Traccia:

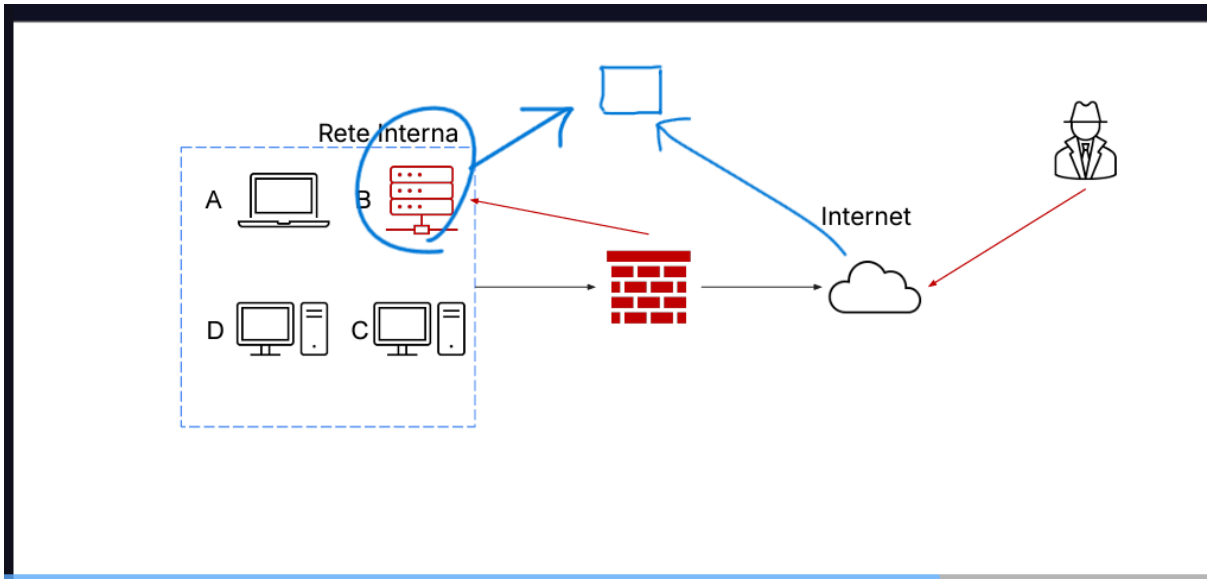
Con riferimento alla figura nella prossima slide, il sistema **B (un database con diversi dischi per lo storage)** è stato compromesso interamente da un attaccante che è riuscito a bucare la rete e accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

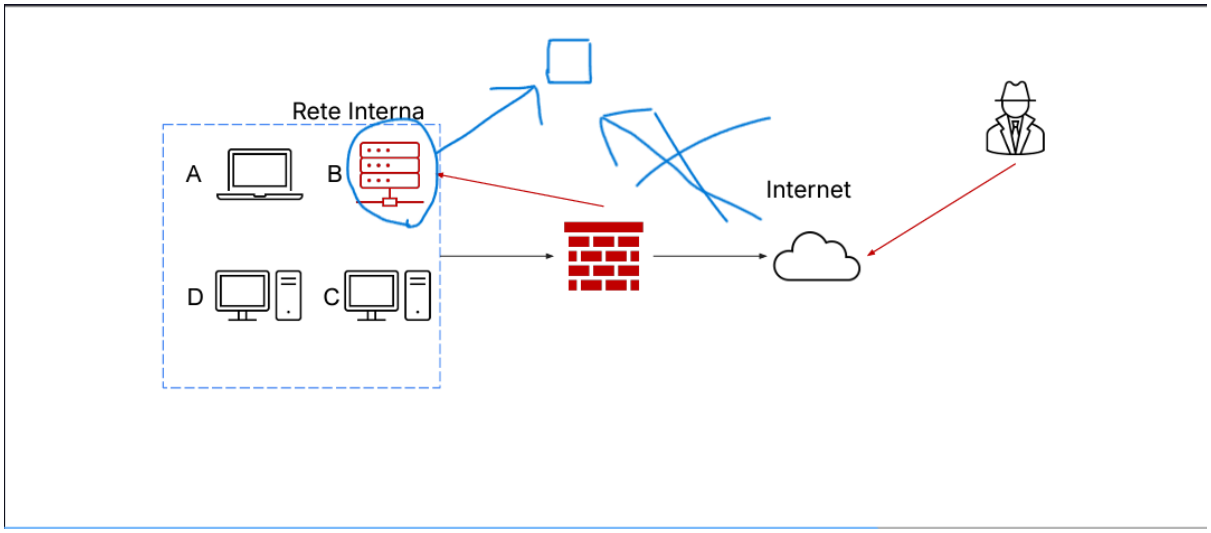
- Mostrate le tecniche di: I) **Isolamento** II) **Rimozione** del sistema **B infetto**
- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. **Indicare anche Clear**

ISOLAMENTO



ISOLAMENTO: Permette di isolare un sistema infetto dal resto della rete, per limitare i danni e l'accesso a un attaccante alla rete interna. Tuttavia il sistema infetto è ancora raggiungibile dall'attaccante.

RIMOZIONE



RIMOZIONE: Questa tecnica elimina completamente il sistema infetto dalla rete, rendedolo inaccessibile sia da internet che dalla rete interna, diventerà inaccessibile pure all'attaccante

PURGE: per Purge si intende l'eliminazione permanente dei dati su un disco più sul logico che sul fisico, tuttavia le tecniche fisiche utilizzte non sono invasive

DESTROY: per Destroy si utilizzano tecniche molto invasive a livello fisico,che prevedono la distruzione a livello hardware,rendendolo non più recuperabile