Incident response

Consegna Esercizio

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.

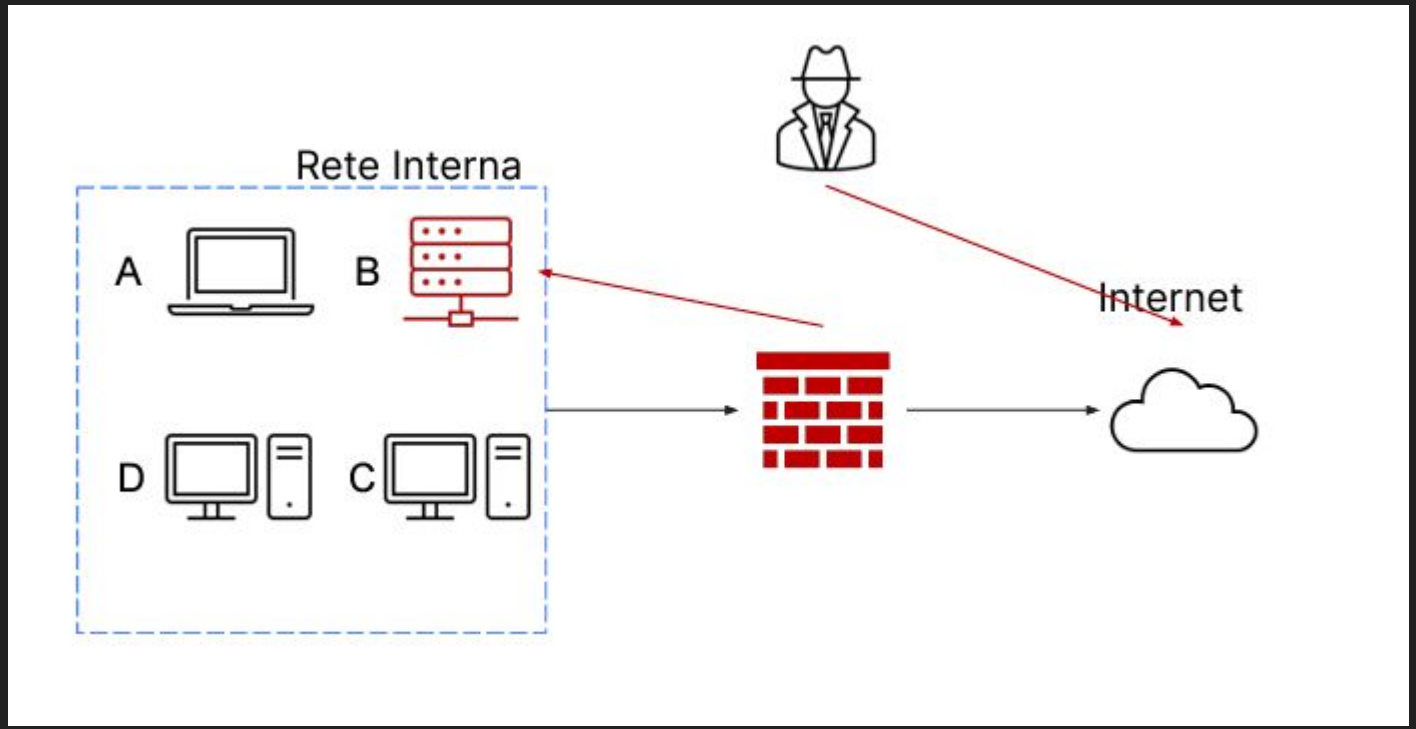
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti. Mostrate le tecniche di:

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

Architettura Rete



Isolamento e Rimozione

Per quanto riguarda l'**isolamento** il sistema infettato dovrà essere "staccato" dalla rete interna ad una rete quarantena, questo è possibile grazie alla segmentazione; così facendo si limitano i danni.

Però il sistema sarà ancora collegato ad internet, e quindi l'attaccante potrà ancora interagire con esso, qui entra in gioco la **rimozione**; scollegando il database da internet l'attaccante non potrà più comunicarci perdendone così il controllo.

Da qui si potrà procedere con la fase di recupero del sistema.

Purge e Destroy

Purge: tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature.