I) Isolamento

Per isolare il sistema B infetto, è necessario prendere le seguenti azioni:

1. **Disconnettere il sistema B dalla rete**:
    - Rimuovere fisicamente il cavo di rete dal sistema B o disabilitare la porta di rete al livello del switch.
    - Configurare il firewall per bloccare tutto il traffico in entrata e in uscita da e verso il sistema B.
2. **Isolare logicamente il sistema**:
    - Utilizzare VLAN per spostare il sistema B in una rete isolata che non abbia accesso ad altri sistemi.
    - Se possibile, utilizzare una sandbox o una rete di quarantena per mettere il sistema in un ambiente sicuro per ulteriori analisi.

II) Rimozione del sistema B infetto

Una volta isolato, il sistema B infetto deve essere rimosso dall'ambiente operativo:

1. **Spegnere il sistema B**:
    - Spegnere il sistema in modo sicuro e fisico per evitare ulteriori danni o compromissioni.
2. **Rimuovere i dispositivi di storage**:
    - Estrarre i dischi dal sistema B per una futura analisi e trattamento.

Purge, Destroy, e Clear

Per eliminare le informazioni sensibili dai dischi compromessi, ci sono diverse tecniche:

1. **Clear**:
    - Questa tecnica prevede la rimozione delle informazioni sensibili utilizzando metodi software o hardware che rendono i dati non facilmente recuperabili, ma senza la necessità di danneggiare fisicamente i dispositivi. Esempi includono la formattazione o il sovrascrivere i dati con pattern specifici.
2. **Purge**:
    - Questa tecnica va oltre il semplice "Clear" e prevede la rimozione dei dati in modo che non possano essere recuperati neanche con strumenti avanzati di recupero dati. Tecniche di "Purge" includono l'uso di strumenti di sovrascrittura multipla e l'uso di strumenti di degaussing per smagnetizzare i dischi.
3. **Destroy**:
    - Questa tecnica implica la distruzione fisica dei dispositivi di storage, rendendo impossibile qualsiasi tentativo di recupero dei dati. Tecniche comuni includono la triturazione dei dischi, la fusione, o la degaussizzazione seguita da una distruzione fisica.

Procedura consigliata

1. **Isolamento**:
    - Disconnettere fisicamente il sistema B dalla rete.
    - Configurare il firewall per bloccare qualsiasi traffico da e verso il sistema B.
2. **Rimozione**:

    - Spegnere il sistema B.
    - Estrarre i dischi di storage.
3. **Eliminazione delle informazioni sensibili**:
    - **Clear**: Utilizzare strumenti di formattazione o software di sovrascrittura.
    - **Purge**: Usare metodi di sovrascrittura multipla o degaussing.
    - **Destroy**: Triturare fisicamente i dischi o utilizzare altri metodi di distruzione fisica.

Seguendo queste tecniche e procedure, si può gestire in maniera sicura ed efficace un incidente di compromissione di un sistema, minimizzando il rischio di ulteriori danni o fughe di dati.