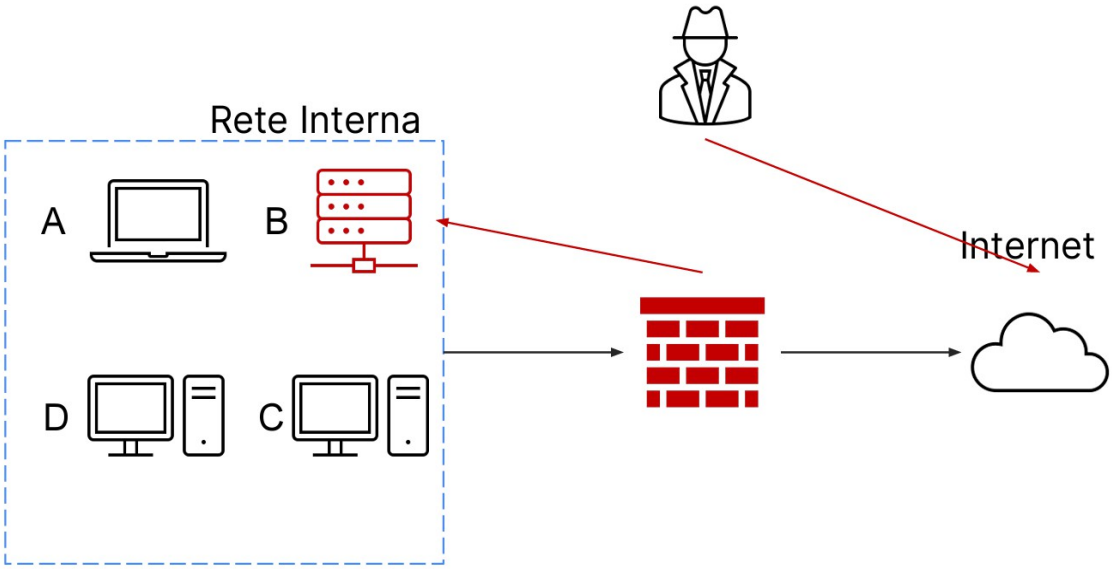
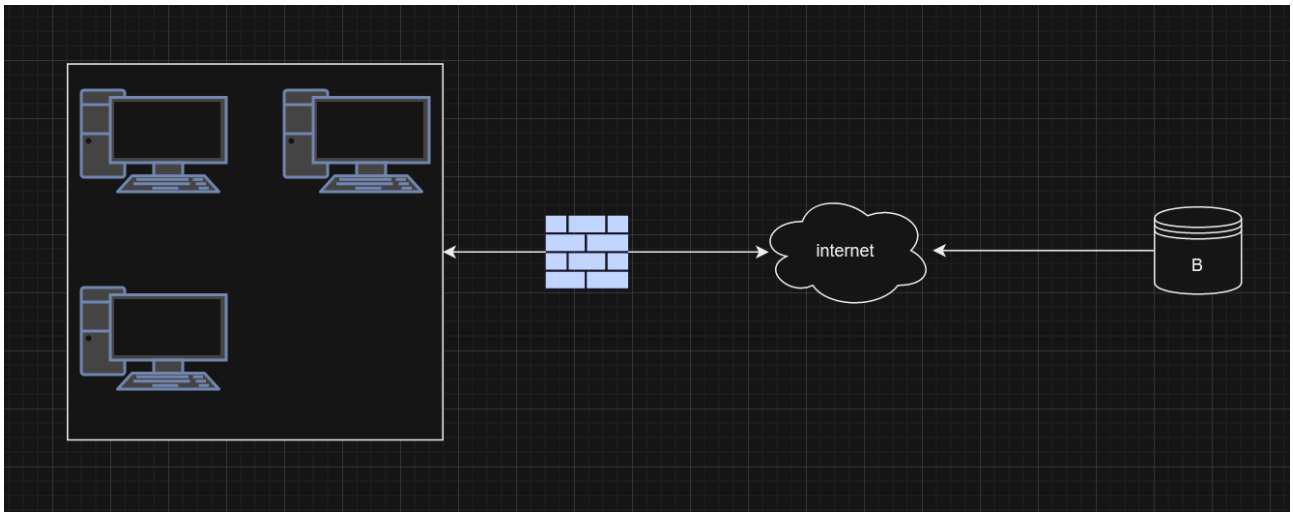
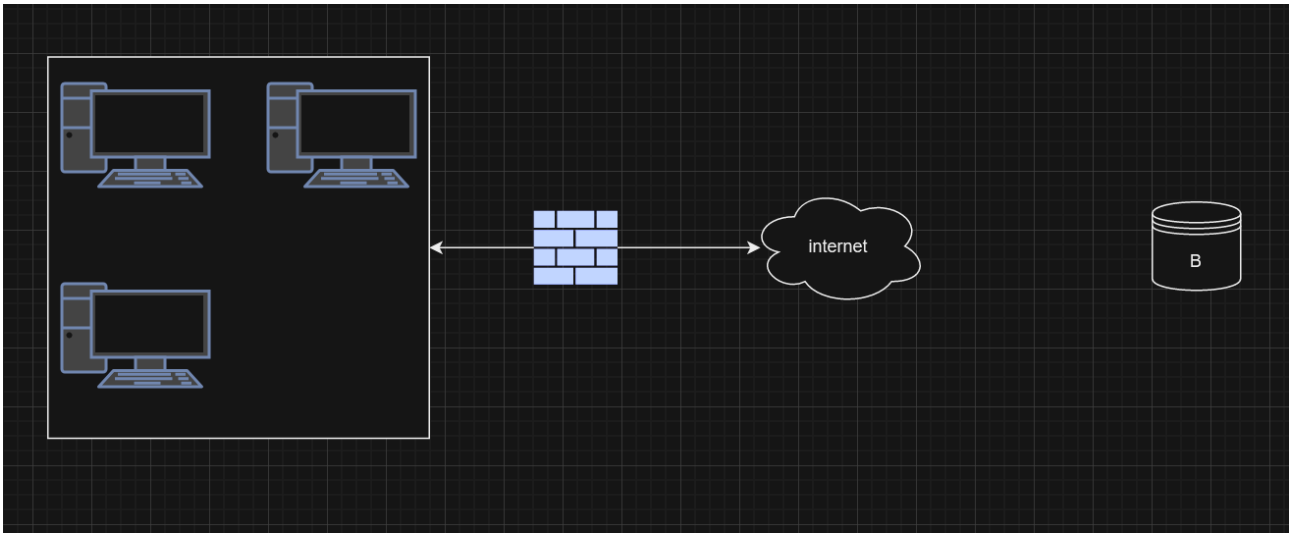
Relazione S9L4



Nell'immagine in questione possiamo osservare come il database B sia stato compromesso da un attaccante. Questo database contiene diversi dischi per lo storage e in quanto parte del team CSIRT è necessario mostrare l'isolamento e la rimozione del sistema infetto.
L'isolamento si utilizza quando non basta la segmentazione della rete e quindi si procede a disconnettere il sistema infetto dalla rete e gli si lascia attivo solo il collegamento con internet.



Con la rimozione invece si disconnette il sistema completamente, quindi non avrà neanche l'accesso ad internet



Una volta che si passa alla fase di recupero invece possiamo cercare di recuperare il sistema infetto e nel caso di hdd potremmo utilizzare la tecnica purge. Questa consiste nell'utilizzo di metodi fisici come un magnete molto potente, per smagnetizzare l'hdd e cancellarne così i dati.
La tecnica destroy invece si utilizza come ultima misura qualora non sia possibile recuperare il dispositivo. Consiste nel distruggerlo tramite tecniche di laboratorio come la disintegrazione o la polverizzazione.

Davide Lecci