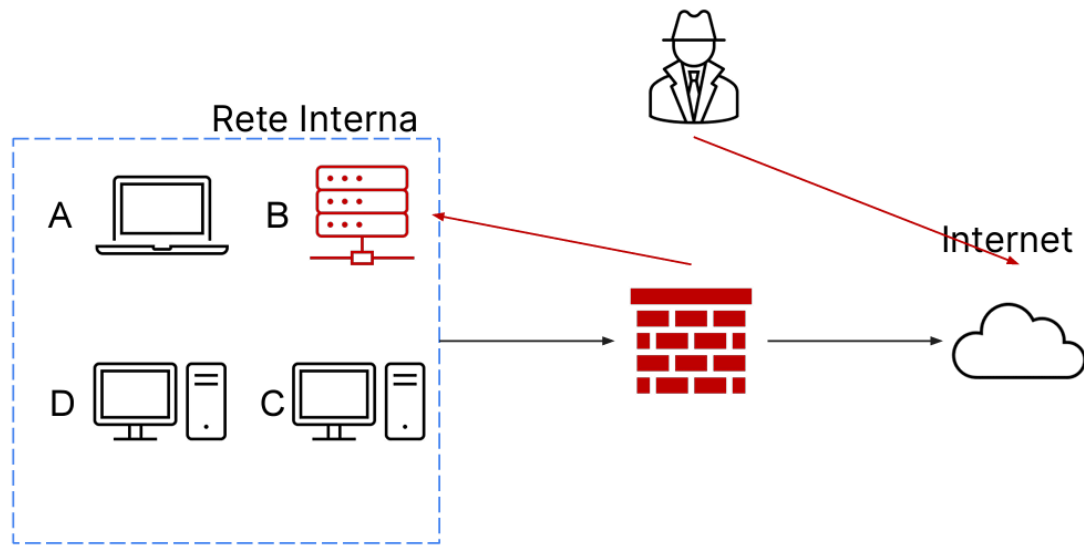


CONSEGNA S9/L4



Con riferimento alla figura sopra, 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

1 - Tecniche di Isolamento Dettagliate:

Isolamento Fisico Approfondito:

- **Rimozione di Connessioni:** Disconnettere il sistema B da tutte le connessioni di rete e qualsiasi altro dispositivo esterno per impedire trasferimenti di dati non autorizzati.
- **Sicurezza Fisica:** Posizionare il sistema in un'area sicura che richiede l'autorizzazione per l'accesso, garantendo che nessun individuo non autorizzato possa fisicamente accedere al dispositivo durante l'analisi.

Isolamento Logico Esteso:

- **Disattivazione di Servizi:** Disabilitare tutti i servizi di rete e i processi che potrebbero consentire la comunicazione remota o il controllo del sistema B.
- **Modifica della Configurazione di Rete:** Cambiare gli indirizzi IP, le credenziali di accesso e le chiavi crittografiche per isolare ulteriormente il sistema B e prevenire l'accesso remoto.

Isolamento a Livello di Sistema Operativo:

- **Modifiche alle Policy di Sicurezza:** Aggiornare le policy di sicurezza del sistema operativo per limitare l'esecuzione di processi e servizi non essenziali.
- **Interruzione dei Processi Sospetti:** Identificare e terminare immediatamente i processi sospetti in esecuzione sul sistema B per prevenire ulteriori danni o furti di dati.

2 - Tecniche di Rimozione del Sistema B Infetto:

Preparazione per la Rimozione:

- **Backup Selettivo:** Creare backup dei dati critici che non sono stati compromessi, assicurandosi di non includere nessun file infetto o sospetto.
- **Cancellazione Sicura della Cache e delle Sessioni:** Pulire tutte le cache e le sessioni attive per rimuovere le informazioni temporanee che potrebbero contenere dati sensibili.

Rimozione Fisica:

- **Etichettatura e Documentazione:** Prima della rimozione fisica, etichettare il sistema B e documentare il suo stato, specificando la posizione, l'ora e la data di rimozione.
- **Gestione dell'Integrità del Sistema:** Mantenere l'integrità fisica del sistema B per l'analisi forense, assicurandosi che non venga alterato o danneggiato durante la rimozione.

Disattivazione e Rimozione Logica:

- **Disattivazione Remota:** Se possibile, utilizzare strumenti di gestione IT centralizzata per disattivare o 'spegnere' il sistema B da remoto prima della rimozione fisica.
- **Rimozione da Inventory e Asset Management:** Aggiornare i sistemi di gestione degli inventari per riflettere che il sistema B è stato rimosso e non è più in uso.

Protocolli di Trasporto e Smaltimento:

- **Trasporto Sicuro:** Assicurarsi che il sistema B sia trasportato in modo sicuro fino al luogo di analisi o distruzione, evitando esposizioni e rischi durante il trasporto.
- **Smaltimento Certificato:** Se il sistema B è destinato alla distruzione, utilizzare servizi certificati per lo smaltimento che garantiscono l'eliminazione sicura e rispettosa dell'ambiente dei rifiuti elettronici.

Differenze tra Purge e Destroy

Purge (Purgare): Questo processo implica la rimozione delle informazioni sensibili in modo che non possano essere recuperate con strumenti standard di recupero dati. Tecniche di purging includono il sovrascrivere i dati con pattern specifici di bit, l'uso di campi magnetici per disturbare i dati sul disco (degaussing) o l'uso di software di cancellazione certificato.

- **Metodi di Sovrascrittura:** Utilizzare standard come quello definito dal National Institute of Standards and Technology (NIST) per sovrascrivere i dati più volte con sequenze di bit casuali.

- **Degaussing:** Applicare un potente campo magnetico che disturba l'allineamento magnetico delle particelle di memoria, rendendo i dati irrecuperabili.

Destroy (Distruggere): La distruzione è il processo di eliminare fisicamente i dispositivi di archiviazione in modo che non possano essere utilizzati o recuperati in alcun modo. Questo può includere il frantumare, il tritare, l'incenerire, o l'annientare completamente i dischi rigidi o altri dispositivi di memorizzazione.

- **Metodi Fisici:** Utilizzare presse idrauliche, martelli pneumatici o inceneritori industriali per distruggere fisicamente i dischi rigidi.
- **Certificazione di Distruzione:** Ottenere una certificazione da parte di un'azienda specializzata che attesti la completa distruzione del materiale, assicurandosi che rispetti i protocolli di sicurezza e ambientali.

Prima di procedere allo smaltimento dei dischi compromessi, è importante considerare il livello di sensibilità dei dati e i requisiti normativi o di conformità. Il purge è spesso preferito quando i dispositivi devono essere riutilizzati o donati, mentre il destroy è più adatto quando i dispositivi sono alla fine del loro ciclo di vita utile o quando i dati presenti sono estremamente sensibili e non devono assolutamente cadere nelle mani sbagliate.