Generated Quizzes

Question 1: Quali tra le seguenti affermazioni riguardanti il principio di Kerckhoffs sono vere?2

Labels:crypto, algoritmi

- Il principio di Kerckhoffs afferma che un sistema crittografico deve essere sicuro anche se l'algoritmo è pubblico, purché la chiave sia segreta. (Correct)

- L'applicazione del principio di Kerckhoffs ha portato alla trasparenza nello sviluppo degli algoritmi crittografici moderni come AES. (Correct)

- La segretezza dell'algoritmo garantisce sempre un livello aggiuntivo di sicurezza rispetto alla trasparenza dell'algoritmo.

- Il principio di Kerckhoffs richiede che l'algoritmo di crittografia e le chiavi siano mantenuti segreti per garantire sicurezza.

- Le vulnerabilità negli algoritmi pubblici sono inevitabili e non possono essere mitigate con il solo uso di chiavi sicure.

Question 2: Alice sta configurando un firewall stateful per proteggere la sua rete aziendale. Vuole consentire solo connessioni HTTPS in uscita dai client interni e bloccare tutto il traffico non correlato. Quali delle seguenti configurazioni soddisfano questo requisito?3

Labels:firewall, configurazione, reti

- Impostare una regola che accetti solo connessioni in uscita verso destinazione porta 443 con stato "NEW" e sorgente interna, e bloccare connessioni con porte diverse. (Correct)

- Configurare una regola che consenta esclusivamente il traffico correlato (RELATED, ESTABLISHED) in entrambe le direzioni per completare le risposte HTTPS. (Correct)

- Bloccare tutto il traffico in ingresso e in uscita, inclusi i pacchetti correlati (RELATED, ESTABLISHED), come misura di sicurezza predefinita.

- Definire una policy predefinita di DROP per tutte le connessioni in uscita non esplicitamente consentite, e ALLOW per le connessioni in ingresso.

- Consentire connessioni HTTPS in uscita e configurare una regola per registrare (log) i pacchetti bloccati al fine di monitorare tentativi di connessione non autorizzati. (Correct)

Question 3: Quali algoritmi vengono utilizzati nei certificati TLS per l'autenticazione?2

Labels:tls, certificati

- RSA (Correct)
- DES
- X.509
- AES
- SHA (utilizzato solo come hash ma non per l'autenticazione)
- AEAD nell’ultima versione di TLS (Correct)

Question 4: Bob sta configurando una rete aziendale con una DMZ per ospitare server pubblici e decide di eseguire un’analisi dei rischi per determinare la configurazione ottimale. Quali misure di sicurezza dovrebbe implementare?3

Labels:analisi dei rischi, firewall, DMZ

- Configurare il firewall per consentire solo traffico specifico verso i server pubblici che intende posizionare nella DMZ. (Correct)
- Implementare un IDS per monitorare il traffico in entrata e in uscita dalla DMZ. (Correct)
- Impostare regole per consentire traffico diretto dalla DMZ alla rete interna senza restrizioni.
- Eseguire test di penetrazione regolari per identificare vulnerabilità nei server della DMZ. (Correct)
- Registrare tutti i dettagli del traffico, inclusi dati personali, senza limiti di tempo.

Question 5: Quali tecniche migliorano la sicurezza complessiva di IPsec e TLS?3

Labels:ipsec, sicurezza

- Abilitare PFS (Perfect Forward Secrecy) per le sessioni. (Correct)
- Aggiornare regolarmente i certificati TLS con chiavi di lunghezza adeguata. (Correct)
- Disabilitare il supporto a TLS 1.3.
- Usare IPsec solo in transport mode.
- Usare protocolli di hash più veloci per ridurre la possibilità di attacchi brute-force.
- Disabilitare versioni obsolete come TLS 1.0 e IPsec con DES. (Correct)
- Usare sempre e solo AH in IPsec.
- Cambiare spesso le SPD per evitare attacchi di tipo brute-force.

Question 6: Quali delle seguenti affermazioni su RC4 e AES sono vere?2

Labels:algoritmi, crypto, simmetrica

- RC4 non richiede padding perché il keystream ha la stessa lunghezza del messaggio da cifrare. (Correct)

- AES, con l’opzione -nopad, può cifrare un messaggio solo se la sua lunghezza è un multiplo della lunghezza del blocco. (Correct)

- RC4 richiede padding per cifrare correttamente messaggi più corti del keystream.

- AES è un algoritmo di cifratura di tipo stream, mentre RC4 è a blocchi.

- Sia RC4 che AES richiedono che il messaggio sia sempre un multiplo della lunghezza del blocco per essere cifrato.

Question 7: Bob ha acquistato un dispositivo con installato un IDS, addrestrato sul traffico reale per rilevare anomalie nella sua rete aziendale. Dopo alcuni giorni, l'IDS segnala costantemente attività sospette su un server critico, ma l'analisi manuale non rileva alcun attacco reale. Quali delle seguenti azioni dovrebbe intraprendere Bob?3

Labels:ids

- Regolare la soglia di rilevamento dell'IDS per ridurre i falsi positivi. (Correct)

- Analizzare i log storici per identificare pattern normali e aggiornare i profili di base. (Correct)

- Aggiornare le firme o il modello di rilevamento dell’IDS per migliorare l’accuratezza del sistema. (Correct)

- Disabilitare temporaneamente l'IDS fino a quando il problema non viene risolto.

- Configurare l'IDS per ignorare completamente gli alert dell’IDS relativi al server critico.

Question 8: Alice ha deciso di implementare la ISO/IEC 27001 e ottenere una certificazione per dimostrare il suo impegno nella sicurezza informatica. Quali delle seguenti affermazioni descrivono correttamente il processo?3

Labels:standard, sicurezza, certificazioni

- La certificazione richiede una verifica indipendente da parte di un ente accreditato. (Correct)

- L’ottenimento della certificazione dipende dall’implementazione di un ISMS adeguata con una adeguata gestione dei rischi post-analisi. (Correct)

- Una volta ottenuta, la certificazione è valida per un tempo illimitato.

- La conformità allo standard include la preparazione alla risposta agli incidenti di sicurezza. (Correct)

- L'implementazione delle misure minime consigliate dalla norma garantisce la certificazione senza bisogno di adattamenti.

Question 9: indica quali delle seguenti affermazioni sul laboratorio relativo ai firewall sono corrette:4

Labels:firewall

- Netfilter/IPtables è un software che fornisce funzionalità di manipolazione e filtraggio di pacchetti IP all'interno del kernel Linux. (Correct)

- La catena INPUT di IPtables si applica esclusivamente ai pacchetti in uscita dalla macchina su cui è installato IPtables, mentre la catena OUTPUT gestisce i pacchetti in ingresso.

- La politica di default di una catena IPtables determina l'azione intrapresa se nessuna regola nella catena corrisponde al pacchetto. (Correct)

- Il comando "iptables -F" elimina tutte le regole nella catena specificata e ripristina automaticamente la politica di default della catena a ACCEPT.e una singola macchina.

- In uno stateless packet filter, la regola "iptables -A FORWARD -p tcp -s IP-Alice --sport 80 --dport 22 -j ACCEPT" permette ad Alice di navigare su qualsiasi sito web esterno, a patto che la destinazione sia la porta 80.

- Con uno stateless packet filter, la porta sorgente 80 può essere utilizzata da Bob per instaurare una connessione verso Alice se è presente una regola che accetta pacchetti con porta sorgente 80. Uno stateful packet filter, invece, può distinguere tra connessioni in entrata e in uscita.

- Il comando "iptables -A FORWARD -p icmp -d IP-Alice --icmp-type echo-request -m limit --limit 20/minute -j ACCEPT" limita il traffico ICMP echo-request a 20 pacchetti al minuto, senza restrizioni sui secondi che devono passare tra l'invio di un pacchetto e il successivo. (Correct)

- La catena OUTPUT di IPtables si applica esclusivamente ai pacchetti in uscita dalla macchina su cui è installato IPtables, mentre la catena INPUT gestisce i pacchetti in ingresso. (Correct)

Question 10: Quali tra le seguenti affermazioni riguardanti il protocollo AH (Authentication Header) di IPsec sono vere?2

Labels:ah, ipsec

- AH garantisce autenticità e integrità dei pacchetti IP tramite hash. (Correct)

- AH non fornisce riservatezza, poiché non cifra il payload del pacchetto. (Correct)

- AH può essere utilizzato per garantire riservatezza tramite crittografia simmetrica.

- AH richiede un certificato digitale per autenticare gli utenti.

- AH supporta Perfect Forward Secrecy come ESP.

Question 11: Quali tra le seguenti affermazioni relative all'uso di Diffie-Hellman sono vere?2

Labels:diffiehellman, asimmetrica

- Diffie-Hellman consente lo scambio sicuro di chiavi senza che queste siano mai trasmesse direttamente. (Correct)

- La sicurezza del protocollo si basa sulla difficoltà computazionale del problema del logaritmo discreto. (Correct)

- Diffie-Hellman può essere utilizzato per cifrare i dati direttamente, senza ulteriori algoritmi.

- La sicurezza di Diffie-Hellman è indipendente dalla lunghezza dei numeri primi utilizzati.