Consegna week 20 day1 – Daniele Rufo

Il CSIRT, una volta portate avanti le primi due fasi del piano di Incident Response (preparazione e rilevamento/analisi), in cui è stato accertato che siamo in presenza di un attacco in corso, passa alla fase di contenimento, rimozione e recupero. In questa fase sono presenti le procedure che il testo dell'esercizio chiede di prendere in esame:

- isolamento: tecnica usata quando la segmentazione risulta inefficace o deficitaria. Consiste nella completa disconnessione del sistema infetto dalla rete. Il terminale compromesso ha però ancora accesso ad internet.
- Rimozione: quando neanche l'isolamento risulta sufficiente si passa alla rimozione del sistema infetto dalla rete. Questo implica che l'attaccante non soltanto non avrà più accesso alla rete interna, ma neanche alla macchina infatti. Essendo l'azione più estrema viene utilizzata solo in casi di necessità, seguendo un approccio a cascata secondo le tecniche di riduzione impatti.

La seconda parte dell'esercizio chiede invece di evidenziare le differenze tra le tecniche per l'eliminazione di dati sensibili prima dello smaltimento definitivo dei dischi compromessi.

- Purge: viene adottato si un approccio logico (come avviene per la tecnica Clear), ma implementandolo con metodologie di rimozione fisica come l'uso di forti magneti.
- Destroy: si rivela invece più aggressiva la tecnica Destroy in cui il disco viene disintegrato meccanicamente o polverizzato o trapanato ecc. È sicuramente la metodologia più sicura, ma anche la più costosa.
- Clear: una specifica sulla tecnica meno invasiva che punta a ripulire completamente l'hardware così che possa essere riutilizzato. Prevede tutti gli approcci logici come "reset factory" o "read and write"