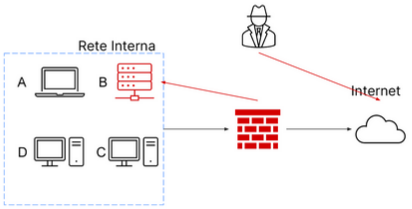
Esercizio S9L4

Traccia:

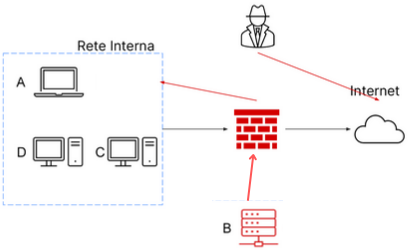


Con riferimento alla figura in slide 4, il sistema **B (un database con diversi dischi per lo storage)** è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

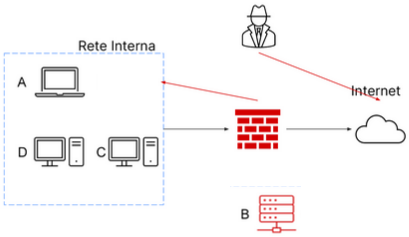
- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema **B infetto**
- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Isolamento



Nell'isolamento il sistema B infetto avrà accesso solo all'internet e rispetto alla quarantena non verrà controllato/monitorato.

Rimozione



Nella rimozione il sistema B infetto non avrà accesso né alla rete interna né a internet quindi per poter inviare dati al sistema B bisogna usare il metodo air-gap che prevede il trasporto dei dati fisicamente tramite chiavette USB

Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche dove il contenuto viene sovrascritto più volte o si riporta il dispositivo nello stato iniziale(factory reset).

Purge: adotta un approccio logico e tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy: Oltre ai meccanismi logici e fisici, utilizza tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature ma questo comporta un costo maggiore rispetto ad altri opzioni .

La differenza tra Purge e Destroy sta nel tipo di metodo che si utilizza per rendere il contenuto inaccessibile e il costo per eseguire questi metodi.