Generated Quizzes

Question 1: Indica quali delle seguenti affermazioni sulla firma digitale, DNSSEC, hash crittografici, certificati digitali, greylisting e attacchi replay sono vere:5

Labels:dnssec, hash, certificati, greylisting, attacchi, sicurezza, email

- La firma digitale di un messaggio di posta elettronica garantisce l'integrità e l'autenticità del messaggio, ma non la sua riservatezza; per quest'ultima è necessaria la crittografia. (Correct)

- L'utilizzo di DNSSEC può migliorare la sicurezza della posta elettronica indirettamente, contribuendo a prevenire attacchi che reindirizzano il traffico email verso server malevoli. (Correct)

- Un hash crittografico di un messaggio è sempre più lungo del messaggio originale.

- Se un certificato digitale è scaduto, la chiave pubblica contenuta nel certificato diventa automaticamente compromessa e inutilizzabile.

- Il protocollo "greylisting" introduce intenzionalmente un ritardo nella consegna della mail per poter distinguere meglio i messaggi legittimi da quelli di spam, confidando sul fatto che i server di spam non ritentino l'invio. (Correct)

- Un attacco di tipo "replay" consiste nel riutilizzare un messaggio precedentemente inviato per ottenere un accesso non autorizzato o ingannare il destinatario: timestamp, sequence numbers e altri accorgimenti possono mitigarlo. (Correct)

- Anche se un messaggio è crittografato end-to-end, le informazioni di routing (mittente, destinatario, IP address) possono comunque essere visibili agli intermediari. Metadati e traffico sono problemi aperti. (Correct)

Question 2: Quali protocolli vengono utilizzati da IPsec per garantire sicurezza?3

Labels:ipsec, ah, esp, ike, sicurezza, protocollo

- TCP

- AH (Authentication Header) (Correct)

- ESP (Encapsulating Security Payload) (Correct)

- HTTPS

- RSSA

- IKE (Internet Key Exchange) (Correct)

Question 3: _Alice ha configurato il firewall del suo sistema con i seguenti comandi:

Labels:firewall, iptables, configurazione

- Tutto il traffico in uscita è consentito (Correct)

- Tutto il traffico in ingresso viene automaticamente inoltrato (default policy ACCEPT)

- Alice non può connettersi ad un server di Bob, perché tutti i pacchetti TCP con flag SYN sono bloccati

- Bob non può instaurare una nuova connessione TCP con Alice (Correct)

- Bob non può individuare i servizi esposti di Alice tramite SYN scan (Correct)

Question 4: Quali delle seguenti affermazioni sull'uso delle funzioni di hash nella sicurezza TLS sono vere?3

Labels:hash, autenticazione, tls, collisioni

- Funzioni di hash sicure come SHA-256 possono svolgere un ruolo importante nella verifica di integrità e autenticazione delle connessioni TLS. (Correct)

- Usare di hash per cui è possibile trovare collisioni potrebbe compromettere l'integrità del certificato usato da un server TLS, se riuscissi a generare un certificato con lo stesso hash. (Correct)

- Le funzioni di hash sono utilizzate esclusivamente per cifrare il traffico TLS.

- L'utilizzo di funzioni di hash obsoleti come MD5 non influisce sulla sicurezza di TLS, se per calcolare i MAC vengono usate chiavi lunghe.

- TLS utilizza funzioni di hash nei certificati per garantire l'autenticità delle identità coinvolte nella connessione. (Correct)

Question 5: Quale approccio riduce al minimo la latenza in una connessione IPsec site-to-site?3

Labels:ipsec, retecore

- Configurare la modalità Transport anziché Tunnel per traffico specifico. (Correct)

- Utilizzare algoritmi di hashing più complessi come SHA-512.

- Abilitare il rinnovo delle chiavi con IKE ogni 10 pacchetti.

- Ottimizzare i percorsi di instradamento per ridurre i ritardi. (Correct)

- Usare solo ESP per Autenticazione e confidenzialità invece di usare anche AH. (Correct)

- Usare un VPN concentrator in tunnel mode invece di un server multipurpose. (Correct)

Question 6: Quale delle seguenti descrive correttamente le chiavi utilizzate nella crittografia asimmetrica?2

Labels:asimmetrica

- Una chiave pubblica che può essere usata per cifrare i dati. (Correct)

- Una chiave privata che può essere usata solo per decifrare i dati.

- Le chiavi pubbliche e private per alcuni algoritmi sono identiche.

- Una chiave asimmetrica condivisa tra mittente e destinatario.

- Una chiave di sessione generata casualmente.

- Due chiavi matematicamente legate da un problema matematico. (Correct)

Question 7: _Alice e Bob vogliono configurare un canale di comunicazione sicuro, ma utilizzano configurazioni differenti. Alice sceglie ESP con AES-128-GCM (AEAD) , mentre Bob utilizza AH con HMAC-SHA1.

Labels:ipsec

- Sono presenti in totale 4 SA e 4 SP (Correct)

- Le SP sono 2 in totale perché, a differenza delle SA, sono bidirezionali

- Bob ha sbagliato la sua configurazione perchè non ha specificato l'algoritmo crittografico da utilizzare

- La configurazione è vantaggiosa perchè protegge sia l'integrità del messaggio che la segretezza del payload usando un singolo algoritmo e una singola chiave (Correct)

- La configurazione di Bob garantisce solo integrità e autenticità, mentre quella di Alice garantisce anche la confidenzialità dei dati trasmessi. (Correct)

Question 8: _Alice e Bob vogliono scambiare un messaggio cifrato, ma non hanno una chiave simmetrica condivisa. Alice, possiede le seguenti chiavi

Labels:crypto, simmetrica, asimmetrica, chiavi

- rsa.key.alice

- rsapub.key.alice

- msg.enc

- aeskey.rsa

- rsa.key.alice

- La chiave simmetrica la può leggere solo chi possiede la sua chiave privata (Correct)

- Ha scelto l'IV in maniera non casuale ma non l'ha riutilizzato

- Ha condiviso la chiave sbagliata (Correct)

- Non ha comunicato l'IV a Bob (Correct)

- Ha condiviso la chiave simmetrica

- Ha utilizzato un algoritmo di cifratura non abbastanza sicuro

Question 9: Alice vuole migliorare la sicurezza della sua rete aziendale integrando firewall e IDS. Quali delle seguenti combinazioni rappresentano un buon compromesso tra prestazioni e sicurezza?3

Labels:firewall, ids, sicurezza

- Un firewall stateful con IDS basato su firme per bloccare traffico noto come malevolo. (Correct)

- Un firewall stateful con IDS basato su anomalie per rilevare comportamenti sospetti. (Correct)

- Un IDS host-based senza firewall per monitorare traffico locale su dispositivi critici.

- Configurare solo un firewall stateless e aggiornare periodicamente le regole corrispondenti agli attacchi.

- Un IDS di rete in modalità passiva con firewall configurato per analisi dei pacchetti correlati. (Correct)

Question 10: Alice sta configurando il firewall aziendale per soddisfare gli standard ISO/IEC 27001 relativi alla sicurezza delle informazioni. Quali delle seguenti azioni sono coerenti con i requisiti dello standard?3

Labels:certificazioni, standard, firewall

- Implementare regole per limitare l'accesso ai server critici solo a indirizzi IP autorizzati. (Correct)

- Documentare e aggiornare regolarmente le regole del firewall per garantire conformità agli standard. (Correct)

- Impostare il firewall per registrare i tentativi di connessione riusciti, ignorando quelli bloccati.

- Effettuare revisioni periodiche delle configurazioni del firewall come parte dell'audit di sicurezza. (Correct)

- Configurare il firewall per accettare tutto il traffico proveniente da dispositivi certificati ISO/IEC 27001, eliminando ulteriori controlli.

Question 11: Alice vuole configurare una rete aziendale che protegga i dati personali in transito e in conformità al GDPR. Quali misure tecniche dovrebbe adottare?3

Labels:gdpr, crittografia, firewall

- Configurare il firewall per consentire solo traffico crittografato tramite TLS verso i server aziendali. (Correct)

- Implementare la crittografia end-to-end per proteggere i dati in transito. (Correct)

- Registrare nei log i contenuti cifrati dei pacchetti per verificare la conformità ai requisiti GDPR.

- Implementare politiche di gestione delle chiavi per garantire la sicurezza dei certificati crittografici utilizzati. (Correct)

- Implementare regole per accettare solo pacchetti con chiavi di cifratura statiche condivise tra client e server.