Generated Quizzes

Question 1: Quali delle seguenti sono tecniche di crittografia simmetrica?2

Labels:simmetrica

- AES (Advanced Encryption Standard) (Correct)

- DES (Data Encryption Standard) (Correct)

- RSA

- ECC (Elliptic Curve Cryptography)

- Elgamal

Question 2: Bob vuole implementare un sistema di sicurezza che protegga attivamente la sua rete, bloccando attacchi in tempo reale e riducendo i falsi positivi. Quale soluzione è più adatta e perché?_3

Labels:ids

- Un IPS configurato con regole specifiche e aggiornamenti regolari delle firme di attacco. (Correct)

- Un IDS basato su anomalie combinato con un firewall che includa componenti stateful. (Correct)

- Un IDS configurato per monitorare i log del traffico HTTPS.

- Una combinazione di proxy server (screened subnet) ma è rischioso collegarlo a sistema di rilevamento attivo.

- Un IPS integrato con un sistema di machine learning per migliorare l'efficacia del rilevamento. (Correct)

Question 3: Quali tra le seguenti affermazioni sul padding nella crittografia a blocchi sono vere?2

Labels:crypto, simmetrica

- Il padding garantisce che l’input della cifratura a blocchi sia un multiplo della lunghezza del blocco. (Correct)

- In CBC, il padding viene aggiunto solo al blocco finale, indipendentemente dalla lunghezza del messaggio. (Correct)

- Il padding è necessario in tutte le modalità operative della crittografia a blocchi.

- Il padding è sempre utilizzato per garantire integrità dei dati cifrati.

- Algoritmi come AES in modalità CBC non richiedono padding se la lunghezza del messaggio è nota.

Question 4: Quali tra le seguenti affermazioni sulla crittografia simmetrica sono vere?2

Labels:crypto, simmetrica

- La crittografia simmetrica richiede una chiave segreta condivisa tra mittente e destinatario per cifrare e decifrare i dati. (Correct)

- Gli algoritmi simmetrici come AES sono generalmente più efficienti di quelli asimmetrici per grandi volumi di dati. (Correct)

- La distribuzione sicura delle chiavi nella crittografia simmetrica è facilmente risolvibile senza l'uso di ulteriori protocolli.

- Gli algoritmi di crittografia simmetrica non sono vulnerabili a brute force se la chiave è sufficientemente lunga.

Question 5: Indica quali affermazioni sui diversi tipi di firewall e il loro funzionamento sono corrette?4

Labels:firewall

- I firewall packet filter operano a livello di rete (L3) e ispezionano l'header di ogni pacchetto IP. (Correct)

- I circuit-level gateway esaminano il contenuto dei pacchetti a livello applicativo per identificare e bloccare minacce specifiche.

- Un proxy application-aware capisce il protocollo applicativo e può quindi applicare regole di sicurezza più specifiche. (Correct)

- I packet filter con funzioni di stateful inspection hanno prestazioni significativamente inferiori rispetto ai packet filter stateless a causa della maggiore complessità.

- Un WAF è un tipo specifico di firewall progettato per proteggere le applicazioni web da attacchi come SQL injection e cross-site scripting. (Correct)

- I componenti di firewall che operano a livello di trasporto (L4) possono autenticare gli utenti direttamente basandosi sulle informazioni contenute nei pacchetti TCP/UDP senza richiedere modifiche alle applicazioni.

- I componenti di firewall che operano usando il protocollo SOCKS creano un "circuito" a livello di trasporto tra client e server, senza necessariamente ispezionare il contenuto dei dati applicativi. (Correct)

Question 6: Indica quali sono le risposte corrette sui firewall e la loro architettura nelle reti?5

Labels:firewall

- Un firewall stateful tiene traccia dello stato delle connessioni, migliorando la sicurezza rispetto ai firewall stateless. (Correct)

- I firewall di livello applicativo (L7) sono più veloci dei firewall packet filter (L4) perché analizzano dati meglio strutturati.

- Un firewall con architettura a "tre gambe" espone una interfaccia di rete per ospitare server pubblici creando una DMZ (De-Militarized Zone). (Correct)

- Usare un firewall con architettura a “screening router” permette di creare una DMZ (De-Militarized Zone) per ospitare server pubblici.

- Un bastion host è un sistema esposto intenzionalmente su una rete per essere un bersaglio facile e quindi analizzabile in caso di attacco.

- Un firewall di tipo stealth non ha un indirizzo IP configurato sulla scheda rete, ma modifica attivamente il traffico per nascondere la rete interna.

- Il principio "blacklisting" offre minore sicurezza ma è più facile da gestire rispetto al principio opposto detto “whitelisting”. (Correct)

- L'utilizzo di un router come firewall è una soluzione sufficientemente sicura, è quindi consigliabile in ambito aziendale.

- Un personal firewall è installato direttamente sul nodo da difendere e può essere usato per autorizzare le comunicazioni dei processi in esecuzione. (Correct)

- Lo scopo di un firewall è bloccare il traffico in ingresso non autorizzato, serve meno attenzione nel controllo del traffico in uscita.

- Un honey pot può essere un sistema esposto intenzionalmente su una rete per essere un bersaglio facile e quindi analizzabile in caso di attacco. (Correct)

Question 7: Quale delle seguenti affermazioni sulle VPN è corretta?2

Labels:vpn, ipsec

- Le VPN operano esclusivamente a livello applicativo per la protezione dei dati.

- OpenVPN può essere preferibile ad IPsec in reti complesse o eterogenee (Correct)

- IPSec in modalità tunnel offre protezione completa incapsulando il pacchetto IP in un nuovo pacchetto IP. (Correct)

- OpenVPN supporta nativamente sia modalità transport che tunnel

- Le VPN IPsec integrano meccanismi di crittografia per la protezione dei dati in maniera opzionale

Question 8: Bob vuole migliorare la sicurezza della sua rete aziendale implementando un IDS. Durante un’analisi dei rischi, nota che i server contengono dati sensibili. Quale strategia dovrebbe adottare per ridurre i rischi?3

Labels:ids, analisi dei rischi, reti

- Posizionare un NIDS sulla DMZ per monitorare il traffico verso i server e identificare potenziali anomalie di accesso. (Correct)

- Configurare l'IDS per segnalare tentativi di accesso non autorizzati, ma non per bloccare automaticamente i pacchetti senza ulteriore analisi. (Correct)

- Impostare l'IDS per interrompere automaticamente qualsiasi connessione con attività insolita senza tenere conto di falsi positivi.

- Integrare l'IDS con un sistema SIEM per correlare eventi e rilevare modelli di comportamento sospetti. (Correct)

- Consentire traffico "trusted" ai server da indirizzi IP interni senza ulteriori verifiche, basandosi sulla segmentazione di rete per la protezione.

Question 9: _Alice e Bob vogliono configurare un canale di comunicazione sicuro utilizzando IPSec. A questo proposito Alice esegue i seguenti comandi:

Labels:ipsec

- Grazie all'utilizzo di IPsec in transport mode, Alice ottiene confidenzialità e protezione dagli attacchi replay (Correct)

- Viene utilizzato l'algoritmo des per la crittografia

- Quando Alice invia un nuovo pacchetto IP a Bob saranno considerate la SP relativa a "in" più la corrispondente SA, se presente

- Quando Alice riceve un nuovo pacchetto IP saranno considerate la SP relativa a "in" più la corrispondente SA (Correct)

- I comandi contengono due SA ridondanti, che possono essere ridotta ad una sola per la configurazione del canale sicuro

Question 10: Seleziona quali parametri della sessione TLS cambiano quando viene sfruttato un SessionID.2

Labels:tls

- protocollo

- chiavi derivate (Correct)

- ciphersuite

- master key

- numeri casuali (Correct)

Question 11: Quali affermazioni sulla crittografia sono corrette?4

Labels:crypto, simmetrica, asimmetrica

- La crittografia a curve ellittiche (ECC) è più efficiente della crittografia simmetrica per grandi volumi di dati.

- La crittografia di flusso è preferibile alla crittografia a blocchi per proteggere le comunicazioni in tempo reale (Correct)

- La firma digitale garantisce autenticità e integrità, ma non confidenzialità del messaggio. (Correct)

- La crittografia simmetrica utilizza una sola chiave per cifrare e decifrare, rendendo critica la sua protezione. (Correct)

- Un certificato digitale contiene solo la chiave pubblica e nessuna informazione sull’identità del proprietario.

- ■■La crittografia end-to-end nei tunnel VPN protegge i dati anche contro attacchi all’interno della rete. (Correct)