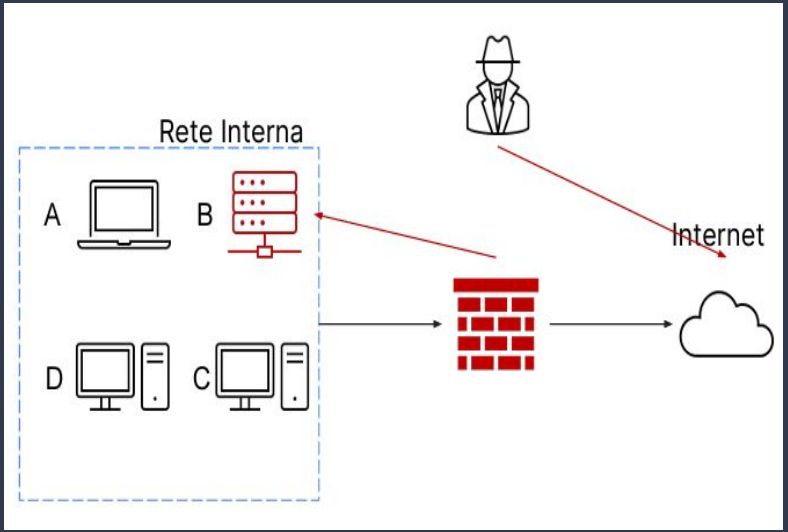
S9/L4 Epicode Cybersecurity

Incident response

Nell’esercizio di oggi viene richiesto di mostrare le tecniche di isolamento e rimozione di un sistema infetto e la differenza tra purge e destroy per l’eliminazione delle informazioni.



Come vediamo nell'immagine, il sistema B, un database con diversi dischi per lo storage, è stato infettato e ci viene richiesto di intervenire prima isolandolo e poi rimovuendolo. Per la fase di isolamento il sistema B verrà totalmente staccato dalla rete interna, ha ancora accesso alla rete Internet ma non filtrato dal firewall e sarà quindi in contatto con l'attaccante. Evidentemente l'isolamento non è bastato, il sistema B viene quindi messo rimosso sia dalla rete interna che da Internet, ma così facendo l'attaccante non avrà modo di accedere. Fatto questo, i dischi di storage passeranno adesso la fase di purge, ovvero la rimozione logica e fisica dei dati sensibili, ma sembrano irrimediabilmente compromessi, quindi si passa alla fase destroy, in cui i dischi vengono distrutti in laboratorio per eliminare ogni traccia dei dati sensibili, anche se comporta un costo economico maggiore.