S9l4,

BENVENUTI LUIGI

Traccia:

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.

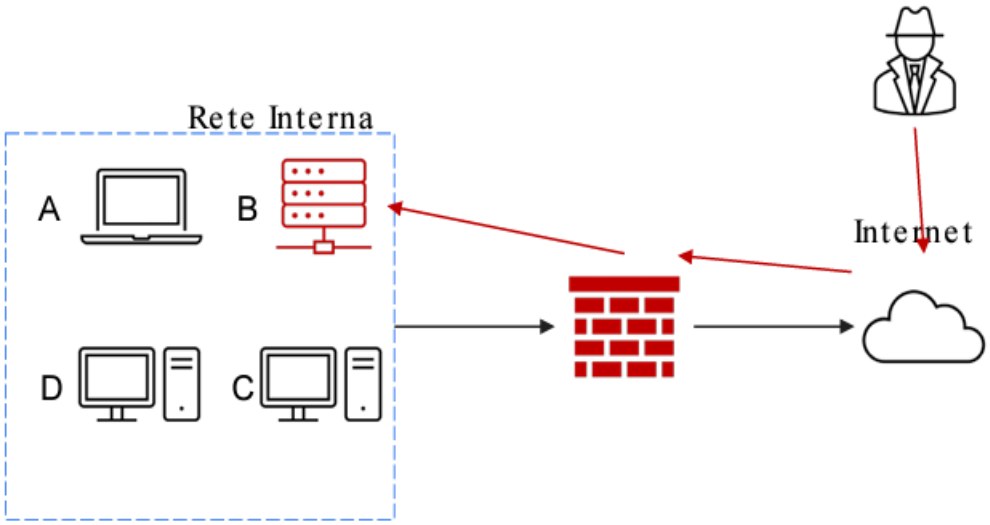
L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

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

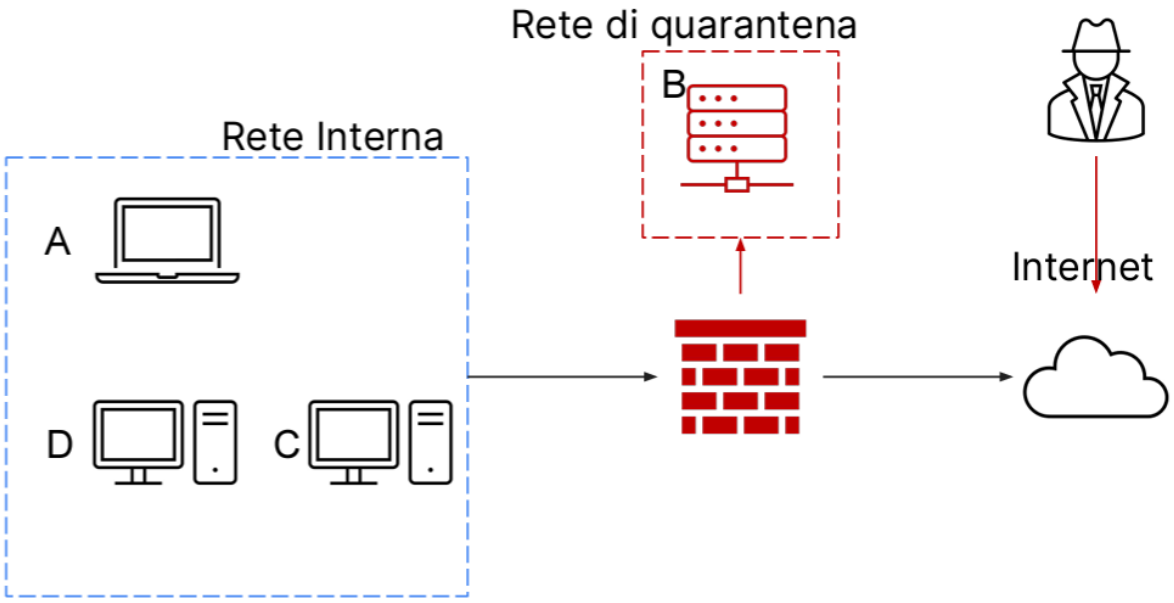
• Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche **Clear**.

Schema del sistema



1- **Tecnica di isolamento**

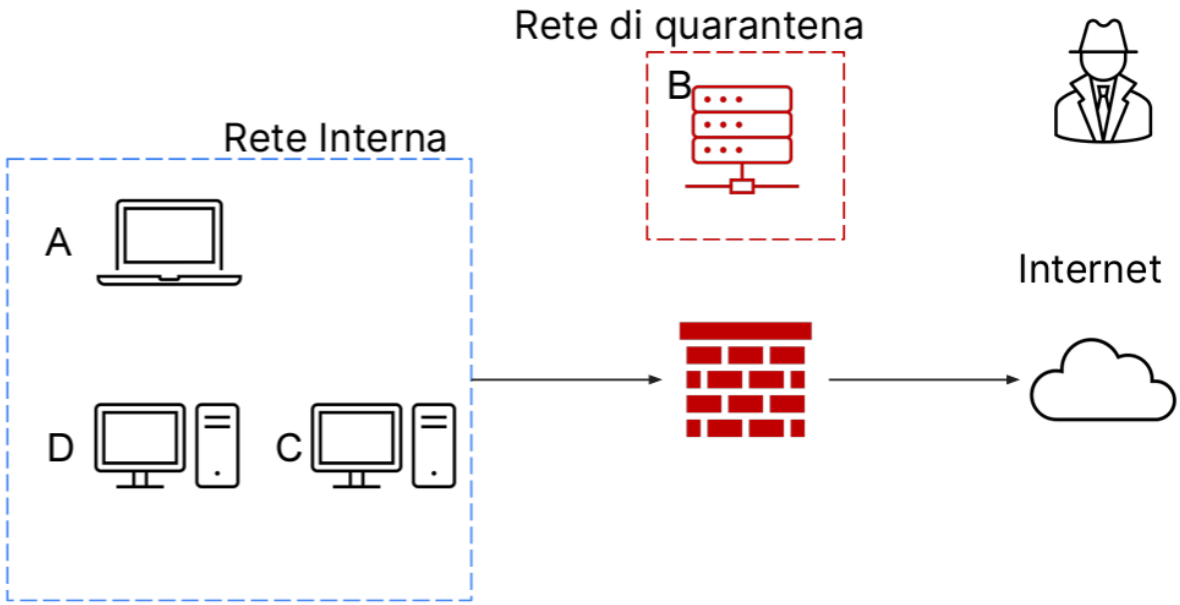
La tecnica di isolamento ci consente di spostare in una nuova rete provvisoria detta "**rete di quarantena**" solamente l'asset infetto, isolandolo dunque dalla rete interna alla quale non avrebbe più accesso se non tramite firewall.



Questo procedimento permetterebbe comunque all'attaccante di raggiungere il target tramite la rete internet.

2- **Tecnica di rimozione**

Per evitare questa situazione, e mettere dunque completamente offline la macchina, si procederà eliminando completamente il target da quella rete.



3 – Clear

Un disco rigido contaminato ha più di una possibile tecnica di cancellazione. La prima è la "clear". Con essa si intende la **sovrascrittura** una o più volte dell'intero disco o addirittura il "**factory reset**", ovvero il ripristino totale del disco.

Questa tecnica però non elimina definitivamente tutti i dati. Infatti, tramite tecniche di recovering più raffinate, si potrebbe risalire ad almeno una parte dei dati.

4 – Purge

La tecnica "**purge**" aggiunge alle tecniche di distruzione logica anche alcune tecniche di distruzione fisica, come l'utilizzo di magneti in grado di intaccare permanentemente i dati senza distruggere completamente l'hardware.

5 – Destroy

La tecnica di "**destroy**" implementa tutte le tecniche precedenti ma va poi ad eseguire completamente anche una distruzione fisica dell'hardware (es. trapanazione, esposizione ad alte temperature, smaltimento chimico ecc).