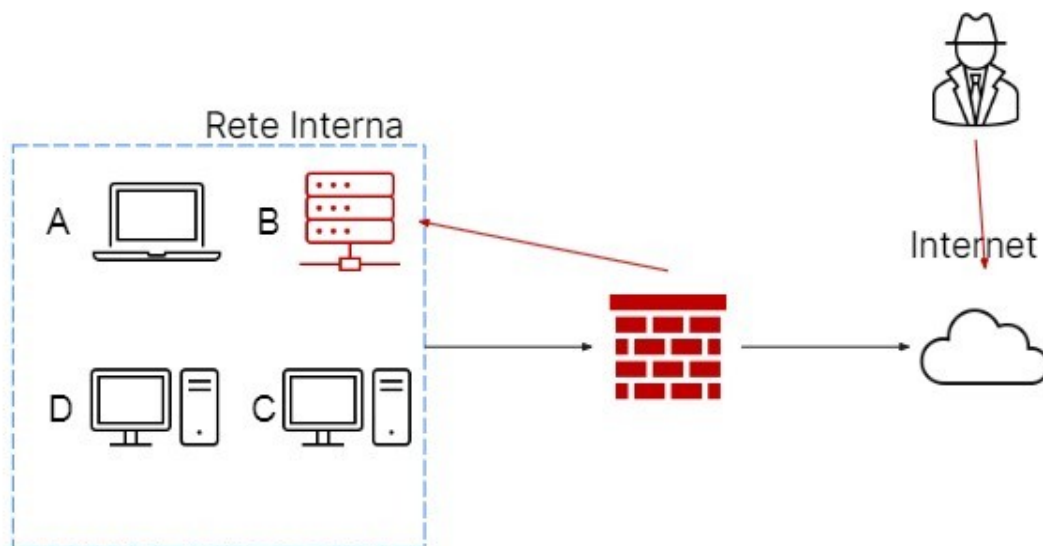


Esercizio 4 Week 1



Nell'esercizio di oggi andiamo a conoscere meglio i metodi di isolamento e rimozione dei sistemi infetti dentro una rete interna. Come possiamo osservare nel disegno il soggetto B è stato compromesso da un attaccante che è riuscito a bucare la nostra rete .

Per isolare il nostro sistema infetto possiamo adottare una tecnica chiamata **SEGMENTAZIONE**, che consiste nel creare una rete diversa dalla principale dove andremo a collocare il soggetto B, questa area prenderà il nome di "RETE DI QUARANTENA".

Nei casi più ingenti sulla rete possiamo usare la tecnica della **RIMOZIONE** che non permetterà all'attaccante di interagire con la rete interna né con la macchina infettata.

La definizione in particolare di **PURGE**, è una tecnica di recupero di un sistema infetto che consiste nella rimozione di contenuti sensibili.

Per quanto riguarda la tecnica di **DESTROY**, è una vera e propria rimozione fisica dei sistemi infetti.