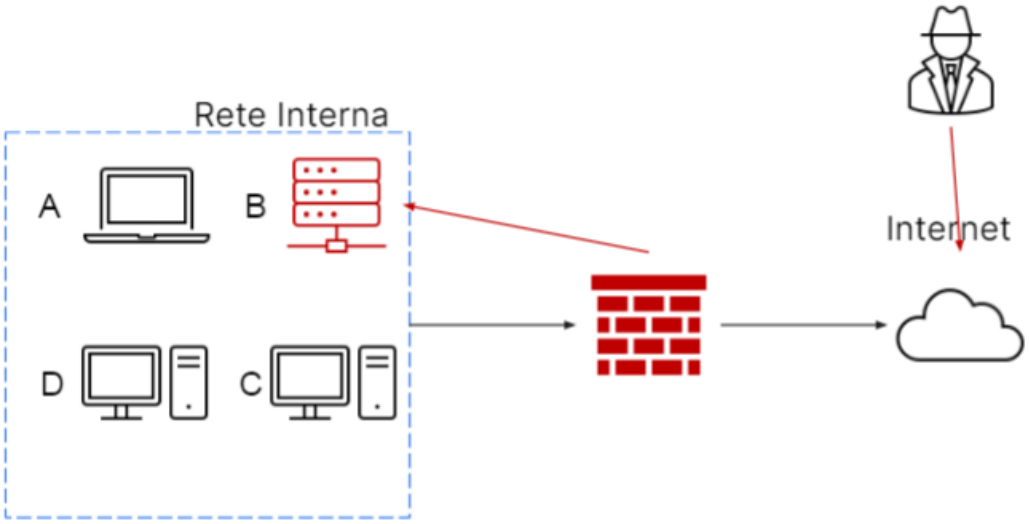
Esercizio 23-03

Traccia: con riferimento alla figura qua sotto, 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.

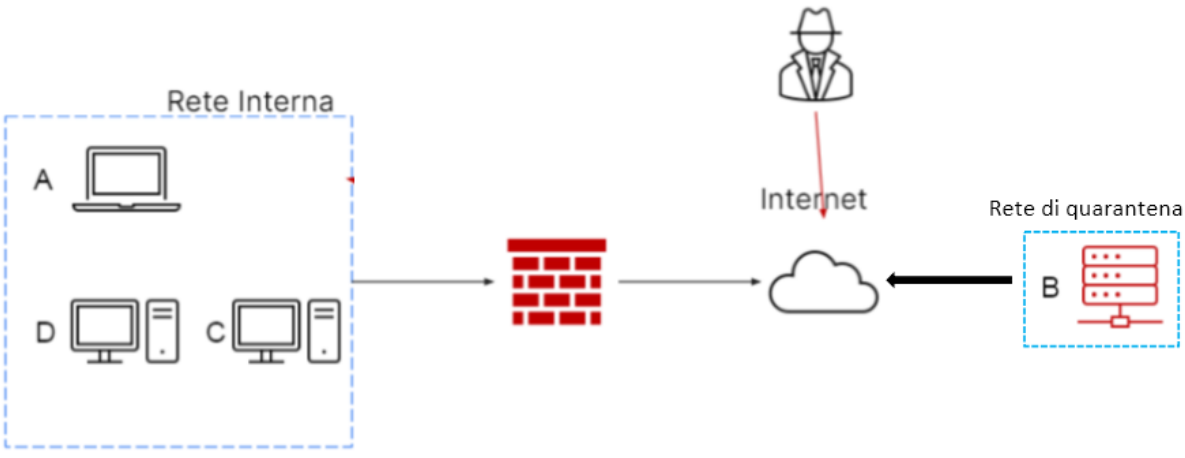
Rispondere ai seguenti quesiti:

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



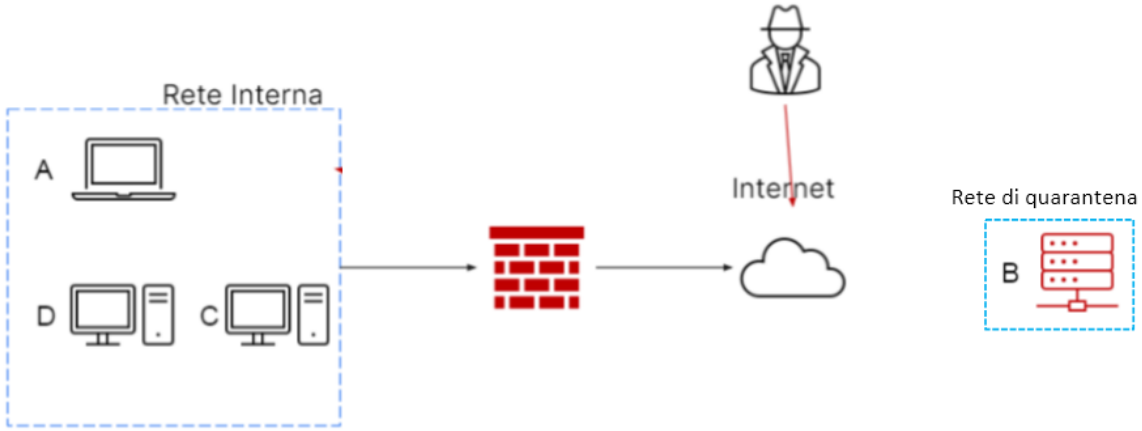
Isolamento

Con la tecnica dell'isolamento, rappresentata sotto, si ottiene un contenimento maggiore rispetto alla tecnica di segmentazione della rete. La tecnica di isolamento è caratterizzata dalla completa disconnessione del sistemo infetto dalla rete, per restringere ancora di più le possibilità di accesso dell'attaccante alla rete interna. Con questa tecnica l'attaccante ha ancora accesso al sistema infetto.



Rimozione

Con la tecnica della rimozione, rappresentata sotto, si ottiene la completa rimozione del sistema dalla rete internet e dalla rete interna. Con questa tecnica l'attaccante non avrà accesso né alla rete interna né al database infettato.



Spiegazione delle tecniche di gestione dei media contenenti informazioni sensibili

Purge

Questa tecnica ha lo scopo di eliminare le informazioni che sarebbero altrimenti recuperabili. I metodi convenzionali includono la smagnetizzazione (per i supporti magnetici) e la cancellazione crittografica, dove i dati sono crittografati, per sanificare la chiave di crittografia anzichè i dati correlati. Clear non garantisce la resistenza agli attacchi di laboratorio, mentre Purge sì.

Destroy

Questa tecnica, oltre a rendere irrecuperabili i dati contenuti dall'hardware, rende anche inutilizzabile l'hardware stesso attraverso metodi come l'incenerimento, la polverizzazione e la trapanazione. È il metodo più sicuro che rendere irreperibili dei dati, ma è anche quello meno economico.

Clear

Questa tecnica sanifica sovrascrivendo i dati contenuti con dati ripetitivi (es. tutti zeri) o il ripristino di un dispositivo alle impostazioni di fabbrica: queste vengono dette tecniche "logiche".

La scelta della tipologia di tecnica da utilizzare dipende dalla classificazione dei dati contenuti.