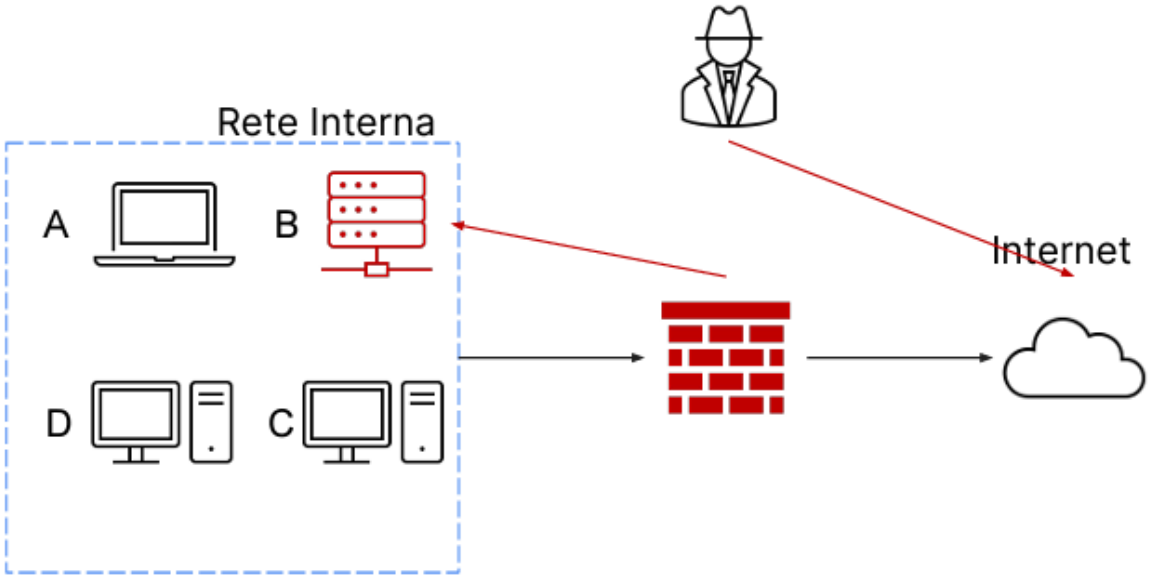
S9 L4

Con riferimento alla figura, 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




Dato che l'attacco è ancora in corso, cercheremo di fermarlo rimuovendo l'accesso alla rete interna all'utente malintenzionato. Per farlo, aggiungeremo una regola al Firewall che blocchi la connessione con l'Hacker.

Successivamente per verificare lo stato del sistema B, procederemo a rimuoverlo dalla rete utilizzando la tecnica della segmentazione-rimozione:

Quindi, mettiamo in quarantena il sistema B isolandolo sia dalla rete interna che da internet, procedendo successivamente alla verifica dell'integrità del sistema.

Se il sistema risulta essere integro, allora possiamo, una volta prese le dovute precauzioni, reinserirlo nella rete.

Se il sistema risultasse compromesso, allora possiamo tentare di ripristinarlo. Qualora questo risultasse impossibile, l'azienda dovrà effettuare un Clear del sistema B e/o caricare un backup precedente all'attacco.

Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi

Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.