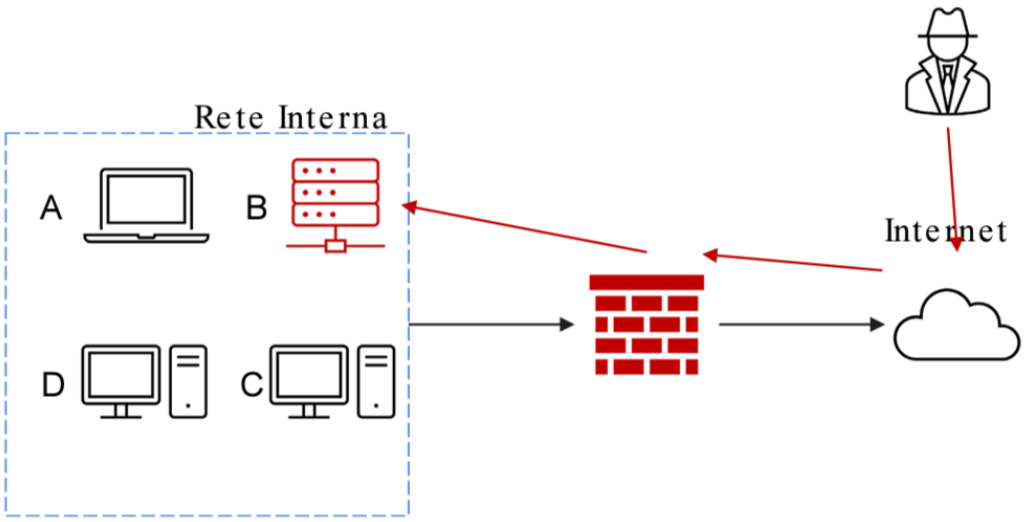

Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

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.

I) Tecniche di Isolamento:

- ***Disconnessione della rete***: Prima di tutto, è fondamentale isolare il sistema compromesso dalla rete per impedire ulteriori infiltrazioni o danni causati dall'attaccante.
- ***Segmentazione di rete***: Se possibile, isolare il sistema compromesso all'interno della rete utilizzando dispositivi di segmentazione come firewall o VLAN. Ciò aiuta a contenere l'attacco e a prevenire la diffusione ai sistemi adiacenti.
- ***Isolamento fisico***: Se necessario, fisicamente isolare il sistema compromesso disconnettendo fisicamente i cavi di rete o spegnendo i dispositivi di comunicazione.
- ***Blocco degli account compromessi***: Se l'attaccante ha ottenuto accesso tramite credenziali compromesse, bloccare immediatamente tali account per impedire ulteriori accessi non autorizzati.
- ***Monitoraggio attivo***: Una volta isolato, monitorare attivamente il traffico in entrata e in uscita dal sistema per rilevare eventuali tentativi di comunicazione dell'attaccante.

II) Rimozione del sistema B infetto:

- ***Analisi dell'impatto***: Valutare l'entità del danno e l'estensione dell'infezione per determinare il percorso migliore per la rimozione del sistema compromesso.
- ***Backup delle informazioni critiche***: Prima di procedere alla rimozione del sistema, eseguire un backup di tutte le informazioni critiche presenti su di esso per evitare la perdita di dati importanti.

- ***Formattazione dei dischi rigidi***: Formattare completamente i dischi rigidi del sistema compromesso per eliminare qualsiasi traccia dell'attacco e delle informazioni compromesse.
- ***Reinstallazione del sistema operativo***: Dopo la formattazione, reinstallare il sistema operativo e tutti i software necessari da fonti affidabili e sicure.
- ***Implementazione di misure di sicurezza aggiuntive***: Dopo la reinstallazione, implementare misure di sicurezza aggiuntive come patch di sicurezza, firewall e software antivirus per proteggere il sistema da futuri attacchi.

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

- **Purge**: Purge si riferisce al processo di eliminazione sicura delle informazioni sensibili o dei dati dal sistema. Questo processo implica la sovrascrittura dei dati con dati casuali o con zeri multiple volte per garantire che le informazioni precedenti non siano più recuperabili. Il processo di purga non danneggia fisicamente il dispositivo di memorizzazione.

- **Destroy**: Destroy, d'altra parte, implica la distruzione fisica del dispositivo di memorizzazione contenente le informazioni sensibili. Questo può essere fatto mediante metodi come la triturazione, la demolizione o l'incenerimento del dispositivo. Destroy garantisce che le informazioni sensibili non possano essere recuperate da nessun mezzo e che il dispositivo stesso sia reso completamente inutilizzabile.

Clear:

- Clear si riferisce alla semplice eliminazione dei dati o delle informazioni sensibili dal dispositivo di memorizzazione senza alcun tipo di sovrascrittura o distruzione fisica. Quando si esegue un'operazione di clear, i dati vengono segnati come spazio disponibile per nuovi dati, ma non vengono necessariamente sovrascritti. Questo significa che i dati rimossi possono essere ancora recuperabili utilizzando strumenti specializzati di recupero dati, a meno che non venga sovrascritto da nuovi dati. In termini di sicurezza dei dati, clear non è considerato un metodo affidabile per eliminare le informazioni sensibili, poiché esiste ancora il rischio che i dati possano essere recuperati. Pertanto, quando si tratta di dati sensibili o critiche per la sicurezza, è consigliabile utilizzare metodi di purge o destroy per garantire l'eliminazione sicura e permanente delle informazioni.