Report Esercizio

W20-D2

Redatto da Andrea Sciattella

02/07/2024

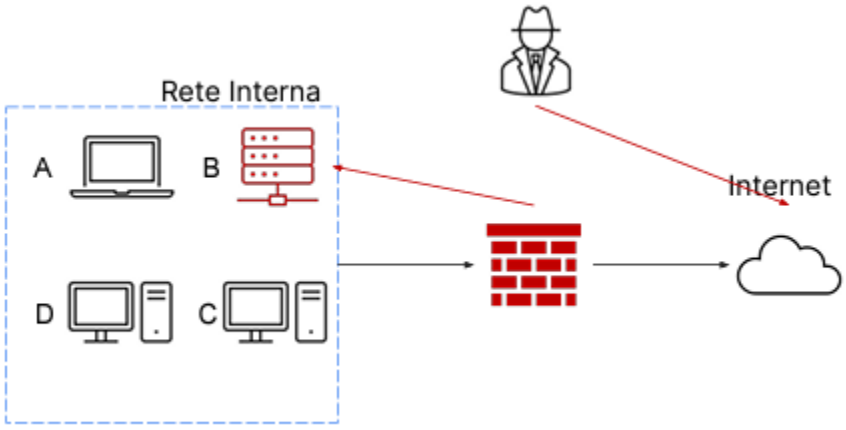
TRACCIA

Con riferimento alla figura in slide 4, 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:
    1. Isolamento,
    2. 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.



SVOLGIMENTO ESERCIZIO

In una situazione in cui un database è stato compromesso, il team di CSIRT (Computer Security Incident Response Team) deve agire rapidamente per mitigare i danni.

Di seguito vengono descritte le tecniche di isolamento e rimozione del sistema infetto, ed infine si distinguono le differenze tra Clear, Purge & Destroy per l'eliminazione delle informazioni sensibili.

- ***Tecniche di Isolamento***

L'isolamento è il primo passo cruciale per limitare l'impatto di un attacco in corso e può essere fatto in vari modi:

1. **Disconnessione dalla rete:**
    - Disconnettere immediatamente il sistema B dalla rete per impedire ulteriori accessi da parte degli attaccanti e la propagazione dell'attacco ad altri sistemi. Questo può includere la disconnessione fisica dei cavi di rete o la disabilitazione delle interfacce di rete.
2. **Segmentazione della rete:**
    - Se la disconnessione completa non è possibile, si può isolare il sistema compromesso all'interno di una sottorete separata (quarantena) con accesso limitato solo agli amministratori di sistema per la gestione della crisi.
3. **Utilizzo di firewall:**
    - Configurare firewall per bloccare il traffico verso e dal sistema infetto. Questo include la chiusura delle porte non necessarie e il blocco degli indirizzi IP sospetti.
4. **Creazione di una VLAN di Quarantena:**
    - Spostare il PC infetto in una VLAN di quarantena con accesso limitato. Questa VLAN dovrebbe essere isolata dal resto della rete e consentire solo l'accesso necessario per la gestione e la mitigazione dell'incidente.

- ***Tecniche di Rimozione del Sistema Infetto***

Una volta che il sistema è stato isolato, si può procedere alla rimozione del sistema infetto. I passi tipici includono:

1. **Backup dei dati:**
    - Prima di procedere alla rimozione, è fondamentale effettuare o utilizzare un backup dei dati ancora integri e non compromessi. Questo backup deve essere utilizzato in un ambiente sicuro e isolato per prevenire ulteriori compromissioni.
2. **Analisi forense:**

- Condurre un'analisi forense del sistema compromesso per comprendere la natura dell'attacco, raccogliere prove e identificare eventuali backdoor o software malevoli. Questo passo è essenziale per prevenire future compromissioni.

3. **Pulizia e ripristino:**
   - Dopo l'analisi, è necessario pulire il sistema da qualsiasi software malevolo. In alcuni casi, potrebbe essere necessario azzerare e resettare il sistema operativo e il software applicativo da zero, utilizzando backup precedenti all'attacco.

Purge, Destroy e Clear:

1. **Clear:**
   - La procedura di "Clear" implica la sovrascrittura delle informazioni sensibili con tecniche “logiche”. Questo metodo è utilizzato per rendere i dati precedenti non recuperabili tramite strumenti software standard dove si utilizza una tecnica di sovrascrittura ripetuta o la funzione di “factory reset”. Può non essere sufficiente contro attacchi sofisticati che utilizzano tecniche di recupero avanzate.
2. **Purge:**
   - La procedura di "Purge" va oltre il "Clear" e coinvolge tecniche più avanzate per rendere i dati irrecuperabili, inclusa la sovrascrittura multipla dei dati e tecniche fisiche aventi forti magneti per rendere inaccessibili i dati. Questo metodo è più sicuro rispetto al "Clear" e mira a prevenire il recupero delle informazioni anche con strumenti avanzati di recupero dati.
3. **Destroy:**
   - La procedura di "Destroy" implica la distruzione fisica del supporto di memorizzazione. Questo può essere fatto tramite degaussing (demagnetizzazione), frantumazione, o altre tecniche che rendono fisicamente inutilizzabili i dischi. Questo metodo garantisce che i dati non possano essere recuperati in alcun modo.