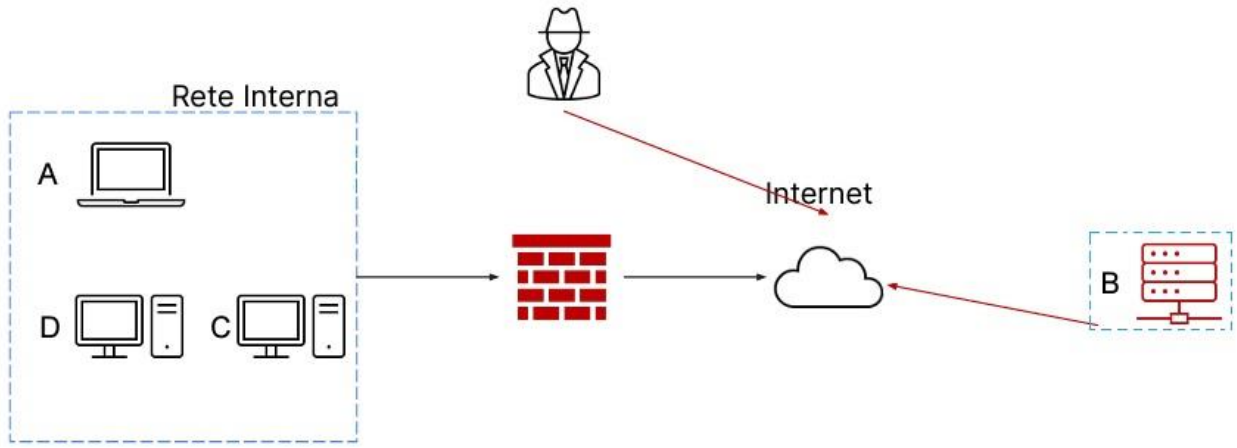
Esercizio epicode 23.11.2023

Mostrare le tecniche di: I) Isolamento II) Rimozione del sistema B infetto

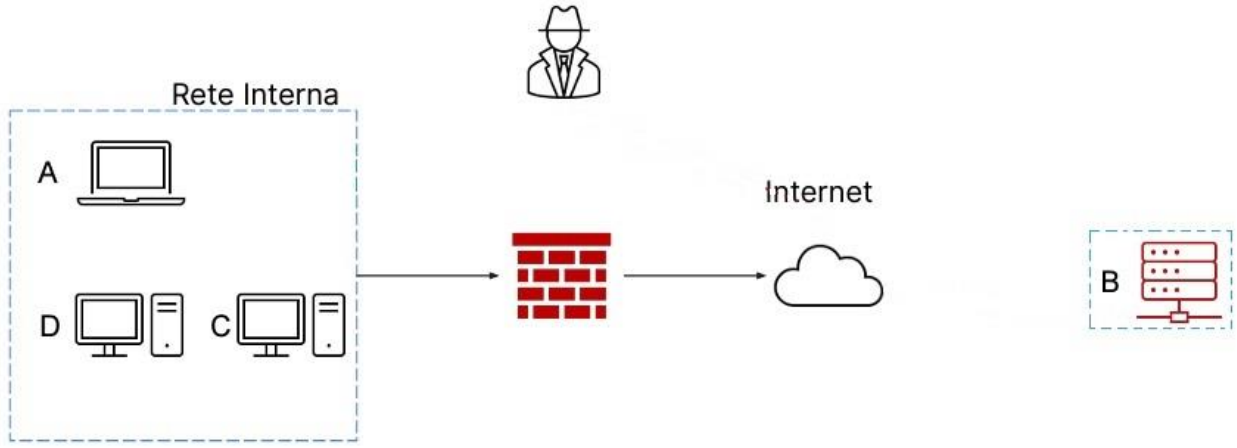
Isolamento

L'isolamento consiste nella completa disconnessione del sistema B infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante



Rimozione

Con la rimozione (Air gap) del sistema B dalla rete sia interna sia internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata



● **Purge:** si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come per esempio la ripetuta sovrascrittura del contenuto per il ripristino del dispositivo allo stato iniziale, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi

● **Destroy:** è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature.