EPICODE

Esercizio S9 – L4

TRACCIA

Con riferimento alla figura di seguito:

Immagine che contiene testo, diagramma, linea, schermata

Descrizione generata automaticamente

Il sistema B (un database con diversi dischi per lo storage) 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 Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear.

SOLUZIONE

• Per fermare l’attacco ed evitare l’aggravarsi della situazione dobbiamo isolare il database.  
In questo specifico caso si decide di isolare completamente il database disconnettendolo sia dalla rete LAN che da internet. Si può farlo inserendo, nelle impostazioni del router, l’indirizzo MAC del database in una black list. Se si è sul luogo fisico è anche possibile staccare direttamente e fisicamente il cavo di connessione.  
Se, invece, si volesse studiare il comportamento dell’hacker, si potrebbe creare una rete di quarantena tramite tecniche di segmentazione.  
Bisogna poi procedere con l’eliminazione delle attività, le componenti, i processi che restano dell’incidente all’interno della rete o sui sistemi. Questa attività può includere, ad esempio, la rimozione di eventuali backdoor installate, oppure ripulire dischi e chiavette USB compromesse.

Per comprendere come abbia fatto l’hacker ad entrare nella rete si può usare, per esempio, Wireshark. Si utilizza anche un antivirus o un antimalware per la rilevazione del codice dannoso. Non sempre è possibile rilevare il malware; in questi casi bisogna ripulire completamente i dischi con i metodi elencati di seguito.

• I metodi per ripulire un disco sono:

- Clear: il metodo clear consiste nell’usare tecniche logiche come, per esempio, un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte. È considerato un metodo sicuro, ma per dati particolarmente sensibili è consigliabile utilizzare uno dei due metodi che seguono.

- Purge: il metodo purge consiste nell’usare delle tecniche o degli strumenti specializzati per rendere i dati irrecuperabili anche con software e hardware avanzati. Questo metodo può includere la degaussing, che distrugge il campo magnetico del disco. È un metodo affidabile di cancellazione dei dati sensibili.

- Destroy: il metodo destroy consiste nell’usare delle tecniche o degli strumenti fisici per distruggere il dispositivo e i dati in esso contenuti. Questo metodo può includere la triturazione, la perforazione, l’incenerimento, la disintegrazione del disco. È il metodo più sicuro in assoluto per l’eliminazione dei dati sensibili. Spesso risulta più costoso.