

Simulazione d'Esame - Domande

**Set di simulazione
Versione Finale**

ISTQB® Security Test Engineer Syllabus Specialist Level

Compatibile con il Syllabus versione 1.0.1

International Software Testing Qualifications Board



Avviso di copyright

Avviso sul Copyright © International Software Testing Qualifications Board (di seguito chiamato ISTQB®).

ISTQB® è un marchio registrato di International Software Testing Qualifications Board.

Tutti i diritti riservati.

Gli autori dichiarano con la presente di trasferire il copyright a ISTQB®. Gli autori (come attuali titolari del copyright) e ISTQB® (come futuro titolare del copyright) hanno concordato le seguenti condizioni di utilizzo:

Possono essere copiati estratti di questo documento per un uso non commerciale se la fonte è riconosciuta.

Qualsiasi azienda Training Provider accreditata alla Formazione può utilizzare questa Simulazione d'Esame nei propri corsi di formazione se gli autori e ISTQB® sono riconosciuti come fonti e proprietari del copyright della Simulazione d'Esame, e a condizione che qualsiasi pubblicità di tale corso di formazione sia fatta dopo che l'accREDITAMENTO ufficiale dei materiali di formazione è stato ricevuto da un Member Board riconosciuto da ISTQB®.

Qualsiasi individuo o gruppo di individui può utilizzare questa Simulazione d'Esame negli articoli e nei libri, a condizione che gli autori e ISTQB® siano riconosciuti come fonti e possessori del copyright della Simulazione d'Esame.

È proibito qualsiasi altro utilizzo di questa Simulazione d'Esame senza prima avere ottenuto l'approvazione scritta di ISTQB®.

Qualsiasi Member Board riconosciuto da ISTQB® può tradurre questa Simulazione d'Esame a condizione di riprodurre il sopra menzionato Avviso di Copyright nella versione tradotta della Simulazione d'Esame.

Responsabilità del documento

Exam Working Group ISTQB® è responsabile di questo documento.

Questo documento è mantenuto da un team dedicato di ISTQB®, che consiste nei Syllabus Working Group e nell'Exam Working Group.

Riconoscimenti

Questo documento è stato prodotto da un core team di ISTQB®: Dr. Frank Simon (chair), Alain Ribault, Gabriel Firmino Barjollo, Michael Pott, Beata Karpinska, Maria Kispal, Frans Dijkman

Il core team ringrazia il team di review Exam Working Group, il Syllabus Working Group e il National Board per i loro suggerimenti e contributi.

Traduzione italiana a cura di ITA-STQB (www.ita-stqb.org) – info@ita-stqb.org

Revisione della traduzione italiana a cura di: Raffaele Bozzini, Salvatore Reale.

Cronologia delle revisioni

Simulazione d'esame - Modello di layout delle domande utilizzato: Versione 2.6 Data: 20 settembre 2023

Versione	Data	Osservazioni
1.0	2024/09/10	Versione finale per l'approvazione GA
1.0.1	2025/01/31	Versione finale dopo revisione EWG

Indice dei contenuti

Avviso di copyright	2
Responsabilità del documento	2
Riconoscimenti	2
Cronologia delle revisioni	4
Indice dei contenuti	5
Introduzione	7
Scopo del documento	7
Istruzioni	7
Domande	8
Domanda 1 (1 punto)	8
Domanda 2 (1 punto)	8
Domanda 3 (1 punto)	9
Domanda 4 (1 punto)	9
Domanda 5 (1 punto)	9
Domanda 6 (1 punto)	10
Domanda 7 (1 punto)	10
Domanda 8 (1 punto)	11
Domanda 9 (1 punto)	12
Domanda 10 (1 punto)	12
Domanda 11 (1 punto)	13
Domanda 12 (1 punto)	13
Domanda 13 (1 punto)	13
Domanda 14 (1 punto)	14
Domanda 15 (1 punto)	14
Domanda 16 (1 punto)	14
Domanda 17 (1 punto)	15
Domanda 18 (1 punto)	15
Domanda 19 (1 punto)	16
Domanda 20 (1 punto)	17
Domanda 21 (1 punto)	17
Domanda 22 (1 punto)	18
Domanda 23 (1 punto)	19
Domanda 24 (1 punto)	19
Domanda 25 (2 punti)	20
Domanda 26 (2 punti)	20
Domanda 27 (1 punto)	21
Domanda 28 (2 punti)	21
Domanda 29 (1 punto)	22
Domanda 30 (1 punto)	22
Domanda 31 (1 punto)	23
Domanda 32 (1 punto)	23
Domanda 33 (1 punto)	24
Domanda 34 (1 punto)	24
Domanda 35 (1 punto)	25
Domanda 36 (1 punto)	25



Domanda 37 (1 punto)	26
Domanda 38 (1 punto)	26
Domanda 39 (1 punto)	27
Domanda 40 (1 punto)	27

Introduzione

Scopo del documento

Le domande di questa simulazione, le risposte e le relative giustificazioni associate alle domande di questa simulazione d'esame sono state create da un team di esperti in materia e da scrittori esperti di domande, con l'obiettivo di:

- Supportare i Member Board e l'Exam Board ISTQB® nelle loro attività di scrittura delle domande
- Fornire ai Training Provider e ai candidati all'esame esempi di domande d'esame

Queste domande non possono essere utilizzate senza essere modificate in nessun esame ufficiale.

Si noti che gli esami reali possono includere un'ampia varietà di domande, e che questa simulazione d'esame **non** intende includere esempi di tutti i possibili tipi, stili o lunghezze di domande; inoltre, questa simulazione d'esame può essere più difficile oppure meno difficile di qualsiasi esame ufficiale.

Istruzioni

In questo documento potete trovare:

- Domande¹, ognuna delle quali include:
 - Qualsiasi scenario richiesto dal testo della domanda
 - Valore del punteggio
 - Insieme delle opzioni di risposta
- Domande aggiuntive, ognuna delle quali include [non si applica a tutte le simulazioni d'esame]:
 - Qualsiasi scenario richiesto dal testo della domanda
 - Valore del punteggio
 - Insieme delle opzioni di risposta
- Le risposte, compresa la giustificazione, sono contenute in un documento separato.

¹ In questa simulazione d'esame le domande sono ordinate in base al LO di riferimento; non ci si deve aspettare lo stesso ordine in una prova d'esame reale.

Domande

Domanda 1 (1 punto)

Quale delle seguenti opzioni descrive MEGLIO il livello di sicurezza degli asset in termini di integrità?

- a) Solo agli utenti autenticati dovrebbe essere concesso l'accesso per modificare file e applicazioni
- b) Solo ai proprietari dei file è possibile concedere l'accesso per modificare i dati al fine di garantire la corretta integrità
- c) La cronologia dei tentativi non autorizzati deve essere conservata per due anni
- d) Stabilire una procedura che consenta agli utenti di accedere ai dati non modificati ogni volta che ne hanno bisogno

Selezionare UNA opzione.

Domanda 2 (1 punto)

Quale delle seguenti opzioni è un'alternativa adeguata per descrivere in che modo il testing di sicurezza può confermare che la confidenzialità delle informazioni sensibili è adeguatamente protetta?

- a) Verifica che esistano controlli adeguati che impediscano l'accesso non autorizzato alle informazioni riservate
- b) Verifica che esistano controlli adeguati che garantiscano che solo gli aggiornamenti autorizzati possano essere effettuati e che tutti i dati rimangano affidabili
- c) Verifica i meccanismi di ripristino rapido per ripristinare prontamente i servizi dopo un incidente
- d) Verifica che la risposta dell'organizzazione agli incidenti sia efficace, riducendo al minimo i danni e il downtime

Selezionare UNA opzione.

Domanda 3 (1 punto)

Quale delle seguenti opzioni descrive MEGLIO un audit di sicurezza?

- a) Una valutazione sistematica del testing di sicurezza e della strategia di sicurezza complessiva in tutta l'organizzazione
- b) Una valutazione sistematica della sicurezza del sistema informativo misurando il grado di conformità a una serie di criteri prestabiliti
- c) Una valutazione sistematica volta a impedire l'accesso al sistema da parte di intrusi non autorizzati
- d) Una valutazione sistematica volta a ridurre i rischi identificando l'hardware e il software soggetti a vulnerabilità

Selezionare UNA opzione.

Domanda 4 (1 punto)

Quale delle seguenti opzioni descrive il modello Zero Trust?

- a) Tutti gli utenti richiedono una verifica continua dell'identità indipendentemente dalla loro posizione
- b) Tutti i dispositivi e gli utenti con accesso al sistema sono considerati affidabili a prescindere
- c) Solo i dispositivi all'interno della rete affidabile hanno accesso ai sistemi
- d) A tutti gli utenti viene concesso il livello di accesso di cui hanno bisogno

Selezionare UNA opzione.

Domanda 5 (1 punto)

Quale delle seguenti opzioni includeresti per verificare che il concetto di Zero Trust sia stato implementato correttamente?

- a) Implementare controlli che verificano ogni singola richiesta di accesso a qualsiasi risorsa sensibile
- b) Le richieste di accesso avviate da account di servizio non umani sono sempre considerate affidabili
- c) Verificare che i registri di accesso prodotti dal sistema forniscano una registrazione permanente e contrassegnata da data e ora di tutte le attività
- d) Implementare set di autorizzazioni standard basati sui ruoli e sulle responsabilità degli utenti
- e) Focalizzarsi sui controlli di accesso alla rete esterna invece che sui controlli di applicazioni, risorse, dati e asset specifici

Selezionare DUE opzioni.

Domanda 6 (1 punto)

Quando si utilizza software open source, quale dei seguenti NON è un fattore critico da considerare quando si affrontano le questioni relative alla sicurezza?

- a) Allineamento con OWASP e audit di sicurezza attivi da parte dei contributori
- b) Frequenza e disponibilità di patch e aggiornamenti di sicurezza
- c) La capacità del tuo team di gestire e personalizzare lo strumento per il tuo ambiente
- d) Requisiti di licenza e conformità alle linee guida di sicurezza open source

Selezionare UNA opzione.

Domanda 7 (1 punto)

Una banca ha subappaltato lo sviluppo di nuove funzionalità per il proprio portale clienti, al fine di migliorare la user experience. Lo sviluppo delle funzionalità è stato completato e consegnato alla banca. La banca ti chiama per pianificare ed eseguire test di sicurezza su un ambiente di pre-produzione prima del deployment.

Quale delle seguenti opzioni descrive meglio il tuo approccio a questa attività?

- a) Eseguire testing white-box per coprire tutto il codice sorgente e assicurarsi che non ci siano più difetti prima del deployment
- b) Eseguire uno scanning delle vulnerabilità grey-box per assicurarsi che tutte le vulnerabilità note nell'ambito del progetto, potenzialmente sfruttabili da un attacker, siano o saranno identificate
- c) Eseguire testing di fault injection black-box per individuare potenziali punti di ingresso vulnerabili
- d) Verificare che le regole di codifica di sicurezza siano state applicate utilizzando uno strumento di testing di sicurezza statico delle applicazioni
- e) Verificare se le vulnerabilità rilevate dal testing white-box potrebbero essere sfruttabili

Selezionare DUE opzioni.

Domanda 8 (1 punto)

In qualità di security test engineer nel progetto, hai il compito di definire le tecniche di test di sicurezza che devono essere applicate come testing di sicurezza statico.

Quale sarebbe il tuo approccio?

- a) Verificare che gli sviluppatori applichino le regole di codifica di sicurezza, controllare che la progettazione abbia seguito le best practice "security by design" e quindi verificare che i requisiti di sicurezza siano completi
- b) Verificare che le regole di codifica siano applicate dagli sviluppatori, quindi creare l'applicazione ed eseguire alcuni SQL injection per verificare che i campi di input siano correttamente protetti contro gli SQL injection
- c) Verificare che i requisiti di sicurezza siano completi, verificare che la progettazione abbia seguito le best practice "security by design" e quindi verificare che gli sviluppatori applichino le regole di codifica di sicurezza
- d) Verificare che l'insieme dei requisiti di sicurezza sia pertinente e completo, quindi eseguire testing sui valori limite sull'applicazione creata per verificare che i buffer overflow siano evitati applicando regole di codifica di sicurezza dedicate

Selezionare UNA opzione.

Domanda 9 (1 punto)

Ti è stato fornito il seguente requisito per il testing di sicurezza:

Un utente potrà richiedere il reset della propria password. Se effettua questa richiesta, dovrà rispondere correttamente a due delle tre domande di sicurezza. Se risponde correttamente, riceverà un link al proprio indirizzo e-mail. Il link lo reindirizzerà a una pagina in cui potrà reimpostare la password. Una volta reimpostata, potrà effettuare il login con la nuova password. Il link dovrà diventare non valido 1 ora dopo l'invio o se l'utente invia un'altra richiesta di reset della password. Se l'utente invia più di due richieste di reset della password senza completare la reimpostazione, l'ID utente verrà bloccato. Per sbloccare l'ID, l'utente dovrà contattare l'help desk.

Quale dei seguenti è l'elenco minimo delle condizioni di test per testare adeguatamente la sicurezza funzionale coperta da questo requisito?

- a) Utente non valido; utente valido; 2 risposte corrette; 2 risposte errate; reset completo della password; link valido; link scaduto; due richieste senza reimpostazione; 3 richieste senza reimpostazione
- b) Utente valido; utente valido; 2 risposte corrette; 3 risposte corrette; reset completo della password; link valido; due richieste senza reimpostazione
- c) Utente non valido; utente non valido; 2 risposte errate; link scaduto; 3 richieste senza reimpostazione; caratteri non validi
- d) Utente non valido; utente valido; utente non valido; utente valido; 2 risposte corrette; 2 risposte errate; buffer overflow su ogni campo di immissione; SQL injection

Selezionare UNA opzione.

Domanda 10 (1 punto)

Nella tua organizzazione, sei responsabile dell'Identification & Access Management per gestire e mantenere gli account e i diritti degli utenti. Negli ultimi due mesi, ci sono state due nuove assunzioni e una persona dell'azienda ha cambiato reparto. Ai loro profili sono stati assegnati i nuovi ruoli e diritti. Quali tecniche di test di sicurezza dovresti pianificare in base alle tue responsabilità?

- a) Non è necessario alcun test perché gli account e i diritti sono stati gestiti
- b) Revisionare i permessi dei ruoli della persona che ha cambiato reparto
- c) Testare i ruoli e i privilegi assegnati ai nuovi assunti per assicurarsi che siano impostati correttamente
- d) Non è necessario alcun test perché i nuovi assunti hanno ruoli e privilegi di base e la persona che ha cambiato reparto ha meno privilegi rispetto a prima
- e) Dopo aver applicato le modifiche, verificare che l'accesso alle nuove applicazioni funzioni correttamente

Selezionare DUE opzioni.

Domanda 11 (1 punto)

Quale delle seguenti opzioni descrive CORRETTAMENTE le tecniche di test di sicurezza per il meccanismo di autenticazione?

- a) Verificare se gli utenti possono gestire le risorse di sistema in base ai loro ruoli
- b) Verificare le credenziali di accesso preimpostate e valutare i requisiti di sicurezza delle password
- c) Verificare i livelli di autorizzazione degli utenti attraverso l'analisi dei profili
- d) Monitorare i registri delle attività degli utenti durante il processo di login

Selezionare UNA opzione.

Domanda 12 (1 punto)

Quale delle seguenti affermazioni descrive MEGLIO come testare i controlli di protezione dei dati?

- a) Il testing dovrebbe valutare le misure di sicurezza verificando la conformità delle funzionalità di crittografia, controllo degli accessi e mascheramento dei dati
- b) Il testing dovrebbe misurare esclusivamente la rapidità e l'efficienza con cui le misure di protezione operano nel sistema
- c) Il testing dovrebbe esaminare come gli utenti interagiscono con le funzionalità di sicurezza attraverso gli elementi dello schermo e i controlli
- d) Il testing dovrebbe analizzare le prestazioni dei sistemi di archiviazione dei dati quando le funzionalità di sicurezza sono attive

Selezionare UNA opzione.

Domanda 13 (1 punto)

Ti viene chiesto di spiegare le procedure per valutare il system hardening come esempio tipico di tecnologia di protezione. Quale procedura potresti seguire per garantire che i meccanismi di hardening messi in atto funzionino come previsto?

- a) Monitorare attentamente i vari report e metriche sulle prestazioni di sicurezza per determinare se è stato raggiunto il livello corretto di accesso e autenticazione, ovvero se non è troppo restrittivo né troppo ampio
- b) Effettuare audit frequenti dell'autenticazione forte per garantire che venga mantenuto in ogni momento un elevato livello di protezione dalle intrusioni
- c) Valutare i componenti hardware sottoposti a hardening e confrontarli con gli altri componenti software protetti, al fine di garantire il raggiungimento di una condizione di equilibrio
- d) Chiedere a un hacker noto di condurre una valutazione indipendente dell'efficacia dell'hardening

Selezionare UNA opzione.

Domanda 14 (1 punto)

Sei responsabile di tutti gli aspetti del processo di sicurezza, compreso il testing. Per questa attività specifica, devi utilizzare test di alto livello come base per i test manuali ed eseguirli dal punto di vista di un vendor esterno. Quale attività di test di sicurezza può essere svolta in parallelo con questa?

- a) Creazione delle condizioni di test e degli obiettivi di test dei test di sicurezza
- b) Implementazione dei test di sicurezza
- c) Valutazione complessiva e reporting del testing di sicurezza
- d) Analisi e progettazione dei test di sicurezza

Selezionare UNA opzione.

Domanda 15 (1 punto)

Quale delle seguenti è una caratteristica principale di un ambiente di test di sicurezza efficace?

- a) Strettamente legato ai sistemi di produzione per migliorare la sicurezza in tutti i punti
- b) Isola le diverse versioni precedenti dei sistemi operativi da utilizzare nell'ambiente
- c) Imita l'ambiente di produzione in termini di diritti di accesso
- d) Include tutti i plug-in dell'ambiente di produzione e altri plug-in non presenti nell'ambiente di produzione per garantire la configurazione più completa

Selezionare UNA opzione.

Domanda 16 (1 punto)

Durante il testing di componente, quale warning del compilatore attiverrebbe maggiormente il security tester?

- a) Quelli che indicano problemi di sicurezza che devono essere risolti
- b) Quelli che indicano potenziali problemi da sottoporre a indagine
- c) Quelli che indicano problemi di codifica che causeranno difetti di adeguatezza funzionale
- d) Quelli che indicano pratiche di programmazione inadeguate che aumenteranno la manutenibilità

Selezionare UNA opzione.

Domanda 17 (1 punto)

Data la seguente specifica di progettazione: il Componente A e il Componente B comunicano tramite un'API REST. Quale delle seguenti opzioni è un esempio di test di sicurezza eseguito a livello di integrazione dei componenti?

- a) Testare la crittografia dei dati durante le chiamate API tra il componente A e il componente B
- b) Testare la possibilità del componente A di chiamare l'API del componente B
- c) Testare che i componenti esterni provengano da fornitori affidabili
- d) Testare il tempo di risposta tra il componente A e il componente B

Selezionare UNA opzione.

Domanda 18 (1 punto)

Quale delle seguenti opzioni descrive MEGLIO la procedura corretta per l'implementazione di testing di sicurezza end-to-end per testare la gestione da parte del sistema dei tentativi di login non riusciti?

- a) Prima dell'esecuzione dei test, predisporre un generatore di password manager per cambiare la password al momento del login. Effettui il logout, quindi effettui il login utilizzando la password appena creata. Tre tentativi di login non riusciti genereranno un messaggio di blocco
- b) Dopo diversi tentativi di login, ricevi un messaggio di blocco e chiami il Service Desk per ottenere una password temporanea via e-mail. Effettui il login con la password temporanea, effettui il logout, poi effettui nuovamente il login e inserisci una nuova password
- c) Dopo aver provato ad effettuare il login più volte senza successo, premi il pulsante per ottenere un link per modificare la password. Dopo aver ottenuto il link, riutilizzi la tua vecchia password. Il sistema accetta la password.
- d) Dopo il primo tentativo di utilizzare una password non valida, apri un elenco di password sul blocco note del tuo PC per assicurarti di utilizzare quella corretta. Provi un'altra password dall'elenco e funziona

Selezionare UNA opzione.

Domanda 19 (1 punto)

Lavori come test manager presso una banca che sta sviluppando una nuova applicazione di online banking. L'applicazione gestirà dati sensibili dei clienti e transazioni finanziarie. Ti viene chiesto di eseguire il testing di sicurezza per la nuova applicazione. Non ci sono requisiti espliciti, quindi selezioni i tuoi test case dagli standard e dalle best practice.

Quali tre (3) delle seguenti affermazioni ti guidano meglio nella selezione dei test case?

- i. Le norme costituiscono un input valido in quanto approvate da un organismo di riferimento riconosciuto
- ii. Gli standard possono essere classificati in standard industriali, standard de facto e standard specifici del produttore. Gli standard industriali e gli standard de facto sono input validi, mentre gli standard del produttore potrebbero non essere adatti a un contesto specifico
- iii. Poiché gli standard sono obbligatori, sono input validi in quanto devono essere applicati in tutti gli ambienti
- iv. Le best practice non sono input validi in quanto solitamente sono di livello molto elevato
- v. Gli standard de facto sono input validi poiché spesso hanno le loro radici negli standard industriali

- a) i, ii e v
- b) i, ii e iii
- c) ii, iii e v
- d) iii, iv e v

Selezionare UNA opzione.

Domanda 20 (1 punto)

Una nuova start-up nel settore bancario ha sviluppato un nuovo sistema core. Finora il team di sviluppo si è concentrato sulla buona usabilità e sulle eccellenti prestazioni. Prima del go-live, il consiglio di amministrazione desidera ottenere un parere indipendente sul livello di sicurezza. Ti chiedono, in qualità di security tester, di eseguire un penetration test black-box. L'attività consiste nel testare le vulnerabilità più critiche che potrebbero essere sfruttate per la nuova app bancaria.

Se volete svolgere questo lavoro, come potete utilizzare gli standard per il vostro compito?

- a) Selezioni le debolezze rilevanti all'interno dello standard CWE ed esegui i test case elencati
- b) Selezioni le debolezze rilevanti all'interno del CWE, scegli gli exploit disponibili per i CWE selezionati e li applichi
- c) Selezioni le debolezze rilevanti all'interno del CWE, prioritizzi i CWE selezionati in base allo standard CWSS e selezioni i CVE rilevanti che coprono i CWE prioritizzati
- d) Selezioni le debolezze rilevanti all'interno del CWE, prioritizzi i CWE selezionati in base allo standard CVSS e derivi i singoli test case relativi al CVSS
- e) Per ogni CVE selezionato, derivi test case per l'app bancaria e li esegui

Selezionare DUE opzioni.

Domanda 21 (1 punto)

Quando utilizzi oracoli del test per un'applicazione basati su standard e best practice, cosa è necessario considerare?

- a) Tali oracoli del test sono validi indipendentemente dai parametri dell'applicazione
- b) Tali oracoli di test possono essere utilizzati solo come indizi approssimativi per i test di sicurezza
- c) Tali oracoli del test non possono essere utilizzati per il testing di sicurezza
- d) Meno specifica è un'applicazione e il suo contesto, più efficiente è il riutilizzo di tale test

Selezionare UNA opzione.

Domanda 22 (1 punto)

Le best practice e gli standard forniscono molti artefatti che possono essere utilizzati efficacemente per il testing di sicurezza. Quali combinazioni di artefatti e attività corrispondono correttamente?

1. Terminologia coerente
2. Conoscenza di esperti
3. Benchmarking
4. Panoramica olistica della sicurezza

che può essere utilizzata per:

- A. comunicazione più semplice
- B. riutilizzo delle conoscenze di esperti in materia di sicurezza per il testing di sicurezza
- C. doppio controllo della completezza delle attività del testing di sicurezza
- D. dimostrare facilmente l'efficacia delle attività del testing di sicurezza applicate

- a) 1-A, 2-B, 3-D, 4-C
- b) 1-A, 2-B, 3-C, 4-D
- c) 1-D, 2-A, 3-B, 4-C
- d) 1-B, 2-D, 3-A, 4-C

Selezionare UNA opzione.

Domanda 23 (1 punto)

Sei stato assunto come security tester dal management di una società di ingegneria di medie dimensioni che produce diversi componenti per il settore automotive e dipende fortemente dai propri fornitori, poiché il prezzo delle materie prime influisce direttamente sui profitti. L'azienda dispone solo di un sito web pubblico e di un dominio di posta elettronica ben noto, ma non offre ulteriori servizi web. Il tuo compito è ottenere l'accesso all'ambiente di produzione interno, costituito da diversi impianti industriali moderni, e compromettere almeno un sistema.

Quali DUE opzioni rappresentano al meglio il modo in cui potresti trarre vantaggio dal contesto organizzativo?

- a) Infiltrarsi in uno dei fornitori più utilizzati per avvicinarsi all'azienda target effettiva
- b) Eseguire un attacco di social engineering fingendo di essere un fornitore esistente o un nuovo potenziale fornitore e cercare di ottenere maggiori informazioni sull'obiettivo, ad esempio visitandolo e chiedendo di poterlo visionare brevemente
- c) Identificare l'indirizzo e-mail del reparto contabilità e inviare fatture false contenenti contenuti dannosi, ad esempio per ottenere l'accesso remoto tramite una shell inversa
- d) Spargere chiavette USB nell'edificio dell'azienda e attendere che qualcuno le raccolga e le colleghi
- e) Effettuare un attacco brute force contro il login SSH del server web

Selezionare DUE opzioni.

Domanda 24 (1 punto)

La tua azienda sviluppa diversi prodotti per l'industria aeronautica. All'inizio dell'anno è stato annunciato un nuovo prodotto. Per la prima volta, si tratterà di un dispositivo di comunicazione. Il tuo compito è eseguire il testing di sicurezza del nuovo prodotto prima che venga lanciato sul mercato.

Quale dei seguenti aspetti descrive MEGLIO ciò che devi prendere in considerazione?

- a) Il settore aeronautico è un settore regolamentato; pertanto, il nuovo prodotto e l'intero processo di sviluppo devono essere conformi alle normative vigenti
- b) Alcuni paesi hanno normative proprie in materia di antenne radio e standard utilizzati. Il prodotto deve funzionare correttamente, anche se alcune frequenze potrebbero interferire con quelle utilizzate dal prodotto stesso
- c) I test di sicurezza devono essere eseguiti molto rapidamente, poiché il prodotto deve essere lanciato il prima possibile
- d) I dipendenti devono dimostrare le loro conoscenze in materia di radiocomunicazioni attraverso certificazioni personali

Selezionare UNA opzione.

Domanda 25 (2 punti)

Durante il testing di sicurezza di un sistema core, trovi diversi file sospetti che non sono stati creati né da te né da altri tester durante il testing, e non sono utilizzati dalle applicazioni in esecuzione su quel sistema.

Scegli l'opzione che descrive MEGLIO come procederesti.

- a) Continuare il test di sicurezza e creare report sulle tue scoperte dopo aver completato tutte le attività di testing
- b) Sospendere il test di sicurezza e inviare un'e-mail informativa almeno a tutti i colleghi che hanno accesso al sistema. Continuare, se nessuno ha obiezioni.
- c) Interrompere il test di sicurezza e spegnere immediatamente il sistema, poiché si è verificato un accesso non autorizzato e occorre prevenire ulteriori potenziali danni
- d) Interrompere il test di sicurezza e seguire i passaggi definiti dalla politica di sicurezza aziendale per il reporting di un incidente. Se non esiste una politica per il reporting degli incidenti, segnalare al responsabile designato (ad esempio, IT Security Officer, CISO...)
- e) Interrompere il test di sicurezza e avviare le indagini seguendo i passaggi definiti dalla politica di sicurezza aziendale in materia di indagini

Selezionare UNA opzione.

Domanda 26 (2 punti)

Ogni attacco è diverso. Tuttavia, alcune fasi sono comuni a quasi tutti gli attacchi. Queste fasi possono essere definite come:

- a) Fase di raccolta delle informazioni, seguita dallo sfruttamento/ottenimento dell'accesso e, alla fine, dalla persistenza/mantenimento dell'accesso
- b) Social engineering, seguita da attacco brute force e infine persistenza/mantenimento dell'accesso
- c) Sfruttamento/ottenimento dell'accesso seguito da social engineering per comprendere i risultati e, alla fine, cancellazione delle tracce
- d) Raccolta di informazioni, seguita dalla cancellazione delle tracce e, alla fine, social engineering per ottenere una baseline migliore

Selezionare UNA opzione.

Domanda 27 (1 punto)

Quale delle seguenti affermazioni descrive MEGLIO come dovrebbe essere implementato il testing di sicurezza nel ciclo di vita dello sviluppo?

- a) Ogni attività di sviluppo dovrebbe avere una corrispondente attività di testing di sicurezza
- b) Con un'adeguata analisi delle minacce e una corretta progettazione della sicurezza è possibile individuare la maggior parte delle vulnerabilità
- c) SAST e DAST dovrebbero essere eseguiti in tutte le fasi del ciclo di vita dello sviluppo software
- d) Il testing di sicurezza dovrebbe essere eseguito durante tutte le fasi del ciclo di vita dello sviluppo software per rimanere sincronizzati con il testing funzionale manuale

Selezionare UNA opzione.

Domanda 28 (2 punti)

Quali DUE delle seguenti affermazioni descrivono MEGLIO l'impatto di un modello di sviluppo software sul testing di sicurezza?

- a) Il team può coinvolgere un team di abilitazione alla sicurezza (security enabling team) per eseguire i test di sicurezza in ogni modello.
- b) Il modello Waterfall supporta al meglio il testing di sicurezza durante il ciclo di vita dello sviluppo software
- c) DevOps può fornire un supporto migliore per il testing di sicurezza da eseguire durante le operazioni
- d) È più facile eseguire il testing di sicurezza utilizzando Kanban rispetto a Scrum
- e) Il testing di sicurezza può essere pianificato meglio utilizzando i modelli di sviluppo software Agile rispetto al modello Waterfall

Selezionare DUE opzioni.

Domanda 29 (1 punto)

Quale delle seguenti quattro affermazioni è vera per il testing di sicurezza nel contesto del testing di manutenzione?

- a) Focalizzarsi sulla conferma della soddisfazione di tutti i requisiti di sicurezza dopo la modifica
- b) Eseguire il set di regressione esistente sulle singole funzioni per verificare che la modifica funzioni
- c) Testare le nuove vulnerabilità che potrebbero essere state introdotte dalla modifica
- d) Eseguire test di sicurezza confermativi e di regressione dopo che è stata apportata una modifica

Selezionare UNA opzione.

Domanda 30 (1 punto)

Quale delle seguenti opzioni descrive MEGLIO il motivo per cui è necessario analizzare i risultati del testing di sicurezza?

- a) Per comprendere meglio le minacce e i rischi specifici per la sicurezza sulla base di valutazioni della sicurezza, audit e fonti standard di vulnerabilità note
- b) Per tradurre i test concettuali in test che possono essere eseguiti manualmente o con strumenti
- c) Per definire un ambito di testing appropriato che corrisponda ai rischi di sicurezza
- d) Per portare a termine le attività di testing di sicurezza in modo che i test possano essere mantenuti ed eseguiti regolarmente per supportare eventuali nuovi requisiti di sicurezza e/o rilevare nuove minacce

Selezionare UNA opzione.

Domanda 31 (1 punto)

Sei responsabile della sicurezza del sistema. Un membro del tuo team è interessato al testing di sicurezza ed esegue un penetration test sul tuo sistema, che include le vulnerabilità di OWASP Top-10. Il test report corrispondente consiste solo di test case riusciti e falliti che coprono queste vulnerabilità. Quale ragionamento sull'accettazione o il rifiuto del test report è corretto?

- a) Accettare, poiché il penetration test è stato condotto da un collega interno esperto delle linee guida di sicurezza specifiche
- b) Rifiutare, poiché i tuoi criteri di accettazione per la sicurezza non sono stati comunicati e non sono stati presi in considerazione nel test report. Pertanto, non è chiaro se siano state utilizzate le tecniche di test corrispondenti e se i risultati dei test siano rilevanti per la verifica annuale della conformità alle vostre linee guida sulla sicurezza
- c) Accettare, poiché OWASP è una best practice e definisce un elenco generale di criteri di accettazione
- d) Rifiutare, perché linee guida sulla sicurezza del codice dovrebbero essere testate con approcci di testing white-box, non con penetration test dinamici black-box
- e) Accettare, poiché OWASP riflette le tue linee guida sulla sicurezza del codice

Selezionare DUE opzioni.

Domanda 32 (1 punto)

Per utilizzare il testing di sicurezza al massimo livello di efficienza ed efficacia, deve:

- a) Essere integrato in un processo di sicurezza complessivo, che cerchi di ridurre al minimo i rischi e garantire la continuità del business
- b) Essere applicato su base annuale a tutti i sistemi IT utilizzati
- c) Essere utilizzato per limitare in modo proattivo l'impatto di una violazione della sicurezza
- d) Tenere conto delle vulnerabilità comunicate quotidianamente
- e) Garantire che tutte le vulnerabilità identificate siano risolte entro un periodo di tempo adeguato inferiore a 6 mesi

Selezionare DUE opzioni.

Domanda 33 (1 punto)

Le dimensioni tipiche che un security test engineer può utilizzare per migliorare l'ambito dell'ISMS sono:

- 1) Aggiungere ulteriori oggetti di test al suo ambito di test
- 2) Aggiungere ulteriori tecniche di test alla sua progettazione di test
- 3) Migliorare la copertura dei test mantenendo gli oggetti di test e gli approcci di test esistenti
- 4) Aumentare l'automazione dell'esecuzione dei test di sicurezza

Che possono essere utilizzate per:

- A. apportare ulteriori approfondimenti su un determinato sistema che possono essere utilizzati per migliorare un ISMS esistente
- B. identificare ulteriori debolezze di componenti noti per migliorare un ISMS esistente
- C. identificare ulteriori debolezze per componenti che non fanno ancora parte dell'ISMS complessivo
- D. rendere più sicuro il sistema IT esistente

Quale delle seguenti alternative presenta il corretto abbinamento tra le azioni e gli obiettivi del security test engineer?

- a) 1-C, 2-A, 3-B
- b) 1-B, 2-D, 3-B
- c) 1-C, 2-A, 4-B
- d) 1-D, 2-C, 4-A

Selezionare UNA opzione.

Domanda 34 (1 punto)

In che modo il testing di sicurezza può migliorare la misurabilità all'interno di un ISMS?

- a) I test di sicurezza possono essere utilizzati come analisi oggettiva nella fase Check del ciclo PDCA per misurare l'efficacia di un ciclo PDCA
- b) Tutti i test di sicurezza generano informazioni quantificabili sulla sicurezza di un sistema che possono essere utilizzate per misurare l'efficacia dell'ISMS
- c) Più test di sicurezza hanno esito positivo per un sistema in fase di test, migliore e più efficace è l'ISMS
- d) L'efficacia di un ISMS è tanto migliore quanto più vengono utilizzate tecniche di testing di sicurezza

Selezionare UNA opzione.

Domanda 35 (1 punto)

I test report di sicurezza dovrebbero essere trattati con un elevato livello di confidenzialità. Quale tipo di dati presenti nella maggior parte dei test report di sicurezza motiva questa classificazione?

- a) Nome del security tester, tempistica di esecuzione dei test, risultati dei test (test case superati e falliti)
- b) Ambiente di test utilizzato, precondizioni preimpostate dei test eseguiti, dati di test utilizzati, procedura di esecuzione dei test, comportamento rilevato
- c) Elenco delle vulnerabilità CVE testate, elenco dei nomi degli sviluppatori, metodo di sviluppo software identificato, strumenti di sviluppo software identificati
- d) Convenzioni di codifica di sicurezza utilizzate, copertura dei test funzionali identificata, scan delle vulnerabilità applicate

Selezionare UNA opzione.

Domanda 36 (1 punto)

Immagina di aver eseguito alcuni test case di sicurezza come parte di un penetration test per un sistema business-critical. Uno di questi è fallito e sembra che tu abbia identificato una possibile vulnerabilità, che potrebbe avere un impatto drammatico per il business. Cosa è necessario fare prima di motivarne direttamente la mitigazione?

- a) Demarcazione della vulnerabilità, ovvero eseguire test case simili per identificare la demarcazione della vulnerabilità identificata
- b) Stima dell'effort necessario per l'azione di mitigazione, ovvero elaborazione di una break down structure della mitigazione prevista
- c) Progettazione della mitigazione, ovvero progettare la soluzione che mitiga la vulnerabilità identificata
- d) Regolazione del rischio 1, ovvero ricontrollare che la vulnerabilità identificata possa essere sfruttata in produzione
- e) Inizi immediatamente a mitigare la vulnerabilità identificata

Selezionare DUE opzioni.

Domanda 37 (1 punto)

Immagina di aver identificato una vulnerabilità al livello 9.8 del CVSS. Hai verificato che questa vulnerabilità possa essere sfruttata anche in produzione e l'azienda ha confermato che questa vulnerabilità può avere un impatto negativo molto forte. D'altra parte, l'applicazione è business-critical, quindi si decide di mitigare il rischio identificato associato alla vulnerabilità identificata: Qual è la tua raccomandazione?

- a) Se la vulnerabilità influisce su un insieme specifico di funzionalità, è necessario analizzare se è possibile disattivare la funzionalità specifica che contiene la vulnerabilità
- b) Nella maggior parte dei casi è più facile bloccare il traffico specifico a livello di rete, quindi il compito è bloccare il traffico vulnerabile specifico all'interno del firewall
- c) Se si dispone di un moderno firewall per applicazioni web, le vulnerabilità vengono identificate e mitigate automaticamente
- d) Se è possibile aggiungere un ulteriore controllo di sicurezza all'elenco degli utenti (ad esempio tramite filtraggio IP o aggiunta di MFA), si può considerare di ridurre la probabilità del rischio con questa tecnica
- e) Nella maggior parte dei casi, l'azione di mitigazione più rapida ed economica consiste nell'evitare completamente il problema riparando la vulnerabilità dei sistemi interessati

Selezionare DUE opzioni.

Domanda 38 (1 punto)

In un ambiente CI/CD, viene creata una nuova pipeline per il prossimo progetto a cui stai lavorando. Quale delle seguenti opzioni consiglieresti come primo passo da attivare nell'ambito della pipeline?

- a) SCA
- b) SAST
- c) DAST
- d) IAST

Selezionare UNA opzione.

Domanda 39 (1 punto)

Quali dei seguenti scanner e metodi di test eseguono la scansione dell'applicazione sottoposta a test durante il runtime?

- a) DAST
- b) Analisi statica
- c) SCA
- d) SAST

Selezionare UNA opzione.

Domanda 40 (1 punto)

Quali oggetti di test possono essere analizzati dagli strumenti di testing statico?

- a) File di configurazione
- b) Progettazione della sicurezza
- c) Endpoint API
- d) Processi nella RAM

Selezionare UNA opzione.