Generated Quizzes

Question 1: Bob vuole proteggere la sua rete da scansioni delle porte e tentativi di accesso non autorizzato. Quali configurazioni di firewall sono più efficaci per prevenire questi attacchi?3

Labels:firewall, vulnerabilit

- Impostare una regola per bloccare i pacchetti con flag incoerenti. (Correct)

- Abilitare il logging per analizzare tentativi di connessione su porte non aperte. (Correct)

- Consentire tutto il traffico ICMP per evitare interferenze con i controlli di rete.

- Impostare una policy di ACCEPT per tutto il traffico in entrata e utilizzare regole per bloccare attacchi specifici.

- Limitare il numero di connessioni simultanee per ogni indirizzo IP tramite regole connlimit. (Correct)

Question 2: _Ti è stato assegnato il compito di impostare un canale di comunicazione sicuro tra due host, Alice e Bob, usando IPsec. Hai deciso di usare strongSwan per la negoziazione IKE e hai già configurato i file /etc/ipsec.conf e /etc/ipsec.secrets su entrambe le macchine. Alice deve iniziare la connessione con Bob. Sono disponibili sia una chiave pre-condivisa che dei certificati. Usi il comando ipsec up host-host per iniziare la connessione. Quali affermazioni sono corrette?_4

Labels:ipsec, tls, ike

- Prima di eseguire "ipsec up host-host", devi assicurarti che il servizio strongSwan sia in esecuzione, cosa che può essere verificata usando il comando "ipsec start". (Correct)

- Se il comando "ipsec up host-host" fallisce, la prima cosa da controllare è la connettività di rete tra Alice e Bob usando il comando "ping".

- Dopo aver stabilito con successo il tunnel IPsec, puoi usare il comando "ip xfrm state list" sia su Alice che su Bob per verificare che le Associazioni di Sicurezza (SA) siano state create. (Correct)

- Se vuoi usare l'autenticazione basata su certificati invece della PSK, puoi modificare il comando "ipsec up" includendo l'opzione "--cert" seguita dal percorso del file del certificato.

- Il comando "ip xfrm policy list" può essere usato per controllare se il traffico tra Alice e Bob è indirizzato attraverso il tunnel IPsec.

- Se la connessione viene stabilita con successo, ma il traffico non è cifrato, dovresti controllare che su Bob il file "/etc/ipsec.conf" abbia il parametro "type" impostato a "start" per la connessione "host-host". (Correct)

- Per assicurare che la connessione IPsec sia ristabilita automaticamente dopo un riavvio, dovresti modificare il file "/etc/ipsec.conf" sia su Alice che su Bob per includere la riga "auto=start" all'interno della definizione della connessione. (Correct)

- Se vuoi proteggere solo il traffico TCP, devi aggiungere una riga con il parametro "proto tcp" al comando "ip xfrm state add".

Question 3: Bob sta progettando una rete aziendale e vuole combinare un IDS e un firewall per ottimizzare la sicurezza. Quali strategie può adottare?3

Labels:ids, firewall, reti

- Utilizzare il firewall per bloccare traffico noto come malevolo e l'IDS per rilevare attività sospette. (Correct)

- Posizionare l'IDS in modalità monitoraggio passivo in una posizione strategica della rete. (Correct)

- Configurare l'IDS per modificare direttamente le regole del firewall senza revisione umana.

- Utilizzare un sistema SIEM per correlare i log dell’IDS e del firewall, permettendo un’analisi approfondita. (Correct)

- Impostare il firewall per ignorare il traffico segnalato dall'IDS senza ulteriori controlli.

Question 4: Quali tra le seguenti affermazioni sull’hashing nella crittografia sono vere?2

Labels:hash, funzioni di hash, crypto

- Gli algoritmi di hash, come SHA-256, generano un digest di lunghezza fissa indipendentemente dalla dimensione del messaggio in input. (Correct)

- Un hash crittografico è sicuro contro collisioni se non esistono metodi pratici per trovarne una in un tempo computazionale ragionevole. (Correct)

- Un hash crittografico può essere invertito con una chiave segreta utilizzando un algoritmo avanzato.

- L’algoritmo di hashing MD5 è considerato ancora sicuro per applicazioni crittografiche che richiedono resistenza alle collisioni nel caso di second preimage attack.

- Gli algoritmi di hash vengono utilizzati esclusivamente per proteggere le password memorizzate nei database.

Question 5: Quali tra le seguenti affermazioni sull'algoritmo AES sono vere?2

Labels:algoritmi, crypto, simmetrica

- AES prevede tre versioni con lunghezza della chiave diversa, 128, 192 o 256 bit. (Correct)

- AES è un algoritmo a blocchi che opera su blocchi di 128 bit indipendentemente dalla lunghezza della chiave. (Correct)

- AES supporta lunghezze di chiave di 64, 128 o 256 bit per garantire flessibilità.

- AES è stato progettato per garantire confidenzialità ma non può essere usato per garantire integrità e autenticità dei dati.

Question 6: _Bob configura il suo firewall con la seguente regola:

Labels:firewall, configurazione, forwarding

- Il traffico SSH dalla rete 192.168.1.0/24 verso il server 10.0.0.1 è consentito. (Correct)

- Il traffico HTTP tra la rete interna e 10.0.0.1 è bloccato dalla configurazione.

- Bob può monitorare l'attività di questa regola aggiungendo una regola di LOG prima di essa. (Correct)

- Il firewall inoltra i pacchetti solo se la policy predefinita della chain FORWARD è ACCEPT o se esistono regole aggiuntive che consentono esplicitamente il traffico. (Correct)

- La regola consente connessioni in entrata su tutte le porte dal server 10.0.0.1.

Question 7: Quali affermazioni riguardanti la crittografia a stream sono corrette?2

Labels:crypto, stream, simmetrica

- Nel CBC, l'algoritmo è sempre più sicuro rispetto ai metodi di cifratura stream.

- Nel CBC, l'IV deve essere un numero casuale sempre riutilizzabile per risparmiare risorse.

- Nel CBC, come in TLSv1, l'IV deve essere un numero generato dal traffico precedente per risparmiare risorse.

- Nel CBC, un errore di trasmissione in un blocco cifrato si riflette solo su quel blocco e sul successivo durante la decifratura. (Correct)

- Nel CBC, un errore di trasmissione si propaga solo in avanti senza alterare i blocchi precedenti.

- L'IV per la modalità EBC deve essere un numero casuale utilizzabile solo una volta.

- Nell'EBC blocchi di plaintext identici producono ciphertext identici. (Correct)

Question 8: Indica quali affermazioni relative alla risposta agli incidenti, ai SOC e alla sicurezza informatica sono vere?4

Labels:incident, SOC, sicurezza

- Un data breach si riferisce ad una divulgazione non autorizzata di dati sensibili. (Correct)

- La preparazione alla risposta agli incidenti è una fase che può essere ignorata se l'organizzazione dispone di strumenti avanzati per il blocco degli attacchi.

- Un Incident Response Team ha il compito di definire politiche di risposta agli incidenti e piani di azione. (Correct)

- Un data disclosure si riferisce ad una esposizione di dati sensibili.

- L'obiettivo principale di un SIEM è bloccare attivamente gli attacchi informatici in tempo reale.

- Un SOC include diverse figure professionali impegnate anche a monitorare continuamente la sicurezza di un sistema informativo. (Correct)

- Il personale del SOC è responsabile solo dell'implementazione di misure preventive, mentre la gestione degli incidenti è compito dell'incident response team.

- Un honeypot è un sistema progettato per simulare risorse legittime, attrarre attività malevole e consentire l'analisi di eventi in tempo reale per migliorare la sicurezza complessiva. (Correct)

Question 9: Indica quali delle seguenti affermazioni sulle tecniche anti-spam sono vere:3

Labels:spam, tecniche, email, sicurezza

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

- I primi tentativi di sicurezza della posta elettronica prevedevano l'uso di codici segreti incorporati direttamente nel corpo del messaggio.

- 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)

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

Question 10: Bob deve implementare la crittografia per proteggere i dati personali trattati dalla sua azienda. Quali delle seguenti affermazioni rispettano il GDPR?3

Labels:gdpr, sicurezza, crittografia

- La crittografia è una misura di sicurezza appropriata, ma non obbligatoria per tutti i tipi di dati personali in transit. (Correct)

- Se i dati personali crittografati vengono rubati, l'obbligo di notifica può essere evitato in alcuni casi se opportunamente documentati dal DPO. (Correct)

- Se si scelgono algoritmi forti, l'uso della crittografia garantisce che l'organizzazione non sia responsabile per una violazione dei dati.

- Anche se i dati sono cifrati, devono essere accessibili solo agli utenti autorizzati, garantendo riservatezza e disponibilità. (Correct)

- Il GDPR richiede che tutti i dati personali, indipendentemente dal loro livello di sensibilità, siano crittografati at rest senza eccezioni.

Question 11: _Alice e Bob vogliono scambiare un messaggio cifrato, ma non hanno una chiave simmetrica condivisa. Alice, possiede le seguenti chiavi

Labels:crypto, simmetrica, chiavi, attacchi

- rsa.key.alice

- rsapub.key.alice

- msg.enc

- aeskey.enc

- Questa procedura è vulnerabile ad un attacco Man In the Middle (Correct)

- Questa procedura è vulnerabile ad un attacco IP Spoofing

- Bob deve sapere l’IV per decifrare la chiave

- Bob deve decifrare prima la chiave con la sua chiave privata e poi usare quella chiave per decifrare il messaggio (Correct)

- Bob deve decifrare prima la chiave con la chiave pubblica di Alice e poi usare quella chiave per decifrare il messaggio