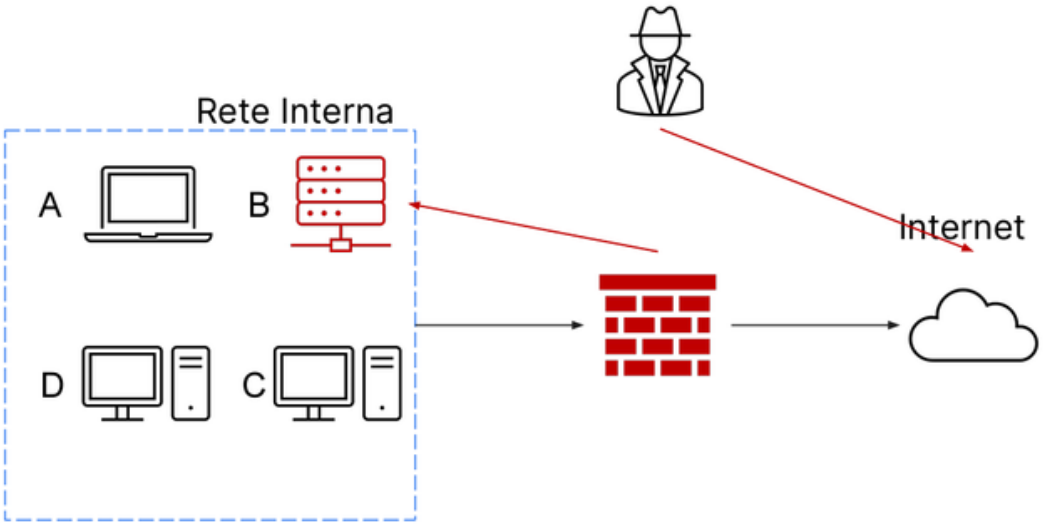
S9/L4

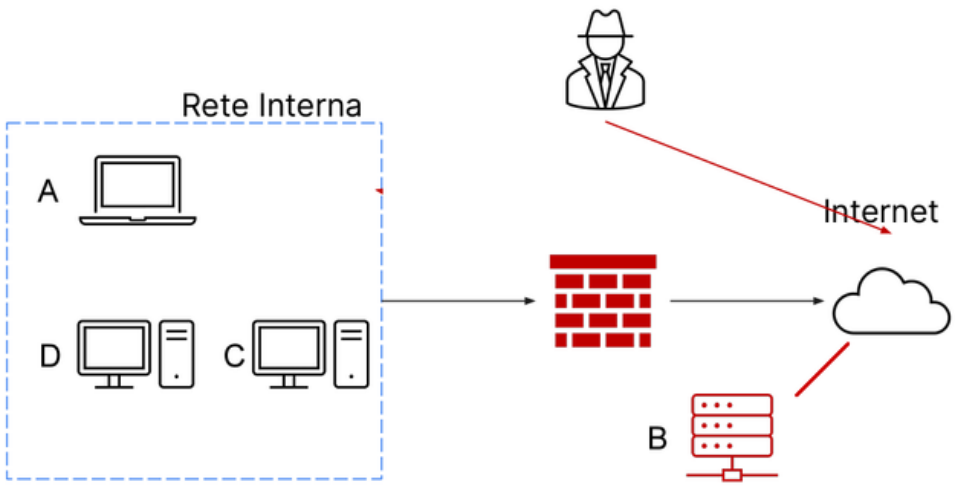


Nell'esercizio di oggi andremo a rispondere ad un attacco attualmente in corso come riportato in figura.
Come possiamo vedere il sistema B è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

Possiamo utilizzare due tecniche per ridurre gli impatti causati dall'incidente:

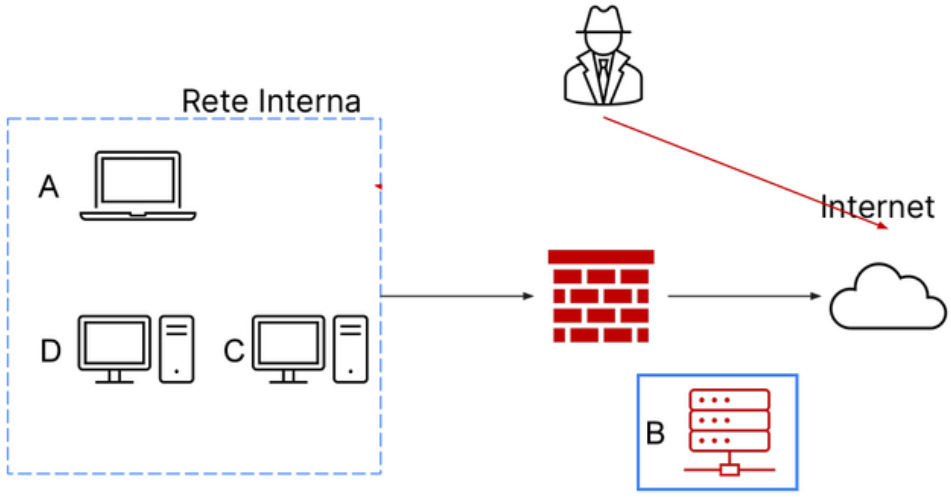
- ISOLAMENTO

In questo caso si provvede ad isolare il sistema compromesso B dalla rete interna per evitare di compromettere le altre macchine, ma l'attaccante ha ancora accesso al sistema B tramite internet



- RIMOZIONE

In questo caso se l'isolamento non è sufficente si provvede alla completa rimozione del sistema infetto sia dalla rete interna che dalla rete internet.
In questo modo l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.



FASE DI RECUPERO

Terminata questa fase andremo a mettere in sicurezza il database andando a correggiere i dischi infetti.
Durante questa fase dobbiamo adottare delle azioni in merito alla gestione dei media contenenti informazioni sensibili che possono essere:

- Purge

Si effettua una pulizia profonda e completa del sistema, assicurandosi che i dati eliminati siano praticamente irrecuperabili ricorrendo all'uso tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili.

- Destroy

Si distrugge completamente il dispositivo utilizzando tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature.