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.

I) **Isolamento**

Isolare il sistema compromesso è fondamentale per impedire ulteriori danni e per proteggere altri sistemi nella rete. Le seguenti sono alcune tecniche che possono essere utilizzate per isolare il sistema compromesso:

1. Disconnettere il sistema dalla rete: Questo impedisce all'attaccante di comunicare con il sistema compromesso e di eseguire ulteriori azioni dannose.

2. Disattivare le connessioni in uscita: Se possibile, bloccare tutte le connessioni in uscita dal sistema compromesso per impedire che l'attaccante trasferisca dati al di fuori del sistema.

3. Utilizzo di firewall e ACL: Configurare il firewall per bloccare il traffico indesiderato verso e dal sistema compromesso. È possibile anche utilizzare le liste di controllo degli accessi (ACL) per limitare quali indirizzi IP possono comunicare con il sistema.

4. Creazione di VLAN o segmentazione di rete: Se il sistema compromesso è parte di una rete più ampia, è possibile isolare il traffico verso e dal sistema utilizzando VLAN o segmentando la rete.

5. Monitoraggio del traffico di rete: Monitorare attentamente il traffico di rete per individuare eventuali tentativi dell'attaccante di comunicare con altri sistemi o di eseguire ulteriori azioni dannose.

II) **Rimozione del sistema B infetto**

Una volta isolato il sistema compromesso, è essenziale rimuoverlo dalla rete e ripristinare la sicurezza. La differenza principale tra "Purge" e "Destroy" riguarda il modo in cui vengono trattate le informazioni sensibili:

- Purge: Il processo di purga comporta la cancellazione sicura dei dati sensibili dal sistema compromesso. Questo processo rende i dati irrecuperabili utilizzando metodi standard di recupero dati, ma il sistema stesso rimane intatto. La purga può essere utile quando è necessario conservare l'hardware del sistema per scopi futuri, ma si desidera eliminare in modo sicuro i dati sensibili.

- Destroy: La distruzione coinvolge la demolizione fisica o la cancellazione irreversibile del sistema compromesso. Questo processo assicura che sia i dati sensibili che l'hardware del sistema non siano recuperabili. La distruzione è appropriata quando non ci sono requisiti per mantenere l'hardware del sistema e quando è necessario garantire che nessuna informazione sensibile sia compromessa.

- Clear: Il processo di "Clear" coinvolge la rimozione delle informazioni sensibili in modo che non siano più accessibili da un utente non autorizzato, ma lascia intatto il sistema stesso. Questo può essere fatto mediante la formattazione dei dischi o l'eliminazione dei file sensibili. Tuttavia, è importante notare che la cancellazione dei dati può non essere sufficiente per garantire che non possano essere recuperati, quindi, se necessario, possono essere utilizzati metodi aggiuntivi come sovrascrittura dei dati o criptazione.

In questo scenario di attacco in corso, la scelta tra Purge, Destroy e Clear dipenderà dalle esigenze specifiche del caso, inclusi i requisiti di conservazione dei dati e la sicurezza dell'organizzazione.