Generated Quizzes

Question 1: Indica quali affermazioni relative a IDS, IPS e sicurezza di rete sono corrette?4

Labels:IDS, IPS, sicurezza

- Un IDS passivo si limita a rilevare e segnalare attività sospette, senza intervenire attivamente. (Correct)

- Gli NGFW vengono venduti e pubblicizzati come in grado di identificare applicazioni e utenti, applicando policy di sicurezza specifiche. (Correct)

- Un IPS è sempre preferibile a un IDS perché previene attivamente le intrusioni, senza rischio di falsi positivi.

- Gli IDS possono utilizzare diverse tecniche di analisi, tra cui l'analisi dei log, il monitoraggio del traffico di rete e la verifica dell'integrità del sistema. (Correct)

- Un sensore IDS può essere posizionato sia per monitorare tratti di rete che su un singolo host. (Correct)

- I NIDS possono utilizzare diverse tecniche di analisi, tra cui l'analisi dei log file monitor, il monitoraggio del traffico di rete e la verifica dell'integrità del sistema.

- Gli IDS/IPS possono identificare applicazioni e utenti, applicando policy di sicurezza specifiche.

- L'integrazione di firewall, VPN e IDPS in un unico dispositivo (UTM) comporta un aumento dei costi di gestione a causa della maggiore complessità dei task che il dispositivo è in grado di svolgere.

Question 2: Quali tra le seguenti affermazioni sul protocollo ESP di IPsec sono vere?2

Labels:esp, ipsec

- ESPv1+ fornisce riservatezza cifrando il payload del pacchetto IP. (Correct)

- ESPv2+ può essere configurato per garantire autenticità e integrità dei dati tramite algoritmi di keyed-hash. (Correct)

- ESPv1+ crittografa sempre l’intero pacchetto IP, inclusi gli header, indipendentemente dalla modalità utilizzata.

- ESPv2 è progettato per funzionare esclusivamente in modalità Tunnel.

- ESPv3+ non può essere utilizzato insieme al protocollo AH.

Question 3: Quali affermazioni descrivono meglio l’utilizzo di TLS nella sicurezza di canale e nella sicurezza di messaggio?2

Labels:tls, sicurezza

- In entrambe le situazioni, il certificato del server deve essere verificato esplicitamente per garantire l’autenticità. (Correct)

- TLS puro non può essere utilizzato nella sicurezza di messaggio a meno che non si usi STARTTLS o STLS con protocolli tipo SMTP o POP/IMAP.

- Sono entrambi vulnerabili a downgrade della connessione o attacchi man-in-the-middle.

- Entrambi mantengono un canale sicuro dall’inizio della connessione.

- STARTTLS può permettere sia connessioni sicure che non sicure, dipende dalle ciphersuite scelte durante l’handshake. (Correct)

Question 4: Alice vuole proteggere i dati personali trattati dalla sua azienda attraverso un firewall. Quali delle seguenti affermazioni rispettano i requisiti del GDPR e le migliori pratiche di sicurezza?3

Labels:analisi dei rischi, firewall, GDPR

- Il firewall deve bloccare il traffico non autorizzato e registrare i tentativi di accesso. (Correct)

- La configurazione del firewall deve essere documentata come parte delle misure di sicurezza adottate. (Correct)

- Il GDPR richiede che i log del firewall includano i dati personali completi degli utenti per scopi di verifica (deep packet inspection).

- Il firewall deve essere aggiornato regolarmente per proteggere i dati personali da attacchi noti. (Correct)

- L'uso di un firewall e la sua corretta configurazione rendono superfluo adottare ulteriori misure di sicurezza per proteggere i dati personali.

Question 5: Indica quali delle seguenti affermazioni sulla struttura e sui protocolli della posta elettronica sono vere:5

Labels:email, protocollo, mta, msa, mua, smtp, tls

- MUA sta per Mail User Agent, MSA sta per Message Submission Agent e MTA sta per Message Transfer Agent. (Correct)

- SMTP è un protocollo orientato alla connessione utilizzato per l'invio di email. (Correct)

- Una sfida nella sicurezza della posta elettronica è la presenza di MTA potenzialmente non attendibili nella catena di consegna. (Correct)

- ESMTP è un'estensione di SMTP che introduce funzionalità aggiuntive, incluso il supporto per miglioramenti della sicurezza. (Correct)

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

- Il comando "HELO" in ESMTP viene utilizzato dal client per introdurre una nuova comunicazione tra due server.

- TLS può essere utilizzato per proteggere il canale di comunicazione tra un MUA e un Mail Store (MS). (Correct)

Question 6: Indica quali delle seguenti affermazioni su PKCS sono vere:3

Labels:pkcs12, pkcs7, pkcs, chiavi, certificati, crittografia

- PKCS #12 è un formato standard per l'archiviazione e il trasporto di materiale crittografico, incluse chiavi private e certificati. (Correct)

- I file PKCS #12 sono comunemente usati per esportare e importare identità digitali. (Correct)

- PKCS #12 è ampiamente supportato dai browser web e dai client di posta elettronica. (Correct)

- PKCS #7 è un formato standard per l'archiviazione e il trasporto di materiale crittografico, incluse chiavi private e certificati.

- I file PKCS #7 sono comunemente usati per esportare e importare identità digitali.

- PKCS #12 è considerata una soluzione di gestione delle chiavi altamente sicura e universalmente raccomandata per la sua efficienza.

- I file PKCS #12 possono memorizzare solo una singola chiave privata e un singolo certificato.

Question 7: Alice sta implementando un sistema di gestione della sicurezza delle informazioni (ISMS) conforme alla ISO/IEC 27001. Quali delle seguenti affermazioni sono corrette?_3

Labels:standard, sicurezza, analisi dei rischi

- Un ISMS efficace deve essere basato su un’analisi dei rischi documentata e continuamente aggiornata. (Correct)

- La certificazione ISO/IEC 27001 implica che l'organizzazione sia in grado di gestire correttamente i rischi associati alle informazioni sensibili. (Correct)

- La conformità alla ISO/IEC 27001 garantisce protezione contro le vulnerabilità software.

- La scelta delle misure di sicurezza deve tenere conto del contesto aziendale e delle esigenze specifiche dei processi. (Correct)

- Si può evitare di aggiornare l’analisi dei rischi se l’organizzazione implementa tutte le misure idonee identificate durante il processo di certificazione.

Question 8: Scegli le affermazioni corrette riguardo IPsec e la sicurezza delle reti:2

Labels:ipsec, sicurezza, ah, attacchi, integrit

- Durante l’invio di un pacchetto IPsec, il campo TTL errato causa un errore di integrità, scartando il pacchetto.

- Il protocollo ARP è sicuro grazie a meccanismi di autenticazione AH che proteggono integrità e confidenzialità.

- Gli attacchi di tipo replay non possono essere mitigati in IPsec senza algoritmi asimmetrici.

- Gli attacchi di tipo replay su reti IP possono essere mitigati tramite numeri di sequenza e timestamp. (Correct)

- IPsec consente la protezione del traffico dati, ma anche integrità degli header tramite AH. (Correct)

Question 9: Indica quali delle seguenti affermazioni sulla crittografia, il filtraggio anti-spam e altri aspetti della sicurezza della posta elettronica sono vere:3

Labels:crittografia, sicurezza, email, prestazioni, anti

- La scelta tra crittografia simmetrica e asimmetrica in un sistema di posta elettronica sicura spesso dipende da un compromesso tra prestazioni e sicurezza: la simmetrica è più veloce, l'asimmetrica offre gestione delle chiavi più semplice e non ripudio ma non permette di cifrare grandi quantità di dati. (Correct)

- L'efficacia di un sistema di filtraggio anti-spam basato su blacklist dipende fortemente dalla sua capacità di aggiornamento costante e dalla precisione nel distinguere tra spam e messaggi legittimi. (Correct)

- L'implementazione di un sistema di autenticazione a due fattori per l'accesso alla posta elettronica elimina completamente il rischio di attacchi di phishing.

- Mentre sia IPsec che TLS forniscono canali di comunicazione sicuri, IPsec opera a livello di rete (IP), proteggendo tutto il traffico tra due host, mentre TLS opera a livello di trasporto (TCP), proteggendo singole connessioni applicative. (Correct)

- Un attacco "man-in-the-middle" è più facilmente realizzabile su una connessione protetta con TLS che su una connessione protetta con IPsec.

Question 10: Alice sta configurando un server per trasferire file che devono rimanere confidenziali a Bob. Bob riferisce che i file inviati risultano leggibili da terzi. Alice esamina la configurazione e si accorge che mancano adeguate misure di autenticazione e cifratura. Quali modifiche potrebbe implementare per garantire la sicurezza del trasferimento?2

Labels:sicurezza, autenticazione, cifratura, TLS, RSA, AES

- Configurare un sistema di protezione end-to-end, es. mediante RSA, per proteggere i file durante il trasferimento, usando chiavi pubbliche per la cifratura e chiavi private per la confidenzialità

- Implementare l’autenticazione del server e del client tramite TLS, garantendo che entrambi possiedano certificati validi per verificare le rispettive identità. (Correct)

- Definire un metodo per condividere la chiave privata di Alice con Bob, garantendo che la cifratura avvenga in modo trasparente.

- Imporre l’uso di funzioni di hash per garantire la riservatezza dei file durante la trasmissione.

- Utilizzare cifratura simmetrica, come AES, per un trasferimento più efficiente, assicurandosi che le chiavi simmetriche siano scambiate in modo sicuro tramite un protocollo come Diffie-Hellman. (Correct)

Question 11: Alice gestisce una rete aziendale e vuole usare un firewall per proteggere i dati personali dei clienti in maniera conforme alle normative GDPR. Quali delle seguenti configurazioni e misure sono corrette?3

Labels:firewall, certificazioni, GDPR

- Configurare il firewall per registrare i log tecnici necessari alla sicurezza della rete, assicurandosi che siano conservati per un periodo proporzionato e con scopo dichiarato (Correct)

- Impostare una regola per registrare tutti i dettagli del traffico, inclusi dati personali, per un periodo illimitato

- Implementare politiche di accesso basate su principi di "least privilege" per ridurre l'accesso non necessario ai log del firewall (Correct)

- Utilizzare un SIEM (Security Information and Event Management) per analizzare i log generati, rispettando le normative sulla gestione dei dati personali. (Correct)

- Consentire il traffico in entrata su tutte le porte per facilitare la trasparenza delle comunicazioni.