Scenario di Attacco Ransomware Umano

Fase 1: Infiltrazione

- **Obiettivo:** L'attaccante cerca di ottenere accesso iniziale alla rete aziendale.
- **Metodo:** L'attaccante invia email di phishing ai dipendenti contenenti allegati malevoli o link a siti web infetti.
    - Alcuni dipendenti potrebbero aprire il file o cliccare sui link, scaricando inconsapevolmente un trojan che crea una backdoor sul loro sistema.

Fase 2: Ricognizione

- **Obiettivo:** Dopo aver ottenuto accesso a un sistema, l'attaccante cerca di esplorare la rete interna e ottenere informazioni su sistemi critici.
- **Metodo:** L'attaccante utilizza strumenti come **Nmap** o **Netstat** per identificare altri dispositivi sulla rete, cercando server con dati sensibili, come server di database o file server.
    - L'attaccante può anche accedere a strumenti di amministrazione per esaminare utenti con permessi elevati o cercare credenziali salvate nel sistema compromesso.

Fase 3: Escalation dei Privilegi

- **Obiettivo:** L'attaccante cerca di ottenere diritti amministrativi per avere il controllo totale sulla rete aziendale.
- **Metodo:** Utilizza vulnerabilità note nel sistema operativo o sfrutta errori di configurazione nei permessi di accesso. Ad esempio, l'attaccante potrebbe utilizzare exploit come **Mimikatz** per ottenere credenziali amministrative memorizzate.
    - L'attaccante ottiene l'accesso al dominio e inizia a muoversi lateralmente tra i sistemi per aumentare il suo controllo.

Fase 4: Distribuzione del Ransomware

- **Obiettivo:** Una volta ottenuti i privilegi necessari, l'attaccante inizia a distribuire il ransomware su più dispositivi.
- **Metodo:** Utilizza script come **PowerShell** o strumenti di gestione di rete per distribuire in modo rapido il payload del ransomware su tutta la rete. Il ransomware inizia a criptare i file critici e bloccare l'accesso agli utenti.
    - L'attaccante lascia anche file di testo sui dispositivi compromessi con le istruzioni per il riscatto.

Fase 5: Riscatto

- **Obiettivo:** L'attaccante contatta l'azienda per chiedere un riscatto in criptovaluta (es. Bitcoin) in cambio della chiave di decriptazione.
- **Metodo:** Attraverso email anonime o comunicazioni tramite **Tor** o il dark web, l'attaccante stabilisce un canale di comunicazione con l'azienda. A questo punto, i sistemi critici sono compromessi e l'attività dell'azienda è bloccata.

Test di Risposta

Durante questa simulazione, la tua azienda dovrà:

1. **Individuare l'attacco:** Quanto tempo impiegano i team di sicurezza per rilevare la presenza di attività anomale?

2. **Mitigare l'attacco:** Quali azioni intraprendono per isolare i sistemi compromessi? La risposta viene automatizzata o manualmente eseguita?
3. **Recuperare i dati:** C'è un piano di backup efficace che consente di ripristinare i dati senza pagare il riscatto?
4. **Comunicare con le parti interessate:** Come viene gestita la comunicazione interna ed esterna? C'è un piano di crisi?
5. **Eseguire analisi post-attacco:** Dopo aver risolto l'attacco, il team è in grado di identificare come è avvenuto l'attacco, come prevenire future infiltrazioni e quali vulnerabilità sono state sfruttate?

Azioni Aggiuntive da Testare:

- Testare i **tempi di risposta** del team IT e i protocolli di isolamento delle macchine infette.
- Verificare i **backup** e i tempi di ripristino.
- Simulare una **negoziazione** con gli attaccanti (anche solo come esercizio teorico).
- Esaminare le **conseguenze legali** e comunicative di un attacco ransomware.

Questo scenario ti permette di mettere alla prova le capacità della tua azienda di difendersi da un attacco reale. Può anche essere personalizzato ulteriormente, ad esempio simulando diverse varianti di ransomware o livelli di sofisticazione dell'attaccante.