S9-L4

Analizziamo le tecniche di isolamento, di rimozione e le differenze tra "Purge", "Destroy" e "Clear"; indicando, infine, un piano risolutivo della traccia.

1. Isolamento del Sistema Infetto

FInalizzato a limitare il danno causato dall'attacco e prevenire ulteriori compromessi di altri sistemi.

Tecniche utili:

- **Scollegamento della rete**: il sistema B deve essere immediatamente scollegato dalla rete per impedire agli attaccanti di continuare a interagire con il sistema compromesso.
  Questo può essere fatto fisicamente scollegando i cavi di rete o attraverso la configurazione della rete (disabilitazione delle interfacce di rete sul sistema).
- **Attivazione del firewall**: configurare il firewall per bloccare tutte le comunicazioni in entrata e in uscita dal sistema B (regole di firewall).
- **Modalità di sicurezza**: se possibile, il sistema B dovrebbe essere avviato in modalità di sicurezza, che disabilita la maggior parte dei servizi di rete e delle applicazioni non essenziali.

2. Rimozione del Sistema Infetto

Finalizzato ad eliminare la minaccia e ripristinare il sistema a uno stato sicuro.

Tecniche utili:

- **Analisi Forense**: prima della rimozione completa, eseguire una copia di tutti i dati e le configurazioni del sistema B per l'analisi forense.
  Questo passaggio è cruciale per capire come l'attacco è avvenuto e per migliorare le difese future.
- **Formattazione e reinstallazione**: dopo aver eseguito l'analisi forense, il sistema B deve essere completamente formattato e il software reinstallato da zero.
  Questo include il sistema operativo e tutte le applicazioni necessarie.
- **Applicazione di patch e aggiornamenti**: assicurarsi che tutte le patch di sicurezza e gli aggiornamenti siano applicati al sistema reinstallato per chiudere eventuali vulnerabilità che potrebbero essere state sfruttate durante l'attacco.

3. Differenze tra Purge, Destroy e Clear

Sono tutti metodi finalizzati ad eliminare i dati sensibili dai dischi prima dello smaltimento.

- **Clear (pulizia)**: rende i dati meno accessibili cancellando le directory e i file e sovrascrivendo l'area del disco con dati casuali o uno schema di cancellazione.
  Tuttavia, i dati possono essere recuperati con tecniche avanzate di recupero.
  Questa tecnica è adeguata quando il livello di minaccia è relativamente basso.
- **Purge (purificazione)**: va oltre il semplice "clear", rendendo i dati illeggibili e irrecuperabili anche con strumenti avanzati.
  Questo può essere fatto tramite metodi come la sovrascrittura multipla con dati casuali o la smagnetizzazione (degaussing) del disco.
- **Destroy (distruzione)**: è il metodo più sicuro e consiste nella distruzione fisica del supporto di memorizzazione. Questo può essere fatto triturando il disco, fondendolo o smagnetizzandolo in modo irreversibile. La distruzione garantisce che i dati non possano essere recuperati in alcun modo.

Conclusione

In questa situazione, poiché il sistema B è stato compromesso, è importante procedere con un'analisi forense, seguita dall'isolamento immediato, dalla rimozione sicura e dalla considerazione della distruzione fisica del supporto di memorizzazione per garantire che i dati sensibili non possano essere recuperati.