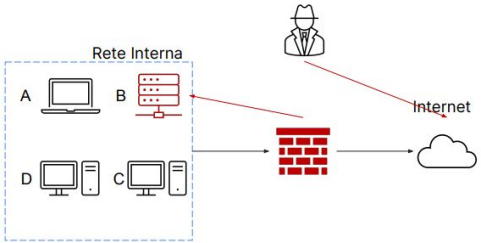
Compito S9-L4

Traccia

il sistema B è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Clear, Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



Esercizio

Isolamento del Sistema Infetto B:

- **Disconnessione dalla Rete:** Il primo passo consiste nella disconnessione immediata del sistema compromesso (B) dalla rete per impedire la propagazione dell'attacco e isolare il sistema dal resto della rete
- **Firewall e Segmentazione di Rete**: Utilizzare il firewall per bloccare ogni traffico non autorizzato tra il sistema compromesso e il resto della rete. Inoltre, considerare la segmentazione di rete per limitare ulteriormente il possibile movimento laterale dell'attaccante.
- **Isolamento Fisico o Virtuale**: A seconda della gravità dell'attacco, potrebbe essere necessario isolare il sistema infetto fisicamente dalla rete o virtualmente utilizzando soluzioni di virtualizzazione o containerizzazione.

Esercizio

Rimozione del Sistema B Infetto:

- **Analisi Forense:** Prima di rimuovere il sistema compromesso, eseguire un'analisi forense per raccogliere informazioni sulla natura dell'attacco, gli artefatti dell'intrusione e le possibili vulnerabilità sfruttate.
- **Backup dei Dati Importanti:** Effettuare un backup dei dati critici e delle informazioni necessarie per le indagini forensi prima di procedere con la rimozione del sistema compromesso.
- **Formattazione e Reinstallazione:** Formattare il sistema infetto e reinstallare il sistema operativo da una fonte sicura. Applicare patch di sicurezza e configurare le impostazioni di sicurezza in modo appropriato.

Esercizio

Differenza tra Purge e Destroy per l'Eliminazione delle Informazioni Sensibili:

- **Clear:** Rappresenta la rimozione dei dati in modo che non siano più accessibili senza, tuttavia, distruggere fisicamente il dispositivo. Questo potrebbe coinvolgere la cancellazione dei dati senza sovrascrittura o la pulizia del dispositivo per renderlo vuoto.
- **Purge**: Indica la rimozione sicura di dati o informazioni, spesso attraverso procedure di sovrascrittura multiple dei dati con caratteri casuali. Il processo di purga può consentire il riutilizzo del dispositivo.
- **Destroy**: Implica la distruzione fisica o logica irreversibile del dispositivo o dei dati. Ad esempio, la distruzione fisica di un disco rigido o la cancellazione completa di informazioni crittografate in modo che non possano essere recuperate.

Esercizio

Smaltimento dei Dischi Compromessi:

- **Distruzione Fisica:** Se la sicurezza delle informazioni è di primaria importanza, la distruzione fisica dei dischi compromessi tramite triturazione o altri metodi può garantire che i dati non siano recuperabili.
- **Cancellazione Sicura:** Utilizzare procedure di cancellazione sicura o sovrascrittura multiple per rendere i dati inaccessibili prima dello smaltimento. Questo approccio preserva il dispositivo fisico per un possibile riutilizzo.