**Pratica S9L4**

Dopo la compromissione della macchina B a causa di un incidente di sicurezza, possiamo andare ad adottare i seguenti due step:

**Isolamento:**

L'isolamento può avvenire in due modi principali:

1. **Disconnessione fisica o logica:** Questo può essere fatto disconnettendo fisicamente il dispositivo dalla rete o configurando i dispositivi di rete per isolare il traffico proveniente o diretto verso la macchina compromessa.
2. **Segmentazione di rete:** Utilizzare tecniche di segmentazione di rete per limitare la comunicazione del sistema compromesso con altri dispositivi nella rete. Ciò può essere realizzato utilizzando VLAN apposita.

**Rimozione:**

1. **Ripristino da backup:** Ripristinare il sistema da un backup pulito precedentemente archiviato. Assicurarsi che il backup non contenga codice dannoso e che sia stato creato prima dell'incidente di sicurezza.
2. **Ripristino di configurazioni sicure:** Se possibile, ripristinare la configurazione del sistema a uno stato noto e sicuro, rimuovendo le modifiche apportate dall'attaccante.

## Differenza tra Purge e Destroy:

1. **Purge:**
    - **Descrizione:** Purge si riferisce alla rimozione di informazioni sensibili in modo sicuro, rendendo le informazioni originali non recuperabili. Può coinvolgere la sovrascrittura dei dati o altre tecniche di cancellazione sicura come l'utilizzo di forti magneti.

2. **Destroy:**
    - **Descrizione:** Destroy implica la distruzione fisica della macchina o dei supporti di archiviazione. Può coinvolgere la demolizione fisica del dispositivo o l'uso di procedure specializzate per distruggere in modo permanente i dati.