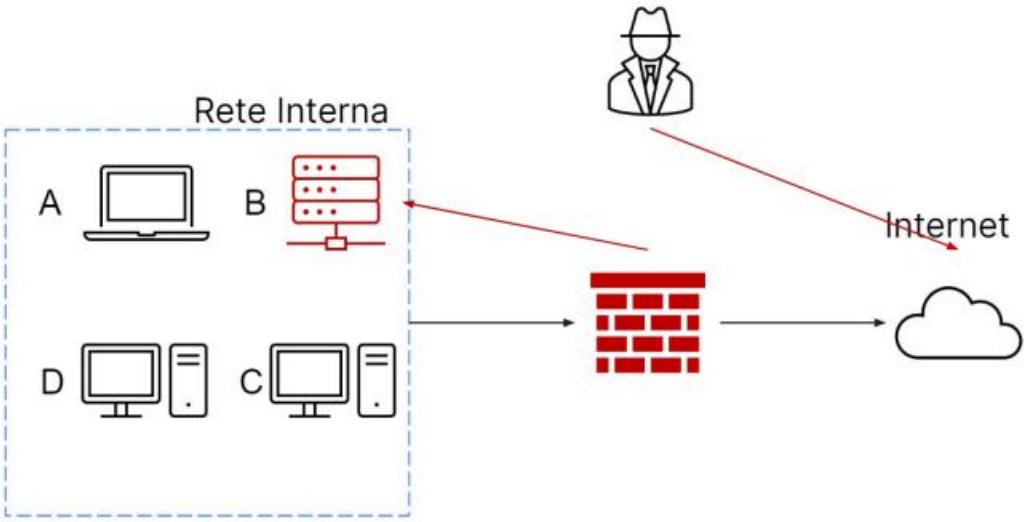
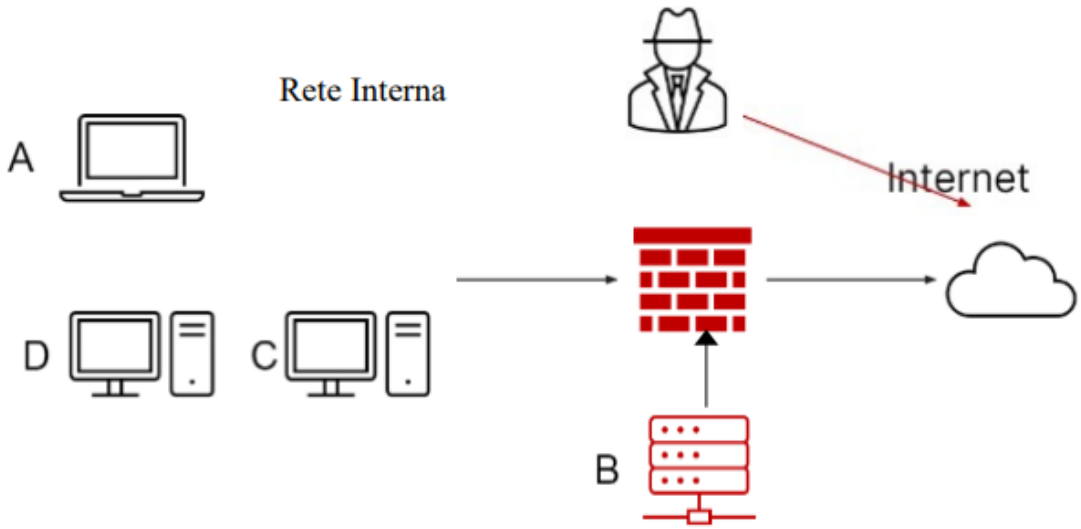
Report Incident Response

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

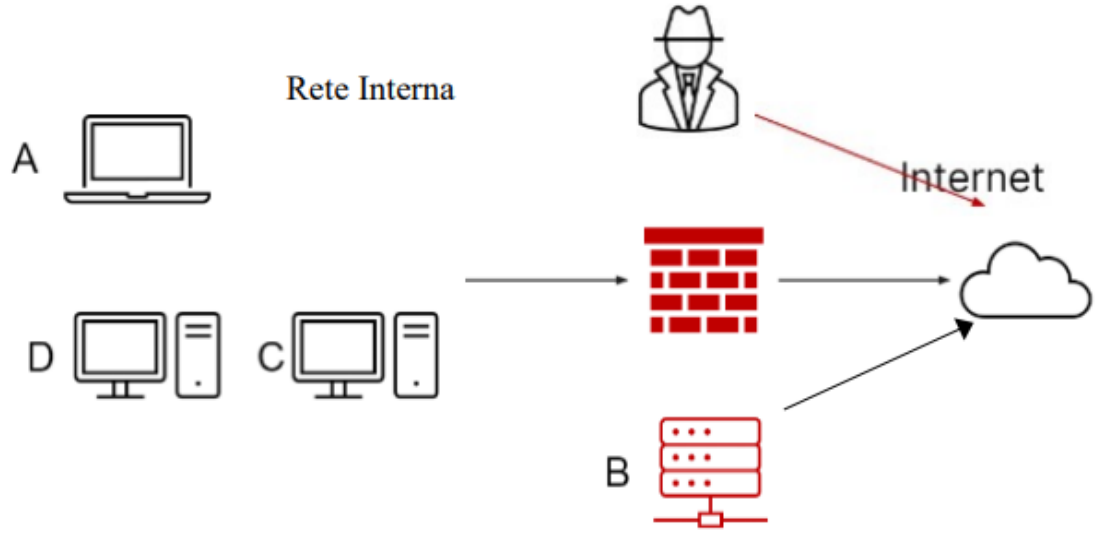


Possiamo utilizzare due metodi per isolare un sistema infetto.
Di seguito possiamo vedere il primo, cioè quello di estromettere il sistema infetto dalla rete interna mettendolo in quarantena.

Metodo 1:

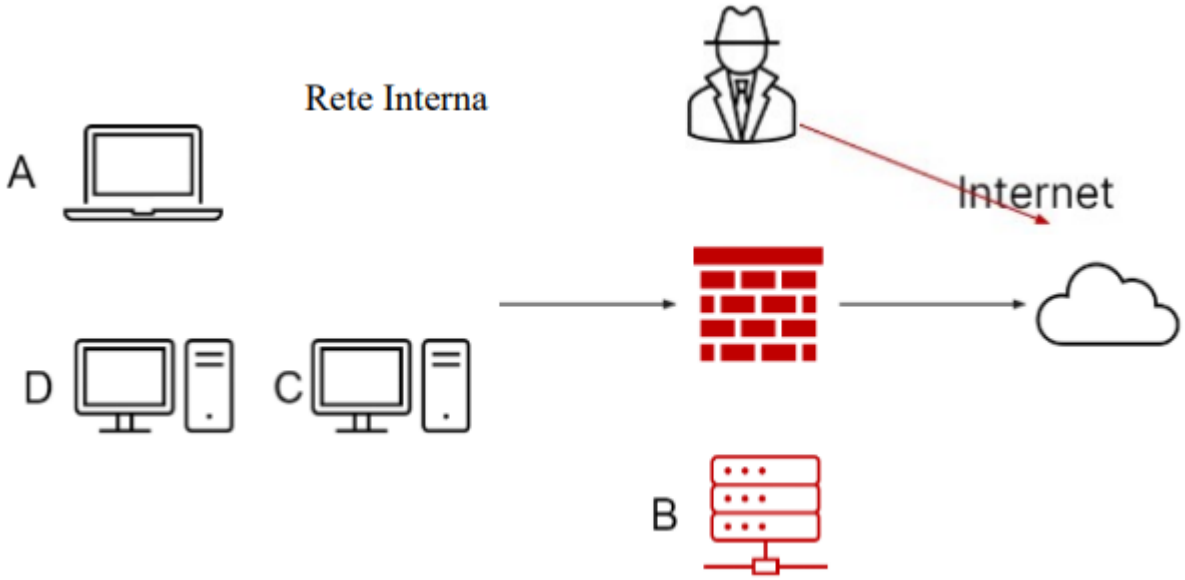


Metodo 2:



In caso l'isolamento non basti l'ultimo metodo è quello di estromettere completamente il sistema scollegandolo in modo fisico (e non) dalle reti aziendali, quindi negandogli l'accesso sia alla rete interna che a quella internet.

Eliminazione sistema infetto:



Per concludere, le distinzioni principali tra Clear, Purge e Destroy risiedono nel trattamento del dispositivo. Esaminando il Clear, si adotta un approccio di lettura e scrittura, sovra-scrivendo il contenuto più volte, con un massimo di sette cicli, oppure si utilizza la funzione di ripristino alle impostazioni di fabbrica. D'altra parte, nel caso del Purge, si impiega un approccio simile al Clear, ma con l'aggiunta di tecniche fisiche, come l'uso di potenti magneti per rendere inaccessibili le informazioni. Infine, con il metodo Destroy, il dispositivo viene direttamente danneggiato o distrutto, ad esempio attraverso il trapanamento. Sebbene questo metodo sia il più efficace nel rendere le informazioni inaccessibili, comporta costi significativi e uno sforzo maggiore.