2024

EPICODE

CS0124

REPORT

Week 9 Lesson 4

PREPARED BY : Bruno Falconi

Report sulla Compromissione del Sistema B e le Misure di Mitigazione

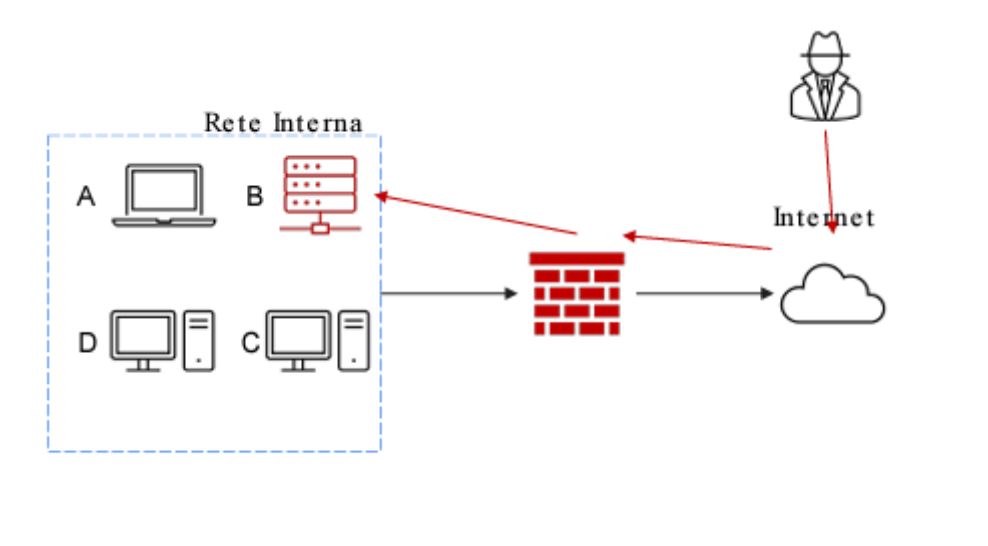
Traccia:

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, Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear**

Situazione Attuale:

Il sistema B, un database con diversi dischi per lo storage, è stato completamente compromesso da un attaccante che è riuscito a violare la rete e ad accedere al sistema tramite Internet. L'attacco è attualmente in corso, richiedendo una risposta immediata da parte del team CSIRT per limitare i danni e ripristinare l'integrità del sistema.



Tecniche di Isolamento:

1. **Disconnessione dalla Rete: Il sistema B compromesso deve essere immediatamente disconnesso dalla rete per prevenire ulteriori accessi non autorizzati.**
2. **Segmentazione della Rete: Se il sistema B condivide la rete con altri dispositivi, è necessario segmentare la rete per impedire la propagazione dell'attacco ad altri dispositivi.**
3. **Configurazione del Firewall: Verificare e aggiornare le regole del firewall per bloccare qualsiasi traffico sospetto o non autorizzato che potrebbe compromettere ulteriormente il sistema B.**

Tecniche di Rimozione del Sistema B Infetto:

1. **Isolamento Fisico: Il sistema B compromesso deve essere fisicamente isolato dalla rete e dagli altri dispositivi per evitare la diffusione dell'attacco.**
2. **Backup dei Dati: Prima della rimozione, è essenziale eseguire un backup completo dei dati critici per garantirne la disponibilità e l'integrità.**
3. **Formattazione dei Dischi: Tutti i dischi del sistema B devono essere formattati per eliminare qualsiasi traccia dell'attacco e dei dati compromessi.**
4. **Analisi Forense: Condurre un'analisi forense per identificare l'estensione dell'attacco, le vulnerabilità sfruttate e le contromisure necessarie per prevenirne il ripetersi.**

Differenza tra Purge, Destroy e Clear per l'Eliminazione delle Informazioni Sensibili:

1. **Purge: Questa tecnica comporta il sovrascrivere ripetutamente i dati sensibili con sequenze casuali di bit, rendendo i dati originali irrecuperabili. È utile per eliminare in modo permanente informazioni altamente sensibili.**
2. **Destroy: Questo metodo implica la distruzione fisica dei dispositivi di storage, come i dischi rigidi, garantendo che le informazioni non possano essere recuperate. È una misura estrema utilizzata quando la sicurezza dei dati è di massima importanza.**
3. **Clear: "Clear" indica la rimozione dei dati da un dispositivo senza danneggiarlo fisicamente. Tuttavia, questa tecnica non garantisce la totale irrecuperabilità delle informazioni e potrebbe consentire il recupero dei dati tramite tecniche avanzate.**

Conclusioni:

La risposta a un attacco che ha compromesso interamente il sistema B richiede una serie di misure di isolamento e rimozione immediate. È cruciale adottare le tecniche di isolamento del firewall, insieme a misure fisiche e digitali, per garantire la sicurezza dei dati sensibili e prevenire futuri attacchi. La comprensione delle differenze tra Purge, Destroy e Clear è fondamentale per garantire l'irrecuperabilità delle informazioni sensibili durante la gestione dell'incidente. Una corretta analisi forense può anche fornire informazioni cruciali per migliorare le difese del sistema e prevenire futuri attacchi.