Introduzione

Questo libro vi aiuterà a conoscere gli elementi fondamentali della sicurezza, a partire dalla triade CIA fino alla gestione delle identità e degli accessi. Descrive l'infrastruttura di rete e come sta evolvendo con l'implementazione della virtualizzazione, i diversi modelli di cloud e le modalità di storage.Vedremo come rendere sicuri i dispositivi e le applicazioni utilizzati in azienda.

A chi è rivolto questo libro

Questo libro è rivolto a tutti coloro che vogliono affrontare l'esame di certificazione CompTIA Security+ SY0-501, un passo importante per chiunque voglia diventare un professionista della sicurezza o lavorare nel campo della sicurezza informatica.
Questa guida alla certificazione Security+ non presuppone alcuna conoscenza pregressa sull'argomento.

Struttura del libro

- Il Capitolo 1, *Gli aspetti fondamentali della sicurezza*, passa in rassegna concetti di base della sicurezza, che vengono poi ulteriormente sviluppati nei capitoli successivi.
- Il Capitolo 2, *Conduzione di un'analisi dei rischi*, esamina i tipi di minacce e di vulnerabilità e i ruoli che svolgono i diversi attori delle minacce.
- Il Capitolo 3, *Implementazione di policy e procedure di sicurezza*, esamina le architetture di riferimento, le diverse guide e come eliminare al meglio i dati.
- Il Capitolo 4, *Identità e gestione degli accessi*, esamina i diversi tipi di autenticazione, partendo dai concetti di identità e gestione degli accessi.
- Il Capitolo 5, *Componenti delle reti*, esamina i componenti delle reti e come possono incidere sulla sicurezza della rete. Parleremo di firewall, switch e router.
- Il Capitolo 6, *Modelli cloud e virtualizzazione*, parla di virtualizzazione, deployment e problemi di sicurezza. Approfondiremo i diversi modelli cloud, esaminandone il deployment e gli ambienti di storage.

- Il Capitolo 7, *Gestione di host e deployment di applicazioni*, esamina i diversi dispositivi mobili e le loro caratteristiche, nonché le applicazioni che vengono eseguite su questi dispositivi.
- Il Capitolo 8, *Protezione contro attacchi e vulnerabilità*, esplora i diversi tipi di attacchi e di vulnerabilità, nonché le loro caratteristiche peculiari. Questo è probabilmente il modulo i cui temi sono testati più a fondo nell'esame Security+.
- Il Capitolo 9, *Implementazione dell'infrastruttura a chiave pubblica*, approfondisce le diverse tecniche crittografiche e il modo in cui vengono emessi e utilizzati i certificati.
- Il Capitolo 10, *Risposta agli incidenti di sicurezza*, affronta la risposta agli incidenti, concentrandosi in particolare sulla raccolta delle prove volatili per l'analisi forense.
- Il Capitolo 11, *Gestione della continuità di business*, rivolge la propria attenzione all'ambiente di business per considerazioni sulla disponibilità dei sistemi e sulla scelta del metodo più appropriato per il recovery dopo un disastro.
- L'Appendice A, *Preparazione all'esame CompTIA Security+ 501*, è una guida che vuole aiutare lo studente a superare l'esame al primo tentativo.
- Le Appendici B e C, *Simulazione d'esame 1* e *Simulazione d'esame 2*, presentano ciascuna una serie di 50 domande, formulate in modo analogo a quelle che si incontrano nell'esame, che permettono di valutare il grado di preparazione al test.
- L'Appendice D, *Risposte alle simulazioni d'esame*, fornisce le risposte corrette alle domande delle Appendici B e C, con l'integrazione di un commento e di ulteriori spiegazioni.
- L'Appendice E, *Acronimi*, elenca tutti gli acronimi utilizzati nel testo e il loro significato.

Convenzioni utilizzate

Nella redazione del testo sono state utilizzate alcune convenzioni.

- Il testo in `carattere monospaziato` è utilizzato per codice di linguaggi di programmazione, nomi di file o cartelle e simili.
- Le espressioni in *corsivo* indicano termini importanti, in particolare là dove vengono definiti per la prima volta, nonché gli elementi di interfaccia (come comandi di menu, titoli di finestre di dialogo ecc.).

Nel testo compaiono due tipi di note.

NOTA

Questo tipo di note contiene informazioni accessorie o aggiuntive al testo, riferimenti per approfondimenti e simili.

SUGGERIMENTO PER L'ESAME

Questo tipo di note contiene precisazioni e puntualizzazioni mirate specificamente all'esame, alla terminologia usata in quel contesto, alle cose a cui prestare particolare attenzione.

Nota all'edizione italiana

L'esame CompTIA Security+ 501 viene erogato in lingua inglese: per questo nel testo vengono frequentemente introdotti i termini inglesi, anche quando esistono specifici corrispettivi nella lingua italiana. Le simulazioni d'esame sono presentate in inglese con una traduzione italiana fra parentesi quadre: non si tratta di una traduzione ufficiale (che non esiste) ma solo di un aiuto per chi avesse difficoltà o dubbi in merito alla formulazione originale.