Esercizio Incident Response

Situazione: 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.

Quesiti:

I) Isolamento

L'isolamento è una tecnica fondamentale per contenere un attacco in corso e prevenire ulteriori danni. I passaggi per isolare il sistema B compromesso sono i seguenti:

1. **Disconnessione dalla Rete:**
   - Scollegare immediatamente il sistema B dalla rete interna e da Internet per interrompere la comunicazione con l'attaccante.
   - Assicurarsi che il firewall blocchi tutto il traffico in entrata e in uscita verso e dal sistema B.
2. **Isolamento Fisico:**
   - Se possibile, rimuovere fisicamente i cavi di rete dal sistema B.
   - Considerare l'utilizzo di una VLAN separata per isolare logicamente il sistema compromesso.
3. **Monitoraggio del Traffico:**
   - Continuare a monitorare il traffico di rete per identificare eventuali altre anomalie o tentativi di compromissione su altri sistemi.

II) Rimozione del Sistema B Infetto

La rimozione del sistema B infetto comporta diverse azioni per garantire che il sistema sia completamente disinfettato o sostituito. I passaggi sono:

1. **Spegnimento del Sistema:**
   - Spegnere il sistema B per prevenire ulteriori attività dannose.
   - Documentare lo stato attuale per l'analisi forense.
2. **Backup dei Dati:**
   - Eseguire un backup completo dei dati presenti sul sistema B, se non già compromessi, per analisi successiva e recupero.
3. **Analisi Forense:**
   - Avviare un'analisi forense per identificare la modalità di compromissione e l'entità dei danni.
   - Raccogliere log e altre evidenze per future indagini.
4. **Formattazione e Reinstallazione:**
   - Formattare i dischi del sistema B e reinstallare il sistema operativo e il software necessario.

    - Applicare tutte le patch di sicurezza e configurare correttamente i firewall e le misure di sicurezza.
5. **Ripristino dei Dati:**
    - Ripristinare i dati da backup verificati.
    - Assicurarsi che i dati non compromessi siano reintegrati nel sistema in modo sicuro.

Purge, Destroy, e Clear:

- **Purge:**
    - Il purge è un metodo per eliminare dati in modo tale che la ricostruzione, anche con l'uso di tecniche avanzate di recupero, sia estremamente difficile. Questo può includere l'uso di tecniche di sovrascrittura multiple.
- **Destroy:**
    - Il destroy implica la distruzione fisica del supporto di memorizzazione. Questo può includere la degaussazione (demagnetizzazione), lo shredding (frantumazione) dei dischi o altre tecniche che rendono il supporto inutilizzabile.
- **Clear:**
    - Il clear è un processo meno rigoroso rispetto al purge e involve la sovrascrittura dei dati con uno schema semplice, rendendo i dati non recuperabili con strumenti software standard ma potenzialmente recuperabili con tecniche avanzate.

Questi metodi sono critici per garantire che le informazioni sensibili non possano essere recuperate da supporti compromessi prima dello smaltimento.