ESERCITAZIONE S9 4

Incident response

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.

Viene richiesto di mostrare le tecniche di **isolamento** e **rimozione del sistema infetto.**

ISOLAMENTO

Per isolare il sistema B compromesso, bisogna adottare alcune misure specifiche, quali:

- Interrompere immediatamente la connessione con il resto della rete interna per evitare la propagazione dell'attacco
- Segmentare la rete, attraverso una subnet o l'utilizzo di un firewall per limitare la connessione, così da contenere l'attacco e proteggere gli altri host della rete interna
- Disattivare momentaneamente i servizi critici forniti dal Sistema B
- Monitorare attivamente l'intera rete, così da rilevare ulteriori attacchi o comportamenti sospetti.

Attraverso l'isolamento, tuttavia, l'attaccante continua ad avere accesso al sistema B, in quanto ancora connesso a Internet.

RIMOZIONE

Una corretta procedura di rimozione può essere:

- Effettuare un backup del Sistema B, così da eseguire futuri controlli forensi e garantire la continuità operativa dei servizi forniti

- Condurre un’analisi forense sui dischi, così da raccogliere informazioni dettagliate, come i vettori di attacco e le vulnerabilità sfruttate
- Isolare fisicamente il Sistema B
- Smaltimento sicuro dei dischi:

  Scegliere la modalità di eliminazione delle informazioni sensibili memorizzate sui dischi:

  - **Purge**

    Generalmente quella più utilizzata, in quanto permette il riutilizzo dei dischi, una volta sovrascritti più volte, così da rendere i file precedentemente immagazzinati non più leggibili.

  - **Destroy**

    Metodo più costoso e sicuro, in quanto i dischi di memoria vengono distrutti a livello fisico, attraverso la triturazione, incendio e con l’utilizzo di potenti magneti. Comporta la distruzione totale del disco, divenendo inutilizzabile, motivo per cui è quello più costoso e vieni utilizzato solamente in alcune circostanze.

Con la rimozione, l’attaccante non ha più accesso al sistema B, in quanto non più connesso alla rete Internet.