1. Isolamento del Sistema Compromesso (Sistema B)

L'isolamento è il primo passo per contenere l'attacco e limitare la propagazione della compromissione ad altri sistemi.

Passaggi per l'Isolamento:

- **Scollegare il sistema dalla rete**: Il sistema B deve essere scollegato immediatamente dalla rete interna e da Internet per impedire ulteriori attività dannose o movimenti laterali (esplorazione di altri sistemi all'interno della rete). Questo può essere fatto disabilitando le interfacce di rete, scollegando cavi fisici o configurando regole di firewall che blocchino il traffico verso e dal sistema infetto.
- **Bloccare l'accesso remoto**: Impedire ulteriori accessi remoti al sistema compromesso, soprattutto se l'attaccante ha acquisito credenziali amministrative o creato backdoor. Si possono usare tecniche come disabilitare l'accesso SSH, chiudere porte aperte e revocare accessi VPN.
- **Limitare i privilegi degli utenti**: Se ci sono utenti con accessi privilegiati sul sistema B, le loro credenziali dovrebbero essere temporaneamente disabilitate o revocate, per ridurre il rischio che vengano abusate dall'attaccante.
- **Monitoraggio delle comunicazioni**: Configurare sistemi di monitoraggio (ad esempio, intrusion detection systems - IDS) per rilevare tentativi di comunicazione anomali tra il sistema infetto e altri nodi. Se necessario, utilizzare uno strumento come Wireshark o tcpdump per ispezionare il traffico in tempo reale.
- **Isolare altri componenti**: Se il database compromesso è distribuito, potrebbe essere necessario isolare anche gli altri dischi o nodi coinvolti nello storage per evitare che i dati infetti o l'accesso malevolo si propaghino su altri segmenti del sistema.

2. Rimozione del Sistema B Infetto

Una volta isolato il sistema compromesso, è necessario rimuoverlo e iniziare le operazioni di ripristino e bonifica.

Passaggi per la Rimozione:

- **Spegni il sistema compromesso**: In alcuni casi, può essere utile spegnere completamente il sistema per prevenire ulteriori danni e per preservare lo stato attuale per la successiva analisi forense. Tuttavia, spegnere il sistema può eliminare informazioni cruciali, come la memoria volatile, quindi valuta attentamente questa azione.
- **Backup e raccolta prove**: Prima di procedere con la pulizia o la reinstallazione del sistema, è importante raccogliere prove forensi. Crea un'immagine completa del disco, raccogli file di log, dump di memoria, e altre tracce utili per l’analisi successiva. Questa fase è fondamentale per comprendere l’entità della compromissione e, eventualmente, identificare l’attaccante.
- **Analisi forense**: Utilizza strumenti di analisi forense per investigare la causa e l'entità della compromissione. Strumenti come **FTK Imager** o **Autopsy** possono aiutare a identificare file modificati, malware installati, o tracce lasciate dall'attaccante.
- **Ripristino da backup**: Dopo aver isolato e rimosso il sistema infetto, ripristina il sistema da un backup verificato, assicurandoti che i backup non siano stati compromessi dall'attaccante. Il backup dovrebbe essere precedente all'attacco e attentamente esaminato per evitare di reintrodurre malware.

- **Rimozione del malware e bonifica**: Se non è possibile ripristinare il sistema da un backup, procedi con la rimozione del malware e la pulizia del sistema. Questo può includere:
    - **Scansione antivirus** e anti-malware.
    - Rimozione di eventuali backdoor o strumenti di controllo remoto installati.
    - Bonifica delle chiavi di registro, servizi anomali, o processi sospetti.
- **Reinstallazione del sistema operativo e applicazioni**: In molti casi, la soluzione più sicura è una reinstallazione completa del sistema operativo. Una reinstallazione pulita garantisce che il sistema sia completamente privo di malware o configurazioni compromesse. Assicurati di applicare tutte le patch e aggiornamenti di sicurezza più recenti.
- **Verifica dell'integrità dei dati**: Dopo il ripristino, è essenziale verificare l'integrità dei dati del database. Controlla che non ci siano state alterazioni o corruzioni, e se necessario, esegui una revisione manuale dei dati critici.

Differenza tra Purge,Destroy e Clear

1. Clear (Cancellazione superficiale o sovrascrittura semplice)

Clear è il processo che prevede la rimozione delle informazioni dagli strumenti di archiviazione in modo tale che possano essere riutilizzati nel medesimo ambiente operativo. Questo metodo di cancellazione è considerato meno sicuro rispetto a "Purge" e "Destroy" poiché si limita alla rimozione logica o alla sovrascrittura dei dati. Può essere effettuato con:

- **Cancellazione software**: Ad esempio, eliminando file o directory tramite comandi standard del sistema operativo. Tuttavia, ciò non garantisce la rimozione definitiva dei dati, poiché rimangono tracce nei settori fisici del disco.
- **Sovrascrittura singola**: Sovrascrive i dati una o più volte con valori casuali o con zeri per evitare che possano essere facilmente recuperati tramite strumenti software. Questo metodo è generalmente efficace per proteggere da tentativi di recupero di dati casuali, ma i dati possono ancora essere recuperati con tecniche avanzate.

Scenario di utilizzo: Si usa per dischi che devono essere riutilizzati in ambienti controllati e dove non vi è una minaccia significativa di attacchi avanzati (ad esempio, dischi di backup che rimangono all'interno dell'organizzazione).

2. Purge (Sanitizzazione avanzata)

Purge è una tecnica più sicura di cancellazione dei dati rispetto a "Clear". Questo metodo rende i dati irrecuperabili anche utilizzando strumenti software o hardware avanzati. La sanitizzazione in modalità Purge può essere effettuata in vari modi:

- **Sovrascrittura multipla**: I dati vengono sovrascritti più volte (ad esempio, tre passaggi) con valori casuali o modelli specifici per rendere difficile, se non impossibile, il recupero dei dati anche con strumenti di recupero sofisticati.
- **Cancellazione crittografica (Cryptographic Erase)**: Se il disco utilizza crittografia a livello di hardware o software, "Purge" può essere eseguito distruggendo semplicemente le chiavi crittografiche che proteggono i dati. Questo rende i dati illeggibili senza dover sovrascrivere effettivamente l'intero contenuto del disco.
- **Demagnetizzazione (Degaussing)**: Per i dischi magnetici, come gli hard disk tradizionali, può essere utilizzato un degausser che distrugge i dati creando un potente campo magnetico che azzera i dati registrati.

Scenario di utilizzo: È adatto per dischi che devono essere riutilizzati in ambienti meno controllati, ma dove vi è necessità di una maggiore sicurezza rispetto alla semplice sovrascrittura (ad esempio, per la dismissione di server o dischi contenenti dati sensibili in ambienti aziendali).

3. Destroy (Distruzione fisica)

Destroy è il metodo più drastico e sicuro per l'eliminazione dei dati sensibili. Questo processo implica la distruzione fisica del disco, rendendo impossibile il recupero delle informazioni contenute all'interno. Le tecniche di distruzione includono:

- **Frantumazione**: Il disco viene fisicamente frantumato in piccoli pezzi utilizzando attrezzature specializzate come uno **shredder** (trituratore). Questa è una delle tecniche più comuni e garantisce che i dati non possano essere recuperati.
- **Incenerimento**: Il disco viene distrutto bruciandolo ad alte temperature in un forno apposito. Questo metodo assicura che il supporto fisico e i dati vengano completamente distrutti.
- **Perforazione o schiacciamento**: Il disco viene perforato o schiacciato tramite dispositivi specifici che rendono impossibile il suo utilizzo e il recupero dei dati.

Scenario di utilizzo: "Destroy" viene impiegato quando i dischi o i supporti devono essere definitivamente dismessi e vi è una necessità assoluta di evitare qualsiasi possibilità di recupero dei dati (ad esempio, per dischi contenenti segreti industriali, dati personali sensibili o informazioni riservate governative).

Riepilogo:

- **Clear**: Metodo di cancellazione logico o sovrascrittura leggera, utile quando si intende riutilizzare il disco in ambienti controllati. Non protegge contro attacchi avanzati di recupero dati.
- **Purge**: Sanitizzazione avanzata che impedisce il recupero dei dati anche tramite strumenti specializzati. Adatto a dischi che potrebbero essere riutilizzati o dismessi in ambienti meno controllati, ma che contengono dati sensibili.
- **Destroy**: Distruzione fisica del disco, rendendo i dati irrecuperabili. È la tecnica più sicura e definitiva per la gestione di informazioni estremamente sensibili.

La scelta tra questi metodi dipende dal livello di sensibilità dei dati e dall'ambiente in cui verranno riutilizzati o smaltiti i supporti di archiviazione.