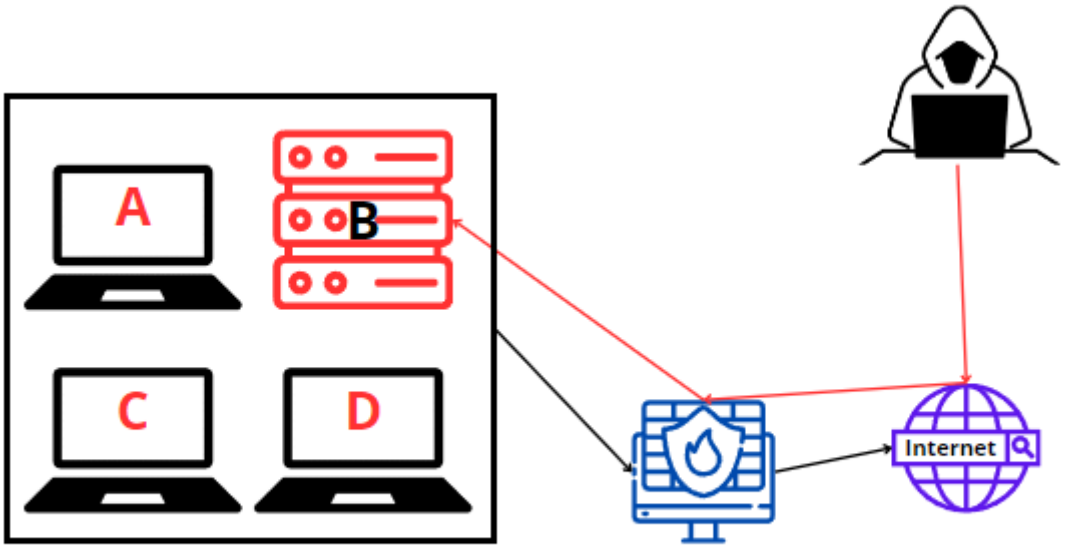
Traccia:
Con riferimento alla figura sotto, il sistema **B (un database con diversi dischi per lo storage)** è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di **CSIRT**.

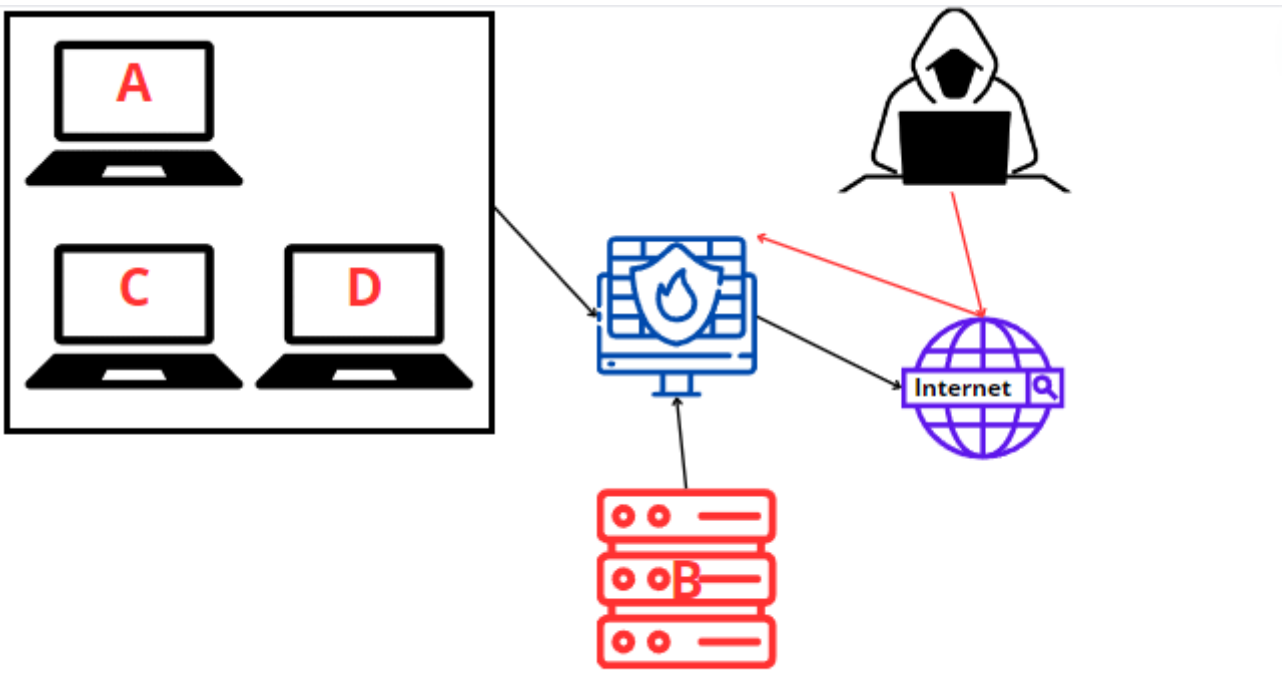
Figura



Rispondere ai seguenti quesiti:

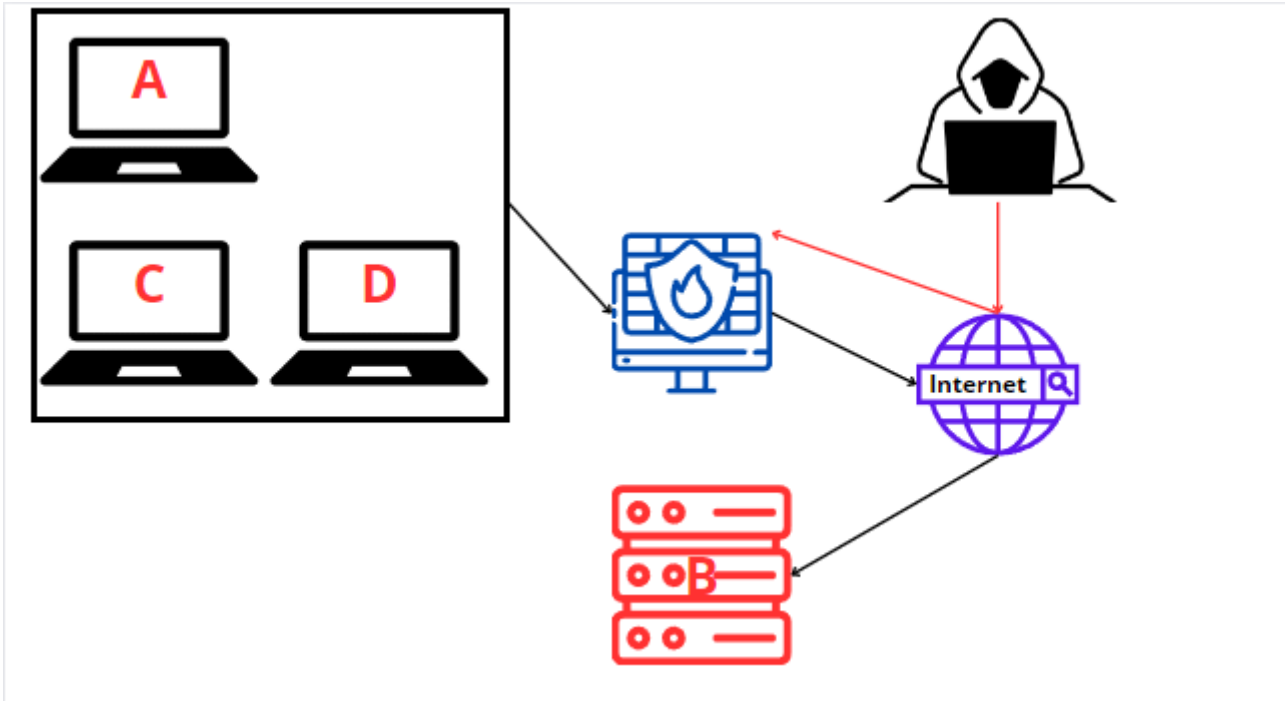
• Mostrate le tecniche di:
- Isolamento

Quarantena



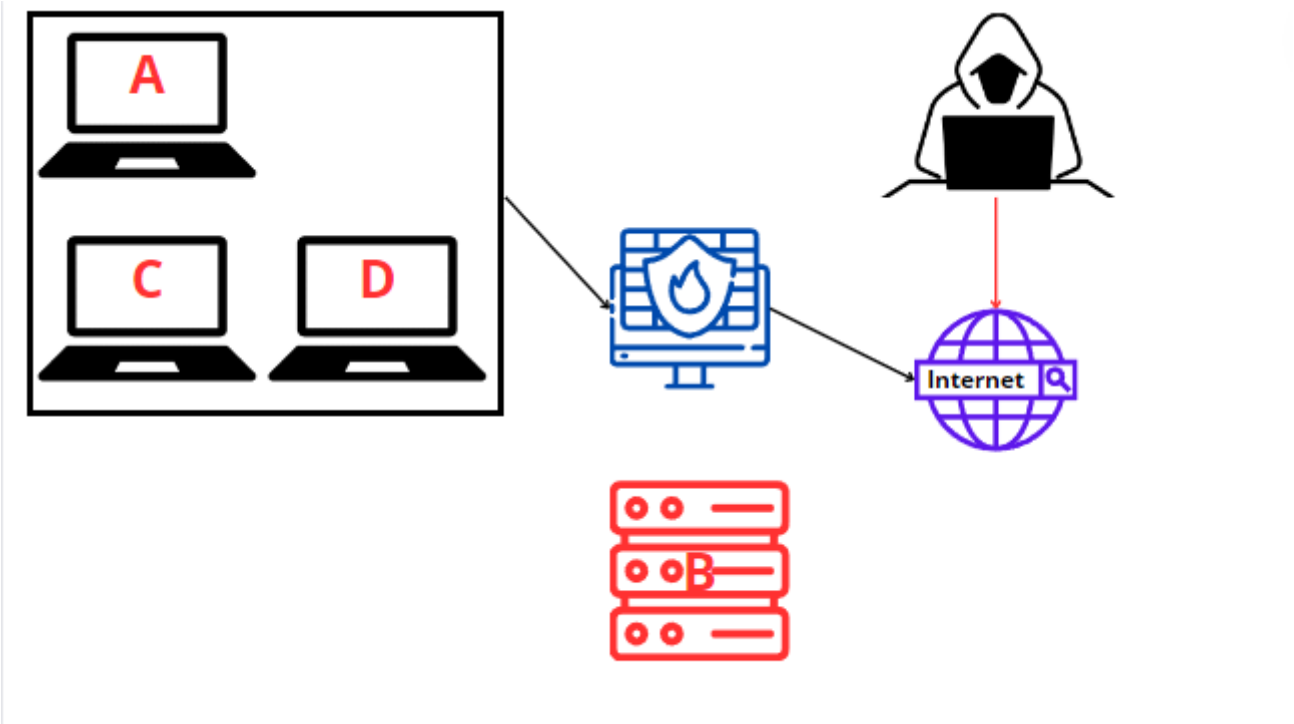
In questo modo l'Hacker non riuscirebbe ad intrufolarsi all'interno degli altri dispositivi.

Isolamento



L'Hacker rimarrebbe totalmente isolato dal resto della rete interna.

- Rimozione del sistema B infetto



L'Hacker non avrà né accesso alla rete interna né alla macchina infettata.

• Spiegate la differenza tra le seguenti tecniche di smaltimento o riutilizzo di un disco o sistema di storage:

- **Clear**: Tecnica logica dove si applicano comandi, tecniche e strumenti di lettura/scrittura per sovrascrivere i dati presenti in tutte le posizioni di archiviazione. Utilizzata per Floppy Disk, HDD, SSD, USB etc.
- **Purge**: Tecnica sia logica (come Clear) che fisica, tramite l'utilizzo di potenti magneti.
- **Destroy**: Rende impossibile il recupero dei dati target utilizzando tecniche di distruzione fisica, come la triturazione, la fusione, la polverizzazione, l'incenerimento etc.. È molto efficace per rendere le informazioni inaccessibili, ma ha un costo economico elevato.