Progetto S9-L4

Studente: Simone Mininni

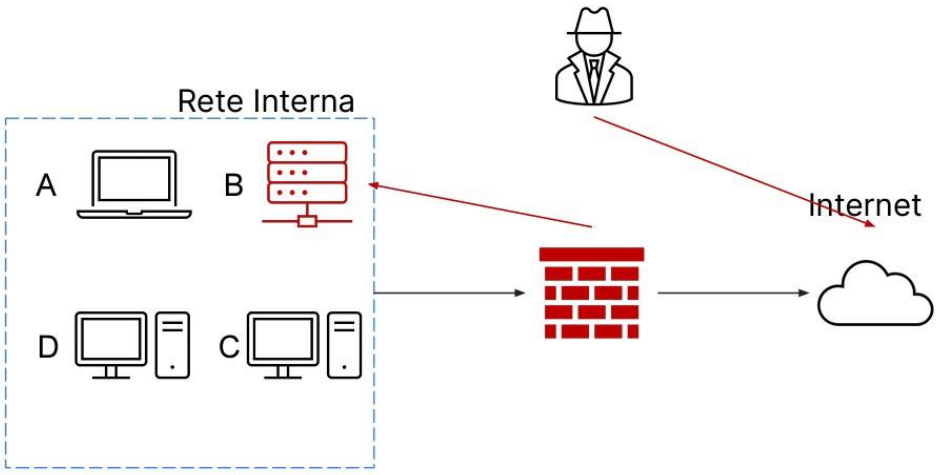
Traccia :

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

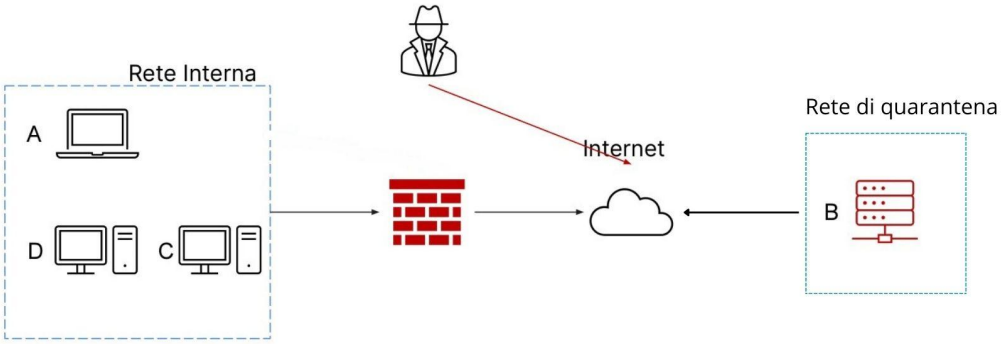
Situazione Iniziale:



L'attaccante è riuscito ad accedere alla rete interna, compromettendo il database.

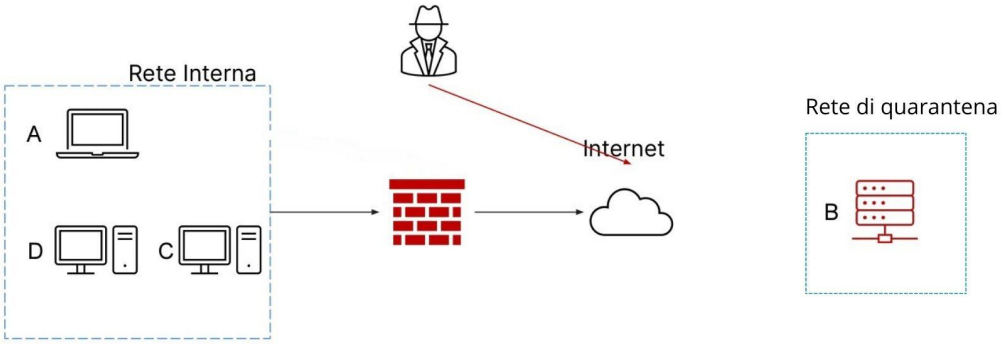
Per rispondere all'evento, andiamo a conifgurare il sistema compromesso su una rete di quarantena.

Isolamento:



Il sistema compromesso non comunica più con la rete interna, ma l' attaccante può ancora accedervi attraverso internet.

Rimozione:



Il sistema compromesso è stato completamente scollegato dalla rete in attesa di ripristino.

Essendo il sistema compromesso, può essere considerato non più affidabile, quindi per rimuovere le informazioni dagli hard disk prima di smaltirli o riutilizzarli bisogna ricorrere ad alcune tecniche quali:

- Purge
- Destroy

Purge è una tecnica che mira alla rimozione dei contenuti attraverso l'utilizzo di forti magneti, oltre alla sovrascrittura dei dati più volte.

Destroy, invece, punta a disintegrare, polverizzare i media, al fine di rendere le informazioni quasi sicuramente inaccessibili.