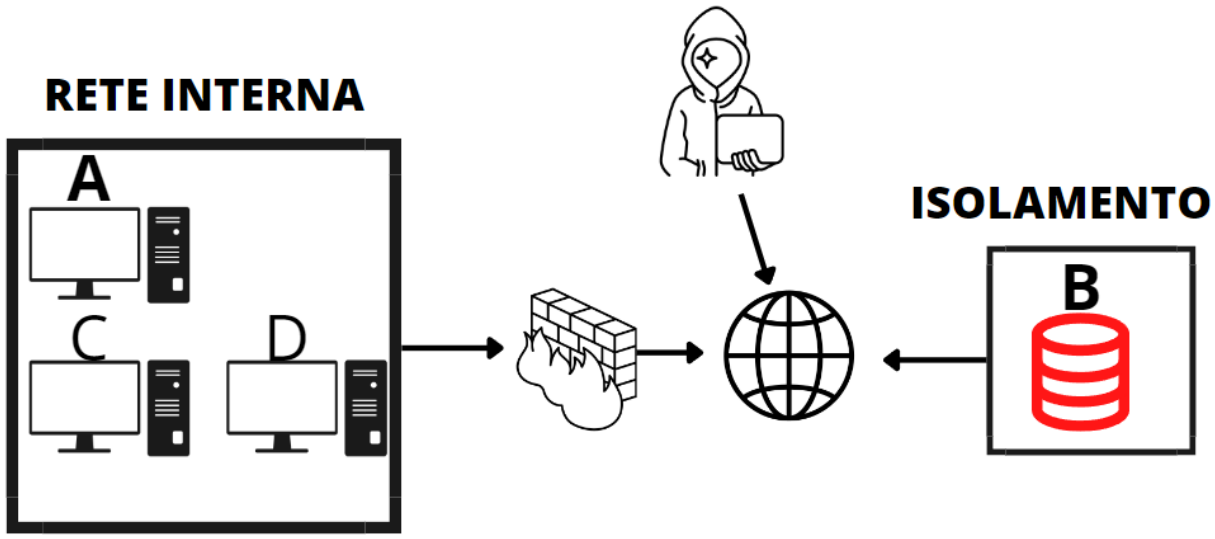
CUORE ANDREA

22/12/2022

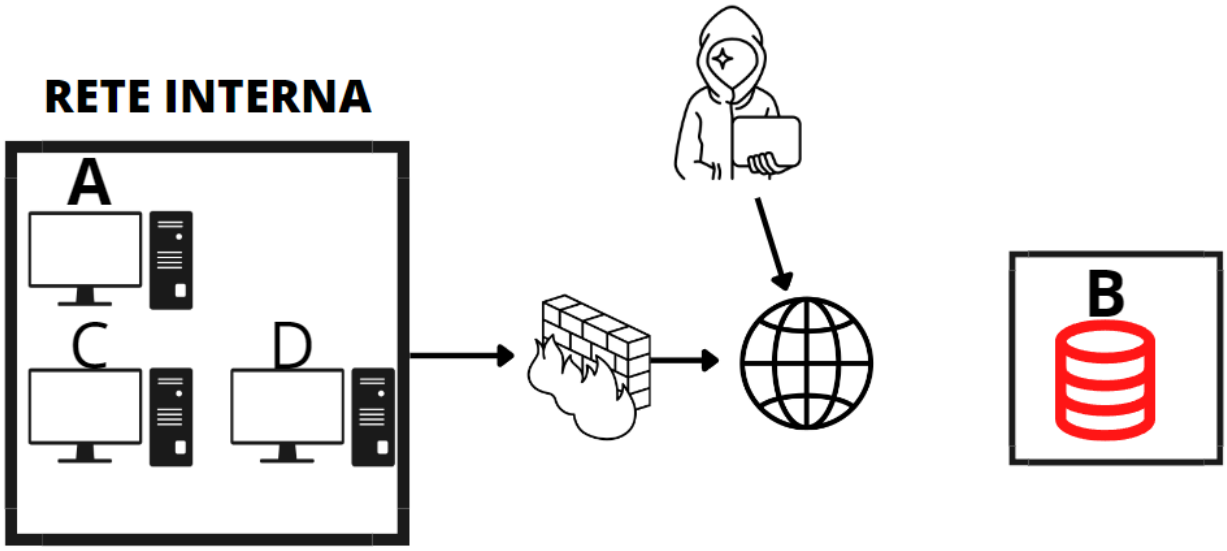
ISOLAMENTO E RIMOZIONE DEL SISTEMA INFETTO

ISOLAMENTO:



Nel nostro metodo di isolamento abbiamo provveduto appunto ad isolare il database infetto dalla rete interna per evitare di infettare le altre macchine, ma è stato lasciato sulla linea internet in modo tale che possa funzionare da honeypot, cercando cosi di reperire qualche informazione dell'attaccante.

RIMOZIONE:



Dopo aver raccolto informazioni sufficienti sull'attaccante siamo andati a togliere il sistema infetto dalla linea cosi l'attaccante non potrà più averne accesso.

FASE DI RECUPERO:

Al termine di tali operazioni ci ritroviamo a mettere in sicurezza il database andando a correggere i dischi infetti.

Durante questa fase di recupero dobbiamo adottare delle azioni in merito alla gestione dei media contenenti informazioni sensibili che possono essere:

- Clear: Il sistema viene completamente ripulito dal suo contenuto con tecniche <<logiche>> tipo il sovrascrivere più volte il disco (read and write) oppure si utilizza il factory reset.
- Purge: Si adotta non solo l'approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili
- Destroy: Questo è l'approccio più netto, oltre alle tecniche logiche e fisiche come abbiamo appena visto si utilizzano anche tecniche da laboratorio come la disintegrazione, polverizzazione dei media ad alte temperature. Per ovvie ragioni questo metodo risulta il più efficacie e rende il ripristino delle informazioni impossibile.