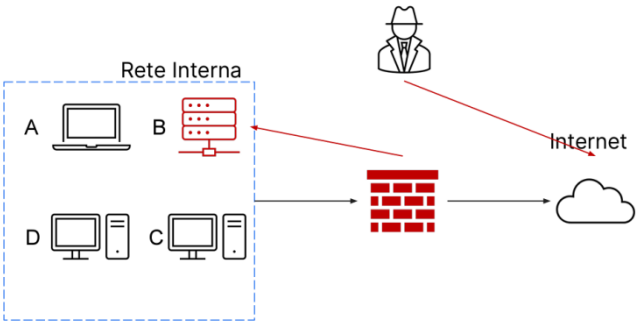
**Traccia:**

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**




Per affrontare questa situazione di compromissione del sistema B, ecco come affronterei i quesiti:

**1) Tecniche di Isolamento:** Per isolare il sistema compromesso (Sistema B) e impedire ulteriori danni, è necessario intraprendere le seguenti azioni:

1. **Disconnettere il Sistema B dalla Rete:** Interrompere immediatamente la connessione Internet del Sistema B per prevenire ulteriori accessi non autorizzati e limitare la diffusione dell'attacco ad altri sistemi.

2. **Creare una Rete Isolata:** Isolare fisicamente o virtualmente il Sistema B in una rete separata per analizzare il traffico e gli eventi all'interno del sistema senza rischio di ulteriori compromissioni.

3. **Bloccare le Connessioni Esterne:** Verificare e bloccare qualsiasi connessione uscente non autorizzata dal Sistema B per prevenire la trasmissione di dati sensibili all'esterno.

4. **Monitoraggio Costante:** Monitorare attentamente il Sistema B isolato per rilevare attività sospette o tentativi di comunicazione non autorizzati.

**2) Rimozione del Sistema B infetto:** Per rimuovere il sistema compromesso in modo sicuro e completo:

1. **Backup dei Dati Critici:** Effettuare un backup dei dati critici (se possibile) prima di procedere con la rimozione del sistema.

2. **Formattazione e Reinstallazione:** Formattare completamente i dischi del Sistema B e reinstallare il sistema operativo e le applicazioni da fonti attendibili. Questa azione è fondamentale per rimuovere completamente eventuali software dannosi e backdoor.

3. **Scansioni Antivirus:** Eseguire scansioni antivirus approfondite su tutti i dati e i file del Sistema B per individuare e rimuovere eventuali minacce rimanenti.

**Differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili:**

- **Purge:** Il processo di "Purge" si riferisce alla rimozione di informazioni sensibili in modo sicuro dal sistema. In genere, questo coinvolge la sovrascrittura dei dati con dati casuali per rendere irrecuperabili le informazioni originali.
- **Destroy:** "Destroy" implica la distruzione fisica del dispositivo o del mezzo di memorizzazione contenente le informazioni sensibili. Ad esempio, distruggere fisicamente un disco rigido attraverso la frantumazione o la demolizione.

**Clear:**

- **Clear (Cancellazione):** La "Clear" si riferisce alla cancellazione logica dei dati, dove i dati vengono marcati come non più necessari e rimossi dal sistema di file. Tuttavia, i dati eliminati in questo modo possono essere recuperabili con strumenti specializzati a meno che non vengano sovrascritti con nuovi dati.

In conclusione, utilizzando una combinazione di isolamento, rimozione sicura e distruzione dei dati sensibili, è possibile contenere e risolvere l'attacco al Sistema B.