REPORT 22/12/2022 LORENZO SCORBAIOLI

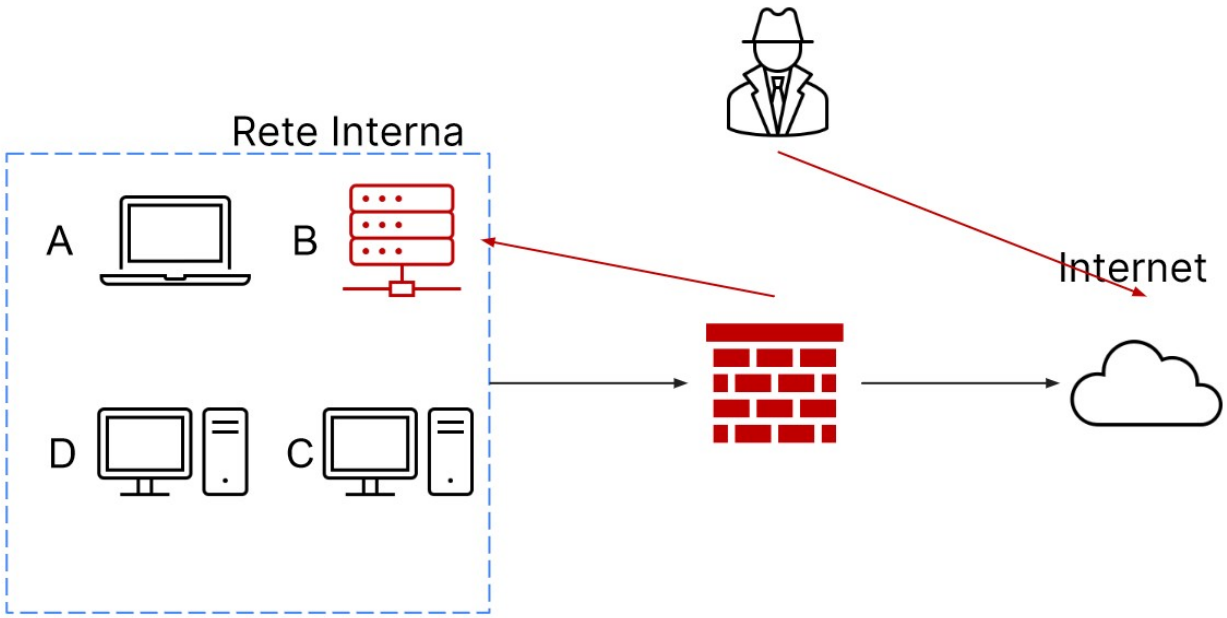
TASK:
Con riferimento alla figura, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team CSIRT. Rispondere ai seguenti quesiti:

- Mostrare le tecniche di:

    1. Isolamento
    2. Rimozione del sistema B infetto

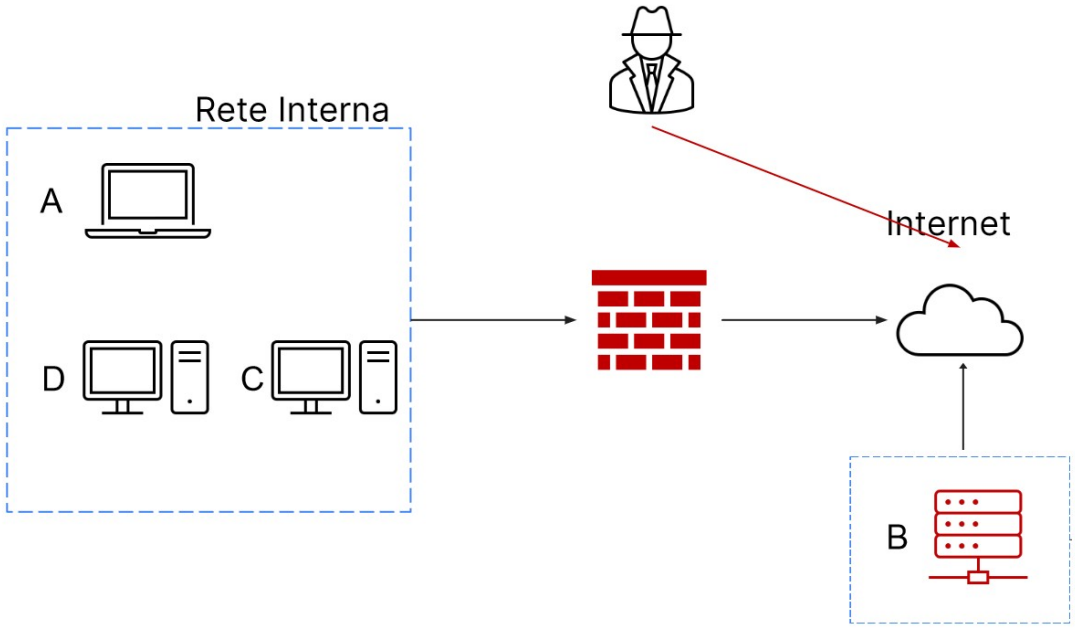
- Spiegare le differenze per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi tra:

    1. Purge
    2. Destroy
    3. Clear



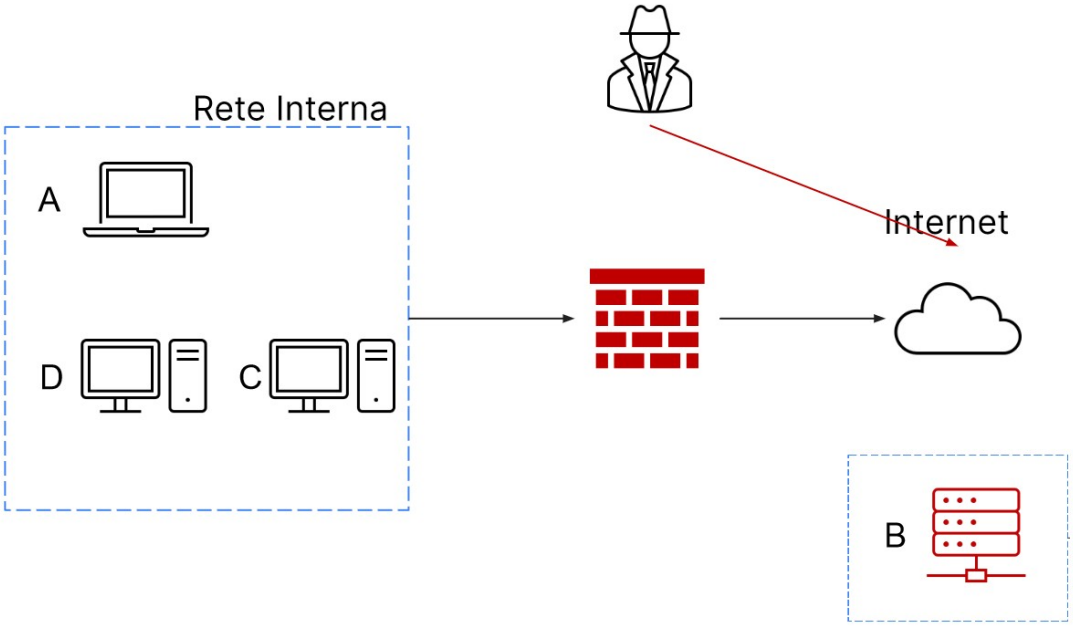
Da quanto descritto nella traccia, ci troviamo nella fase di contenimento, in quanto, come sappiamo, il sistema B è soggetto di un attacco ancora in corso. La fase di contenimento è la terza fase di un piano di risposta agli incidenti e deve cominciare il prima possibile. Il suo scopo primario è quello di isolare l'incidente in modo che non possano essere fatti ulteriori danni ai sistemi che sono sulla stessa rete o alle reti adiacenti. Una tra le varie tecniche preventive e strategiche per la gestione di tali incidenti è la segmentazione. La traccia ci richiede di mostrare 2 tecniche di contenimento.

ISOLAMENTO:



L’immagine qui sopra rappresenta la soluzione di contenimento denominata “ISOLAMENTO”. Con questa modalità il sistema B infetto viene levato dalla rete interna in modo che l’accesso alla rete interna da parte dell’attaccante sia ristretto. Tuttavia come possiamo vedere dall’immagine il sistema infetto ha ancora la possibilità di accedere ad internet.

RIMOZIONE



La soluzione di contenimento, denominata “RIMOZIONE”, che può essere vista nell’immagine qui sopra,invece rappresenta la tecnica di contenimento più stringente. Il sistema infetto viene completamente rimosso sia dalla rete interna che da internet. In questo modo l’attaccante non ha più accesso né alla rete interna né alla macchina infettata.

La fase di contenimento, una volta completata, è seguita dalla fase di rimozione dell'incidente. Tale fase ha come scopo quello di eliminare qualunque attività, componente o processo che rimane dell'incidente all'interno delle reti o sui sistemi.

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia quindi la fase di recupero. Durante questa fase dobbiamo andare a gestire lo smaltimento o eventualmente il riutilizzo di un disco o di un sistema di storage del sistema che è stato compromesso. Diventa quindi fondamentale che ci si accerti che le informazioni contenute sulla componente di memoria siano inaccessibili e non recuperabili. Vengono individuate tre opzioni per la gestione di questo tipo di problematica, denominata "Media Sanitization":

1) CLEAR:

Applica tecniche logiche per disinfettare i dati in tutte le posizioni di archiviazione indirizzabili dall'utente per la protezione da semplici tecniche di recupero dati non invasive; tipicamente applicato tramite i comandi standard di lettura e scrittura al dispositivo di archiviazione, ad esempio tramite la riscrittura con un nuovo valore o utilizzando un'opzione di menu per ripristinare il dispositivo allo stato di fabbrica (dove la riscrittura non è supportata).

2) PURGE:

Applica tecniche fisiche o logiche che rendono impossibile il recupero di Target Data utilizzando tecniche di laboratorio all'avanguardia. Un esempio di purge è l'utilizzo di forti magneti per rendere inaccessibili le informazioni contenute su dischi magnetici.

3) DESTROY:

Rendere impossibile il recupero dei dati Target e si traduce nella conseguente impossibilità di utilizzare il supporto per la memorizzazione dei dati. Si usano approcci logici e fisici come quelli utilizzati sia nel clear che nel purge insieme a tecniche di laboratorio quali la disintegrazione e la polverizzazione dei media ad alte temperature

http://acloudguru-content-attachment-production.s3.amazonaws.com/1596474778843-nist-sp-800-88r1_1514321198.pdf

METODO	DESCRIZIONE
CLEAR	Un metodo per disinfettare i supporti consiste nell'utilizzare prodotti software o hardware per sovrascrivere spazio di archiviazione indirizzabile sul supporto con dati non sensibili, utilizzando lo standard read e scrivere i comandi per il dispositivo. Questo processo può includere la sovrascrittura non solo della logica posizione di archiviazione di uno o più file (ad es. tabella di allocazione dei file) ma dovrebbe anche includere tutte le sedi indirizzabili. L'obiettivo di sicurezza del processo di sovrascrittura è sostituire i dati di destinazione con dati non sensibili. La sovrascrittura non può essere utilizzata per supporti danneggiati o meno riscrivibile e potrebbe non indirizzare tutte le aree del dispositivo in cui potrebbero essere presenti dati sensibili trattenuto. Anche il tipo e le dimensioni del supporto possono influenzare l'idoneità della sovrascrittura metodo di sanificazione. Ad esempio, i dispositivi di archiviazione basati su memoria flash possono contenere unità di riserva celle ed eseguire il livellamento dell'usura, rendendo impossibile per un utente disinfettare tutti i dati precedenti utilizzando questo approccio perché il dispositivo potrebbe non supportare l'indirizzamento diretto di tutte le aree in cui i dati sensibili sono stati archiviati utilizzando l'interfaccia di lettura e scrittura nativa. L'operazione Clear può variare contestualmente per supporti diversi dai dispositivi di archiviazione dedicati, dove il dispositivo (come un telefono cellulare di base o un'apparecchiatura per ufficio) fornisce solo la possibilità di riporta il dispositivo allo stato di fabbrica (in genere semplicemente eliminando i puntatori di file) e non direttamente supportare la capacità di riscrivere o applicare tecniche specifiche del supporto ai contenuti di archiviazione non volatile. Laddove la riscrittura non è supportata, i reset del produttore e le procedure che non includono la riscrittura potrebbe essere l'unica opzione per cancellare il dispositivo e il supporto associato. Ciò soddisfa ancora la definizione di CLEAR fintanto che l’interfaccia del dispositivo disponibile per l’utente non facilita il recupero dei dati cancellati.
PURGE	Alcuni metodi di spurgo (che variano a seconda del supporto e devono essere applicati con considerazioni descritti più avanti in questo documento) includono sovrascrittura, cancellazione di blocchi e cancellazione crittografica, attraverso l'uso di comandi dedicati e standardizzati di sanificazione del dispositivo che applicano tecniche specifiche dei media per aggirare l'astrazione insita nella tipica lettura e scrivere comandi. Le tecniche distruttive rendono anche il dispositivo Purged quando applicato efficacemente al tipo di supporto appropriato, inclusi incenerimento, triturazione, disintegrazione, smagnetizzazione e polverizzazione. Il vantaggio comune a tutti questi approcci è la garanzia che i dati siano impossibile da recuperare utilizzando tecniche di laboratorio all'avanguardia. Tuttavia, piegatura, taglio e l'uso di alcune procedure di emergenza (come l'uso di un'arma da fuoco per sparare un buco attraverso un dispositivo di archiviazione) può solo danneggiare il supporto in quanto parti del supporto potrebbero rimanere intatti e quindi accessibili mediante tecniche di laboratorio avanzate. La smagnetizzazione rende un Legacy Magnetic Device Purged quando la forza della smagnetizzazione è accuratamente abbinata alla coercitività mediatica. La coercitività può essere difficile da determinare basandosi solo su informazioni fornite in etichetta. Pertanto, fare riferimento al produttore del dispositivo per i dettagli sulla coercitività. La smagnetizzazione non dovrebbe mai essere utilizzata esclusivamente per i dispositivi di archiviazione basati su memoria flash o per dispositivi di archiviazione magnetica che contengono anche memoria non magnetica non volatile. La smagnetizzazione rende inutilizzabili molti tipi di dispositivi (e in questi casi anche la smagnetizzazione è una distruzione tecnica)
DESTROY	Esistono molti tipi, tecniche e procedure diversi per la distruzione dei media. Mentre alcune tecniche potrebbero rendere impossibile il recupero dei dati target attraverso il dispositivo interfaccia e non utilizzabile per la successiva memorizzazione dei dati, il dispositivo non è considerato distrutto a meno che il recupero dei dati target non sia fattibile utilizzando un tecniche di laboratorio all'avanguardia. • Disintegrare, polverizzare, fondere e incenerire. Questi metodi di sanificazione sono progettati per distruggere completamente i media. Di solito vengono eseguiti con la distruzione di metalli in una struttura di incenerimento autorizzata con la specifica capacità di svolgere queste attività • Distruggi. I distruggidocumenti possono essere utilizzati per distruggere supporti flessibili come i dischetti una volta che i supporti sono stati rimossi fisicamente dai loro contenitori esterni. La

dimensione del brandello dei rifiuti dovrebbe essere abbastanza piccolo da garantire una ragionevole sicurezza proporzionalmente alla riservatezza dei dati che i dati non possono essere ricostruiti.

A rendere ancora più difficile la ricostruzione dei dati, il materiale triturato può essere mescolato con materiale non sensibile dello stesso tipo (ad esempio, carta triturata o supporti flessibili triturati). L'applicazione di tecniche distruttive può essere l'unica opzione quando i media falliscono e le tecniche Clear o Purge non possono essere applicate efficacemente ai media o quando la verifica dei metodi Clear o Purge non riescono (per motivi noti o sconosciuti).