Isolamento del sistema B infetto:

Isolamento: Per isolare il sistema B infetto, è essenziale disconnetterlo dalla rete e da qualsiasi altro sistema interconnesso. Questo può essere fatto fisicamente, disconnettendo i cavi di rete o utilizzando strumenti di isolamento software che blocchino le comunicazioni in entrata e in uscita. È importante anche disattivare le connessioni wireless e chiudere eventuali porte aperte che potrebbero essere utilizzate dall'attaccante per mantenere l'accesso.

Rimozione del sistema B infetto:

Rimozione: La rimozione del sistema infetto può essere eseguita in diversi modi, a seconda della gravità dell'attacco e della necessità di conservare eventuali prove per un'indagine forense. In generale, è consigliabile spegnere immediatamente il sistema compromesso per impedire ulteriori danni e avviare un processo di analisi e ripristino.

Una volta che il sistema è stato isolato, si possono seguire questi passaggi per la rimozione:

Backup delle prove: Prima di effettuare qualsiasi azione di rimozione, è importante effettuare un backup di tutte le prove digitali pertinenti che possono essere utilizzate per l'indagine sull'attacco. Questo potrebbe includere registri di sistema, registri di rete, file di log e copie di eventuali file danneggiati.

Formattazione del disco rigido: La formattazione del disco rigido del sistema compromesso è un modo efficace per eliminare completamente il malware e le tracce dell'attacco. Tuttavia, è importante fare attenzione a non formattare accidentalmente parti del disco contenenti prove cruciali per l'indagine.

Reinstallazione del sistema operativo: Dopo la formattazione del disco rigido, è necessario reinstallare il sistema operativo e tutti i software utilizzati nel sistema B. È consigliabile utilizzare copie di installazione sicure e aggiornate per evitare reinfezioni.

Aggiornamenti di sicurezza: Una volta reinstallato il sistema operativo, è importante applicare immediatamente tutti gli aggiornamenti di sicurezza disponibili e configurare adeguatamente le impostazioni di sicurezza per ridurre al minimo il rischio di futuri attacchi.

Differenza tra Purge, Destroy e Clear:

Purge: Il termine "purge" indica il processo di eliminazione sicura dei dati da un dispositivo di archiviazione, come un disco rigido. In questo contesto, la purga dei dati comporta sovrascrivere ripetutamente i dati memorizzati sul disco rigido con informazioni casuali o con zeri, in modo che i dati originali diventino irrecuperabili anche con strumenti specializzati.

Destroy: Il termine "destroy" indica il processo fisico di distruggere fisicamente il supporto di archiviazione, come ad esempio un disco rigido, rendendolo irreparabilmente danneggiato e non recuperabile. Questo può essere fatto attraverso metodi come la triturazione, la perforazione o la fusione del supporto.

Clear: Il termine "clear" indica il processo di cancellazione dei dati da un dispositivo di archiviazione. Tuttavia, a differenza della purga, il processo di "clearing" potrebbe non essere sufficiente per garantire che i dati siano completamente eliminati e non recuperabili, in quanto potrebbero rimanere tracce residuali che potrebbero essere recuperate con strumenti specializzati.