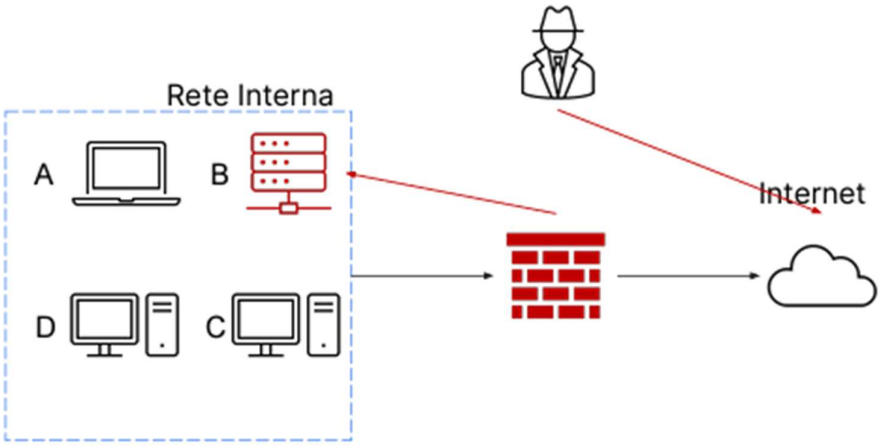
PRATICA S9L4 – Giorgio Trovesi

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.

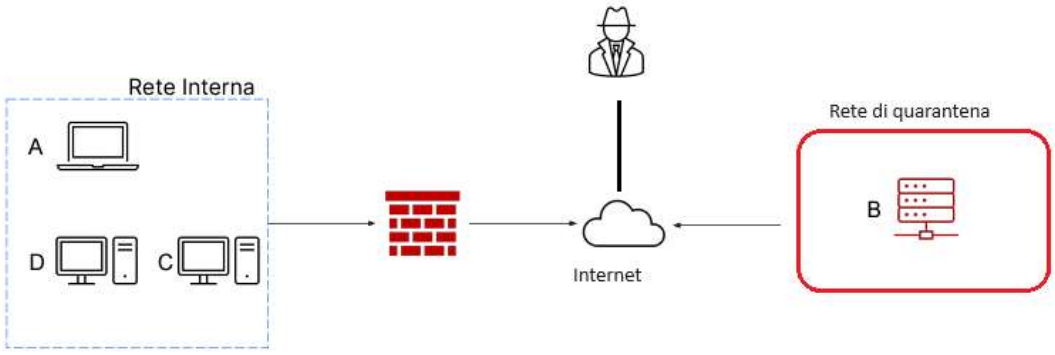
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

- 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



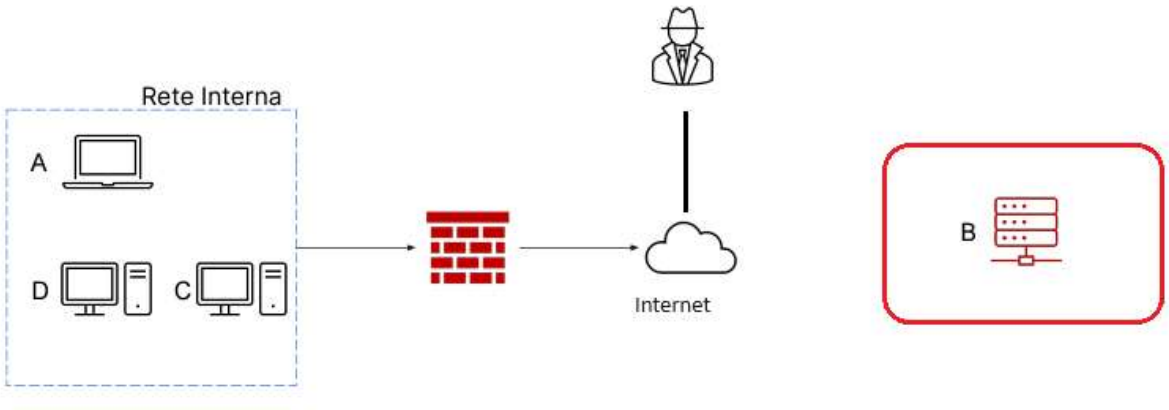
Isolamento:

A differenza della semplice segmentazione, creando una separazione del sistema B dagli altri computer sulla rete, l'isolamento è considerato un contenimento maggiore, che consiste in una completa disconnessione del sistema infetto dalla rete, in tal modo limita maggiormente un possibile accesso alla rete interna dall'attaccante.



Rimozione:

Qualora l'isolamento non fosse sufficiente, si utilizza una politica ancora più restrittiva, ovvero la completa rimozione del sistema B sia dalla rete interna che da internet, impedendo all'attaccante sia l'accesso alla rete interna che alla macchina infetta.



Purge:

Oltre alla rimozione dei contenuti sensibili, si utilizzano anche tecniche fisiche come per esempio forti magneti che rendono inaccessibili le informazioni su determinati dispositivi.

Destroy:

In questo caso l'approccio è più drastico, utilizzando tecniche di laboratorio come la polverizzazione ad alte temperature, disintegrazione e trapanazione dei dispositivi contenenti dati sensibili.

Questo metodo richiede un costo maggiore anche se più efficace.