Generated Quizzes

Question 1: _Alice ha configurato il firewall del suo server con le seguenti regole:

Labels:firewall, configurazione, iptables

- Il server accetta connessioni SSH sulla porta 22 e HTTP sulla porta 80. (Correct)

- Qualsiasi connessione in ingresso su altre porte verrà bloccata, inclusi i ping. (Correct)

- Alice può accedere da remoto al server tramite SSH solo se si trova nella stessa rete locale.

- Le risposte alle connessioni HTTP stabilite dal server non sono influenzate da queste regole. (Correct)

- Le regole configurate garantiscono automaticamente protezione contro attacchi DoS.

Question 2: Alice sta valutando i rischi legati al trattamento dei dati personali in conformità al GDPR. Quali delle seguenti azioni rappresentano buone pratiche?3

Labels:gdpr, analisi dei rischi, sicurezza

- Considerare l'impatto di una violazione dei dati sia a livello finanziario che reputazionale. (Correct)

- Coinvolgere i responsabili delle aree interessate nel processo di analisi dei rischi. (Correct)

- Documentare i rischi associati ai dati sensibili è necessario, mentre gli altri tipi di dati non sono tutelati dal GPDR è pertanto l'adeguata documentazione risulta opzionale.

- Valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate. (Correct)

- Concludere l'analisi dei rischi una volta definite le misure di protezione iniziali.

Question 3: Alice vuole ottenere la certificazione ISO/IEC 27001 per la sua rete aziendale e decide di implementare un IDS per monitorare le attività sospette. Quali delle seguenti pratiche sono necessarie per la conformità allo standard?3

Labels:standard, certificazioni, IDS

- Analizzare regolarmente i log generati dall'IDS per identificare potenziali minacce. (Correct)

- Integrare l'IDS con un sistema SIEM per garantire una gestione centralizzata degli eventi. (Correct)

- Impostare l'IDS per ignorare automaticamente tutto il traffico autorizzato, senza generare log.

- Definire politiche documentate per l’uso dell’IDS e la gestione delle sue configurazioni. (Correct)

Question 4: Bob gestisce un server che deve essere accessibile sia per connessioni VPN sicure che per accesso HTTPS per i clienti. Quali differenze fondamentali tra IPsec e TLS dovrebbero influenzare la sua configurazione?3

Labels:ipsec, tls, differenze, sicurezza

- IPsec opera a livello di rete, mentre TLS opera a livello di trasporto, rendendo TLS più adatto per la protezione di applicazioni specifiche all’interno dello stesso server. (Correct)

- IPsec può fornire sicurezza per tutto il traffico di rete (unicast), inclusi protocolli non orientati alla connessione, mentre TLS protegge solo protocolli basati su TCP. (Correct)

- L'autenticazione in TLS è spesso basata su certificati, mentre IPsec può supportare autenticazione con chiavi precondivise o certificati. (Correct)

- TLS può essere utilizzato per proteggere il traffico multicast, mentre IPsec no.

- IPsec è ottimale per la protezione di pagine web dinamiche come HTTPS, mentre TLS non è progettato per questo.

Question 5: Bob sta configurando il suo server SMTP e vuole garantire connessioni sicure ai suoi client. Quali delle seguenti configurazioni sono corrette?3

Labels:sicurezza

- Con il tipo di messaggio Clear-Signed, il contenuto del messaggio è leggibile da chiunque, anche se qualcuno potrebbe non riuscire a validare la firma digitale. (Correct)

- Grazie a messaggi di tipo EnvelopedData, si garantiscono autenticità e integrità, ma non riservatezza senza una cifratura aggiuntiva.

- Utilizzando il tipo SignedData, ogni destinatario può verificare l’autenticità della firma digitale, ma il processo potrebbe non essere automatizzato senza strumenti adeguati. (Correct)

- Con il tipo EnvelopedData, il contenuto cifrato può essere decifrato solo da un MUA specifico approvato dal mittente.

- Nella modalità in cui il dato viene prima inserito in una struttura SignedData e poi in una EnvelopedData, il messaggio è firmato digitalmente e il contenuto è sempre leggibile da chiunque.

- Bob dovrebbe configurare il server SMTP per utilizzare TLS su specifiche porte (es. porta 465 per SMTPS). (Correct)

- Bob dovrebbe installare certificati digitali per permettere l’autenticazione del server. (Correct)

- Bob può configurare il server SMTP per garantire che i messaggi di posta siano cifrati con S/MIME e gli header SMTP siano cifrati tramite TLS.

- Il server SMTP di Bob potrebbe accettare email cifrate anche se il client non supporta TLS. (Correct)

Question 6: Indica quali delle seguenti affermazioni sull'uso di TLS e STARTTLS nella posta elettronica sono vere:1

Labels:tls, starttls, email, sicurezza, protocollo

- Nei protocolli IMAP e POP3, l'uso di STARTTLS implica che la connessione viene prima stabilita in chiaro e solo successivamente, su richiesta del client, parte la negoziazione di un canale sicuro. (Correct)

- Il comando "EHLO" in SMTP viene utilizzato dal client per avviare una connessione TLS sicura.

- La differenza principale tra TLS e STARTTLS è che STARTTLS richiede una configurazione end-to-end mentre TLS opera solo a livello di trasporto.

- SMTP, nella sua versione base, offre nativamente crittografia obbligatoria su porta 25 per garantire sicurezza nei trasferimenti.

Question 7: Indica quali delle seguenti affermazioni sul formato MIME sono vere:3

Labels:mime, email, formato, header, body

- MIME è stato introdotto per superare le limitazioni del formato email originale, come la restrizione ai caratteri ASCII a 7 bit. (Correct)

- I messaggi MIME sono composti da un header e un body, dove l'header contiene metadati e il body contiene il contenuto del messaggio. (Correct)

- MIME supporta i messaggi multipart, consentendo l'inclusione di vari tipi di contenuto e allegati. (Correct)

- Gli header MIME non includono campi per specificare il mittente o il destinatario del messaggio che sono invece usati solo dal formato RFC822.

- MIME viene utilizzato solo per email basate su testo e non supporta allegati binari.

- MIME viene utilizzato per email basate su testo, ma è ormai obsoleto perché non permette di allegare immagini.

Question 8: Seleziona le affermazioni corrette sulle differenze tra PIA (Privacy Impact Assessment) e il RMF (Risk Management Process)?2

Labels:pia, analisi

- Il RMF fornisce un framework obbligatorio per la gestione dei rischi legati alla privacy nelle organizzazioni.

- Il PIA include una valutazione dell’impatto sui diritti degli individui, mentre il RMF si concentra sull’impatto sui sistemi e sugli asset organizzativi. (Correct)

- L’output del PIA è un documento che descrive esclusivamente le vulnerabilità tecniche dei sistemi.

- Il RMF prevede un monitoraggio continuo per aggiornare le strategie di mitigazione, mentre il PIA si limita a una valutazione iniziale.

- l PIA e il RMF sono processi complementari e possono essere utilizzati insieme in un'organizzazione. (Correct)

Question 9: Indica quali delle seguenti affermazioni sulla sicurezza dei messaggi sono vere:3

Labels:sicurezza, messaggi, TLS, riservatezza, integrit

- Sicurezza di messaggio vuol dire richiedere di garantire alcune proprietà di sicurezza, tra le quali riservatezza, integrità, autenticazione e non ripudio. (Correct)

- I primi tentativi di sicurezza della posta elettronica prevedevano l'uso di protocolli di canale come TLS.

- Il non ripudio nella posta elettronica significa che il mittente non può negare di aver inviato uno specifico messaggio di posta. (Correct)

- L'implementazione della sicurezza dei messaggi richiede modifiche alle applicazioni di posta elettronica esistenti. (Correct)

- S/HTTP è una versione più recente del protocollo HTTP sviluppata appositamente per funzionare con TLS.

Question 10: Quale ruolo svolge il protocollo IKE in IPsec?3

Labels:ipsec, ike, sicurezza autenticazione

- Negoziazione dei parametri di sicurezza tra i peer. (Correct)

- Gestione delle chiavi crittografiche. (Correct)

- Fornisce cifratura end-to-end per i dati.

- Configura le policy DNS per la risoluzione dei peer.

- Crea AH header e trailer.

- Offre diversi metodi di autenticazione tra cui CRA asimmetrico. (Correct)

Question 11: Indica quali delle seguenti affermazioni sul confronto tra S/MIME e PGP, e altri aspetti della sicurezza della posta elettronica, sono vere:2

Labels:smime, pgp, sicurezza, email, standard

- Sebbene sia S/MIME che PGP forniscano servizi di sicurezza per la posta elettronica, S/MIME è stato standardizzato dall IETF. (Correct)

- Sebbene sia S/MIME che PGP forniscano servizi di sicurezza per la posta elettronica, PGP è stato standardizzato dall IETF.

- L'utilizzo di una VPN garantisce la sicurezza end-to-end dei messaggi di posta elettronica, indipendentemente dal client e dal server utilizzati.

- A differenza di TLS, che protegge la comunicazione in transito, S/MIME protegge il messaggio stesso, indipendentemente dal percorso che compie. (Correct)

- A differenza di S/MIME, che protegge la comunicazione in transito, TLS protegge il messaggio stesso, indipendentemente dal percorso che compie.

- La crittografia a chiave simmetrica è intrinsecamente più sicura della crittografia a chiave asimmetrica perché utilizza chiavi più lunghe e complesse.