Consegna S11-L1

Consegna: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

⚜️ **Tag:** #remediation #phishing #DoS #cybersecurity

Introduzione

Questo esercizio si concentra su due minacce comuni: **Phishing** e **Attacchi DoS (Denial of Service)**. Lo studente potrà scegliere uno dei due scenari proposti per approfondire le strategie di remediation e mitigazione.

Parte 1: Minaccia di Phishing

- **Scenario:** Sei un amministratore di sicurezza in un'azienda che ha scoperto una campagna di phishing mirata contro i propri dipendenti.
- **Istruzioni:**
  1. **Identificazione della Minaccia:** Ricerca su come funziona un attacco di phishing.
  2. **Analisi del Rischio:** Identifica i potenziali danni (es. credenziali rubate, furto di dati).
  3. **Pianificazione della Remediation:**
     - Blocca le email fraudolente.
     - Informazione ai dipendenti.
     - Monitoraggio per rilevare compromissioni.
  4. **Implementazione della Remediation:** Applica misure come filtri anti-phishing e 2FA.

5. **Mitigazione dei Rischi Residuali:** Pianifica test di phishing simulati e aggiornamenti continui.

Parte 2: Attacco DoS (Denial of Service)

- **Scenario:** Gestisci una rete aziendale colpita da un attacco DoS che rende i server inaccessibili.
- **Istruzioni:**
  1. **Identificazione della Minaccia:** Analizza l'origine e il funzionamento di un attacco DoS.
  2. **Analisi del Rischio:** Valuta i danni ai servizi aziendali e ai sistemi critici.
  3. **Pianificazione della Remediation:** Mitigazione del traffico malevolo e utilizzo di servizi anti-DoS.
  4. **Implementazione della Remediation:** Configura firewall, load balancer e collaborazioni con servizi terzi.
  5. **Mitigazione dei Rischi Residuali:** Test periodici, monitoraggio continuo e formazione.

Documentazione e Report

Compila un report finale che includa:

- Analisi della minaccia selezionata.
- Piano dettagliato di remediation.
- Misure implementate per mitigare i rischi residui.
- Valutazioni delle simulazioni e raccomandazioni future.

🔑 **Chiavi:**
[remediation, phishing, DoS, cybersecurity]