Incident response

CYBER SECURITY & ETHICAL HACKING

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.

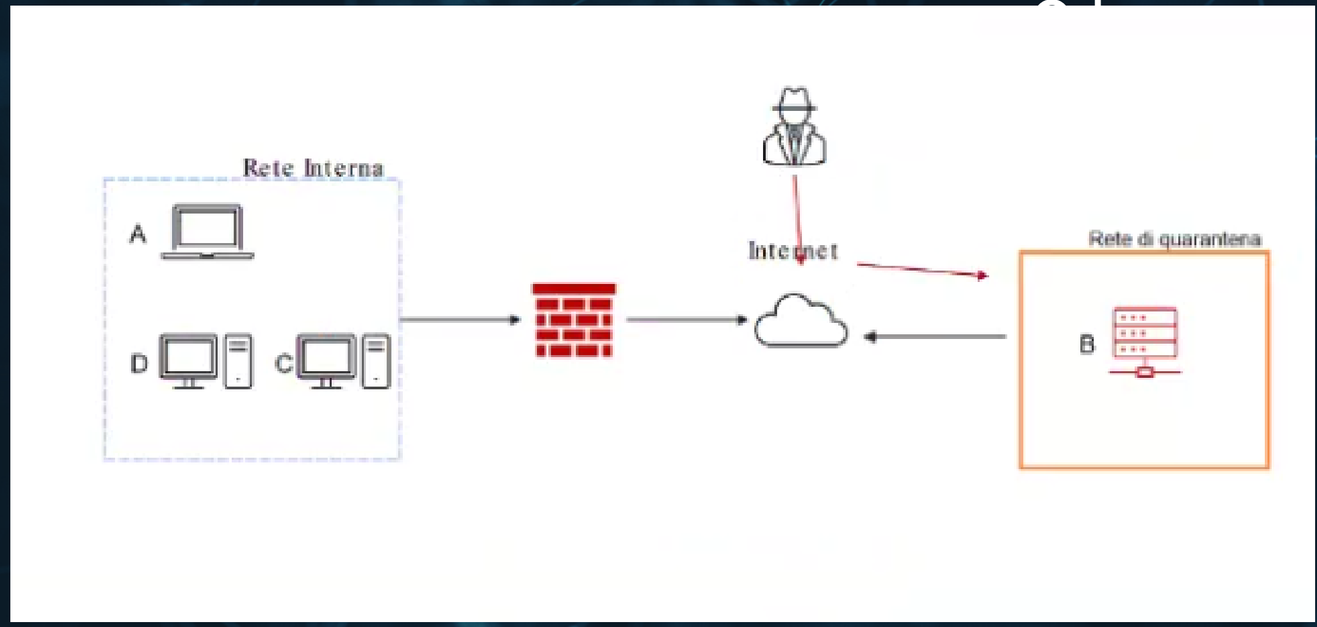
Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: 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**

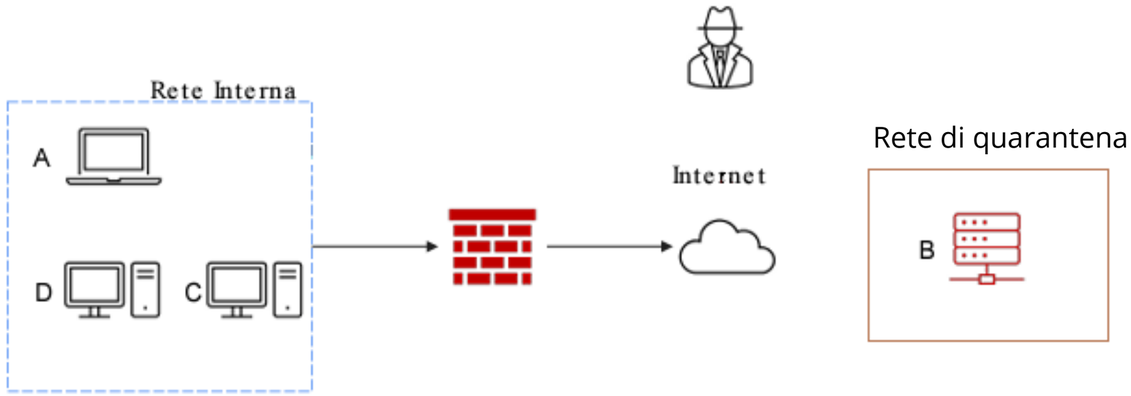
Isolamento

Isolamento del sistema:

- Disconnetti il sistema dalla rete: Questo impedisce al malware di comunicare con server remoti o di diffondersi attraverso la rete.
- Isola il sistema da altri dispositivi: Se possibile, scollega il dispositivo infetto da altri dispositivi per prevenire la diffusione del malware attraverso la rete locale.



Rimozione



Isolamento del sistema:

- Disconnetti il sistema dalla rete: Questo impedisce al malware di comunicare con server remoti o di diffondersi attraverso la rete.
- Isola il sistema da altri dispositivi: Se possibile, scollega il dispositivo infetto da altri dispositivi per prevenire la diffusione del malware attraverso la rete locale.

Rimozione del malware:

- Utilizza software antivirus/antimalware aggiornato: Assicurati di utilizzare un'utility di sicurezza aggiornata per rimuovere il malware rilevato.
- Rimozione manuale: In alcuni casi, potrebbe essere necessario rimuovere manualmente il malware seguendo le istruzioni fornite dal fornitore di sicurezza o da fonti affidabili.

Function About Technology

Purge: Non solo si avvale di un approccio logico per l'eliminazione dei contenuti sensibili, come nel caso di "clear", ma implementa anche tecniche di rimozione fisica, ad esempio l'utilizzo di potenti magneti per rendere le informazioni inaccessibili su dispositivi specifici.

Destroy: Rappresenta l'approccio più radicale per eliminare dispositivi contenenti dati sensibili. Oltre agli accorgimenti logici e fisici precedentemente menzionati, si impiegano metodologie di laboratorio, quali disintegrazione, polverizzazione dei supporti a elevate temperature e trapanazione. Sebbene questo metodo sia indubbiamente il più efficace per garantire l'inaccessibilità delle informazioni, comporta anche un impegno economico maggiore.