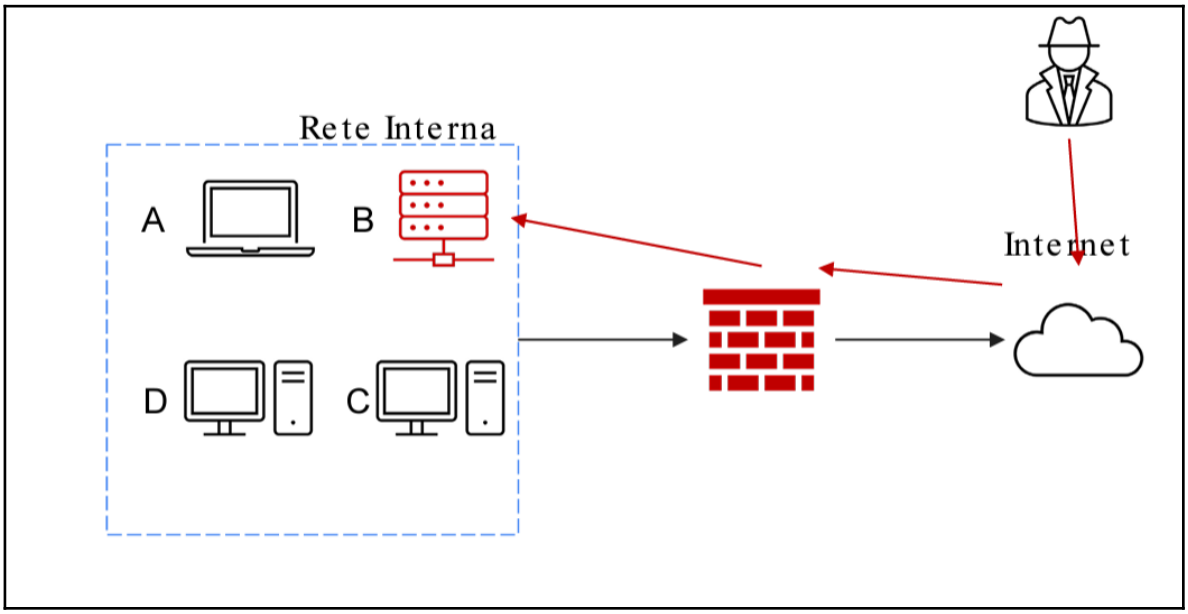
PRATICA S9-L4

TRACCIA: Un sistema B è stato compromesso interamente da un attacante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

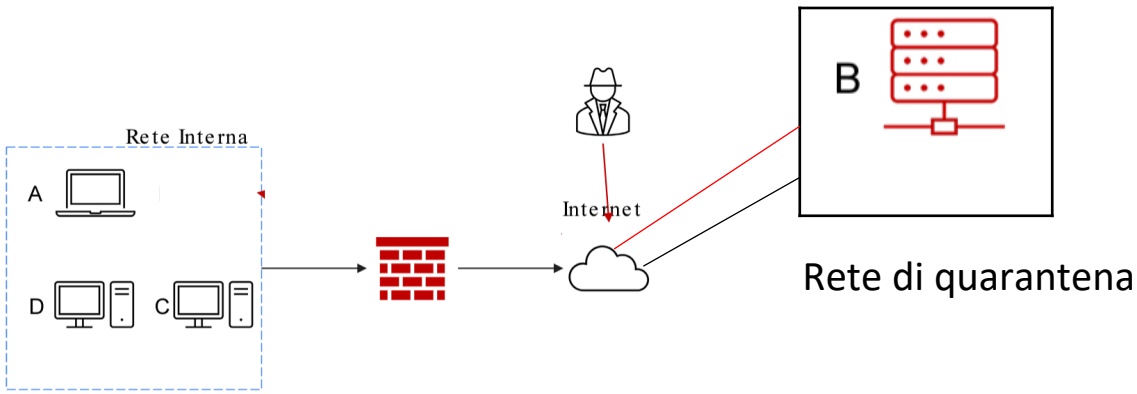
Risponderemo a seguenti quesiti:

-Mostrare le tehniche di: isolamento e rimozione del sistema B.

-spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.indicheremo anche clear.



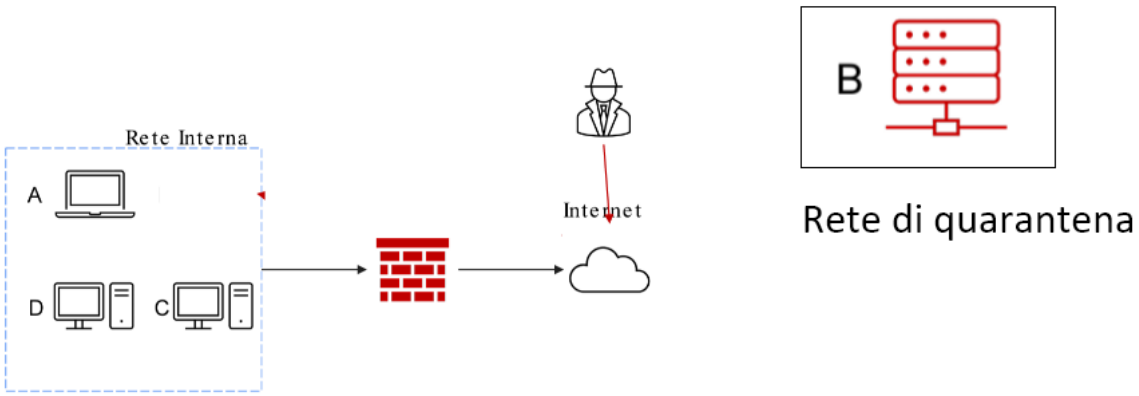
1-) Mostriamo le tehniche di: isolamento e rimozione del sistema B.



PRATICA S9-L4

L'isolamento,consiste nella completa disconnessione del sistema infetto dalla rete per restringe ancora maggiormente l'accesso alla rete interna da parte dell'attacante ,quindi partendo della sua definizione come possiamo vedere sull'imagine sopra abbiamo isolato il 'sistema B',togliendolo della rete interna e metendolo in quarantena.

Tuttavia quest'azione in questo caso non risolve il problema,visto che il sistema è sempre conesso ad Internet e l'attacante anche; quindi può continuare l'attacco.per risolvere questo problema abbiamo proceduto con la **RIMOZIONE** che consiste a disconettere complettamente il sistema B da internet come possiamo vedere sull'imagine qua sotto:



In questo caso l'attaccante non ha più accesso al "sistema B".

2-)-spiegare la differenza tra Purge e Destroy e clear per l'eliminazione delle informazioni.

Clear: permette di pulire completamente il dispositivo con techniche logiche,togliendo contenuti sensibili.

Purge: in più di togliere dei contenuti sensibili,utilizza dei forti magneti per rendere le informazioni inaccessibile su determinati dispositivi.

Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili, oltre ai meccanismi logici e fisici utilizzato da

PRATICA S9-L4

clear e purge,Destroy utilizza techniche di laboratorio come disintegrazione,polverizzazione dei media ad alte temperature,trapazione.

E visto che il sistema B è stato compromesso interamente dobbiamo utilizzare **Destroy** per lo smaltimento dei dati compromessi. Ma tuttavia questa soluzione costa molto.