Esercizio S9-L4

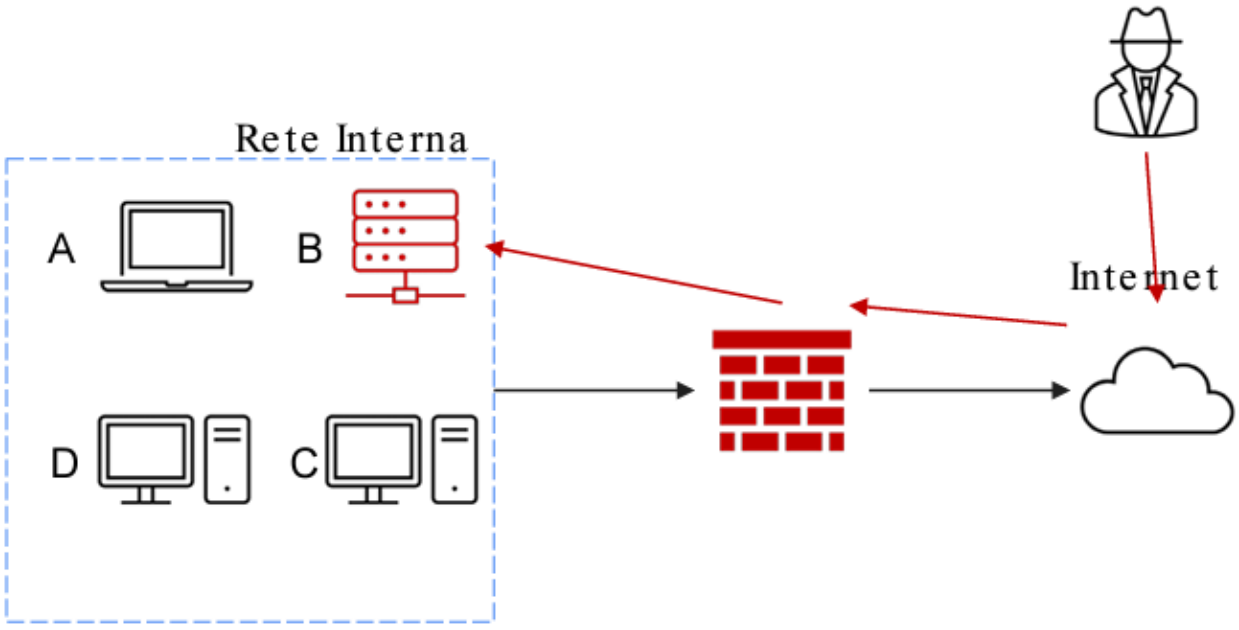
Traccia:

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:

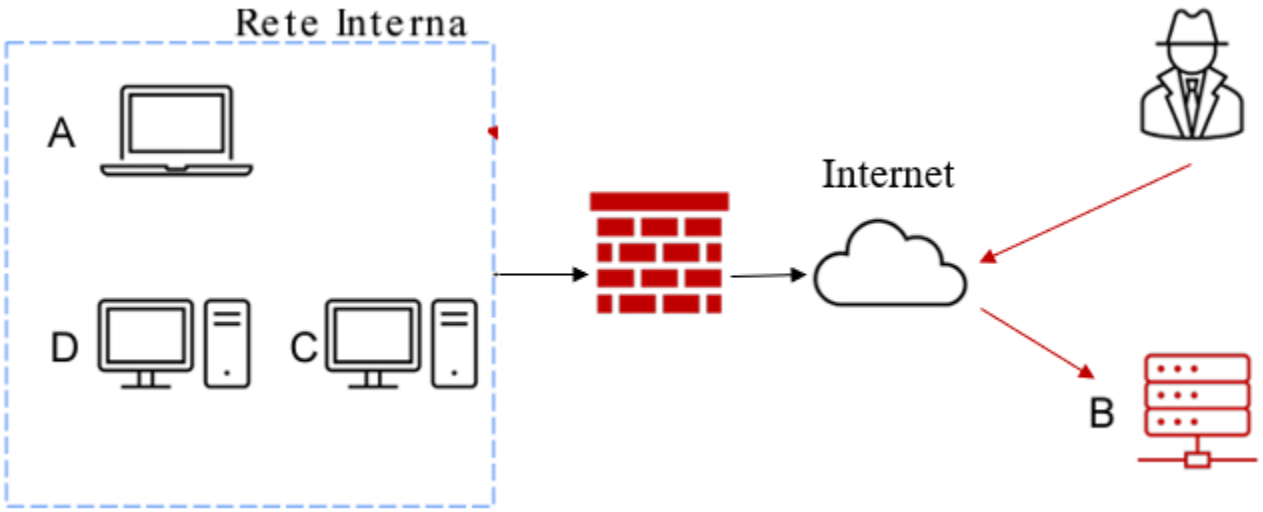
• Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto;

• Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



Tecniche ti contenimento:

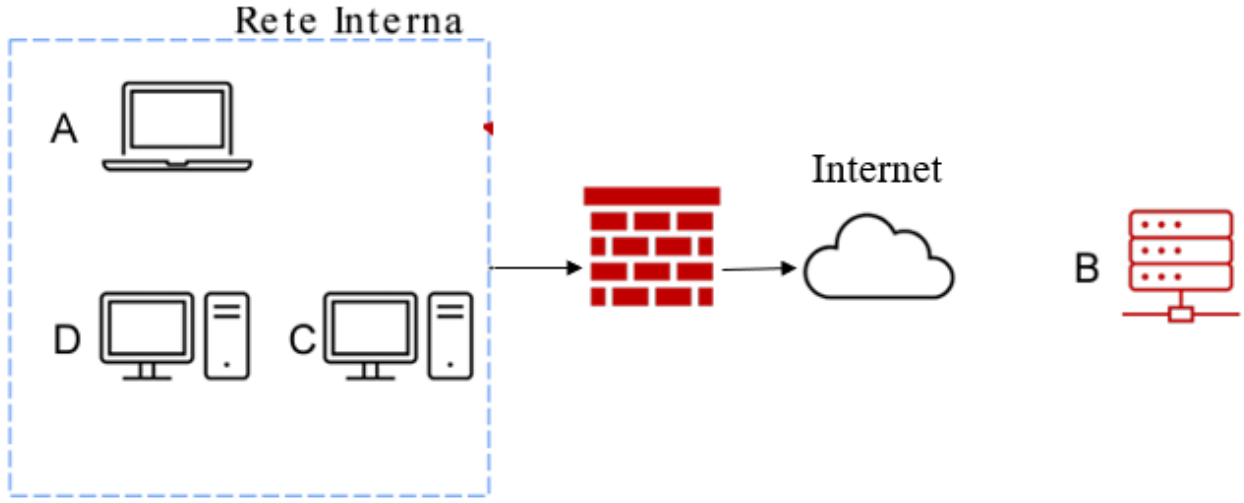
ISOLAMENTO:



Il dispositivo infetto B viene isolato dalla rete interna per evitare danni ulteriori.

Esercizio S9-L4

RIMOZIONE:



Il dispositivo infetto viene rimosso direttamente dalla rete così l'attaccante non ha più accesso e si possono intraprendere azioni di recupero.

Fase di recupero:

Ci sono vari metodi per recuperare un disco fisico e tra questi troviamo:

Purge: Elimina i dati in modo sicuro usando sia tecniche come quelle del "Clear" (sovrascrittura o reset di fabbrica), sia tecniche di rimozione fisica come la smagnetizzazione, senza però distruggere fisicamente il supporto.

Destroy: Distrugge fisicamente il supporto utilizzando metodi come la disintegrazione, polverizzazione o trapanazione, rendendo i dati irrecuperabili ma con un impatto significativo sull'economia.

Clear: Elimina i dati tramite sovrascrittura o reset di fabbrica, ma non garantisce la loro irrecuperabilità completa come nel caso di Purge o Destroy.