Analisi della Sicurezza Informatica aziendale o privata

Descrizione dettagliata del servizio

Fase 1: Pianificazione e Preparazione

1. **Incontro Iniziale (1 giorno presso la sede fisica del Cliente)**:
    - **Obiettivo**: Stabilire gli obiettivi e la portata dell'analisi di sicurezza.
    - **Attività**: Incontro con i responsabili della sicurezza IT per discutere le aree critiche della rete, le applicazioni da testare e i requisiti specifici.
2. **Definizione del Perimetro**:
    - **Obiettivo**: Definire chiaramente il perimetro dell'analisi, inclusi i segmenti di rete, i sistemi e le applicazioni.
    - **Attività**: Creare una mappa di rete dettagliata e identificare le risorse critiche.
3. **Autorizzazioni e Consensi**:
    - **Obiettivo**: Ottenere le autorizzazioni necessarie per eseguire l'analisi di sicurezza.
    - **Attività**: Formalizzare accordi di servizio (SLA) e ottenere consensi scritti per le attività di scansione e test.
4. **Installazione della Sonda (InterBox by DEV74) per la scansione da interno**:
    - **Obiettivo**: Rilevare e monitorare il traffico di rete per identificare potenziali vulnerabilità.
    - **Attività**: Installare la sonda di sicurezza nello switch primario della LAN per raccogliere dati sul traffico di rete.

Fase 2: Rilevazione delle Vulnerabilità (Da remoto)

4. **Scansione della Rete**:
    - **Obiettivo**: Identificare dispositivi, porte aperte e servizi attivi nella rete.
    - **Attività**: Utilizzare strumenti come Nmap per eseguire scansioni di rete e mappare tutti i dispositivi connessi.
5. **Scansione delle Vulnerabilità**:
    - **Obiettivo**: Individuare vulnerabilità note nei sistemi e nelle applicazioni.
    - **Attività**: Utilizzare scanner di vulnerabilità come Nessus, OpenVAS o Qualys per eseguire scansioni approfondite su tutti i dispositivi identificati.

Fase 3: Analisi e Valutazione (Da remoto)

7. **Analisi dei Dati Raccolti**:
    - **Obiettivo**: Analizzare i risultati delle scansioni per identificare le vulnerabilità critiche.
    - **Attività**: Valutare le vulnerabilità rilevate, classificandole in base alla gravità e al rischio associato.
8. **Test di Penetrazione**:
    - **Obiettivo**: Confermare la presenza delle vulnerabilità e valutarne l'impatto.
    - **Attività**: Eseguire test di penetrazione mirati utilizzando strumenti come Metasploit per sfruttare le vulnerabilità identificate e verificare l'efficacia delle misure di sicurezza esistenti.

Fase 4: Mitigazione e Correzione (Da remoto)

9. **Sviluppo del Piano di Mitigazione**:
    - **Obiettivo**: Proporre soluzioni per mitigare le vulnerabilità identificate.

- **Attività**: Collaborare con il team IT per sviluppare un piano di azione che includa patch di sicurezza, configurazioni di sistema e miglioramenti delle policy di sicurezza.

10. **Implementazione delle Correzioni**:
    - **Obiettivo**: Applicare le correzioni necessarie per risolvere le vulnerabilità.
    - **Attività**: Installare patch, aggiornare software, modificare configurazioni e implementare misure di sicurezza raccomandate.

Fase 5: Verifica e Validazione (Da remoto)

11. **Riscansione e Verifica**:
    - **Obiettivo**: Verificare l'efficacia delle correzioni applicate.
    - **Attività**: Eseguire una nuova scansione delle vulnerabilità per assicurarsi che le vulnerabilità siano state risolte e non siano presenti nuove vulnerabilità.
12. **Valutazione Finale**:
    - **Obiettivo**: Valutare lo stato complessivo della sicurezza della rete.
    - **Attività**: Redigere un rapporto finale che riassuma i risultati delle scansioni e dei test di penetrazione, includendo le misure di mitigazione implementate e le raccomandazioni per la sicurezza futura.

Fase 6: Generazione del Rapporto (Da remoto)

13. **Creazione del Rapporto Finale**:
    - **Obiettivo**: Documentare tutti i risultati e le azioni intraprese.
    - **Attività**: Preparare un rapporto dettagliato che includa:
        - Panoramica della rete e del perimetro dell'analisi.
        - Dettagli delle vulnerabilità rilevate e il loro impatto.
        - Descrizione delle azioni correttive implementate.
        - Raccomandazioni per miglioramenti futuri.
        - Allegati con i risultati delle scansioni e dei test.
14. **Presentazione del Rapporto**:
    - **Obiettivo**: Comunicare i risultati e le raccomandazioni ai responsabili aziendali.
    - **Attività**: Organizzare una riunione di presentazione con il team di sicurezza IT e gli amministratori aziendali per discutere i risultati del rapporto e pianificare le azioni future.