S9_L4
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

Giorno 4 - Incident response

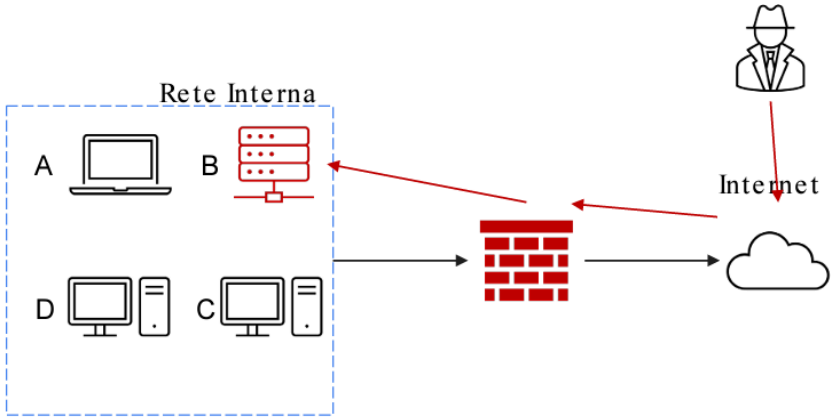
TRACCIA

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**



SVOLGIMENTO

Il sistema B, ovvero un database con diversi dischi per lo storage, è stato compromesso da un attaccante che ha bucato la rete ed è riuscito ad accedere tramite Internet. L'attacco è attualmente in corso e come parte del team CSIRT, dobbiamo rispondere alle seguenti domande.

1. Mostrate le tecniche di: I) **Isolamento** II) **Rimozione** del sistema **B infetto**

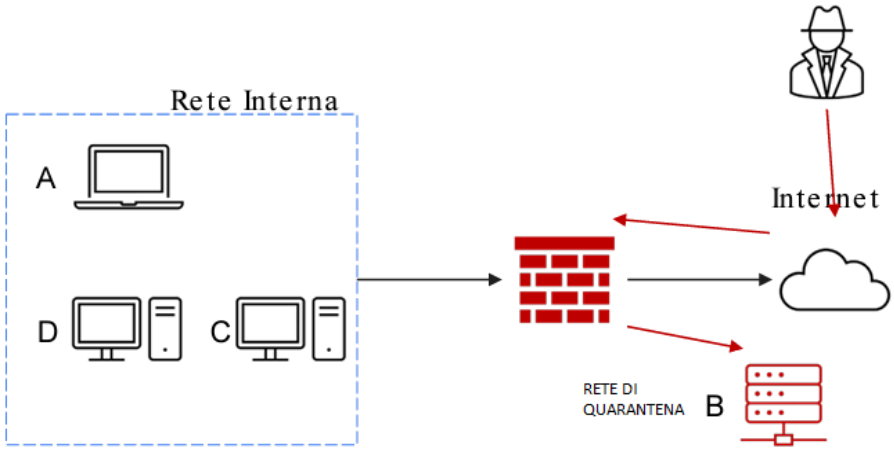
I) Isolamento

L'isolamento del sistema compromesso è il primo passo per contenere l'incidente e limitare i danni.

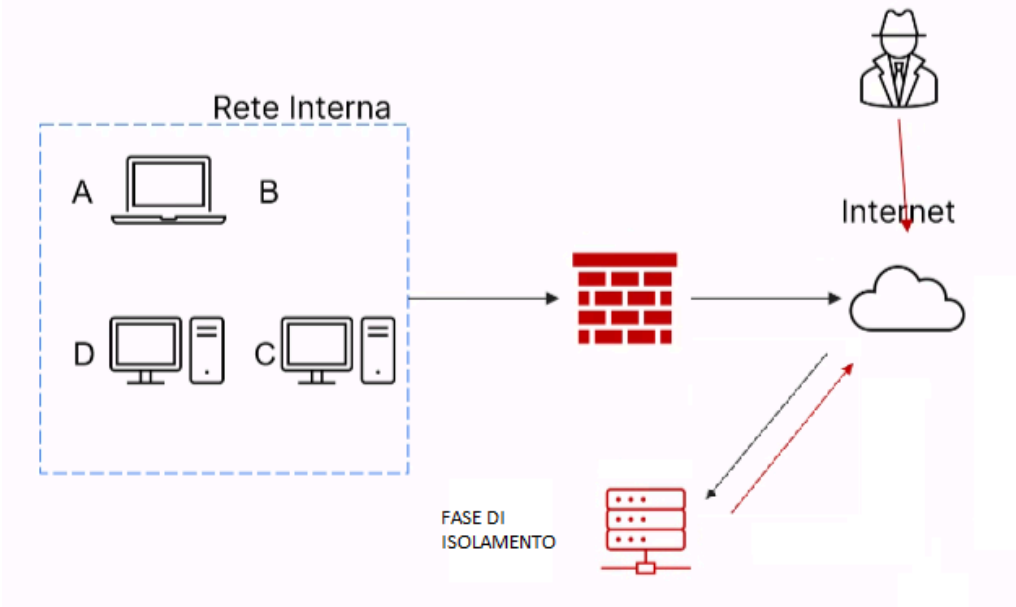
Si procede con le diverse tecniche di isolamento:

- Disconnessione dalla rete
- Segmentazione della rete
- Blocco degli indirizzi IP

La prima cosa da fare è mettere in quarantena il sistema B



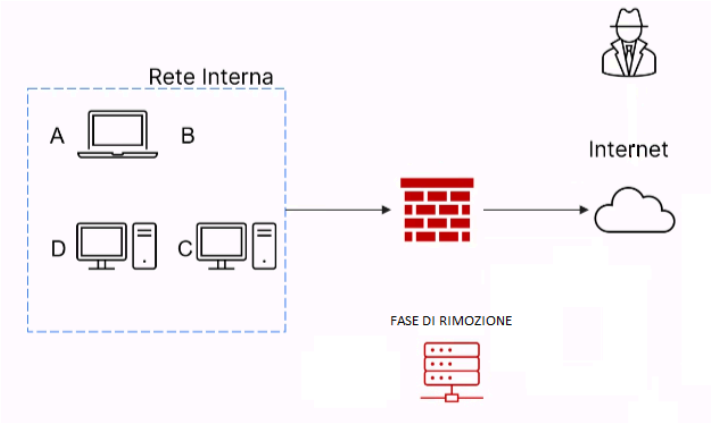
Successivamente si può isolare il sistema.



II) Rimozione del sistema B infetto

Una volta isolato, è necessario rimuovere il sistema compromesso dalla rete e iniziare il processo di pulizia o ricostruzione.

- Analisi forense
- Shutdown del sistema
- Backup dei dati
- Rebuilding o Reconstruction



2. Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. **Indicare anche Clear**

Purge

Implica la rimozione delle informazioni sensibili utilizzando sia tecniche logiche che fisiche:

- Sovrascrittura: Sovrascrivere i dati più volte con informazioni casuali.
- Smagnetizzazione: Utilizzare magneti potenti per rendere i dati illeggibili.
- Rimozione fisica: Metodi come la perforazione del disco per danneggiarlo fisicamente.

Il Purge garantisce che i dati siano praticamente inaccessibili, ma il dispositivo potrebbe essere riutilizzabile in alcuni casi.

Destroy

E' il metodo più drastico per eliminare le informazioni sensibili e comporta la distruzione fisica del dispositivo:

- Disintegrazione: Ridurre il disco a polvere.
- Polverizzazione: Applicare alte temperature per distruggere completamente il disco.
- Trapanazione: Perforare ripetutamente il disco per renderlo inaccessibile.

Questo metodo assicura che le informazioni siano totalmente inaccessibili, ma rende il dispositivo inutilizzabile.

Clear

E’ il metodo meno drastico e implica la pulizia logica dei dati. Tecniche comuni includono:

- Sovrascrittura: Sovrascrivere i dati con informazioni casuali una o più volte.
- Reset di fabbrica: Riportare il dispositivo alle impostazioni di fabbrica, eliminando tutti i dati utente.

Il Clear è efficace per impedire l'accesso casuale ai dati, ma potrebbe non essere sufficiente contro attacchi sofisticati che cercano di recuperare i dati cancellati.