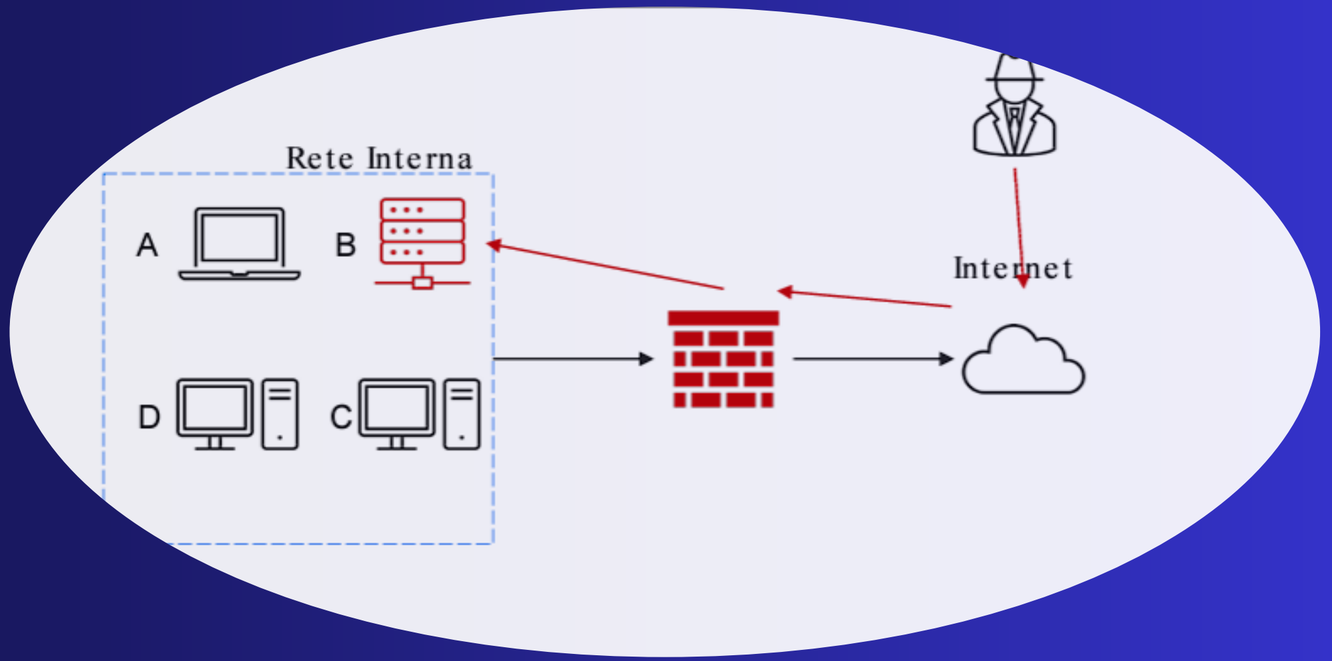
INCIDENT RESPONSE

report: rafael Mango

TRACCIA

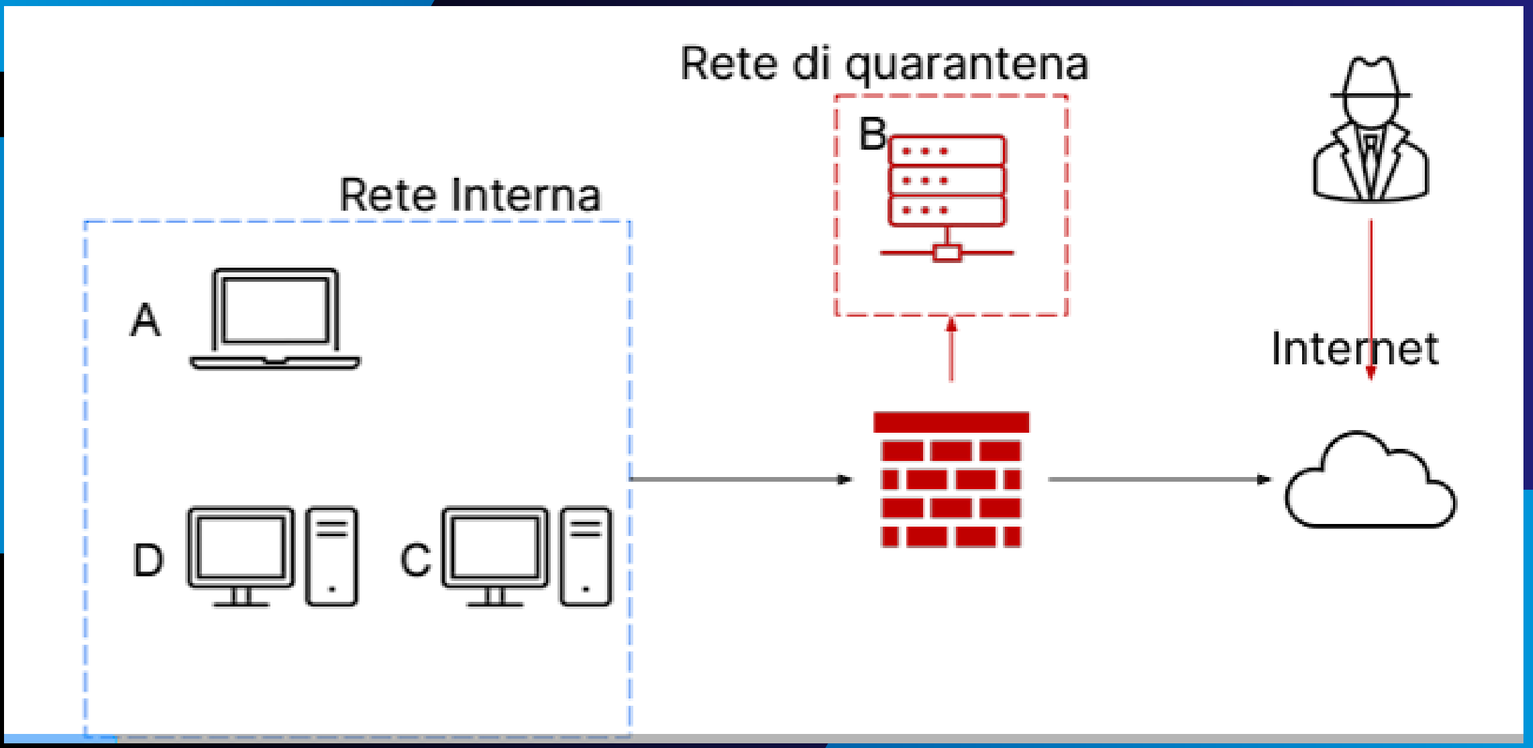
- Con riferimento alla figura in slide il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L’attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.
- Mostrate le tecniche di: I) Isolamento II) Rimozionedel sistema B infetto
- Spiegate la differenza tra Purgee Destroyper l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



LA FASE DI CONTENIMENTO, RIMOZIONE E RECUPERO

Durante la fase di rilevamento e analisi, il team CSIRT avvia le prime operazioni per comprendere la natura dell'incidente, identificare i sistemi interessati e valutare potenziali rischi per altri sistemi. Una volta completata questa valutazione, il team si impegna a trovare rapidamente una soluzione per mitigare gli effetti dell'incidente. Questo processo inizia con le fasi di contenimento, eliminazione e ripristino, volte a limitare ulteriori danni, rimuovere la minaccia e ripristinare la normale operatività dei sistemi colpiti.

SOLUZIONE ISOLAMENTO



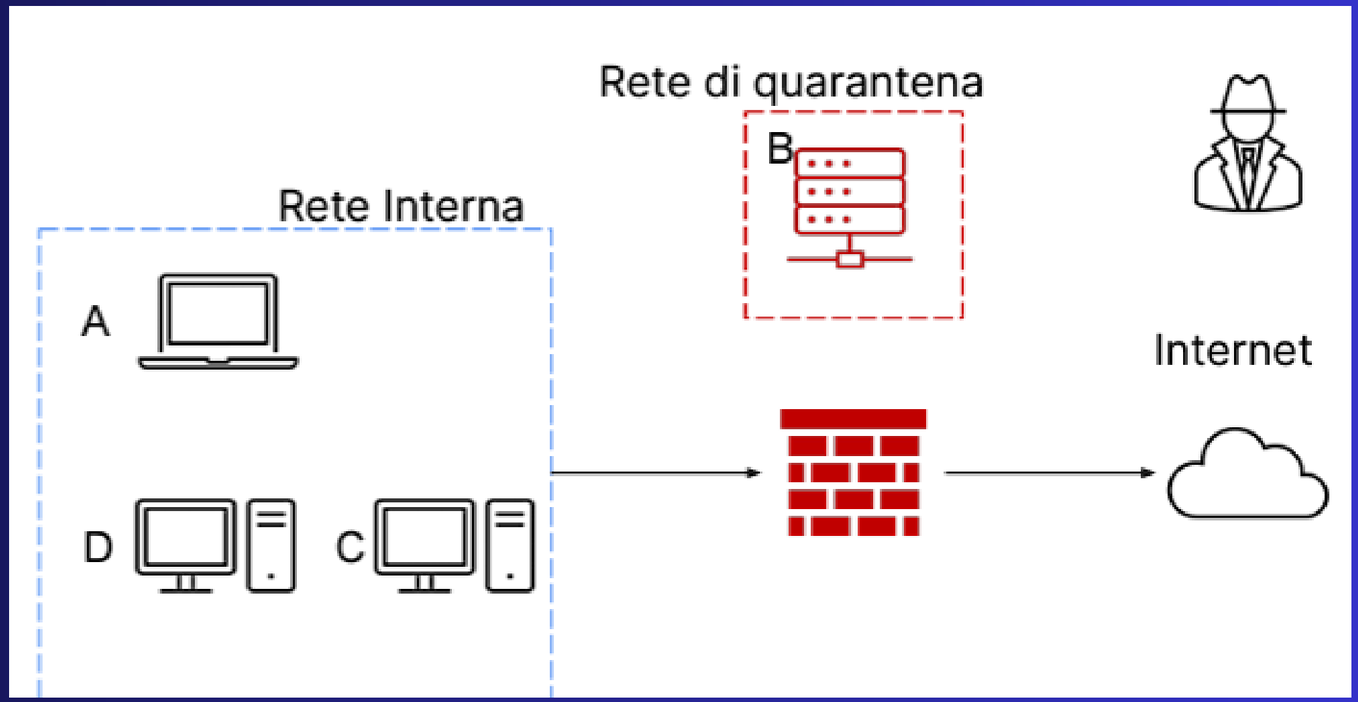
Inizialmente, abbiamo adottato un approccio di contenimento utilizzando una strategia di isolamento. Questo ha comportato la separazione del sistema compromesso per limitare l'accesso dell'attaccante alla rete interna. È importante notare che, nonostante l'isolamento, il sistema compromesso rimane ancora accessibile all'attaccante attraverso Internet.

(come vediamo in figura)

Soluzione di rimozione

Dopo aver passato la fase di isolamento andiamo alla fase di rimozione che consiste :
Nella completa eliminazione del sistema dalla rete, rendendolo totalmente inaccessibile sia dalla rete interna che da Internet. Questa azione impedisce all'attaccante di avere qualsiasi accesso al sistema compromesso, limitando così anche la possibilità di accesso alla rete interna.

(come vediamo in figura)



Differenze tra Purge e Destroy

PURGE

In questo approccio, vengono impiegate sia procedure logiche che fisiche per eliminare definitivamente i dati su un disco o un dispositivo di storage. Le tecniche fisiche coinvolte, tuttavia, non comportano alcuna invasività e non comportano la distruzione dell'hardware coinvolto.

DIFFERENZE

la purge è un processo che mira a eliminare i dati in modo sicuro senza necessariamente distruggere l'hardware, mentre il destroy comporta la distruzione fisica dell'hardware o del supporto dei dati per rendere i dati irrecuperabili. Entrambi i processi sono utilizzati in ambito di sicurezza informatica per proteggere i dati sensibili o riservati da accessi non autorizzati.

DESTROY

E un metodo di sanificazione è un procedimento che rende impossibile recuperare i dati desiderati utilizzando le più avanzate tecniche di laboratorio. Questo processo assicura che i supporti in questione non possano essere più utilizzati per archiviare ulteriori dati.

CLEAR

Questo metodo di sanificazione utilizza tecniche logiche per eliminare i dati da tutte le aree di archiviazione accessibili dall'utente. Serve a proteggere i dati da semplici tentativi di recupero non invasivi. Di solito, si applica attraverso operazioni standard di lettura e scrittura sul dispositivo di archiviazione, come sovrascrivere i dati con nuovi valori o utilizzare un'opzione nel menu per ripristinare il dispositivo alle impostazioni di fabbrica, se supportata.

Thank You