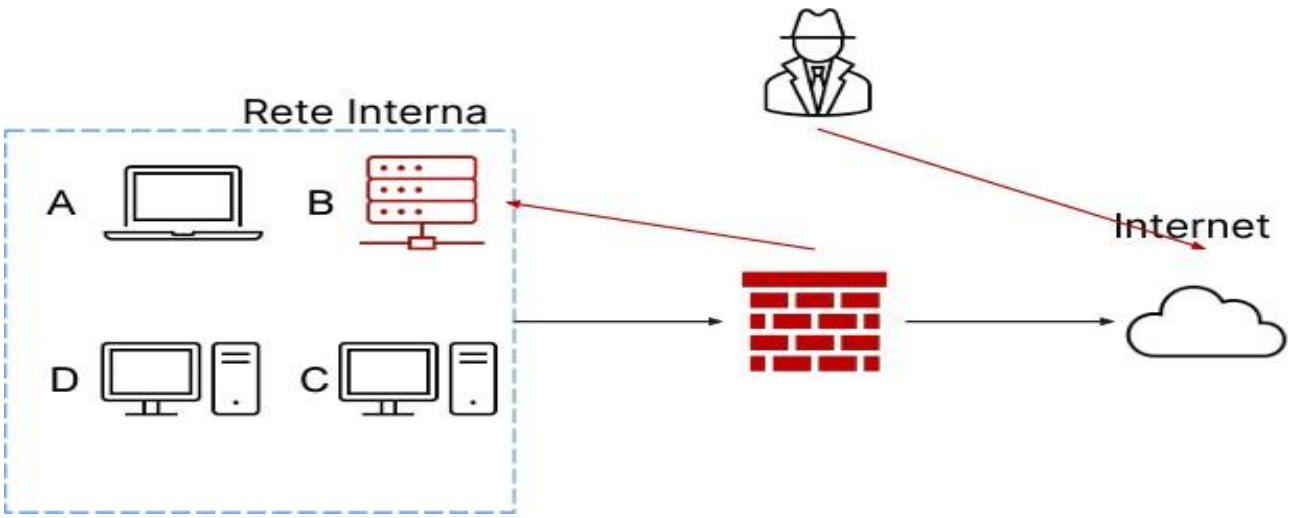
S9L4



Come mostrato nella figura, il Sistema B (un database con più dischi per l'archiviazione) è stato completamente compromesso da un utente malintenzionato che è riuscito a penetrare nella rete e ad accedere al sistema tramite Internet.

È attualmente in corso un attacco e fai parte del team CSIRT.

Rispondi alle seguenti domande. Dimostrare le seguenti tecniche: I) Quarantena II) Rimozione di sistemi infetti B

Spiegare la differenza tra «Purge» e «Destroy» per rimuovere informazioni riservate prima di smaltire un disco danneggiato

Mentre l'attacco continua, cercheremo di fermarlo rimuovendo l'accesso dell'aggressore alla rete interna. Per fare ciò, aggiungeremo una regola al firewall per bloccare le connessioni agli hacker.

Successivamente, per verificare lo stato del Sistema B, lo rimuoveremo dalla rete utilizzando tecniche di rimozione segmentata:

Pertanto, isoliamo il sistema B isolandolo dalla rete interna e da Internet e successivamente verifichiamo l'integrità del sistema.

Se il sistema risulta essere intatto, possiamo ricollegarlo alla rete dopo aver preso le precauzioni necessarie.

Se il sistema è compromesso allora possiamo provare a ripristinarlo. Se ciò si rivela impossibile, l'azienda dovrà cancellare il sistema B e/o caricare un backup prima di attaccare.

Purge: non vengono utilizzati solo metodi logici per rimuovere contenuti sensibili (come nel caso chiaro), ma vengono utilizzate anche tecniche di rimozione fisica, come l'utilizzo di potenti magneti per rendere le informazioni inaccessibili su determinati dispositivi

Destroy: è il modo più pulito per smaltire un dispositivo contenente dati sensibili. Oltre ai meccanismi logici e fisici appena visti, vengono utilizzate tecniche di laboratorio, come la decomposizione e la sminuzzamento dei fluidi ad alte temperature. Questo approccio è senza dubbio il modo più efficace per rendere difficile l'ottenimento delle informazioni, ma è anche quello che richiede uno sforzo maggiore in termini economici.