MALIZIA MARCO S9L4

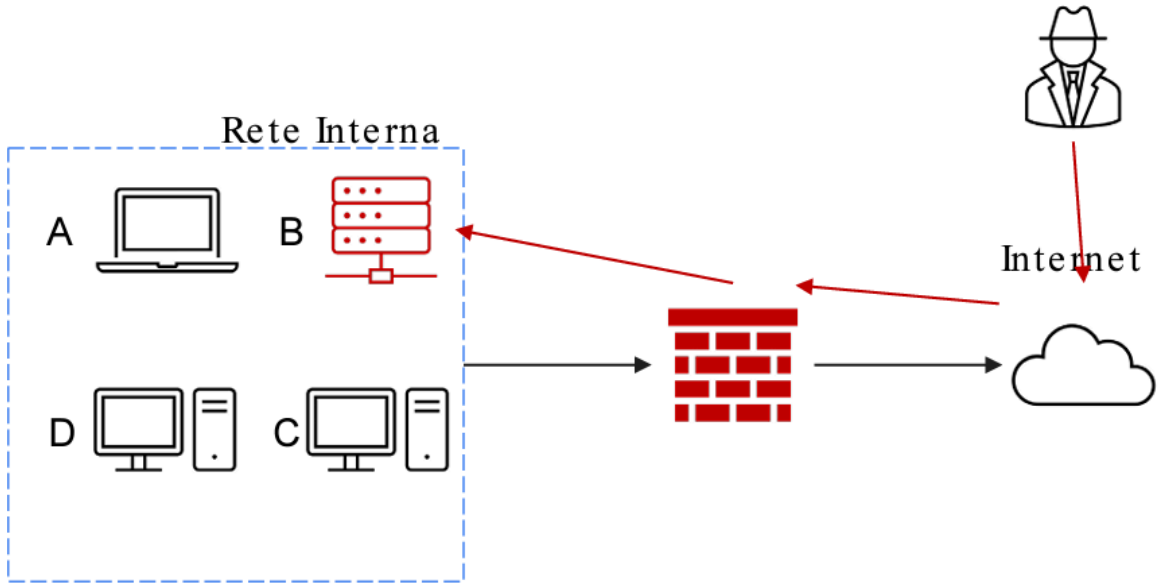
TRACCIA

Esercizio Incident response 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

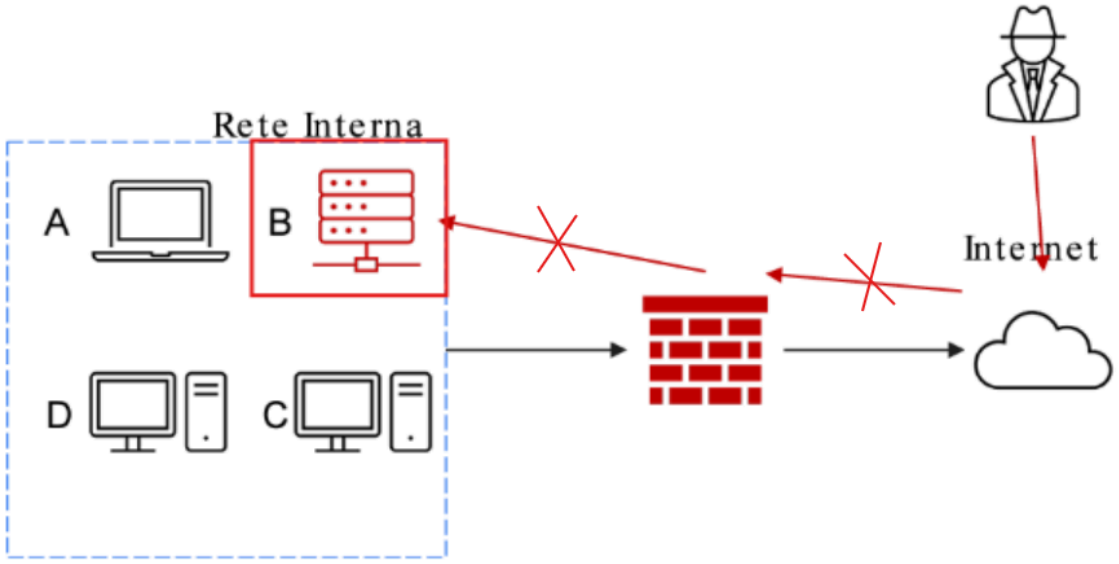


SVOLGIMENTO

Tecniche consigliate per isolare e/o rimuovere il sistema B Infetto:

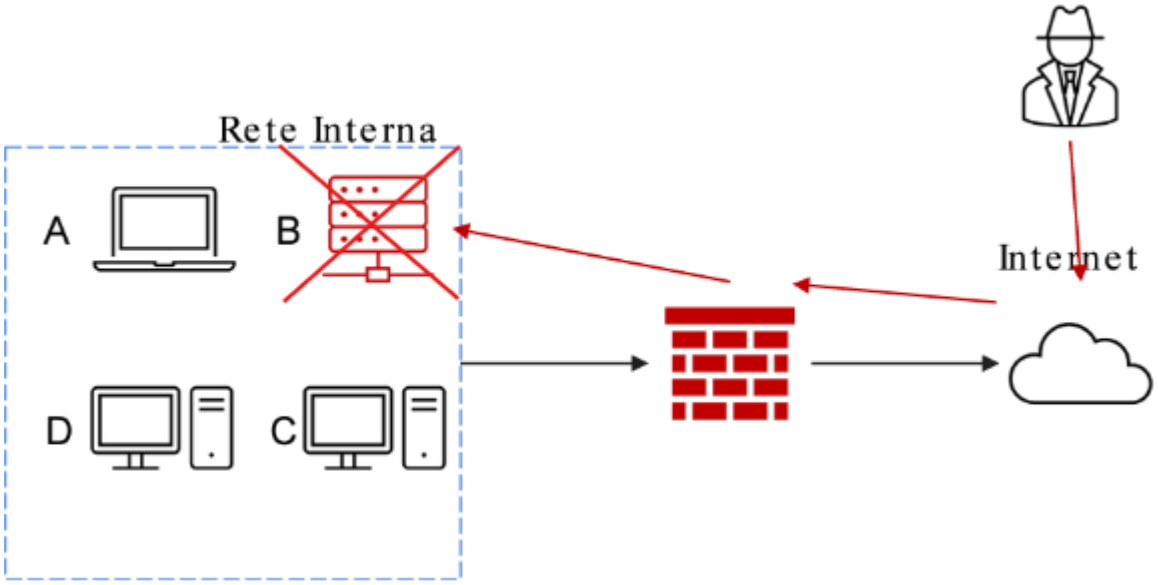
Isolamento:

1. Disconnessione dalla rete: Scollegare il sistema B dalla rete interna e da Internet per impedire ulteriori accessi non autorizzati.
2. Blocco delle comunicazioni: Configurare il firewall per bloccare tutto il traffico in entrata e in uscita dal sistema B.
3. Rete isolata: Se la disconnessione immediata non è possibile, spostare il sistema B in una rete (VLAN) isolata per limitare le interazioni con altri sistemi.



Rimozione:

1. Spegnimento sicuro: Spegnere il sistema B per prevenire ulteriori danni ai dati.
2. Rimozione: 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.
3. Analisi dell'infezione: Avviare un'analisi per determinare l'entità della compromissione e raccogliere prove sull'attacco.



Differenza tra Clear, Purge e Destroy:

Clear (Pulizia): Rende le informazioni inaccessibili agli utenti normali.

Purge (Cancellazione sicura): Elimina le informazioni in modo che siano difficili da recuperare anche con ricerche avanzate.

Destroy (Distruzione): Rende le informazioni completamente irrecuperabili distruggendo fisicamente i supporti.