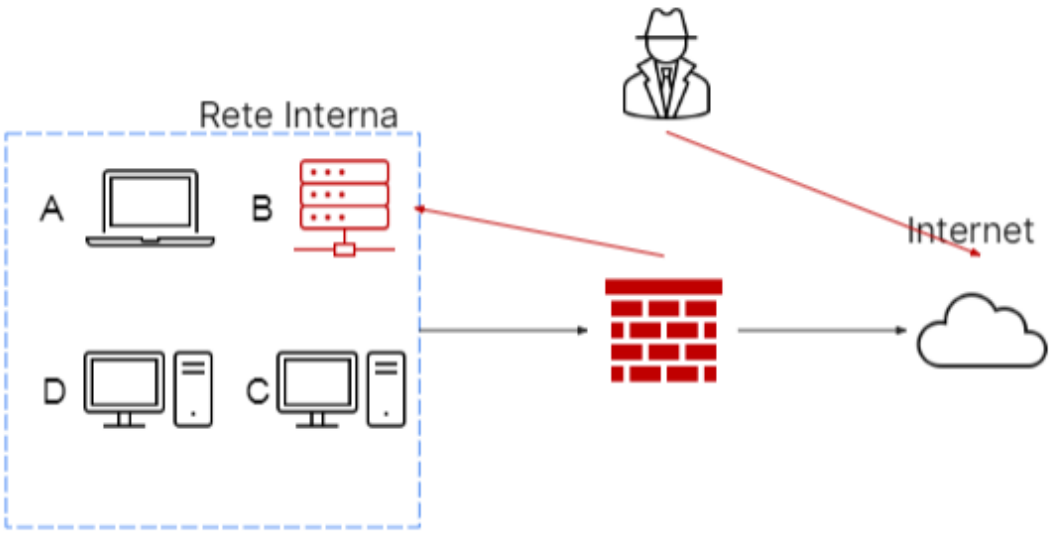
INCIDENT RESPONSE



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.

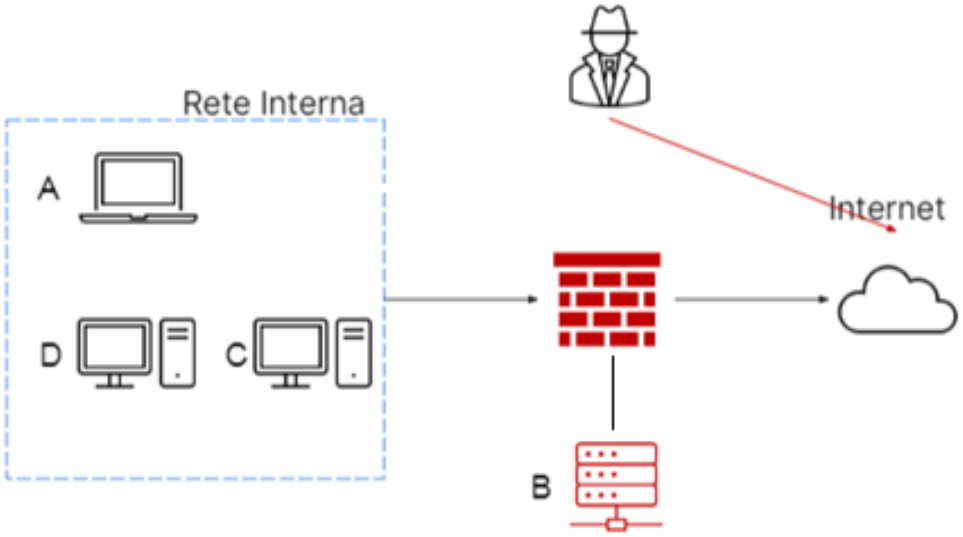
Rispondere ai seguenti quesiti.

- 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. **Indicare anche Clear**

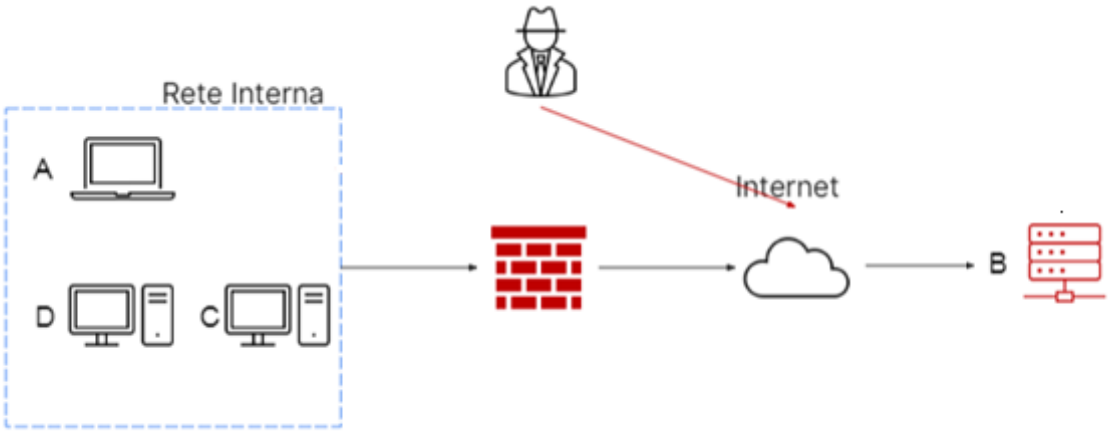
Lo scopo dell'esercitazione è quella di mostrare come intervenire in caso di attacco in corso su uno dei nostri sistemi.

Come primo step, è necessario, una volta identificato l'attacco, contenere i danni che potrebbero essere causati; possiamo operare in più modi:

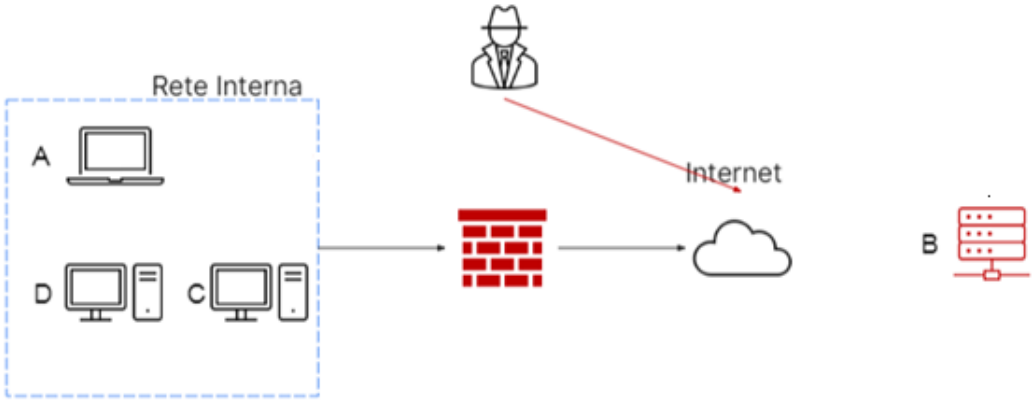
Segmentazione, che consiste nel separare una rete in più LAN/VLAN in modo da creare una rete chiamata di quarantena che permette di bloccare il propagarsi del malware sul resto del network:



Isolamento, cioè la completa disconnessione del sistema infetto dalla rete che garantisce un contenimento maggiore rispetto alla segmentazione:



Rimozione, letteralmente togliere il sistema infettato da qualsiasi rete, che sia interna o internet:



Essendo il sistema compromesso un database con dischi per lo storage, dobbiamo accertarci durante la fase di recupero che le informazioni al loro interno siano ancora accessibili o meno; nel caso non lo fossero, dovremmo passare allo smaltimento che può avvenire, generalmente, in tre modi:

Clear, soluzione con tecniche logiche, cioè pulizia del disco per riportarlo allo stato iniziale o sovrascrittura dei dati;

Purge, approccio sia logico che fisico, cioè rimozione/sovrascrittura dei dati oppure ad esempio utilizzo di magneti per rendere inaccessibili le informazioni;

Destroy, l'approccio più radicale che utilizza tecniche di laboratorio per disintegrare/polverizzare i dispositivi da smaltire; è il sistema più efficace ma comporta sforzi economici maggiori.