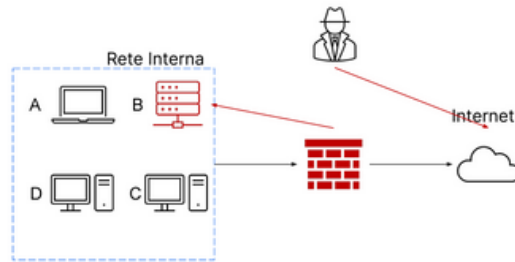


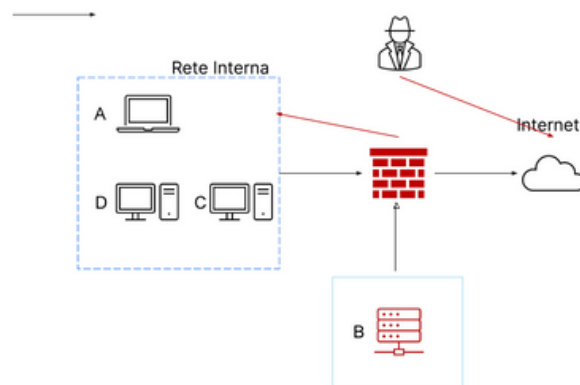
Esercizio S9 L4



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.

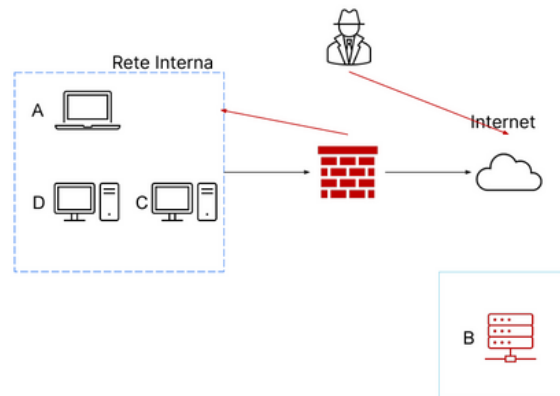
Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto.

Tecnica di isolamento:



L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.

Tecnica di rimozione:



La tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.

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

Purge: Questo processo non si limita a un'approccio puramente logico per eliminare contenuti sensibili, come nel caso di "clear", ma incorpora anche tecniche di rimozione fisica. Come ad esempio, impiega potenti magneti con l'obiettivo di rendere le informazioni inaccessibili su specifici dispositivi. Questa metodologia mira non solo a cancellare i dati in modo virtuale, ma anche a garantire la loro completa eliminazione anche a livello fisico, assicurando un livello aggiuntivo di sicurezza e protezione delle informazioni sensibili.

Destroy: Questo rappresenta l'approccio più definitivo per eliminare dispositivi contenenti dati sensibili. Oltre ai precedenti meccanismi logici e fisici, vengono impiegate sofisticate tecniche di laboratorio, come la disintegrazione e la polverizzazione dei supporti a temperature elevate. Sebbene questo metodo risulti certamente il più efficace per rendere le informazioni irraggiungibili, è anche quello che richiede un impegno economico maggiore, rappresentando quindi una soluzione più onerosa ma altamente sicura per garantire la distruzione completa dei dati sensibili.