Pratica W20D1

Traccia:

EPICODE

Esercizio
Incident response

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**

Soluzione:

Per risolvere la situazione di compromissione del sistema B, è necessario seguire un approccio metodico che coinvolga l'isolamento del sistema compromesso, la sua rimozione e la gestione delle informazioni sensibili contenute nei dischi compromessi. Di seguito, verranno descritte le tecniche richieste:

I) Isolamento:

1. **Disconnettere il sistema dalla rete:** Questo impedisce all'attaccante di continuare a eseguire azioni dannose o di estrarre ulteriori informazioni.
2. **Disabilitare le connessioni remote:** Assicurarsi che non ci siano sessioni attive o possibilità di accesso remoto al sistema compromesso.
3. **Isolare fisicamente il sistema:** Se possibile, disconnettere fisicamente il sistema dalla rete e da altri dispositivi per evitare la diffusione dell'attacco.

II) Rimozione del sistema B infetto:

1. **Spegnere il sistema:** Interrompere tutte le attività in corso e prepararsi per la rimozione fisica.
2. **Rimuovere i dischi rigidi:** Estrai i dischi rigidi dal sistema compromesso.
3. **Sostituire i dischi rigidi:** Se possibile, sostituire i dischi rigidi compromessi con nuovi dischi per evitare il rischio di reinfezione.
4. **Analisi forense:** Prima di rimuovere completamente il sistema dalla rete, effettuare un'analisi forense per identificare la natura e l'entità dell'attacco.

Differenza tra Purge, Destroy e Clear:

1. **Purge:** Nel contesto della sicurezza informatica, "purge" si riferisce alla procedura di eliminazione sicura dei dati. In questo caso, si tratta di sovrascrivere i dati sui dischi rigidi compromessi con dati casuali per rendere le informazioni precedentemente memorizzate irrilevanti e irrecuperabili.
2. **Destroy:** "Destroy" indica la distruzione fisica dei dispositivi di memorizzazione, come dischi rigidi o supporti di memoria, per impedire il recupero dei dati. Questa può includere la perforazione dei dischi rigidi o l'uso di macchine per la distruzione fisica.
3. **Clear:** Questo termine può riferirsi a una varietà di operazioni volte a eliminare i dati sensibili dai dispositivi di memorizzazione. Tuttavia, in genere non garantisce la sicurezza totale dei dati eliminati e può essere soggetto a recupero tramite tecniche specializzate.

Prima di eseguire qualsiasi azione di Purge, Destroy o Clear, è fondamentale consultare le politiche di sicurezza dell'organizzazione e seguire le procedure stabilite per la gestione dei dati sensibili e la distruzione dei dispositivi di memorizzazione compromessi.