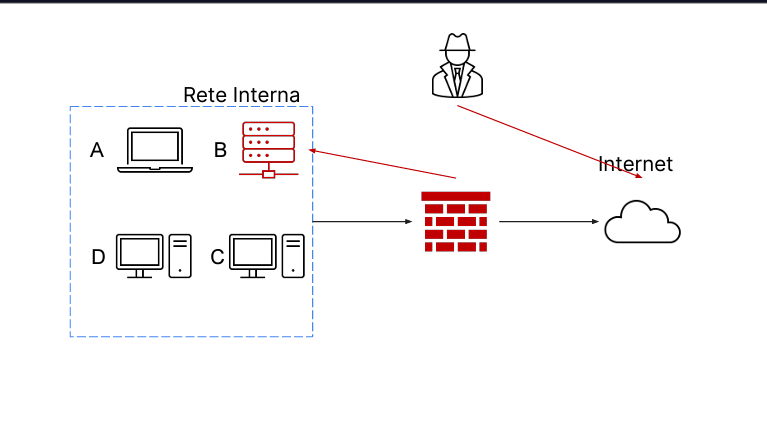
Il sistema B, parte di una rete interna che include anche altri dispositivi (A, C, D) e un database con diversi dischi per lo storage, è stato compromesso da un attacco proveniente da internet. Il compito assegnato è quello di operare come parte di un CSIRT (Computer Security Incident Response Team) e rispondere ai seguenti quesiti:

1. Tecniche di isolamento e rimozione del sistema B infetto.
2. Differenza tra i concetti di "Purge" e "Destroy" per la rimozione di informazioni sensibili prima di smaltire i dischi compromessi.



**Tecniche di Isolamento e Rimozione del Sistema B Infetto**

Isolamento:

L'isolamento di un sistema infetto è il primo passo critico per contenere l'attacco e prevenire ulteriori danni. Le tecniche di isolamento includono:

* Disconnessione fisica: Staccare il sistema B dalla rete, disconnettendo i cavi di rete o disabilitando le interfacce di rete wireless.
* Disconnessione logica: Disabilitare da remoto l'accesso al sistema B attraverso il firewall o lo switch di rete, impedendo il traffico in entrata e in uscita dal sistema.
* VLAN di isolamento: Spostare il sistema B in una VLAN separata configurata per isolare il traffico di rete da e verso il sistema B.
* Regole del firewall: Impostare regole specifiche nel firewall per bloccare tutto il traffico di rete verso e dal sistema B.

Rimozione

Dopo l'isolamento, il passo successivo è la rimozione del malware o l'eliminazione dell'accesso non autorizzato. Le tecniche includono:

* Scansione antivirus/antimalware: Eseguire una scansione approfondita con software antivirus o antimalware aggiornato per identificare e rimuovere le minacce.
* Analisi forense: Utilizzare strumenti di analisi forense per comprendere l'entità della compromissione e rimuovere componenti dannosi.
* Ripristino da backup: Se il sistema è troppo compromesso, può essere necessario ripristinare B da un backup sicuro e pulito.
* Reinstallazione del sistema: In alcuni casi, la rimozione completa del malware può richiedere una reinstallazione completa del sistema operativo e delle applicazioni.

Differenza tra Purge e Destroy

**Purge**: Il processo di purga si riferisce all'uso di metodi software per rimuovere in modo sicuro le informazioni sensibili da un supporto di memorizzazione in modo che non possano essere recuperate. Ciò include la sovrascrittura dei dati con pattern di dati casuali o specifici più volte per impedire il recupero dei dati originari.

**Destroy**: La distruzione fisica del supporto di memorizzazione è la distruzione materiale dei dispositivi di storage (come i dischi rigidi) in modo che non sia fisicamente possibile recuperare i dati. Questo può includere frantumazione, triturazione, smagnetizzazione (degaussing), o incenerimento.

**Clear**: Questo processo consiste nel rimuovere le informazioni in modo che non possano essere recuperate con l'ausilio di strumenti software standard di lettura dei dati. Nella pratica, ciò può essere realizzato sovrascrivendo tutti i dati con zeri o valori casuali una o più volte. Sebbene questo metodo impedisca il recupero dei dati attraverso metodi software comuni, potrebbe non essere sufficiente contro tecniche avanzate di recupero dati che possono utilizzare l'analisi del hardware o laboratori forensi specializzati. Il processo di "Clear" è generalmente considerato sicuro per la protezione da minacce di basso livello ed è spesso impiegato quando il supporto di memorizzazione rimarrà all'interno di un'organizzazione sicura.

In sintesi, il "Clear" è adeguato per la protezione interna e contro attori con capacità limitate, il "Purge" fornisce un livello di sicurezza superiore adatto a quando i dispositivi potrebbero lasciare un ambiente controllato, e il "Destroy" è utilizzato quando non si vuole che i dati siano recuperabili sotto alcuna circostanza.