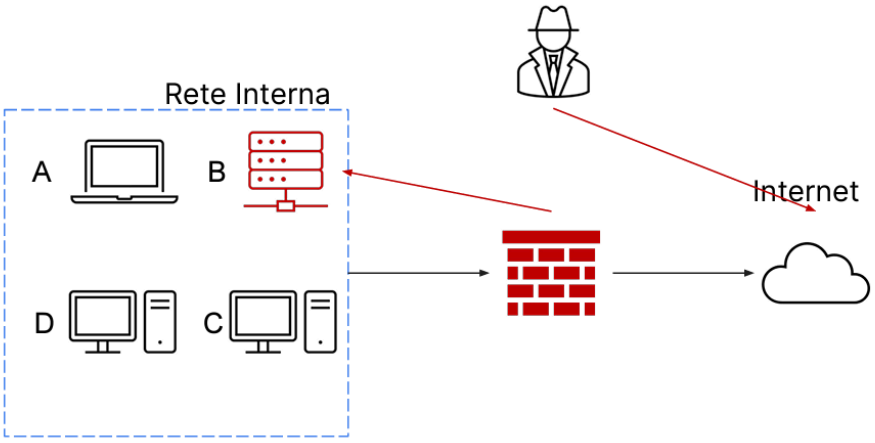
# ESERCIZIO 4 SETTIMANA 9




**Da traccia sappiamo che un criminale informatico è riuscito a compromettere il sistema B (database e dischi di storage) infiltrandosi nella rete tramite internet. Ci viene quindi chiesto di mostrare le tecniche di isolamento e rimozione del sistema B (ricordiamo che l'attacco è ancora in corso) e la differenza tra purge e destroy.**

## ISOLAMENTO

**Diamo per scontato che la rete in figura sia segmentata, se viene infettato da un malware  il sistema B possiamo isolarlo creando una rete fatta apposta che viene chiamata "rete di quarantena" così che il malware non si possa riprodurre nella rete. Con l'isolamento lo disconnetto completamente dalla rete interna ma lasciamo la connessione ad internet, questo può essere utile per studiare l'attaccante, in questo modo il sistema B diventa un vero e proprio honeypot.**

## RIMOZIONE

**Se con l'isolamento non riusciamo a risolvere il problema ci rimane la soluzione della rimozione ovvero eliminare completamente la connessione del sistema B, sia con la rete interna che con internet cosicché l'attaccante non abbia accesso né alla rete interna né alla macchina infetta.**

## PURGE

**Si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.**

## DESTROY

**Ovvero 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. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.**

## CLEAR

**Il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.**