Immagine che contiene testo, schermata, Carattere, algebra

Descrizione generata automaticamente

Immagine che contiene diagramma, testo, linea, Piano

Descrizione generata automaticamente

I) Tecniche di Isolamento:

1. Disconnessione dalla rete e isolamento completo: la prima azione da intraprendere è disconnettere il sistema compromesso, il sistema B (database con diversi dischi per lo storage) dalla rete.
2. Analisi del traffico di rete: dopo aver effettuato l'isolamento completo, è importante condurre un'analisi del traffico di rete per identificare eventuali comportamenti anomali o attività sospette che potrebbero indicare altri dispositivi compromessi o tentativi di attacco in corso. Si effettuano anche i controlli per verificare se sono stati iniettati dei malware nel sistema, se è stato iniettato il malware si dovrebbe procedere con il processo Destroy con il sistema B infetto. Se non è stato iniettato nessun malware, si procede con i metodi Clear e Purge.

Dopo aver verificato, modifichiamo le impostazioni di firewall per bloccare completamente l’attaccante.

II) Rimozione del sistema B infetto:

Una volta che il sistema B è stato isolato dalla rete e sono state implementate le misure di sicurezza aggiuntive, è possibile procedere con la rimozione del sistema infetto utilizzando i metodi di "Clear" e "Purge".

1. Clear: utilizzare il metodo "Clear" per rimuovere i dati sensibili dal sistema B in modo sicuro senza distruggere fisicamente i dispositivi di memorizzazione. Questo può comportare l'eliminazione dei file di log, delle credenziali di accesso e di altre informazioni sensibili che potrebbero essere presenti nel sistema.
2. Purge: successivamente, utilizzare il metodo "Purge" per sovrascrivere in modo sicuro i dati rimanenti sul sistema B con informazioni casuali o inutili. Questo processo rende i dati originali irrecuperabili, garantendo che non possano essere recuperati o utilizzati dall'attaccante.

Dopo aver eseguito le operazioni di "Clear" e "Purge", è consigliabile eseguire un'ulteriore verifica per assicurarsi che tutti i dati sensibili siano stati rimossi in modo sicuro e che il sistema sia pronto per la successiva fase di ripristino o ricostruzione.

Nel caso in cui sia avvenuto l’iniettamento di un malware si procede con Destroy.

Destroy: Il processo di distruzione comporta la fisica distruzione dei supporti di memorizzazione, come dischi rigidi o dispositivi di memorizzazione, rendendoli irrecuperabili e non utilizzabili. Questo metodo è estremamente sicuro, ma può comportare costi aggiuntivi per sostituire l'hardware distrutto.

In conclusione, Clear è il metodo più semplice che elimina i dati ma li rende ancora recuperabili, Purge sovrascrive i dati per renderli irrecuperabili e Destroy distrugge fisicamente il dispositivo di memorizzazione per garantire che i dati non siano più accessibili. La scelta del metodo dipende dall'entità della sensibilità dei dati e dalle politiche di sicurezza dell'organizzazione.