UNITÀ 3/ SETTIMANA 1/ COMPITO 4

1) Tecnica di Isolamento:

-Disconnettere dalla rete: Interrompere immediatamente la connessione Internet al sistema B infetto per impedire ulteriori accessi non autorizzati e diffusione dell'attacco.

-Isolare fisicamente: Spegnere fisicamente il sistema B infetto per evitare la sua comunicazione con altri dispositivi o sistemi nella rete. Questo può includere lo spegnimento dei commutatori di rete o la disconnessione fisica dei cavi di rete.

2)Tecnica di Rimozione:

-Spegnimento sicuro del sistema: Chiudere tutte le applicazioni e i processi attivi in modo sicuro sul sistema compromesso prima di procedere allo spegnimento.

-Avvio in modalità di ripristino: Avviare il sistema B infetto in una modalità di ripristino o di ripristino di emergenza per eseguire operazioni di analisi e pulizia senza rischiare l'esecuzione di codice dannoso.

-Scansione antivirus e anti-malware: Utilizzare software antivirus e anti-malware aggiornati per eseguire una scansione completa del sistema B al fine di individuare e rimuovere tutti i malware presenti.

-Backup dei dati critici: Nel caso in cui vi siano dati critici sul sistema B compromesso, eseguire un backup sicuro prima di procedere con la rimozione dei malware o con la formattazione dei dischi.

La differenza tra “Purge” e “Destroy” nell’eliminazione delle informazioni sensibili

1)Purge:

-Purge si riferisce alla rimozione sicura e definitiva di dati o informazioni sensibili da un sistema o dispositivo. Questo processo implica generalmente la sovrascrittura dei dati con informazioni casuali multiple o con zeri, rendendo i dati originari irrecuperabili.

-È comunemente utilizzato quando si desidera mantenere l'integrità fisica del dispositivo o del supporto di memorizzazione, ma si vuole eliminare completamente tutte le informazioni sensibili.

2)Destroy:

-Destroy implica la distruzione fisica del dispositivo o del supporto di memorizzazione contenente dati sensibili. Questo può essere eseguito tramite metodi come la triturazione, la perforazione o la fusione del dispositivo.

-È un'opzione estrema, riservata ai casi in cui non ci si fida della sicurezza dei metodi di purga e si desidera garantire che i dati non possano essere recuperati in alcun modo.

3)Clean:

-Clean si riferisce al processo di pulizia generale di un sistema o di un dispositivo per rimuovere eventuali residui di malware o altre minacce dopo che è stato compromesso.

-Questo può includere la rimozione dei file temporanei, la pulizia dei registri di sistema, la reimpostazione delle impostazioni predefinite e la verifica della presenza di backdoor o di altre vulnerabilità.

In conclusione, "Purge" e "Destroy" si concentrano sull'eliminazione sicura dei dati sensibili, mentre "Clean" riguarda la pulizia del sistema dopo un attacco per garantire che sia sicuro e privo di minacce residuali.