Generated Quizzes

Question 1: Indica quali delle seguenti affermazioni su S/MIME sono vere:4

Labels:smime, email, sicurezza, integrit

- S/MIME fornisce servizi di sicurezza come integrità, autenticazione, non ripudio e, facoltativamente, riservatezza per i messaggi di posta elettronica. (Correct)

- S/MIME si basa esclusivamente su algoritmi a chiave simmetrica per la crittografia.

- S/MIME utilizza certificati X.509 per gestire le chiavi pubbliche per la crittografia e le firme digitali. (Correct)

- La sicurezza dei messaggi S/MIME dipende dalla sicurezza di tutti gli MTA coinvolti nel percorso di consegna del messaggio.

- S/MIME può essere utilizzato per creare messaggi firmati digitalmente, cifrati o firmati e cifrati. (Correct)

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

Question 2: Indica quali delle seguenti affermazioni su firewall, proxy e DMZ sono corrette?4

Labels:firewall, proxy, DMZ

- Un forward proxy si trova tra i client di una rete esterna e i server esterni, inoltrando le richieste dei client. (Correct)

- Un reverse proxy si limita a bilanciare il carico tra più server interni, senza fornire alcuna funzionalità di sicurezza aggiuntiva.

- L'utilizzo di una DMZ (De-Militarized Zone) permette di isolare i server pubblici dalla rete interna, aumentando la sicurezza. (Correct)

- In un'architettura firewall con DMZ, il gateway è sempre posizionato all'interno della rete interna per garantire una maggiore protezione.

- Un firewall "a tre gambe" è un'architettura che usa un unico gateway per generare una DMZ e isolare la rete interna. (Correct)

- Il mascheramento degli indirizzi IP interni (NAPT) è una funzionalità esclusiva dei proxy application layer.

- I firewall possono essere implementati come software, appliance hardware o servizi cloud. (Correct)

- Un firewall che contiene componenti di tipo application layer filter è in grado di ispezionare il traffico crittografato senza necessità di decifrarlo.

- I firewall possono essere implementati come app mobile o servizi cloud.

Question 3: Quali fasi compongono l'handshake TLS?4

Labels:fasi, tls

- Negoziazione dei parametri di cifratura. (Correct)
- Autenticazione del server (e opzionalmente del client). (Correct)
- Scambio di chiavi per la sessione. (Correct)
- Trasferimento di file tramite HTTP.
- Utilizzo del protocollo IKE per la gestione delle SA.
- Scambio di una Server Challenge Request/Response. (Correct)

Question 4: _Alice ha configurato la seguente regola iptables sul suo sistema.

Labels:iptables, firewall, icmp

- Tutti i pacchetti in ingresso verranno bloccati, a meno che non corrispondano ad una regola esplicita (Correct)
- Bob non è in grado di inviare Ping ad Alice
- Bob è in grado di connettersi via HTTP alla macchina di Alice sulla porta 80 (Correct)
- Il traffico in uscita è completamente consentito (Correct)
- Tutto il traffico mandato ad Alice che non corrisponde ad alcuna delle regole viene inoltrato automaticamente

Question 5: Alice desidera configurare un firewall che permetta solo connessioni SSH e HTTP in ingresso, bloccando tutte le altre connessioni. Quali regole dovrebbe utilizzare?3

Labels:firewall, configurazione, iptables

- iptables -A INPUT -p tcp --dport 22 -j ACCEPT (Correct)
- iptables -A INPUT -p tcp --dport 80 -j ACCEPT (Correct)
- iptables -P INPUT DROP (Correct)
- iptables -P OUTPUT ACCEPT
- iptables -A FORWARD -j ACCEPT

Question 6: _Alice e Bob utilizzano Frank come firewall. La configurazione di iptables su Frank è la seguente:

Labels:firewall, iptables, configurazione

- Alice può collegarsi solo al server web di Bob
- Bob può collegarsi al server web di Alice con qualunque porta

- Ogni pacchetto TCP inviato a Frank da Alice viene automaticamente inoltrato a Bob se la porta di destinazione è 80 (Correct)

- Bob non può inviare richieste HTTP verso qualsiasi server web esterno, ma solo verso Alice

- Qualsiasi altro tipo di traffico (sia in ingresso che in uscita) tra Bob e Alice viene bloccato dalla policy DROP della chain FORWARD. (Correct)

Question 7: indica quali delle seguenti affermazioni sul laboratorio sui firewall sono corrette:6

Labels:firewall

- Il comando "iptables -A FORWARD -p icmp -s IP-Alice --icmp-type echo-request -j ACCEPT" permette ad Alice di inviare pacchetti ping (echo-request). (Correct)

- Abilitare il traffico ICMP senza restrizioni può essere pericoloso perché può portare a leakage di informazioni, attacchi di tipo ICMP redirect e attacchi DoS di tipo Smurf. (Correct)

- Uno stateful packet filter può accettare tutto il traffico associato alle connessioni stabilite, risolvendo il problema di dover aprire porte specifiche per il traffico di ritorno. (Correct)

- Il comando "iptables -A FORWARD -p icmp -d IP-Alice --icmp-type echo-request -m limit --limit 20/minute --limit-burst 1 -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.

- HTTPtunnel può essere utilizzato per creare un tunnel HTTP che permette di aggirare le politiche di un firewall, consentendo, ad esempio, una connessione SSH attraverso la porta 80. (Correct)

- Ptunnel incapsula il traffico TCP all'interno di pacchetti ICMP echo request ed echo reply, e questo può essere un modo per aggirare le politiche di un firewall che permette il traffico ICMP. (Correct)

- La funzionalità di "dynamic port forwarding" di SSH crea un socket in ascolto in locale e inoltra le connessioni su un canale sicuro SSH, agendo come un circuit-level gateway.

- Un application-level gateway come Apache con mod_proxy può fornire filtri applicativi, filtraggio di contenuti e una maggiore protezione contro le vulnerabilità specifiche di determinate applicazioni. (Correct)

Question 8: Alice vuole garantire che un messaggio che invia a Bob non solo sia leggibile solo da Bob, ma che Bob possa verificare che proviene effettivamente da lei. Quale delle seguenti opzioni rappresenta la soluzione più sicura?2

Labels:crypto, rsa, asimmetrica, autenticazione

- Alice cifra il messaggio con la chiave pubblica di Bob e lo firma con la sua chiave privata. (Correct)

- Alice firma il messaggio con la sua chiave privata, poi cifra il messaggio firmato con la chiave pubblica di Bob. (Correct)

- Alice utilizza la sua chiave pubblica per firmare il messaggio, poi lo cifra con la chiave pubblica di Bob.

- Bob decifra il messaggio con la chiave pubblica di Alice e lo verifica usando la sua chiave privata.

- Alice invia il messaggio non cifrato, ma ne firma una copia con la sua chiave privata per autenticazione.

Question 9: Seleziona le affermazioni corrette sulle differenze tra PIA (Privacy Impact Assessment) e il RMF (Risk Management Process)?3

Labels:pia, analisi

- Il PIA è obbligatorio quando il trattamento dei dati personali comporta rischi elevati per i diritti e le libertà degli interessati. (Correct)

- Il PIA si occupa esclusivamente di proteggere gli asset fisici e digitali di un'organizzazione.

- L'analisi dei rischi del RMF si applica solo ai dati personali.

- Entrambi i processi prevedono una fase di identificazione dei rischi e delle contromisure. (Correct)

- Il PIA richiede un coinvolgimento diretto dei rappresentanti legali e degli interessati. (Correct)

Question 10: Quale delle seguenti opzioni descrive correttamente i metodi di funzionamento di IPsec ESP?2

Labels:ipsec, esp, transportmode, tunnelmode, sicurezza, funzionamento

- Transport Mode: Solo il payload del pacchetto IP è crittografato. (Correct)

- Tunnel Mode: L'intero pacchetto IP è incapsulato e protetto. (Correct)

- Broadcast Mode: Protegge la trasmissione di pacchetti su reti multicast.

- Proxy Mode: Instrada e protegge pacchetti attraverso un proxy server.

- Transport Mode: L'intero pacchetto IP è incapsulato e protetto.

- Tunnel Mode: Solo il payload del pacchetto IP è crittografato.

Question 11: indica quali delle seguenti affermazioni sul laboratorio su IPsec e TLS sono corrette:3

Labels:ipsec, tls, ike

- L'opzione "-CAfile" nel comando "openssl s_client" specifica il file contenente la chiave privata del client.

- L'opzione "-cipher" in "openssl s_client" ti permette di specificare la lista di ciphersuite che il client dovrebbe usare. (Correct)

- Per abilitare l'autenticazione del client in una configurazione Apache TLS, devi cambiare la direttiva “SSLVerifyClient” in “require”.

- Il comando “openssl rsa -in client_pkey.pem -out client_decrypted_pkey.pem” può essere usato per decriptare una chiave privata RSA. (Correct)

- Per catturare il traffico durante un attacco MITM con "ettercap" su una connessione TLS, devi prima usare “openssl” per generare un certificato valido firmato da una CA di fiducia.

- Il comando "ipsec up host-host" è usato per iniziare una connessione IKE definita in "ipsec.conf" come una connessione chiamata "host-host" (Correct)