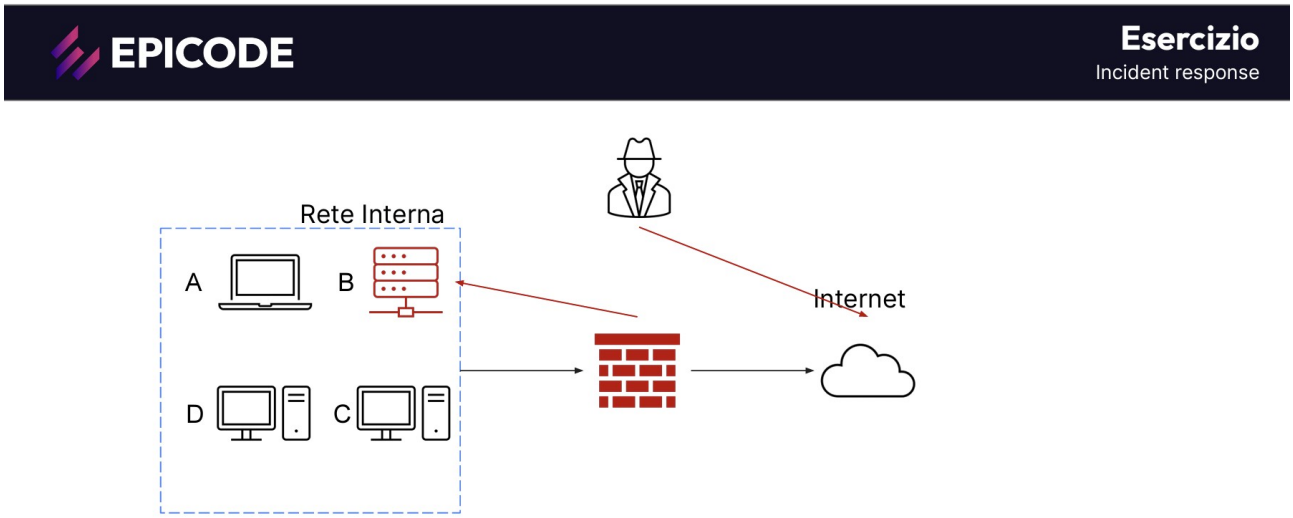
W20D1 EPICODE

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. Indicare anche Clear

Risoluzione:

Il primo metodo è il metodo di SEGMENTAZIONE cioè l'isolamento dalla rete interna e creando una RETE DI QUARANTENA dell'asset compromesso, in questo caso specifico e appunto il database mediante configurazioni a livello Network. Oppure per evitare che il malware si passa ad un vero e proprio ISOLAMENTO che consiste nella completa disconnessione dalla rete dell'asset infetto.
Se tutto ciò non dovesse bastare si dovrà procedere alla completa RIMOZIONE dalla rete dell'asset, scollegandolo completamente anche la internet, mentre negli altri 2 casi si aveva comunque accesso ad esso.

Per PURGE si intende l'utilizzo di mezzi logici e fisici per l'eliminazione dei dati sensibili come esempio forti magneti.

Per DESTROY significa la completa distruzione dell'asset, come polverizzazione, smaltimento, trapanamento ecc ecc

Per CLEAR significa l'utilizzo di metodi logici per eliminare i dati, come factory reset, read and write ecc ecc.