W20D1

Traccia:
Esercizio Traccia Con riferimento alla figura nella prossima slide, 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 e 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**

1. Isolamento e Rimozione del sistema B infetto

I. Isolamento del sistema B infetto

L'isolamento è come mettere in quarantena il sistema compromesso per impedire che l'attacco si diffonda o che l'hacker possa continuare a fare danni. Ecco alcune mosse fondamentali:

- **Scollegare il sistema dalla rete**: La prima cosa da fare è staccare il sistema B da Internet e dalla rete interna, come se togliessimo la spina per evitare che l'attacco possa proseguire.
- **Bloccare il traffico col firewall**: Possiamo poi configurare il firewall per bloccare tutto il traffico verso e da il sistema B. Se vogliamo essere precisi, possiamo bloccare solo le vie che l'attaccante sta usando.
- **Mettere il sistema in una rete separata (sandbox)**: Se possibile, possiamo spostare il sistema compromesso in una zona isolata, dove possiamo studiare l'attacco senza correre rischi.
- **Spegnere servizi critici**: Se ci sono applicazioni o servizi attivi che potrebbero essere sfruttati dall'hacker, li spegniamo temporaneamente.

II. Rimozione del sistema B infetto

Dopo aver isolato il sistema, è il momento di occuparsi della sua "pulizia" o rimozione:

- **Spegnere i servizi attivi**: Disabilitare tutti i servizi attivi per evitare che l'attaccante possa continuare a sfruttarli.
- **Bloccare gli accessi esterni**: Rimuoviamo tutte le modalità di accesso remoto, come chiavi SSH o accessi RDP, per impedire agli hacker di rientrare.
- **Ripristino o reinstallazione**: A seconda della gravità dell'attacco, possiamo scegliere se:
    - Ripristinare il sistema da un **backup sicuro** (un "salvataggio" fatto prima dell'attacco).
    - O, in casi estremi, reinstallare tutto da zero.

2. Differenza tra Purge, Destroy e Clear per l’eliminazione delle informazioni sensibili

Quando si tratta di eliminare dati sensibili da un disco compromesso, ci sono vari livelli di sicurezza che possiamo adottare. Questi livelli sono **Clear**, **Purge** e **Destroy**.

Clear (Cancellazione base)

Il *Clear* è una cancellazione semplice: i dati vengono sovrascritti, rendendoli invisibili e inaccessibili con gli strumenti comuni. È come cancellare file dal computer e poi svuotare il cestino.

- **Quando si usa**: Se il disco deve essere riutilizzato e non c’è il rischio che qualcuno usi strumenti particolarmente sofisticati per recuperare i dati.

Purge (Cancellazione approfondita)

Il *Purge* è un passo oltre la semplice cancellazione. Qui i dati vengono cancellati in modo più approfondito, rendendoli molto difficili da recuperare anche con strumenti avanzati. Si può usare, ad esempio, un campo magnetico (degaussing) o sovrascrivere i dati più volte.

- **Quando si usa**: Quando vogliamo riutilizzare il disco, ma ci serve un livello di sicurezza più alto per evitare che anche un esperto possa recuperare le informazioni.

Destroy (Distruzione fisica)

Il *Destroy* è il metodo più sicuro in assoluto: distruggiamo fisicamente il disco, rendendolo completamente inutilizzabile. Potrebbe significare frantumarlo, perforarlo o bruciarlo.

- **Quando si usa**: Quando vogliamo essere certi al 100% che i dati non possano essere mai più recuperati, e non abbiamo bisogno di riutilizzare il disco.