Generated Quizzes

Question 1: Quali differenze distinguono la sicurezza fornita da IPsec rispetto a TLS?3

Labels:ipsec, tls, sicurezza

- IPsec opera al livello di rete (Layer 3), proteggendo tutto il traffico IP, mentre TLS protegge specifici protocolli applicativi come HTTPS. (Correct)

- IPsec può essere configurato per garantire sicurezza end-to-end o solo per una parte del percorso di trasmissione tramite VPN. (Correct)

- TLS utilizza metodi crittografici per autenticare le parti e negoziare chiavi di sessione simmetriche. (Correct)

- IPsec richiede sempre un certificato digitale per autenticare gli utenti e scambiare le chiavi.

Question 2: Alice vuole configurare un server per autenticare in modo sicuro i client con TLS. Quali delle seguenti affermazioni descrivono correttamente l'utilizzo delle chiavi e dei certificati?2

Labels:crypto, autenticazione, chiavi, tls

- Il server deve utilizzare un certificato digitale firmato da una Certification Authority (CA) nota ai client (es. incluso nella lista nota ai browser) per garantire la propria autenticità ai client. (Correct)

- Un certificato self-signed può essere utilizzato per autenticare il server, ma richiede che i client lo configurino manualmente come attendibile. (Correct)

- I certificati digitali garantiscono sia autenticità che riservatezza senza la necessità di cifratura.

- I client non necessitano mai di un certificato per comunicare con il server TLS, indipendentemente dalla configurazione.

- TLS utilizza esclusivamente chiavi simmetriche generate durante l'handshake per garantire autenticità e integrità.

Question 3: Alice gestisce una rete aziendale che include server pubblici e risorse interne sensibili. Decide di implementare un'architettura firewall a "tre gambe" con una DMZ. Quali sono i vantaggi di questa configurazione?3

Labels:firewall, architettura, sicurezza

- Isolamento dei server pubblici dato il divieto di accesso diretto alla rete interna. (Correct)

- Facilità di applicazione di policy di sicurezza specifiche per ciascun segmento di rete. (Correct)

- Maggiore velocità di trasmissione rispetto a un firewall con DMZ singola.

- I server nella DMZ possono comunicare direttamente con la rete interna senza ulteriori configurazioni.

- Possibilità di monitorare e analizzare il traffico verso i server pubblici senza esporre la rete interna. (Correct)

Question 4: _Alice desidera ottenere un certificato da Carl, il quale svolge il ruolo di Certification Authority (CA). Per procedere, Carl esegue il seguente comando:

Labels:certificati, pkcs, formato, firma

- Il file alice.certreq.pem rappresenta una richiesta di certificato in formato PKCS #10.

- In OpenSSL, Alice può ottenere un certificato da Carl anche senza sottomettere una richiesta di certificato.

- La richiesta di certificato deve essere firmata da Alice per garantire l'integrità della richiesta. (Correct)

- Carl dispone di una base dati che tiene traccia dei certificati emessi e del loro stato, aggiornata automaticamente dopo l'esecuzione del comando. (Correct)

- Il certificato emesso da Carl utilizzerà un numero di serie assegnato automaticamente dal file accessorio serial. (Correct)

- Il file alice.certreq.pem rappresenta una richiesta di certificato in formato PKCS10 (Correct)

Question 5: Quali vulnerabilità sono associate a una configurazione TLS debole?3

Labels:tls, vulnerabilit

- Uso di algoritmi deboli come MD5 per hash. (Correct)

- Mancato controllo della revoca del certificato. (Correct)

- Uso di session resumption per ottimizzare le prestazioni.

- Supporto a TLS 1.0 o SSL 3.0. (Correct)

- Supporto a TLS 1.3

Question 6: Indica quali delle seguenti affermazioni sul laboratorio su IPsec e TLS sono corrette:4

Labels:ipsec, tls, ike

- Il comando "ip xfrm state flush" è usato per cancellare il Database delle Politiche di Sicurezza (SPD).

- Il comando "ip xfrm policy list" mostra le politiche di sicurezza IPsec correnti. (Correct)

- Il comando "ipsec start" è usato per avviare il demone strongSwan. (Correct)

- Dopo aver modificato il file "/etc/ipsec.conf", devi usare il comando "ipsec update" perché le modifiche abbiano effetto immediatamente.

- Il comando "openssl s_server -www" avvia un semplice server TLS che mostra le informazioni di connessione in formato HTML. (Correct)

- In una VPN IPsec site-to-site, ogni gateway necessita solo di una singola Associazione di Sicurezza (SA) per gestire il traffico in entrambe le direzioni.

- Per usare certificati con strongSwan devi posizionare il certificato CA nella directory "/etc/ipsec.d/cacerts" (Correct)

Question 7: _Alice ha configurato il firewall del suo sistema con i seguenti comandi:

Labels:iptables, firewall, icmp, packetfilter

- Alice non riesce ad avviare una connessione SSH verso Bob perché la default policy DROP della chain INPUT blocca i pacchetti di risposta (SYN+ACK). (Correct)

- Bob non riesce a eseguire una scansione delle porte di Alice.

- Le risposte ai ping inviati da Bob vengono accettate, ma le risposte ai pacchetti TCP (ad esempio HTTPS sulla porta 443 o SSH sulla porta 21) non vengono gestite correttamente. (Correct)

- Alice non ha configurato una regola per consentire il traffico correlato (es. RELATED, ESTABLISHED), rendendo il firewall inefficace per connessioni bidirezionali. (Correct)

- La policy DROP della chain INPUT blocca tutto il traffico, inclusi i pacchetti ICMP accettati dalla regola esplicita

- Alice non può creare nuove chain per gestire altri tipi di traffico

Question 8: Bob sta lavorando per ottenere la certificazione ISO/IEC 27001 e garantire la conformità al GDPR. Quali delle seguenti affermazioni sono corrette?3

Labels:standard, analisi dei rischi, GDPR

- I rischi identificati devono essere documentati e gestiti attraverso misure tecniche e organizzative. (Correct)

- La protezione dei dati personali deve essere integrata nel sistema di gestione della sicurezza delle informazioni (ISMS). (Correct)

- Aver ottenuto una certificazione ISO/IEC 27001 garantisce la conformità al GDPR.

- Le valutazioni periodiche dell'efficacia delle misure adottate sono obbligatorie sia per la ISO/IEC 27001 che per il GDPR. (Correct)

- I dati personali protetti da crittografia non richiedono un adeguamento periodico dell''analisi dei rischi.

Question 9: Indica quali delle seguenti affermazioni sullo spam e sulle tecniche anti-spam sono vere:5

Labels:spam, email, blacklisting, greylisting, sicurezza

- Lo spam si riferisce a email di massa non richieste, spesso di natura commerciale. (Correct)

- Una tattica comune degli spammer è quella di nascondere la vera identità del mittente e falsificare le intestazioni delle email. (Correct)

- Gli "open relay" sono MTA che consentono a chiunque di inviare email attraverso di essi, rendendoli obiettivi interessanti per gli spammer. (Correct)

- Blacklist e whitelist vengono utilizzate per filtrare le email in base all'indirizzo IP o al dominio del mittente. (Correct)

- Il greylisting è una tecnica che rifiuta temporaneamente le email da mittenti sconosciuti, richiedendo loro di ritentare la consegna. (Correct)

- Blacklist e Greylisting vengono utilizzate per filtrare le email in base all'indirizzo IP o al dominio del mittente.

Question 10: _Alice e Bob vogliono configurare un canale di comunicazione sicuro utilizzando IPSec. A questo proposito Bob esegue i seguenti comandi:

Labels:ipsec

- Vengono create 2 SA e 2 SP (Correct)

- Le SA contengono 2 SPI differenti perchè identificano la direzione (Correct)

- Le Security Policies (SP) configurate stabiliscono che il traffico tra Alice e Bob deve essere cifrato utilizzando ESP in modalità transport, senza coinvolgere l’intero pacchetto IP. (Correct)

- Le SA configurate utilizzano lo stesso SPI per entrambe le direzioni, perché l’algoritmo AES richiede univocità solo a livello di chiave crittografica.

- Le Security Associations (SA) configurate permettono di proteggere il traffico solo nella direzione da Bob a Alice, mentre il traffico nella direzione opposta rimane non protetto.

Question 11: Indica quali delle seguenti affermazioni sulla struttura CMS sono vere:2

Labels:cms, crittografia, struttura, firma digitale, sicurezza

- CMS sta per Cryptographic Mail Syntax ed è il formato per definire messaggi sicuri nelle ultime versioni di S/MIME.

- La struttura "signedData" in CMS contiene il contenuto del messaggio, gli algoritmi di digest, le firme digitali e le informazioni sul firmatario. (Correct)

- La struttura "envelopedData" in CMS contiene il contenuto del messaggio crittografato e la chiave di sessione crittografata. (Correct)

- La struttura "envelopedData" in CMS contiene il contenuto del messaggio, gli algoritmi di digest, le firme digitali e le informazioni sul firmatario.

- La struttura "signedData" in CMS contiene il contenuto del messaggio crittografato e la chiave di sessione crittografata.

- CMS supporta solo un singolo destinatario per i messaggi crittografati.